Quando ho lanciato Apple Computers nel 1976 con Steve Jobs, non immaginavo che quell'invenzione avrebbe conquistato il mondo. Volevo fare qualcosa di mai visto: creare un computer personale che potesse essere utilizzabile, utile e divertente per tutti. Dopo una quarantina d'anni, quella visione è diventata una realtà.

Con miliardi di personal computer, smartphone, dispositivi intelligenti sparsi in tutto il mondo e con tante tecnologie presenti in ogni aspetto della nostra vita, è importante fare un passo indietro e osservare come possiamo curare la nostra sicurezza e protezione continuando a innovare, a crescere e a lavorare per la prossima generazione.

Adoro lavorare con i giovani d'oggi, ispirandoli a innovare e crescere. Adoro vedere le idee alle quali danno origine, mentre escogitano nuovi modi creativi per utilizzare la tecnologia. E amo davvero vedere come questa tecnologia possa migliorare la vita delle persone.

Detto questo, dobbiamo considerare seriamente il modo in cui proteggere questo futuro. Nel 2004, quando tenni il discorso alla HOPE Conference, dissi che molti hacker stavano giocando con la vita delle persone, inducendole a fare cose strane. Il mio amico Kevin Mitnick ha sviluppato negli anni un'area della sicurezza chiamata *social engineering*.

Questo libro di Chris cattura l’essenza stessa dell’ingegneria sociale, definendola e dandole forma, in modo che tutti possiamo renderci conto di che cosa si tratta. Ha scritto questo libro definendo i principi fondamentali del modo in cui noi esseri umani prendiamo le nostre decisioni e di come questi processi possano essere manipolati.

L’hacking è in circolazione da qualche tempo e l’hacking degli esseri umani esiste da quando esistono gli esseri umani. Questo libro può prepararvi, proteggervi e insegnarvi a riconoscere, a difendervi e a ridurre i rischi che derivano dall’applicazione dell’ingegneria sociale.

Steve Wozniak

“Solo pochi anni fa mi trovavo seduto con il mio amico e mentore, Mati Aharoni, mentre decidevamo di lanciare www.social-engineer.org.”

Erano queste le parole d’apertura di *Social Engineering: The Art of Human Hacking*. Leggendo ora quelle parole, mi sembra quasi di vivere un sogno; ho la memoria confusa e penso che mi sveglierò da un momento all’altro. Ripercorro il viaggio dei miei ultimi dieci anni, soprattutto degli ultimi otto, e vedo che tutto ha preso vita in questo libro.

Negli ultimi otto anni ho lavorato con persone come Paul Ekman, Robin Dreeke, Neil Fallon e tanti altri. Ho avuto l’onore di intervistare persone come Robert Cialdini, Amy Cuddy, Dov Baron, Ellen Langer, Dan Airely e molte altre. Ho avuto il privilegio di tenere un discorso con Apollo Robins e di incontrare Will Smith. Mi sono recato in Gran Bretagna per formare membri dell’MI-5 e dell’MI-6. E sono stato invitato al Pentagono per parlare di ingegneria sociale a trentacinque fra generali, governatori e altri funzionari.

Gli ultimi otto anni sono stati come un incredibile giro sulle montagne russe. Ma come ogni progetto, anche questo non è nato da solo. Queste esperienze, la mia vita e le persone che ho avuto l’onore di conoscere e con le quali ho lavorato… tutto è merito delle tante persone che mi hanno aiutato lungo la strada.

Mia moglie Areesa è una delle donne più pazienti e belle che abbia mai incontrato. Anche se non appartiene al mondo in cui opero, mi

sostiene davvero, mi ama e rende la mia vita felice, piena di risate, avventure e ricordi indelebili.

Quando mio figlio Colin era piccolo, voleva diventare un dottore, poi uno scrittore, poi un volontario. Strano ma vero, si è occupato di cura degli altri, ha provato a scrivere e continua a fare volontariato. Il suo atteggiamento positivo e il suo spirito gentile rappresentano un esempio per me.

Ricordo di aver giurato che non avrei mai permesso a mia figlia, Amaya, di entrare nel mondo dell'ingegneria sociale; intendevo proteggerla. Ma ho scoperto che proteggerla significa insegnarle, includerla, farla entrare nella mia vita. Mi ha dato molto più di quanto le abbia dato io.

Sebbene Paul Ekman non sia direttamente legato a questo libro, la sua gentilezza, motivazione e generosità sono per me fonte di ispirazione. Grazie.

Voglio ringraziare ed esprimere riconoscenza a tutti coloro che hanno fatto parte di questo mio viaggio.

- Ping Look è una fonte infinita e disinteressata di consigli e di supporto.
- L'amicizia e il sostegno di Dave Kennedy significano davvero molto per me.
- La Innocent Lives Foundation è diventata parte integrante di questo processo, quindi voglio ringraziare le seguenti persone.
  - Non avrei mai pensato di poter dire che Neil Fallon e io potessimo diventare amici (datemi un pizzico). Ma ora mi guida, mi indirizza e mi incoraggia. Mi riporta davvero alla mia umanità.
  - Il supporto e la protezione di Tim Maloney sono stati una parte davvero importante nel mettere insieme la ILF. La sua amicizia, la sua fede e il suo supporto in questo processo sono qualcosa per cui non potrò mai ringraziarlo abbastanza.

- L’entusiasmo e l’energia di Casie Hall nel suo essere parte della soluzione è contagioso.
- Ringrazio AJ Cook per il suo supporto con ILF e per averci aiutato nei nostri sforzi per proteggere i più piccoli. La sua dedizione è esemplare.
- L’etica del lavoro, la gentilezza e la capacità di concentrazione di Aisha Tyler (… anche solo digitare il suo nome mi sembra un po’ surreale) sono un modello che tutti dovremmo imitare.

- Il mio team di Social-Engineer, LLC è stato eccezionale. Colin, Mike, Cat, Ryan, Amanda, Kaz, Jenn e Karen: ognuno di loro mi ha aiutato a migliorare e mi ha sostenuto in questo lavoro.
- Giuro che la mia editor Charlotte è la vera ghost writer di questo mio libro. Ha catturato i miei pensieri e mi ha aiutato a sembrare molto più intelligente di quello che sono (ed è stata davvero dura!).
- E i lettori e gli appassionati del podcast Social-Engineer dei SEVillage alle conferenze, dei miei altri libri e degli SE-Event che mi hanno sempre sostenuto, non hanno avuto paura di chiamarmi per parlarmi dei miei stupidi errori e mi hanno spinto costantemente a fare sempre meglio. Grazie!

Ingegneria sociale. Ricordo ancora quando, ricercando quel termine, trovavo video che insegnavano a scroccare hamburger o procurarsi appuntamenti con le ragazze. Ora mi sembra che quel termine esista da sempre. Proprio l'altro giorno un amico di famiglia, che non è affatto del settore, mi parlava di una truffa basata su e-mail. Mi ha detto: "Beh, questo non è che un grande caso di ingegneria sociale!".

La mia vita mi è passata davanti in un secondo, ma eccoci qui: a otto anni dalla decisione di fondare una società incentrata esclusivamente sull'ingegneria sociale, questa è un'industria in piena regola e il termine è ormai diventato familiare.

Quando inizierete a leggere questo libro, forse fraintenderete le mie vere intenzioni. Potreste pensare che voglia istruire "i cattivi" o motivarli a compiere le loro "gesta". Ma questo non potrebbe essere più lontano dalla verità.

Quando scrissi il mio primo libro, molte persone, durante le interviste, si arrabbiavano molto con me e mi accusavano di armare eserciti di pericolosi ingegneri sociali. Ora come allora non potete difendervi dall'ingegneria sociale se non conoscete tutti i modi in cui viene impiegata. L'ingegneria sociale è uno strumento, come un martello, una pala, un coltello o anche una pistola. Ogni strumento ha uno scopo e può essere utilizzato per costruire, proteggere, nutrire o sopravvivere; ogni strumento può anche essere usato per ferire,

uccidere e portare distruzione e rovina. Per imparare a utilizzare l'ingegneria sociale per costruire, nutrire, sopravvivere o proteggere, è necessario comprenderne tutti gli usi. Questo è particolarmente vero se il vostro obiettivo è quello di difendere. Imparare a difendere voi stessi e gli altri dagli usi fraudolenti dell'ingegneria sociale richiede un tuffo nel "lato oscuro della forza", per avere una chiara visione di come viene utilizzata all'atto pratico.

Recentemente ho parlato con AJ Cook del suo lavoro su *Criminal Minds*. Mi ha detto che spesso deve incontrare veri agenti federali che lavorano su veri casi di serial killer per prepararsi a interpretare il ruolo di JJ. A questo libro si applica esattamente la stessa idea.

Leggete questo libro con una mente aperta. Ho fatto del mio meglio per mettere in queste pagine le conoscenze, le esperienze e le tecniche che ho appreso in quest'ultimo decennio. Vi troverete errori, qualcosa che non vi piacerà o qualcosa che potrebbe non risultare chiaro al cento per cento. Parliamone. Potete trovarmi su Twitter come `@humanhacker`. Oppure potete mandarmi una e-mail attraverso uno dei miei siti web: `www.social-engineer.org` o `www.social-engineer.com`.

Quando tengo i miei corsi settimanali, chiedo sempre agli allievi di non trattarmi come un docente infallibile. Se conoscono qualcosa, se hanno in mente qualcosa o anche solo hanno la sensazione che qualcosa che conoscono contraddica quanto sto dicendo loro, amo discuterne. Amo imparare e ampliare la mia comprensione su questi argomenti. Estendo la stessa richiesta anche a voi.

Infine, voglio ringraziarvi. Grazie per aver voluto trascorrere un po' del vostro tempo prezioso con me, nelle pagine di questo libro. Grazie per avermi aiutato a migliorare nel corso degli anni. Grazie per tutti i vostri feedback, le vostre idee, le vostre critiche e i vostri consigli.

Spero davvero che questo libro vi piaccia.

Uno sguardo al nuovo mondo dell’ingegneria sociale professionale

> Suppongo che la vostra sicurezza sia il vostro successo e che la chiave del vostro successo sia il vostro fine palato.
> - *Gordon Ramsay*

Mi ricordo ancora bene quando, seduto di fronte allo schermo del mio computer, iniziai a scrivere il primo paragrafo di *Social Engineering: The Art of Human Hacking*. Era la metà del 2010. Sarei quasi tentato di dirvi che la scrittura del libro è stata un’impresa in tanti i sensi, dovendo usare una macchina per scrivere, ma non voglio essere troppo drammatico.

Al tempo, cercando in Internet il termine “social engineering”, trovavate alcune pagine sulla leggenda dell’ingegneria sociale Kevin Mitnick e alcuni video su come corteggiare le ragazze o scroccare hamburger. Sono trascorsi otto anni e ora il termine ingegneria sociale suona quasi familiare. Negli ultimi tre o quattro anni ho visto applicare l’ingegneria sociale nella sicurezza, nell’amministrazione, nell’istruzione, in psicologia, in ambito militare e in ogni altra realtà che si possa immaginare.

Questa transizione impone di chiedersi il perché. Un collega mi ha detto: “È tutta colpa tua, Chris”. Penso che lo intendesse come un insulto, anche se ho provato un pizzico di orgoglio nel sentirmelo dire.

Tuttavia, non ritengo di essere il solo responsabile della quasi ubiquità del termine *ingegneria sociale* (*social engineering* o SE). Credo che oggi sia usato da tutti non solo perché è il più semplice fra i vettori di attacco – oggi come sette anni fa – ma perché oggi è ancora più redditizio.

Il costo di un attacco di ingegneria sociale è basso. Il rischio è ancora più basso. Il vantaggio potenziale è *enorme*. Il mio team ha raccolto informazioni statistiche sui notiziari e sul Web di attacchi di ingegneria sociale. Credo di poter affermare che nel 2017 oltre l'80% di tutti gli attacchi aveva un elemento di ingegneria sociale.

Il *Cost of Data Breach Study* del 2017 di IBM afferma che il costo medio di un attacco è di 3,62 milioni di dollari. Quando il profitto potenziale è così alto, non è certamente difficile capire perché un malintenzionato ricorra all'ingegneria sociale.

SUGGERIMENTO

Nel 2017, il *Cost of Data Breach Study* di IBM ha compiuto 12 anni. Potete trovarlo su `https://www-03.ibm.com/security/data-breach/`. Oppure potete semplicemente inserire "Cost of Data Breach Study" in qualsiasi motore di ricerca per trovare e scaricare un rapporto completo e aggiornato.

Ricordo anche una delle mie prime interviste dopo la scrittura del mio libro *Social Engineering: The Art of Human Hacking*, pubblicato nel 2010. Mi hanno chiesto: "Non temi di armare i cattivi?". Per me, l'ingegneria sociale è come un nuovo tipo di guerra.

Per spiegarlo in modo più chiaro, rievoco la storia di Bruce Lee e del suo arrivo in America negli anni Sessanta. A quel tempo i pregiudizi razziali erano un problema e lui stava facendo qualcosa che nessun altro faceva: insegnare *jeet kune do* (un'antica arte marziale cinese) a persone di ogni razza, colore o nazionalità. All'università si scontrò con altri studenti che pensavano di sapere tutto sul combattimento. Ma li mise al tappeto uno dopo l'altro. Alla fine, alcuni di quegli avversari divennero persino amici o allievi di Bruce.

Qual è la lezione? Gli altri dovevano adattarsi a questo nuovo tipo di combattimento, o sarebbero stati facilmente e costantemente battuti. C'era il rischio che un allievo di Bruce Lee potesse usare le sue nuove abilità per ferire gli altri e fare del male? Sì, ma Bruce sentiva la necessità di istruire gli altri, in modo che potessero difendersi.

Quindi, la mia risposta alla domanda "Non temi di armare i cattivi?" è la stessa di otto anni fa: non posso controllare come userete queste informazioni. Potete leggere questo libro e poi uscire, attaccare le persone e derubarle. Oppure potete leggere questo libro e imparare a difendervi. La scelta è vostra, ma i bravi ragazzi hanno bisogno che qualcuno insegni loro che cosa fare.

Imparare a difendersi da questo nuovo stile di attacco richiede molto più che imparare a battersi. Come con il *jeet kune do*, occorre equilibrio tra imparare ad attaccare, imparare a difendersi e sapere quando applicare l'una o l'altra cosa. Mentre imparerete a diventare ingegneri sociali, dovete essere in grado di pensare come i cattivi, ricordandovi sempre di comportarvi da bravi ragazzi. Volendo rubare un'altra analogia, dovete sentire dentro di voi la forza, ma non usarla mai per camminare nel lato oscuro.

Potreste chiedervi: "Se non è cambiato molto nella tua risposta, perché abbiamo bisogno di una seconda edizione del tuo libro?". Lasciate che ve lo dica.

Che cosa è cambiato?

Questa è una domanda fondamentale quando si parla di ingegneria sociale. Superficialmente, la risposta è "Non molto". Potete tornare indietro e trovare tanti aneddoti sull'ingegneria sociale. Per esempio, una delle prime storie documentate che ho trovato si trova nella Bibbia, nel libro della Genesi, e si dice che sia avvenuta intorno al 1800 a.C.: Giacobbe desiderava la benedizione che aveva ricevuto il

fratello maggiore, Esau. Sapendo che suo padre, Isacco, non ci vedeva e faceva affidamento su altri sensi per capire con chi stesse parlando, Giacobbe si vestì con gli abiti di Esau e gli preparò il pranzo come lo avrebbe preparato lui. Ecco la parte migliore: Esau era noto per essere particolarmente villoso, mentre Giacobbe non lo era, così si legò le pelli di due giovani capre tra le braccia e la nuca. Quando Isacco allungò la mano per toccare Giacobbe, fece affidamento sull'olfatto, sul tatto e sul gusto, i quali gli dicevano che era con Esau e non Giacobbe. Secondo il racconto della Genesi, l'attacco di ingegneria sociale di Giacobbe funzionò!

Dall'alba della storia, ci vengono riportate truffe, inganni e imbrogli. In apparenza, non sembra esserci molto di nuovo quando si parla di ingegneria sociale, ma ciò non significa che le cose non cambino mai.

Un esempio è il *vishing*. Ricordo bene quando usai per la prima volta la parola *vishing*. La gente mi guardava come se stessi parlando *klingon*. Davvero, avrei potuto dire "laH yIlo' ghogh HablI' Hiv" (questo è per i fan di Star Trek). A partire dal 2015, tuttavia, la parola *vishing* è entrata nell'*Oxford English Dictionary*.

SUGGERIMENTO

Il klingon è una lingua fittizia, ma esiste un vero e proprio istituto (`www.kli.org`) dedicato all'insegnamento, alla traduzione e alla fonetica della lingua klingon. Potete anche trovare numerosi traduttori online. A oggi, tuttavia, non ho avuto notizia di attacchi di "ingegneria sociale" svoltisi in lingua klingon.

Perché è importante che oggi *vishing* sia nel dizionario? Dimostra quanto le azioni di ingegneria sociale abbiano influenzato il mondo. Parole che un tempo sembravano appartenere a una lingua "inventata", ora fanno parte del nostro vocabolario quotidiano.

Ma non è solo questo nuovo vocabolario a essere diventato ormai di uso comune. Ora esistono servizi specializzati nell'aiutare i cattivi a essere sempre più bravi nell'essere cattivi. Per esempio, mentre stavo lavorando per un cliente, mi sono imbattuto in un servizio

specializzato nella correzione e verifica ortografica delle e-mail di *phishing*. Forniva un supporto ventiquattro ore su ventiquattro in lingua inglese. Provate a mettere insieme cose di questo genere con la cultura BYOD (*Bring Your Own Device*) e con il fatto che ormai molti apparecchi mobili sono in pratica mini-supercomputer e poi metteteci insieme la nuova forma di dipendenza globale dai *social media*. Quello che ottenete è la ricetta per un intero panorama di nuovi attacchi: basati sull'ingegneria sociale.

Oltre a essere cambiato il panorama, anche io sono cambiato. Quando scrissi la prima edizione di questo libro, il titolo era *Social Engineering: The Art of Human Hacking*. Ho scelto quel titolo perché sentivo che quello che stavo descrivendo nel libro era molto simile a un'arte. L'arte è soggettiva; ha significati differenti per persone differenti. Può essere applicata in modo differente e può essere utilizzata, visualizzata, apprezzata e detestata per motivi completamente differenti.

Il titolo originale inglese di questa seconda edizione è *Social Engineering: The Science of Human Hacking*. Il dizionario Merriam-Webster definisce la *scienza* come "Lo stato di conoscenza: una conoscenza distinta dall'ignoranza o dal fraintendimento". Otto anni fa, gran parte di quel che facevo era una novità nel campo della sicurezza e stavo imparando. Ora sono in uno "stato di conoscenza", grazie agli anni di esperienza che ho aggiunto al mio curriculum.

Questa esperienza, spero, renderà questo libro ancora più utile per voi, che siate esperti di sicurezza che cercano di capire che cosa sia l'ingegneria sociale o che siate appassionati desiderosi di ampliare i vostri orizzonti o anche educatori che stanno cercando di capire i problemi da considerare nelle lezioni. Qualsiasi sia il motivo per il quale state leggendo questo libro, la mia speranza è che, trattando

questi argomenti a un livello più scientifico, io possa trasmettervi queste informazioni in un modo più utile e completo.

Perché dovreste leggere questo libro?

Penso che questo primo capitolo debba seguire lo stesso schema che ho seguito nel mio primo libro, quindi voglio dedicare del tempo a spiegare perché penso che questo volume sia rivolto a tutti. Sì, mi rendo conto che potrei essere "un pochino" di parte, ma seguitemi per un momento.

Siete esseri umani? Scommetto che se siete seduti di fronte a questo libro, e se state leggendo questo paragrafo, o siete una forma davvero avanzata di intelligenza artificiale o siete esseri umani. Probabilmente il 99,9999999% dei lettori di questo libro è costituito da esseri umani. L'ingegneria sociale parte dal "funzionamento standard" degli esseri umani quando prendono decisioni e nel sfruttare le vulnerabilità.

L'obiettivo di un ingegnere sociale è quello di indurvi a prendere una decisione senza riflettere. Più pensate, più è probabile che vi accorgiate di essere stati manipolati, il che, naturalmente, è contrario agli interessi dell'aggressore. Negli episodi 7 e 70 di *The Social-Engineer Podcast*, ho avuto il privilegio di intervistare la dottoressa Ellen Langer. Mi parlò di qualcosa che ha chiamato *alpha mode* e *beta mode*.

SEPodcast

Di seguito sono riportati gli URL in cui potete trovare gli episodi di *The Social-Engineer Podcast* nei quali ho intervistato la dottoressa Langer.

- L'Episodio 7 contiene la mia prima intervista con la dottoressa Langer, nella quale discutiamo della sua ricerca e dei suoi libri: `www.social-engineer.org/podcast/episode-007-using-persuasion-on-the-mindless-masses/`.

- L’Episodio 70 si svolge cinque anni dopo la mia prima intervista alla dottoressa Langer. È tornata per dirci che cosa ha imparato nel corso degli anni, che cosa è cambiato e come siamo avanzati: www.social-engineer.org/podcast/ep-070-thinking-with-out-a-box.

In *alpha mode* il cervello funziona a 8-13 cicli al secondo. In genere è caratterizzato dal “sognare a occhi aperti” o da quello che la dottoressa Langer ha definito “concentrazione rilassata e focalizzata”.

In *beta mode* il cervello funziona da 14 a 100 cicli al secondo: è attento, vigile e consapevole di quello che gli accade attorno.

Quale stato è più vantaggioso per un ingegnere sociale? Ovviamente, la risposta è l’*alpha mode*, perché gode di una certa rilassatezza del pensiero e della consapevolezza. Questo non vale solo per le situazioni in cui sia in atto un’aggressione. La manipolazione e alcune tecniche di influenzamento sono orientati a farvi agire senza riflettere.

Per esempio, immaginate uno spot come questo: una famosa cantante compare sullo schermo; una canzone molto triste suona in sottofondo. L’immagine cambia: vengono mostrati gattini e cagnolini che sono stati maltrattati e sono feriti e denutriti. Sembrano in procinto di morire. Ma la cantante torna sullo schermo; ora è circondata da animali sani e li sta inondando di coccole. Qual è il messaggio? Che per pochi spiccioli quegli animali denutriti e quasi morti possono diventare animali da compagnia: sani, felici e tutti vostri. Le immagini nello spot sono come quelle della Figura 1.1.



Figura 1.1 Come vi fa sentire questa foto? © Amazon Community Animal Rescue,www.flickr.com/photos/amazoncares/2345707195.

I produttori dello spot vi stanno manipolando per egoismo? Non del tutto. Quello che sanno è che se riusciranno a evocare emozioni in voi, è più probabile che donerete una somma o che intraprenderete l'azione desiderata. Il tasso di successo è maggiore di quello che avrebbero facendo ricorso semplicemente alla conoscenza o alla logica. Più emozioni riescono a innescare e meno penserete in modo razionale. Meno pensate in modo razionale e più velocemente deciderete, basandovi unicamente sulle vostre emozioni.

Quindi, tornando al punto precedente: se siete esseri umani, questo libro può aiutarvi a capire quali tipi di attacchi esistono. Potete imparare come i cattivi possono usare la vostra umanità contro di voi e potete imparare a difendervi da questi attacchi per proteggere voi e i vostri cari.

Permettetemi di iniziare da una panoramica sull'ingegneria sociale.

Una panoramica sull'ingegneria sociale

Ogni volta che parlo di ingegneria sociale, di solito inizio con una definizione che uso da dieci anni. Col tempo l'ho adattata, ma solo leggermente.

Ma prima di darvi la definizione di ingegneria sociale, devo proprio affermare un punto molto importante: l'ingegneria sociale non è *politicamente corretta*. Questa verità può essere difficile da digerire per molte persone, ma è un fatto reale: l'ingegneria sociale si basa sul fatto che esistono pregiudizi di genere, di razza, di età e di stato (oltre a tutte le combinazioni possibili).

Per esempio, immaginate di dovervi infiltrare nell'edificio di un cliente. Per farlo, dovete escogitare un pretesto che vi permetta di accedervi facilmente. Il vostro team è composto da poche persone, di diverso tipo. Se valutate che il miglior pretesto sia fingersi un addetto alle pulizie, quale dei seguenti membri del team sarebbe più efficace?

- Uomo bianco, biondo, di 40 anni.
- Donna asiatica, di 43 anni.
- Donna latina, di 27 anni.

Se valutate che il miglior pretesto sia fingersi un addetto alla cucina, quale dei seguenti membri del team sarebbe più efficace?

- Uomo bianco, biondo, di 40 anni.
- Donna asiatica, di 43 anni.
- Donna latina, di 27 anni.

In realtà, se i tre fossero tutti ingegneri sociali esperti, potrebbero provare e avere successo. Ma quale dei tre solleverà il minor numero di pensieri? Ricordate, i pensieri sono nemici dell'ingegnere sociale.

Con questo in mente, torniamo a come definisco l'ingegneria sociale: *l'ingegneria sociale è ogni atto tendente a influenzare una persona, per spingerla a intraprendere un'azione che non necessariamente è nel suo migliore interesse.*

Perché una definizione così ampia e generale? Perché credo che l'ingegneria sociale non sia *sempre* negativa.

Ci fu un tempo in cui si poteva dire "Sono un hacker" senza che tutte le persone normali cercassero di correre ai ripari, staccando ogni dispositivo elettronico circostante. Essere hacker, un tempo, significava essere qualcuno che aveva *bisogno* di sapere come funzionavano le cose. Un hacker non si accontentava delle conoscenze di base; doveva scavare in profondità nel funzionamento di qualsiasi cosa. Una volta compreso il funzionamento di una cosa, l'hacker avrebbe cercato un modo per aggirare, migliorare, sfruttare o modificare lo scopo originale di quella cosa.

Quando iniziai il mio primo libro, volevo assicurarmi di poter definire l'ingegneria sociale in un modo che non implicasse necessariamente la presenza di un perfido artista della truffa o un imbroglione o un furfante. Gli stessi principi usati dai cattivi possono essere applicati per buoni propositi e voglio che lo sappiate.

Spesso uso questo esempio. Se venite da me e mi dite: "Ehi, Chris. Voglio fare una festa per principesse: tu ti siedi qui e ti dipingo le unghie mentre indossi una sciarpa rosa e parliamo delle principesse Disney", non solo riderei di voi, ma tenterei di allontanarmi

lentamente, cercando l'uscita più vicina. Eppure, devo ammettere che potrebbero esserci situazioni in cui non disdegnerei questo tipo di cose.

In che senso, direte? Mia figlia mi ha chiesto di fare una festa per principesse con lei. Ora, prima che diciate "Ehi, ma non vale come paragone: è tua figlia!", ammetto che questo piccolo particolare ha influenzato non poco la mia decisione di stare al gioco, ma mi interessa che riflettiate sui principi psicologici che erano in gioco quando ho preso questa decisione. Per accettare una cosa che avrei assolutamente rifiutato, in un nanosecondo, se mi fosse stata proposta da qualcun altro, ho dovuto ignorare il mio normale processo decisionale e rispondere "Sì".

Un dettaglio assolutamente inutile

Considerando che un nanosecondo è un miliardesimo di secondo e che una persona, in media, parla a un ritmo di 145 parole al minuto, letteralmente non potevo "dire" la parola "no" in un nanosecondo. D'altra parte, la luce, che viaggia a 300.000 chilometri al secondo, percorre 30 centimetri in un nanosecondo.

Se comprendete in quale modo vengono prese le decisioni, potete iniziare a capire come un aggressore malintenzionato possa usare "grilletti" emotivi, principi psicologici e applicare l'arte e la scienza dell'ingegneria sociale per farvi "intraprendere un'azione che non necessariamente è nel vostro migliore interesse".

Il dottor Paul Zak è apparso nell'Episodio 44 di *The Social-Engineer Podcast*. Ha scritto il libro *La molecola della fiducia: all'origine della prosperità economica e sociale* (Scuola di Palo Alto, Milano 2015). In quel libro, e nel nostro podcast, Zak parlava della sua ricerca relativa a un ormone chiamato *ossitocina*. La sua ricerca ci ha aiutato a vedere quanto l'ossitocina sia strettamente legata alla fiducia, perché fece un commento molto importante sul modo in cui viene rilasciata nel nostro sangue quando sentiamo che qualcuno si fida di noi. Vi prego di comprendere questo punto molto importante: il vostro

cervello libera ossitocina non solo quando voi vi fidate di qualcuno, ma anche quando *sentite* che qualcun altro vi dà fiducia. Secondo la ricerca di Zak, questo fenomeno si verifica di persona, al telefono, via Internet e anche quando non è possibile vedere la persona in questione.

SEPodcast
L'Episodio 44 di *The Social-Engineer Podcast* include l'affascinante conversazione con il dottor Zak sul lavoro della sua vita. Potete trovarlo su www.social-engineer.org/podcast/ep-044-do-you-trust-me/.

Un'altra sostanza chimica prodotta dal nostro cervello è la dopamina. La *dopamina* è un neurotrasmettitore che il nostro cervello rilascia nei momenti di piacere, felicità ed eccitazione. La miscela di ossitocina e di dopamina genera un cocktail cerebrale con il quale un ingegnere sociale può aprire qualsiasi porta.

La dopamina e l'ossitocina vengono rilasciate nel nostro cervello durante i momenti di intimità, ma possono essere rilasciate anche durante le normali conversazioni. Esattamente quelle conversazioni sono al centro dell'ingegneria sociale.

Credo che tutti usiamo questi stessi principi quotidianamente – il più delle volte inconsapevolmente – con il nostro coniuge, con il capo, coi colleghi, coi sacerdoti, coi terapeuti, con il personale di servizio e con tutti quelli che incontriamo. Di conseguenza, sapere che cos'è l'ingegneria sociale e come comunicare con i propri simili è imperativo per tutti.

In un mondo in cui la tecnologia ha facilitato le comunicazioni utilizzando *emoticon* o meno di 280 caratteri, è sempre più difficile imparare a usare le capacità comunicative e ancor più difficile capire quando quelle abilità vengono utilizzate contro di noi. Facendo un ulteriore passo avanti, i *social media* hanno creato una società in cui raccontare a tutti tutto quello che ci accade è accettabile e addirittura valutato positivamente.

Quando parlo dell'ingegneria sociale intesa in senso malevolo, la suddivido nei seguenti quattro vettori.

- *SMiShing* - Sì, esiste: è il *phishing* via SMS o tramite messaggi di testo. Quando Wells Fargo è stata violata nel 2016, ricevetti l'attacco *SMiShing* mostrato nella Figura 1.2.
  Quello che è pazzesco è che non uso nemmeno Wells Fargo, ma ho comunque ricevuto questo attacco (e no, non vi dirò che banca uso… per chi mi avete preso?).
  Con un semplice clic, questi attacchi erano finalizzati a sottrarre credenziali o a caricare *malware* sul dispositivo mobile e a volte a fare entrambe le cose.

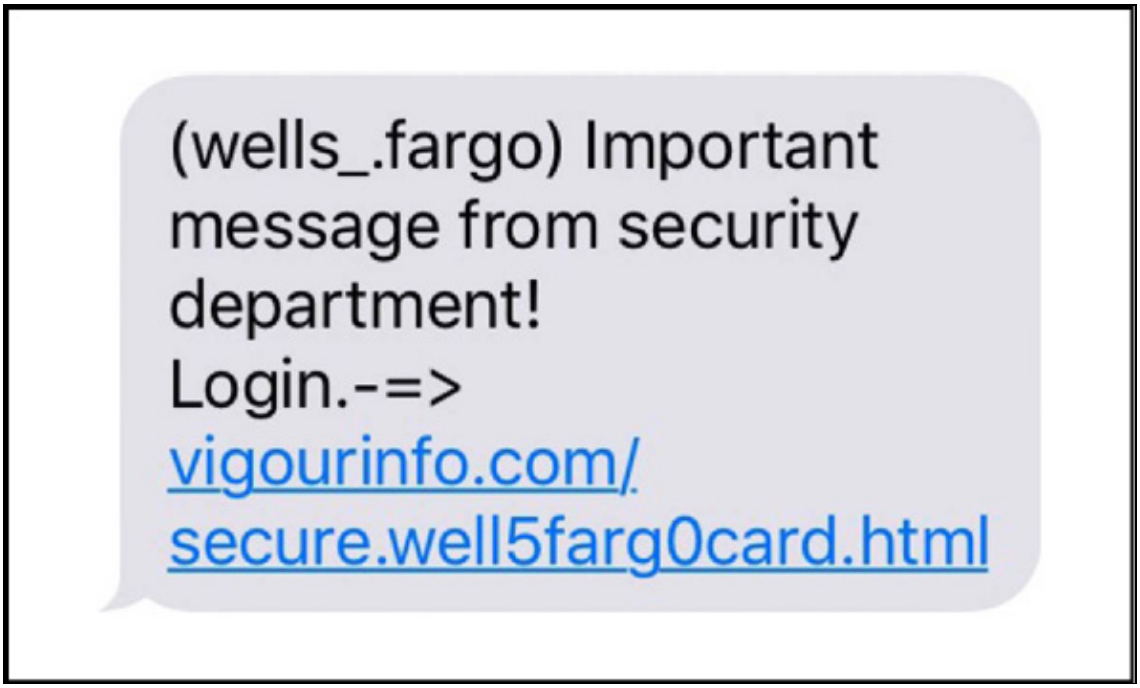


Figura 1.2 In questo attacco SMiShing sono cadute parecchie persone.

- *Vishing* - Come ho già detto, si tratta del *phishing* vocale. è aumentato drasticamente, come vettore, dal 2016. È facile, economico e molto redditizio per chi svolge l'attacco. È anche

quasi impossibile localizzare e poi catturare un malvivente, che impieghi numeri falsi e chiami dall'estero.

- *Phishing* - L'argomento più discusso nel mondo dell'ingegneria sociale è il *phishing*. In effetti, l'editor tecnico di questo libro, Michele, e io abbiamo scritto il libro *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* (Wiley, 2016). Esatto: ho "infilato" nella pagina, senza vergogna, un altro dei miei libri. Il *phishing* è stato utilizzato per chiudere stabilimenti produttivi, per hackerare partiti, per violare la Casa Bianca e decine di grandi aziende e rubare milioni di dollari in diverse truffe. Il *phishing* è di gran lunga il più pericoloso tra i quattro grandi vettori.
- *Impersonificazione* - Lo so, dovrei trovare una qualche forma di "ishing" anche per questo, ma il meglio che posso fare è elencarlo per ultimo, perché è differente. Tuttavia, la sua collocazione in questo elenco non indica affatto che non dobbiate preoccuparvene quanto gli altri. Negli ultimi dodici mesi, abbiamo raccolto centinaia di storie di persone che si spacciano per poliziotti, incaricati del gas e colleghi per commettere crimini davvero orribili. Nell'aprile del 2017, si parlò di un tipo che si fingeva poliziotto e fu catturato. La sua specialità era la pornografia infantile e tutto si basava su quella sua imitazione.

Altre informazioni

Potete trovare questa storia disgustosa in: `www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn-20170418-story.html`.

Ogni attacco di ingegneria sociale di cui si legge rientra in una di queste quattro categorie. Più di recente, stiamo vedendo quello che possiamo chiamare attacco combinato: gli ingegneri sociali utilizzano una combinazione di queste tecniche per raggiungere i loro mezzi.

Quando analizzo questi attacchi, comincio a individuare schemi che non solo identificano il tipo di strumenti e passaggi utilizzati, ma che possono anche aiutare un esperto di sicurezza a definire in modo più chiaro come vengono svolti questi attacchi e quindi a utilizzare i risultati per istruire e proteggere il sistema. Ho chiamato questo sistema *la piramide SE*.

La piramide SE

Permettetemi di presentarvi subito la piramide prima di definire il motivo per cui sono giunto a questa simbologia e di spiegare il significato di ogni sua sezione. La piramide è rappresentata nella Figura 1.3.

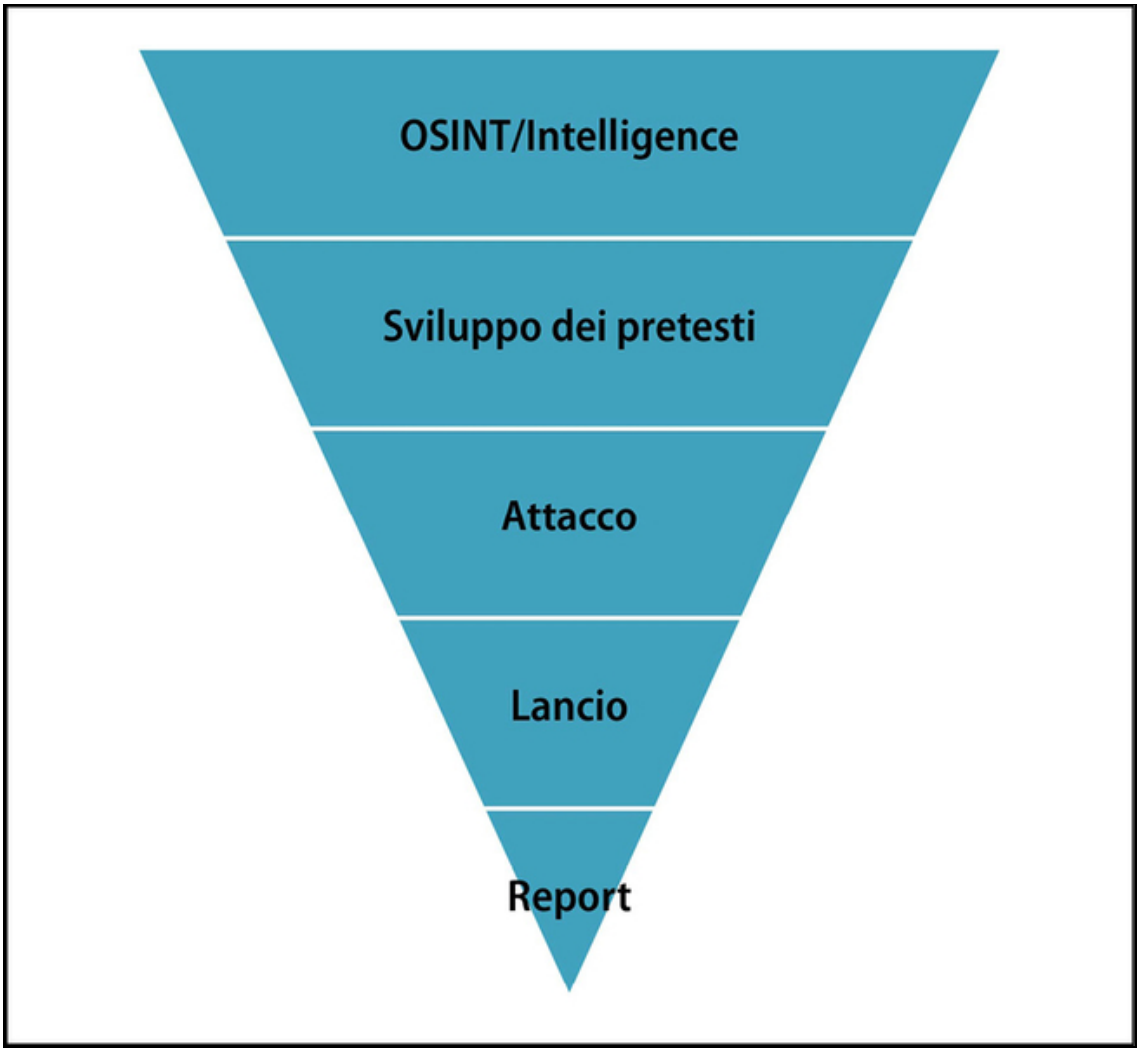


Figura 1.3 La piramide SE.

Come potete vedere, la piramide è suddivisa in poche sezioni e rappresenta l'ingegneria sociale dal punto di vista di un professionista, che utilizza l'ingegneria sociale non per fini malevoli, ma per aiutare i clienti e i consumatori.

Ora definirò ogni sezione della piramide. Nei prossimi capitoli entrerò più in dettaglio dei vari strati.

OSINT

L’OSINT (*Open Source Intelligence*) è la linfa vitale di ogni impegno di ingegneria sociale. È anche la parte che dovrebbe richiedere più tempo. Occupa pertanto la prima e la più grande parte della piramide. Una sezione di questa parte della piramide viene affrontata solo raramente: la documentazione. Come documenterete, salverete e catalogherete tutte le informazioni che avete raccolto? Questo fattore chiave verrà affrontato nel prossimo capitolo.

Sviluppo del pretesto

Sulla base di tutti i risultati della parte OSINT, il successivo passo logico consiste nell’iniziare a sviluppare il pretesto. Questa è una parte cruciale, che è meglio eseguire con l’OSINT bene in mente. Durante questa fase, potete decidere quali modifiche o aggiunte apportare per garantire il successo dell’attacco. è qui che diventa chiaro quali supporti e/o strumenti sono necessari.

Piano d’attacco

Avere un pretesto in mano non significa essere pronti. Il passo successivo è pianificare il che cosa, il quando e il chi.

- Qual è il piano? Che cosa vogliamo fare e stiamo cercando di ottenere? Che cosa vuole il cliente? Queste domande aiuteranno a sviluppare la prossima parte.
- Quando può essere il momento migliore per sferrare l’attacco?
- Chi deve essere disponibile, senza preavviso, per offrire supporto o assistenza?

Attacco

Ora arriva la parte divertente: il lancio dell'attacco. Dopo la preparazione del piano di attacco, siete pronti per procedere a pieno ritmo. È importante essere preparati, ma non al punto da non essere dinamici. Sono convinto che avere un piano scritto possa farvi risparmiare molti mal di testa. Il dubbio che ho è che se elaborate ogni parola che dovrete pronunciare o azione che dovrete prendere, potreste incontrare problemi nel caso di un imprevisto. Il vostro cervello si accorge di non aver predisposto nulla di utile, iniziate a balbettare, a innervosirvi e a mostrare segni di agitazione. Questo può davvero pregiudicare le vostre capacità di successo. Invece di scrivere, suggerisco di strutturare le reazioni, in modo da avere un percorso da seguire ma anche la necessaria libertà d'azione.

Report

Ehi dove andate? Non saltate questo paragrafo. È proprio il caso di leggerlo. Sì, la creazione di report non è divertente, ma pensatela in questo modo: il vostro cliente vi ha appena pagato la somma *x* per un determinato servizio e, molto probabilmente, siete stati dannatamente bravi in questo attacco. Ma il cliente non vi ha pagato solo perché questa è la moda del momento. Vi ha pagato per capire che cosa può fare per risolvere il suo problema. Questo è il motivo per cui la fase di segnalazione si trova al vertice della piramide: è l'apice sul quale poggia *tutto* il resto della piramide.

Le cinque fasi di questa piramide, se ben seguite, vi porteranno al successo non solo come ingegneri sociali, ma come professionisti che offrono servizi di ingegneria sociale ai vostri clienti. Il fatto è che, con l'eccezione del *reporting*, questi sono i passaggi seguiti dagli ingegneri sociali malintenzionati in tutto il mondo.

Nel 2015, Dark Reading ha riferito di un attacco che ha coinvolto proprio questa piramide (potete leggere l'articolo *CareerBuilder*

Attack Sends Malware-Rigged Resumes to Businesses su https://www.darkreading.com/vulnerabilities---threats/careerbuilder-attack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236).

1. Gli aggressori effettuarono indagini attaccando alcuni bersagli e, durante la loro fase OSINT, scoprirono che essi utilizzavano un noto sito: CareerBuilder.
2. Dopo aver completato la fase OSINT, gli aggressori iniziarono a sviluppare il pretesto. Ciò li portò a elaborare una falsa ricerca di lavoro, una persona che stava cercando di farsi assumere in qualunque posizione offerta dagli obiettivi. Scoprirono che gli strumenti di cui avevano bisogno erano alcuni file ben preparati e alcuni curriculum dall'aspetto realistico.
3. Iniziarono a pianificare gli attacchi, rispondendo ad alcune delle domande che ho appena esposto.
4. Iniziarono quindi a lanciare gli attacchi caricando i loro documenti non sul sito dell'obiettivo, ma su quello di CareerBuilder. Le aziende che avevano pubblicato offerte di lavoro sarebbero state informate via e-mail che c'era un nuovo richiedente e tale e-mail conteneva gli allegati caricati dagli aggressori.
5. Non seguì alcuna fase di reporting, ma ci sono alcuni report su questo attacco redatti da alcuni ricercatori di Proofpoint.

Questo attacco ebbe successo perché l'obiettivo ricevette un'e-mail con allegati da una fonte affidabile e attendibile (CareerBuilder). Di conseguenza, l'obiettivo aprì l'allegato senza preoccuparsene troppo. Ed esattamente questo è l'obiettivo di un ingegnere sociale: far sì che l'obiettivo intraprenda un'azione che non è nel suo miglior interesse senza riflettere sui potenziali pericoli coinvolti.

Di che cosa parla questo libro?

Quando iniziai a pianificare questo libro, volevo assicurarmi di mantenere il profilo della prima edizione, in modo che ne godessero anche coloro che avevano già tratto beneficio dalle sue pagine. Allo stesso tempo, volevo cambiare il libro e aggiornarlo per descrivere alcuni nuovi attacchi e argomenti di cui non avevo parlato nel libro precedente.

Volevo assicurarmi di aver considerato tutti i suggerimenti che mi erano arrivati da sostenitori, ricercatori, lettori e revisori, nella speranza di poter scrivere un libro ancora migliore del primo. Permettetemi quindi di delineare i contenuti del libro, in modo che sappiate che cosa vi troverete.

Seguendo il percorso della piramide, il Capitolo 2, *Vedi anche tu quel che vedo io?*, descrive le attività di OSINT e tratta alcune delle tecniche normalmente utilizzate. Mi astengo dall'usare troppi riferimenti a strumenti reali, anche se ne menziono alcuni che sono rimasti nella mia cassetta degli attrezzi nell'ultimo decennio.

Nel Capitolo 3, *Profilare le persone attraverso la comunicazione*, esaminerò un argomento cui ho appena accennato nella prima edizione, approfondendo gli strumenti avanzati di modellazione e creazione di profili di comunicazione.

Il Capitolo 4, *Impersonare chiunque*, è il punto in cui comincio a tuffarmi nel pretexting. Questo è un argomento di cui pochi parlano al di fuori dell'ambito dell'ingegneria sociale. Vi tratto i suggerimenti, i trucchi e molte delle esperienze (successi e fallimenti) che ho avuto nel corso degli anni.

Nel Capitolo 5, *Come cercare di farsi accettare*, raccolgo informazioni tratte da molti podcast, newsletter e conversazioni con alcuni dei più grandi esperti del mondo, come Robin Dreeke, e applico all'ingegneria sociale i principi della creazione di relazioni. Robin

Dreeke è capo dell'unità di analisi comportamentale dell'FBI e mio buon amico. È un maestro nel costruire relazioni e nel conquistare la fiducia e ha definito i passaggi necessari per conseguire entrambi gli obiettivi.

Il Capitolo 6, *Sotto la mia influenza*, descrive il lavoro di uno dei leader nello studio dell'influenza, Robert Cialdini, nel campo dell'ingegneria sociale. Il capitolo prende i principi che ha sviluppato nel corso dei suoi anni di ricerca e mostra come vengono utilizzati dagli ingegneri sociali.

Il Capitolo 7, *Realizzare la propria opera d'arte*, definisce i concetti di quadro di riferimento e sollecitazione e mostra come chiunque possa impadronirsi di tali tecniche.

Nel Capitolo 8, *Vedo anche quello che non mi hai detto*, torniamo a uno dei miei argomenti preferiti: le comunicazioni non verbali. Scavo in profondità in questo argomento nel mio libro *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014), ma questo capitolo è una guida introduttiva alla comunicazione non verbale.

Nel Capitolo 9, *Hacking degli esseri umani*, prendo gli otto capitoli precedenti e li applico a cinque diversi tipi di attacchi di ingegneria sociale. Questo capitolo mostra quanto sia importante per voi, in quanto professionisti dell'ingegneria sociale, applicare i principi presentati in questo libro.

Quasi al termine del libro, il Capitolo 10, *Avete un MAPP?*, tratta gli aspetti di prevenzione e di riduzione dell'impatto. In un libro sull'ingegneria sociale professionale è opportuno che questo capitolo descriva i quattro passaggi utili per imparare a contrastare tutti gli attacchi.

Come tutte le belle cose, anche questo libro deve avere una fine. Quindi il Capitolo 11, *E ora?*, conclude il volume.

Ecco alcune promesse che vi faccio.

- Prometto di non citare Wikipedia come fonte preziosa, specialmente quando si parla di ricerca (ho imparato dai miei errori).
- Prometto di raccontarvi molte storie tratte dalle esperienze che ho avuto negli ultimi sette o più anni. A volte vi racconterò una storia da più punti di vista, per aiutarvi davvero a chiarire tutti gli aspetti. Ma cercherò di mescolare le varie storie, così da non annoiarvi.
- Quando descriverò le ricerche o il lavoro di alcune delle più grandi menti nei rispettivi campi, presenterò tutti i riferimenti disponibili al loro lavoro, così che possiate approfondire ogni argomento.
- Proprio come ho fatto con il mio primo libro, accoglierò tutti i contatti, i commenti, i suggerimenti e le critiche che mi giungeranno.

Tutto quello che vi chiedo in cambio è che leggiate questo libro per l'uso cui è destinato. Se siete alle prime armi, può aiutarvi a capire che cosa è necessario per diventare professionisti nel campo dell'ingegneria sociale. Se siete esperti, spero che le storie, i suggerimenti e i trucchi che condivido vi diamo nuovi strumenti utili per il vostro arsenale. Se siete appassionati, spero che leggiate questo libro con la stessa eccitazione che avevo io mentre lo scrivevo. E se siete scettici, allora leggetelo pensando che non pretendo di essere l'unico e il solo messia dell'ingegneria sociale. Sono solo un ingegnere sociale appassionato, con molti anni di esperienza, che intende condividere con voi nella speranza di rendere questo mondo un luogo un po' più sicuro.

Riepilogo

Nessuno dei miei libri sarebbe completo senza un’analogia culinaria, quindi eccola qui. Dietro ogni ottimo pasto c’è molta pianificazione. Una grande ricetta richiede ingredienti freschi e poi un’esecuzione allo stesso tempo artistica e scientifica. L’ingegneria sociale, nonostante la sua natura semplice, non è una ricetta per principianti. Bisogna capire il modo in cui gli esseri umani prendono le loro decisioni, che cosa li motiva e come controllare le proprie emozioni sfruttandole invece negli altri.

L’argomento di questo libro è attuale oggi come lo era otto anni fa e forse ancora di più. Negli ultimi otto anni ho visto molte persone crescere come professionisti dell’ingegneria sociale. Ho visto emergere e poi schiantarsi anche molti malviventi dell’ingegneria sociale.

Dal momento che la natura degli attacchi poggia così pesantemente sull’elemento umano, è imperativo che tutti i professionisti della sicurezza comprendano l’argomento dell’ingegneria sociale. Ma c’è molto di più. Ricordo che quando iniziai a lavorare come chef (in un’altra vita, molto tempo fa), il mio maestro prendeva gli ingredienti e mi diceva di assaggiarne piccoli pezzi, uno per uno. Ma perché?

Mi disse che non potevo sapere che cosa significasse “assaggiare” se non avessi capito veramente qual era il gusto di ogni ingrediente. Se so che la ricetta richiede un po’ di rafano e voglio che sia un po’ più piccante, capisco che potrei aggiungerne un pizzico di più. Capire che un certo ingrediente ha anche un gusto salato potrebbe farmi correggere il sale per la ricetta, in modo che il piatto non sia troppo salato. Insomma… avete capito.

Anche se lavorate nel settore della sicurezza, è importante che conosciate il “gusto” di ognuno di questi ingredienti, in modo da proteggervene. Che cosa significa costruire un legame con qualcuno e come può essere sfruttato per ottenere del denaro? Lo vedremo nel Capitolo 5. In quale modo l’influenza, quando viene usata in una

conversazione di richiesta, obbliga qualcuno a comunicarvi la sua password al telefono? Lo vedremo nei Capitoli 6 e 7.

Ognuno di questi ingredienti può aiutarvi a raffinare il vostro "gusto". Una volta che li avrete assaggiati, potrete riconoscerli quando qualcuno tenterà di metterli in atto con voi e così sarete più sicuri. Se percepirete che qualcosa non va, potrete prendere le necessarie azioni difensive.

Avete mai assistito a una gara di cucina con Gordon Ramsay? Quando assaggia un piatto che detesta, identifica il problema specifico: "Questo piatto ha troppo pepe e ci hai messo troppo olio". Un inesperto, al contrario, potrebbe dire: "È troppo piccante e unto". Queste due descrizioni sono davvero uguali? Io penso di no. Il mio obiettivo è quello di aiutarvi a diventare un Gordon Ramsay del mondo dell'ingegneria sociale, ma… forse usando un linguaggio un po' meno volgare.

Detto questo, saltiamo nel primo capitolo "sostanzioso" e parliamo dell'OSINT.

Vedi anche tu quel che vedo io?

> Ricorda che il fallimento è un evento, non una persona.
> - *Zig Ziglar*

OSINT, acronimo di *Open Source Intelligence*, è la linfa vitale dell'ingegneria sociale. L'informazione è il punto di partenza e di supporto di qualsiasi iniziativa. Dal momento che l'OSINT è così importante per gli ingegneri sociali, diventa fondamentale comprendere tutti i diversi modi in cui potete ottenere informazioni sui vostri obiettivi.

Indipendentemente da come ottenete l'OSINT, dovete avere un'idea chiara di quello che state cercando. Potrebbe sembrare una cosa facile, ma le cose non sono come sembrano. Potreste semplicemente dire: "Voglio acquisire tutte le informazioni disponibili sull'obiettivo". Ma ogni tipo di informazione ha un valore differente e l'informazione preziosa può cambiare in base al tipo di attacco che state cercando di sferrare.

Un esempio reale di raccolta di OSINT

Vi propongo un esempio. Secondo il sito `www.worldwidewebsize.com`, sono più di 4,48 *miliardi* i siti web indicizzati. Questo numero non

considera tutti quelli che non sono indicizzati, i siti del *dark web* e del *deep web* e così via. Il traffico mondiale annuale di Internet ha raggiunto gli 1,3 zettabyte, ovvero 1.300.000.000.000.000.000.000 (1300 miliardi di miliardi) di byte. Una fonte ci dice addirittura che Internet può contenere dati fino a 10 yottabyte di dati totali, e 10 yottabyte hanno questo aspetto: 10.000.000.000.000.000.000.000.000 (10 milioni di miliardi di miliardi) di byte.

Curiosità
Lo yottabyte, che stranamente arriva dopo lo zettabyte, prende il nome dal maestro Yoda, il personaggio di *Star Wars*. Esistono categorie di numeri ancora più grandi e denominati in modo ancora più strano, per esempio gli shilentnobyte e i domegemegrottebyte.

Perché è importante comprendere la quantità di traffico che transita su Internet? Bene: per esempio, se state cercando di lanciare un attacco di *spear-phishing*, il vostro obiettivo potrebbe essere quello di cercare fra gli hobby personali, le simpatie/antipatie e altri elementi che l'obiettivo trova importanti. Ma se avete intenzione di condurre un attacco vocale, *vishing*, allora potreste voler trovare dettagli sul tipo di lavoro, sul ruolo svolto dalla persona in questione nella sua organizzazione e sui tipi di risorse interne ed esterne dalle quali tale persona si aspetta di essere chiamata. Se il vostro obiettivo è quello di entrare in un luogo, allora dovete sapere se l'obiettivo deve incontrare delle persone e di quali persone si tratta.

Avete ben 4,48 miliardi di potenziali siti web da analizzare per trovare dati che potrebbero esservi utili. Quindi, prima di iniziare a scavare, è importante che pianifichiate bene il vostro impegno di OSINT.

Per aiutarvi a stabilire alcuni parametri relativi a quello che state cercando, utilizzate le domande elencate nella Tabella 2.1.

Naturalmente, le domande presentate nella tabella scalfiscono solo la superficie del problema. Potete aggiungere altri elementi relativi ai tipi di computer utilizzati, agli orari di lavoro, alle lingue utilizzate, al tipo di protezione antivirus utilizzato e molto altro ancora.

Di seguito riporto un fatto di cronaca del 2017 (potete leggere la storia su https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641). È incentrato sull'ex-direttore dell'FBI James Comey. Un blogger Internet e un ricercatore volevano provare a individuare l'account *social media* di James Comey. Poiché Comey era direttore dell'FBI, il fatto che avesse o meno un account *social media* non era certo di dominio pubblico e poi bisognava individuarlo. È qui che inizia questa storia di OSINT.

Lo schema completo dei passaggi utilizzati dal blogger per la sua ricerca si trova nella Figura 2.1. Datele un'occhiata, poi proseguiremo, un passo alla volta.

In primo luogo, il ricercatore doveva stabilire cosa intendeva scoprire: Comey aveva degli account sui *social media*? E se sì, dove?

La ricerca via Internet si rivelò molto difficile. Nel 2016 un sito web elencava "Le 60 principali piattaforme di *social media*". Dato il numero delle piattaforme – e tutte con regole e metodologie differenti – può essere molto difficile individuare una persona.

Per fortuna, una delle più antiche forme di OSINT si dimostrò favorevole per il ricercatore: l'ascolto. In un'apparizione pubblica, Comey aveva rivelato di avere un account Twitter e Instagram.

Tabella 2.1 Esempi di domande OSINT.

Ambito	Domande da porsi

Aziendale	In quale modo l'azienda utilizza Internet? In quale modo l'azienda utilizza i *social media*? L'azienda attua politiche riguardanti quello che i suoi dipendenti possono mettere su Internet? Quanti venditori ha l'azienda? Quali tipi di venditori utilizza l'azienda? In quale modo l'azienda accetta pagamenti? In quale modo l'azienda emette i suoi pagamenti? L'azienda ha un *call center*? Dove si trovano la sede centrale, i *call center* e le altre filiali? L'azienda consente il BYOD (*bring your own device*)? L'azienda è in un solo luogo o ha più sedi? È disponibile un organigramma?
Individuale	Quali account di *social media* utilizza l'obiettivo? Quali sono i suoi hobby? Dove vive? Quali sono i suoi ristoranti preferiti? Qual è la storia della sua famiglia (malattie, affari e così via)? Qual è il suo livello di istruzione? Che cosa ha studiato? Che ruolo lavorativo ricopre? Lavora da casa, è indipendente, a chi fa rapporto? Ci sono siti che menzionano l'obiettivo (magari tiene discorsi, mette post in forum o fa parte di un club)? È proprietario di una casa? Se sì, in quale zona, con quali i privilegi e così via? Quali sono i nomi dei membri della famiglia (e quali sono le informazioni, già citate, sui membri della famiglia)?

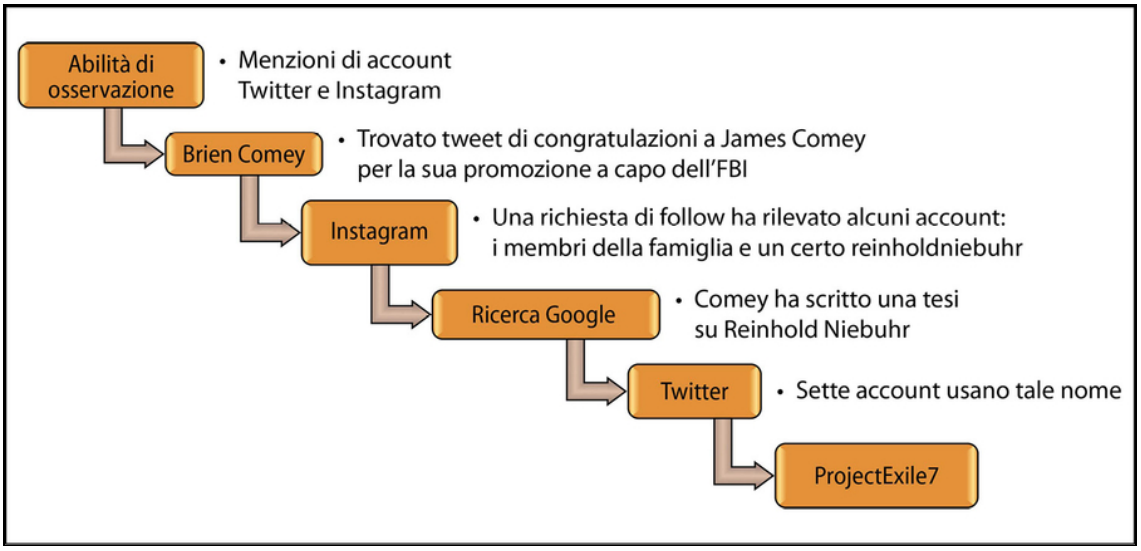


Figura 2.1 Una sorprendente attività di OSINT su un obiettivo protetto.

Questa affermazione aiutò il ricercatore a restringere la ricerca da oltre 60 piattaforme a due. Con due sole piattaforme è più facile predisporre una ricerca.

Non trovando alcun account direttamente collegato a Comey, il ricercatore trovò l'account Twitter di Brien Comey, suo figlio. Legame familiare confermato dal fatto che Brien si era congratulato con il padre per la sua promozione a direttore dell'FBI.

Una delle cose che si possono fare è collegare insieme più account di *social media*. In questo caso, Brien aveva collegato il suo account Instagram al suo account Twitter. Il ricercatore controllò così l'account Instagram, ma Brien ne aveva bloccato l'accesso pubblico, quindi solo coloro ai quali era stato concesso il permesso potevano vedere che cosa pubblicasse.

Il ricercatore decise così di chiedere a Brien di diventare suo follower. Una delle caratteristiche di Instagram è che, mentre si attende che l'utente accetti la richiesta di follow, vengono suggerite le persone della stessa cerchia, nel caso si voglia seguirle. Instagram suggerì un gruppo di utenti che erano membri della famiglia di Brien (escluso però il padre) più l'account reinholdniebuhr.

Se fate qualche ricerca Internet su "Reinhold Niebuhr", scoprirete subito che era un teologo e commentatore politico americano. Morì nel 1971 e questo toglie ogni dubbio sul fatto che possa, oggi, avere un account Instagram. Con ulteriori indagini, il ricercatore apprese che Comey aveva scritto la sua tesi di laurea proprio su Reinhold Niebuhr.

Armato di queste informazioni, il ricercatore cercò su Twitter e vi trovò sette account che utilizzavano quel nome. Fra quei sette, ce n'era uno che usava quel nome pubblicamente con l'handle @ProjectExile7.

Scavando ulteriormente, il ricercatore scoprì che Project Exile era il nome di un programma lanciato da Comey quando era avvocato e viveva a Richmond.

Il ricercatore ha compiuto le sue ricerche senza accedere a nulla di illegale, senza aver hackerato nulla e considerando solo fonti di intelligence open-source mentre vagliava gli indizi.

Questo è un ottimo esempio di mix fra OSINT tecnica e non tecnica, ed è un'ottima lezione per tutti gli ingegneri sociali. Questa è la base del resto del capitolo: quali sono i vari tipi di OSINT e come utilizzarli come ingegneri sociali. L'ho suddiviso in due sezioni principali: prima l'OSINT non tecnica e poi l'OSINT tecnica.

Documentare o non documentare: questo è il problema

Prima di immergerci nei vari tipi di OSINT, vorrei fare una piccola considerazione sulla documentazione.

La domanda non è se è il caso o meno di documentare le attività. La vera domanda è che cosa usare per documentare e quanto documentare.

Pensate a quello che ho detto all'inizio del capitolo: cercando in 10 yottabyte di dati, troverete *molte* informazioni sui vostri obiettivi. Per quanto siate intelligenti, a meno che abbiate la fortuna di disporre di una memoria fotografica, non potrete ricordare ogni dettaglio. E anche chi è dotato di memoria fotografica non potrà completare un report professionale contando esclusivamente sulla memoria.

Ora, non posso dirvi esattamente che cosa e come dovreste documentare le vostre attività, perché subentrano troppe variabili. Per esempio, quando ero agli inizi ed ero un pochino meno esperto di tutto il lavoro necessario, usavo un'applicazione avanzata per note, che mi permetteva di creare una nuova cartella e una nota per ogni cliente. Quindi suddividevo quella nota in diverse sezioni: personale, lavoro, famiglia, social media e così via. Quando trovavo un'informazione di OSINT, la documentavo nella sezione appropriata e ciò mi permetteva di trovare i dati nella stesura del rapporto. Usavo piccoli trucchi, come specifici colori per i fattori che sfruttavo per gli attacchi. Usavo un colore per le informazioni non critiche e un altro per quelle critiche.

Poi il mio team iniziò a crescere: avevo più persone che lavoravano su un progetto, e ciò mi fece capire che lo scambio di note dall'uno all'altro non era la migliore soluzione per tutti. Dovetti trovare una soluzione che consentisse ai membri del team di condividere le note.

All'inizio, considerai cose come Google Drive. Presi in considerazione le applicazioni per note e altri strumenti basati sul cloud.

Queste soluzioni presentarono alcuni problemi.

- Mi era stato affidato il compito di risalire ai numeri di previdenza sociale, ai dati bancari e ad altri dettagli privati e personali sulla vita delle persone.

Che cosa succede se la soluzione che uso viene violata? (Accadde nel 2013, quando Evernote venne violato e dovettero essere cambiate oltre 50 milioni di password.)

- Non potevo controllare l'accesso a queste soluzioni né come venivano gestiti i dati raccolti.
- La sola parola "cloud" faceva rabbrividire molti clienti inducendoli a rispondere automaticamente: "No!".

Questo mi indusse a predisporre i miei server. Ottenemmo spazio in un servizio di server-hosting verificato e protetto. Creammo il nostro server VPN sicuro e installammo il software che avevamo scelto su un server che era situato dietro un firewall, dietro un router e nella nostra VPN.
Ciò significa che controllavo il modo in cui i dati venivano archiviati, gestiti, sottoposti a backup, trasmessi e protetti. Questa soluzione mi ha permesso di dormire tranquillamente, perché ero abbastanza fiducioso del modo in cui sarebbero stati gestiti i dati riservati dei nostri clienti.
Forse avete una soluzione diversa. L'importante è che prendiate sul serio il modo in cui archiviare, gestire, sottoporre a backup, trasmettere e proteggere tutti i dati che raccogliete sui vostri clienti.

OSINT non tecnica

Considero non tecnica un'OSINT che non implica un'interazione *diretta* tra l'ingegnere sociale e un computer. Potreste osservare alle spalle un obiettivo mentre usa il computer, ma *voi* (l'ingegnere sociale) non usate il computer. Si tratta di informazioni raccolte utilizzando mezzi non tecnici. Ci sono molti metodi specifici che potrei elencare, ma posso definirli genericamente tutti come *abilità di osservazione* e nel prossimo paragrafo seguente vi indico alcuni esempi.

Abilità di osservazione

Le abilità di osservazione potrebbero sembrare ovvie e facili da usare, ma la capacità di impiegarle con successo è una competenza non comune – soprattutto nell'era del fiorire di media digitali. Se non altro, le tattiche di marketing di oggi ci hanno abituato a non prestare

attenzione ai dettagli. Uno studio condotto nel 2015 da Emily Drago della Elon University (intitolato *The Effect of Technology on Face-to-Face Communication*) sottolinea il fatto che la qualità di comunicazioni faccia a faccia è drasticamente calata a causa delle tecnologie. Il 62% degli individui osservati nel corso dello studio utilizzava un dispositivo mobile mentre conversava con altri, pur sapendo che ciò avrebbe pregiudicato la qualità di tale comunicazione.

NOTA

Potete leggere il testo integrale di *The Effect of Technology on Face-to-Face Communication* su `www.elon.edu/docs/e-web/academics/communications/research/vol6no1/02DragoEJSpring15.pdf`.

Viviamo in una società che trasmette gran parte dei messaggi con 280 caratteri ed emoji, che comunica attraverso meme o post sui *social media*. I progressi resi possibili da queste cose sono sorprendenti, ma essi hanno anche creato una situazione in cui tutti siamo meno attenti a coloro che stanno comunicando. è anche la ragione per cui le abilità di osservazione sono in cima al mio elenco relativo all'OSINT non tecnica.

Potreste porvi alcune domande.

- Che cosa comprende il termine *abilità di osservazione*?
- Che cosa potete fare per insegnare a voi stessi queste abilità?
- Che cosa dovreste aspettarvi di raccogliere?

Consideriamo ciascuna di queste domande per vedere che cosa potete osservare e imparare (avete visto quello che ho fatto io?).

Che cosa comprendono le abilità di osservazione?

I seguenti scenari vi forniscono alcuni esempi di come possano essere sfruttate, nel mondo reale, le abilità di osservazione.

Scenario 1

Il vostro compito è quello di ottenere l'accesso alla sala di smistamento della corrispondenza di una grande struttura sanitaria. Dovete farlo in pieno giorno. Non potete forzare serrature, scavalcare muri né sfondare finestre. State mettendo alla prova il personale della reception e di sicurezza, per vedere se vi permetterà di accedere all'area protetta, quindi dovrete necessariamente attraversare la parte della struttura sanitaria in cui lavorano i membri del personale.

Di seguito sono elencate solo alcune delle doti che dovreste avere nel vostro arsenale delle abilità di osservazione.

- *Abbigliamento*: questo importante fattore è semplice, ma troppo spesso trascurato. Nel Capitolo 1 dico che l'obiettivo dell'ingegnere sociale è quello di farvi decidere senza riflettere. Se vi state introducendo in un luogo in cui ognuno si veste in modo casual e indossate un completo elegante, vi farete notare. È vero anche il contrario, quindi scoprite come si vestono i dipendenti, in modo da "mimetizzarvi".
- *Ingressi e uscite*: prima di entrare nell'edificio, cercate di capire dove sono ubicate le uscite. C'è una porta dove sono soliti uscire i fumatori? Un ingresso è più sorvegliato di un altro? Ci sono cambi di turno che lasciano un certo punto senza controllo o con un controllo ridotto?
- *Requisiti per l'ingresso*: che cosa è necessario per accedere alla struttura/all'area? Notate dei dipendenti col badge? Quale tipo di badge? Dove lo portano? Devono anche digitare un codice? I visitatori devono essere accompagnati? Anche i visitatori ricevono un badge? Ci sono tornelli, cancelli girevoli, una guardiola o altri dispositivi di sicurezza all'ingresso?
- *Sicurezza perimetrale*: controllate quello che succede all'esterno dell'edificio. Ci sono telecamere di sicurezza? Ci sono guardie? I

cassonetti vengono chiusi con un lucchetto? Ci sono allarmi o sensori di movimento?

- *Personale di sicurezza*: sono occupati a guardare lo smartphone o il computer o sono sempre in allerta e attenti? Sembrano terribilmente annoiati o attivi?
- *Aspetto dell'ingresso*: esistono tastierini o dispositivi di sicurezza configurati in modo che sia possibile sottrarre le password alle spalle? In altre parole, ci si può avvicinare abbastanza per sbirciare sopra la spalla di qualcuno mentre digita la password?

Naturalmente, ci possono essere molte più cose da osservare, ma queste sono solo alcune delle basi.

Per aiutarvi a capire il motivo per cui questi criteri sono così importanti, vi presento un racconto vero che riguarda l'abbigliamento, l'ingresso e l'uscita, i requisiti per l'ingresso e la sicurezza perimetrale. A me e a Michele Fincher (che è l'editor tecnico di questo libro) era stato affidato il compito che ho descritto all'inizio di questo paragrafo. Abbiamo dovuto svolgere una discreta quantità di OSINT tecnica, di cui parlerò più avanti in questo capitolo, ma il lavoro prevedeva anche una discreta quantità di OSINT non tecnica, che ci ha condotti al successo.

Decidemmo di utilizzare come pretesto la chiamata a una società di controllo dei parassiti, che doveva intervenire per debellare un'infestazione di ragni. Chiamammo la nostra azienda Big Blue Pest Control e indossammo completi in perfetto stile Big Blue con tanto di bombolette spray di "insetticida" blu per neutralizzare tutti i ragni incontrati durante la perlustrazione. In realtà l'insetticida era solo Gatorade Cool Blue in un flacone pressurizzato.

Curiosità

La Gatorade blu travestita da insetticida è anche un ottimo modo per portarsi dietro una bevanda rinfrescante, che potete utilizzare per placare la sete quando

vi sentite nervosi durante un'infiltrazione in un edificio e se sudate copiosamente. Tuttavia, se sorseggiate il vostro "insetticida" in ascensore e si aprono le porte, qualcuno potrebbe guardarvi un po' male.

Iniziammo passeggiando lungo il perimetro e prendendo nota degli ingressi, delle uscite e dell'ubicazione delle telecamere, dei luoghi di ritrovo per i fumatori e degli ingressi che sembravano più e meno affollati. Prendemmo anche nota del fatto che i dipendenti che entravano e uscivano avevano dei distintivi e di come erano vestiti. Scegliemmo quindi il nostro punto d'ingresso iniziale e procedemmo lentamente verso quella porta. Camminando lentamente avevamo modo di osservare il modo in cui le persone venivano lasciate entrare.

Notammo due guardie di sicurezza che sorvegliavano le persone mentre premevano i loro badge contro un apparecchio metallico e che concedeva loro l'accesso. C'era anche una guardiola sulla destra e qualcuno che gestiva un registro degli accessi.

Decidemmo di provare a superare le guardie e seguire gli altri. Questo stratagemma non funzionò affatto. Una guardia di sicurezza ci fermò e ci chiese che cosa stessimo facendo e perché eravamo lì. Posai lo sguardo sul suo badge, lessi il suo nome e poi iniziai a dire: "Bene, Andrew, ci è stato chiesto di venire a fare un preventivo per un'irrorazione d'emergenza a causa di un'infestazione di ragni…". La guardia mi interruppe a metà frase dicendo: "Ok, registrati alla reception".

Pensavo di essere ormai entrato, ma mentre ci avvicinavamo alla reception, l'uomo ci chiese i nostri nomi. Demmo generalità false e lui, dopo aver controllato l'elenco, non trovando i nostri nomi, disse: "Mi dispiace, non siete sul nostro elenco dei visitatori di oggi. Non potete entrare senza autorizzazione".

Cercammo di spiegare, di influenzare e perfino usare pressioni e richieste d'aiuto. *Nada*. Zero. Uscimmo dall'ingresso principale, e mentre passeggiavamo discutendo di cosa avremmo fatto poi,

notammo alcuni fumatori all'esterno, mentre si concedevano una pausa. Dissi a Michele di seguirmi e ci incamminammo verso i fumatori, comportandoci come se appartenessimo al gruppo e stessimo ispezionando l'esterno dell'edificio. Feci finta di prendere appunti.

Ancora una volta procedevamo con passo lento, finché non vedemmo alcune persone avvicinarsi alla porta, e così ci infilammo dietro di loro. Dentro l'edificio, seguimmo questa massa di persone e notai subito che ci stavamo dirigendo verso la facciata, dove si trovavano le guardie di sicurezza che ci avevano appena respinto. Vidi un ascensore alla mia destra, ma non c'erano pulsanti. "Maledizione", pensai tra me e me, "un ascensore controllato dalla sicurezza". Proprio mentre formulavo questo pensiero, la porta dell'ascensore si aprì e vi entrai subito, sperando che Michele mi osservasse e seguisse il mio esempio.

Fortunatamente per me, Michele è molto brava in questo tipo di cose e non si dà mai per vinta né mostra segni di stress. C'era un gruppo di persone nell'ascensore e Michele prontamente annunciò, in modo che tutti potesse sentire: "Capo, possiamo finire presto questo lavoro? Sto morendo di fame e mi hai detto che appena finito potevo andare a mangiare un boccone".

Ricevetti uno sguardo di disapprovazione da una donna, che disse: "Fai mangiare quella povera donna". Risposi: "Sono d'accordo, ma prima dobbiamo ispezionare un altro piano. Prima ci sbrighiamo e prima potrà mangiare".

La donna sospirò e disse: "Bene, allora vi porto dove dovete andare…", e mi sono inserito nella frase "nella sala di smistamento della corrispondenza". La donna estrasse il distintivo, lo fece scorrere nell'apparecchio dell'ascensore, digitò un codice e disse: "Vi ci porto".

Fantastico! Fortunatamente, grazie alle grandi abilità di osservazione di Michele e alle mie rapide reazioni non eravamo stati

catturati e avevamo perfino trovato una gentile signora che ci accompagnava proprio dove volevamo (e Michele stava fingendo solo parzialmente, perché in realtà ha *sempre* fame).

Sul piano della sala di smistamento della corrispondenza, uscimmo dall'ascensore solo per scoprire che la porta era chiusa. C'era un campanello con un'etichetta: "Suonare per assistenza". Suonammo e aspettammo.

Arrivò alla porta una donna, che disse: "Come posso aiutarvi?". Sfoggiammo il nostro pretesto dell'ispezione per la disinfestazione e la donna rispose: "Bene, dovrò chiamare il servizio di sicurezza per l'approvazione".

La nostra storia sarebbe saltata se avesse chiamato la sicurezza, così dissi: "Non c'è problema, è stato proprio Andrew a mandarci qui".

Rispose: "Oh, vi ha mandato Andrew? Allora entrate". Ci lasciò nella sala dicendo: "Ma non toccate la posta". E così abbiamo rovistato tra soffitti, pannelli, cavi di rete e una quantità infinita di posta.

Come potete vedere in tutta questa storia, tutto è potuto accadere solo perché abbiamo fatto rapide osservazioni e messo da parte le informazioni utili per poterle riutilizzare in seguito (e questo era solo l'inizio).

Non potevo sapere di aver bisogno del nome di Andrew, e Michele non poteva sapere che avremmo incontrato una donna simpatica in ascensore, e nessuno di noi sapeva che avremmo incontrato un gruppo di fumatori disattenti ai quali non importava nulla che ci fossimo aggregati a loro. Ma queste osservazioni ci hanno permesso di utilizzare ognuna di queste opportunità per avere successo nell'operazione.

Scenario 2

Vi viene chiesto di sferrare un attacco di *spear-phishing* contro un grande avvocato che lavora per un'importante società americana. Vi è

permesso l’uso di qualsiasi informazione possiate trovare su di lei.

Questa storia rivelerà di più quando arriverò alla sezione sull’OSINT tecnica, ma per trasmettervi una lezione molto preziosa, lasciate che vi dica come in questo caso abbiamo fallito miseramente.

La nostra OSINT ci fece scoprire che l’avvocato aveva alcune pratiche in Massachusetts. Scoprimmo un recente aggiornamento delle norme fiscali in Massachusetts che avrebbe potuto attirare il suo interesse ed essere molto efficace nel convincerla a fare clic su un link o ad aprire un allegato dannoso.

Iniziai creando un’e-mail sulle nuove norme fiscali approvate dallo Stato del Massachusetts e pianificai ogni aspetto di questo *spear-phishing*. L’e-mail era scritta con un tono professionale, non conteneva minacce, includeva il payload che volevamo, aveva una scadenza realistica per la lettura e la risposta e forniva sufficienti dettagli per assicurarsi che lei potesse fare clic per saperne di più.

Nel giro di pochi minuti dall’invio dell’e-mail, siamo stati individuati e denunciati e l’attività si è bruscamente interrotta. Avete scoperto l’errore nel paragrafo precedente? Vi darò giusto qualche secondo per tornare a rileggere le frasi prima di svelarvelo.

Tempo scaduto!

Negli Stati Uniti, il Massachusetts non è esattamente uno “Stato” ma un “Commonwealth”. L’avvocato, la cui professione lo spinge a fare attenzione ai dettagli, ricevendo un’e-mail sulle normative fiscali dello *Stato* del Massachusetts si è detta: “Ehi, ma questi dovrebbero sapere che il Massachusetts non è uno Stato ma un Commonwealth!”. Ciò l’ha indotta a controllare l’indirizzo del mittente e l’URL del link e a diventare tanto sospettosa da segnalare la mail. E la nostra copertura è saltata.

Non abbiamo considerato i piccoli dettagli necessari per costruire questa storia e abbiamo pagato questa mancanza di osservazione.

Qual è la morale di questo scenario? Che dovete osservare tutto quello che potete. Pensate come un esperto di ingegneria sociale. Cercate di capire che cosa si aspettano di trovare e offritelo. Altrimenti, i piccoli dettagli potranno tradirvi.

Che cosa potete fare per apprendere queste abilità?

Questo è un argomento difficile da trattare in un breve paragrafo di un libro. Ogni persona è un mix di abilità naturali e abilità apprese, il che può rendere l'apprendimento di queste abilità molto facile o estremamente difficile. Dal momento che non vi conosco personalmente, tutto quello che posso fare qui è dirvi quello che ho fatto io per cercare di migliorare le mie competenze.

Facevo un gioco di hacking chiamato *Capture the Flag*. Se stavo entrando in un edificio, per esempio uno studio medico, dicevo a me stesso: "Lo scopo è quello di ricordare le prime due persone che incontro, di che colore è la camicia che indossano, che rivista stanno leggendo o che cosa stanno facendo".

È il caso di definire alcuni limiti.

- Non potevano essere le persone di servizio, dietro il bancone.
- Dovevo proseguire nel mio compito e non potevo fermarmi o deviare.
- Non potevo scrivere niente.

Poi entravo nell'edificio, osservavo quello che vedevo e facevo del mio meglio per memorizzarlo, finché non lasciavo l'edificio. Qualcosa di simile a quanto segue.

- Donna anziana seduta sulla sinistra; camicia blu, legge la rivista *Donna moderna*.
- Bambino, maschio; maglietta a righe, sta giocando con dei blocchi sul pavimento.

Prendevo nota a mente di ciascuna di queste cose e facevo del mio meglio per ricordarle. Impiegavo piccoli trucchi per la memoria, come ripetermi le cose un paio di volte per provare a memorizzarle.

Quando sentivo di poter prendere appunti mentali in questo modo senza troppa fatica, aggiungevo altri livelli di complessità. Alla fine, il mio elenco aveva il seguente aspetto.

- Sesso di *X* numero di persone.
- Loro abbigliamento.
- Quali attività svolgevano le persone quando le ho viste per la prima volta.
- Profilo di comunicazione percepito (per maggiori informazioni fate riferimento al Capitolo 3).
- Individuare il linguaggio del corpo.

Poi provai a costruirmi una storia in testa: perché erano nel luogo in cui mi trovavo e usavo i dettagli della storia come ausilio della memoria.

Onestamente, la tecnica funzionò così bene – nonostante la mia pessima memoria – che posso ancora ricordare un ufficio in cui sono entrato tre o quattro anni fa, dove ho visto due donne in gonna nera e maglietta bianca che leggevano qualcosa su un iPad. La donna a sinistra non sembrava gradire la donna a destra, ma la sopportava o significava qualcosa per lei. L'avevo dedotto dal fatto che la donna a sinistra si era seduta il più possibile distante dalla donna a destra.

C'era un uomo dietro un bancone con una divisa della sicurezza: abito nero, camicia bianca, cravatta nera. Aveva al polso destro un orologio d'oro e questo stava a indicare che era mancino. Aveva i capelli lisci e una barba ben curata. Stava scrivendo su un blocco note con una penna. Stava osservando me e tutto l'ingresso.

Di fronte al bancone c'era un giovane uomo seduto in attesa. Stava leggendo un giornale, ma sembrava che in realtà fingesse di leggerlo.

Guardava nel vuoto e i bordi del giornale tremavano. Mi sono inventato la storia che fosse lì per un colloquio e che fosse nervoso, ma cercava di stare calmo e di distrarsi con il giornale.

È quasi come se potessi vedere quell'ingresso nella mia mente. Queste piccole osservazioni aiutano molto nel raggiungere gli obiettivi di ingegneria sociale. Il mio suggerimento è quello di studiare i propri punti deboli e poi iniziare poco a poco a costruire competenze. È importante individuare con cura la competenza sulla quale fare pratica. Troppo spesso vedo persone che vogliono ottenere tutto, subito, al 100%, ma ci vuole tempo.

I fallimenti possono insegnarci molto di più dei successi se glielo permettiamo – ecco perché ho bisogno di parlare di aspettative.

Che cosa dovreste aspettarvi di raccogliere?

Nel libro *Unmasking the Social Engineer*, che ho scritto con Paul Ekman, mi sono concentrato unicamente sulla comunicazione non verbale: il linguaggio del corpo e le espressioni facciali. Quando iniziai a imparare innanzitutto a notare e poi a decifrare queste espressioni, mi sentivo come una sorta di supereroe, in grado di leggere la mente. Potevo guardare un volto e individuare le emozioni che quella persona stava cercando di celare e poi univo questa osservazione al linguaggio del corpo e ad altre sue azioni per predeterminare la reazione a determinate domande o situazioni. La cosa strana è che scoprii che le mie previsioni erano corrette più del 50% delle volte. Qui inizia il problema. Diciamo che avevo ragione il 75% delle volte. Ciò significa che sbagliavo nel 25% dei casi. Ma questo influiva sulla mia capacità di percezione e così credevo di poter vedere di più, capire di più e applicare l'ingegneria sociale più di quanto in realtà potessi.

Una delle lezioni più umilianti venne proprio dal mio lavoro con Ekman, che mi corresse più di una volta. Mi disse: "Chris, solo perché

puoi vedere il *cosa*, questo non significa che tu sappia il *perché*".

Prima di parlare delle aspettative, è importante che facciate vostro questo concetto: solo perché potete vedere il cosa, questo non significa automaticamente che conosciate il perché. Come stabilire una connessione tra cosa e perché? Ci sono alcuni modi: domandando, acquisendo maggiori informazioni e compiendo maggiori osservazioni.

Ecco un esempio: stavo insegnando in una classe e stavo raccontando di una mia esperienza di ingegneria sociale. Improvvisamente uno studente ha assunto un'espressione arrabbiata. Il suo linguaggio del corpo raccontava di un passaggio dall'apertura alla chiusura. Le braccia conserte, si è appoggiato allo schienale con le gambe che sporgevano dal banco. Ho percepito che non credeva a quello che stavo dicendo e iniziai a dargli più attenzione. Questo non sembrò sortire alcun effetto su di lui e così si ritirò. Dopo alcuni minuti, si scusò e lasciò la classe.

Ero sbalordito. Avevo fatto tutto per bene. Perché era arrabbiato con me?

Poco dopo, ci prendemmo una pausa. Stavo andando verso i bagni, riflettendo sull'accaduto e su come porvi rimedio. Lo studente mi si avvicinò e mi disse: "Sono veramente dispiaciuto di aver dovuto lasciare l'aula. Il mio capo mi ha mandato un messaggio a metà lezione dicendomi che avevamo un'emergenza al lavoro. Ho cercato di dirgli che non potevo aiutarlo perché ero a lezione, ma lui mi ha ordinato di uscire per partecipare a una stupida *conference call*. Come posso recuperare la lezione che ho perso?".

Sono scoppiato a ridere e dovetti spiegarmi rapidamente, dicendogli di aver mal interpretato quello che avevo visto. Mi sembrava di sentire Ekman nella mia testa: "Chris, che cosa ti ho detto?". Casualmente, quella è stata una grande lezione per me.

Lo stesso vale per l'OSINT e l'osservazione. Non date per scontato che le cose che sto per mostrarvi siano il risultato della "stupidità degli esseri umani". Preferisco pensare che, semplicemente, la gente ignori i potenziali pericoli, piuttosto che pensarla palesemente stupida.

Date un'occhiata all'immagine rappresentata nella Figura 2.2 e prendete nota mentalmente di quello che avete osservato.



Figura 2.2 Che cosa vedete?

Ragionando come ingegneri sociali, che cosa vedete in questa immagine che potrebbe aiutarvi a definire il profilo del proprietario di questa automobile? La Figura 2.3 è una versione ingrandita, che potrebbe aiutarvi.



Figura 2.3 È più facile da vedere?

Sul lato destro c'è l'adesivo della campagna per la prevenzione del cancro al seno. A sinistra un adesivo di supporto alla rete Kids Wish. Poi c'è un adesivo che dice "10-20-Life". Non avevo alcuna idea del suo significato, quindi ho compiuto una rapida ricerca su Internet e ho scoperto che si tratta di un adesivo che invoca pene più severe per coloro che commettono crimini con armi da fuoco.

Che cosa vi dicono questi adesivi di questa persona? Che sostiene enti di beneficenza e quali sono i suoi valori. Forse il proprietario o un membro della sua famiglia ha sofferto di cancro o di una malattia infantile. Inoltre, è fortemente contraria alle leggi e ai crimini sull'uso di armi da fuoco. Forse ne è stata vittima o forse ha conosciuto una vittima.

Armati di queste informazioni parziali, pensate di poter avviare una conversazione di convincimento?

State attenti! Troppe volte ho avuto allievi che dicevano: "Parlerei delle leggi sulle armi e del perché sono sbagliate" o qualcosa del genere. Ma pensate a quanto sia difficile cambiare la propria idea e poi sostenerla in una conversazione. Questa persona non sarà diversa da voi. Mettete insieme il vostro obiettivo – spingere l'obiettivo a *non* riflettere – e ricordate che volete parlare dei loro interessi, non dei vostri. Spiego meglio questo concetto nel Capitolo 7 quando vi parlerò di come convincere.

Ora date un’occhiata alla Figura 2.4.

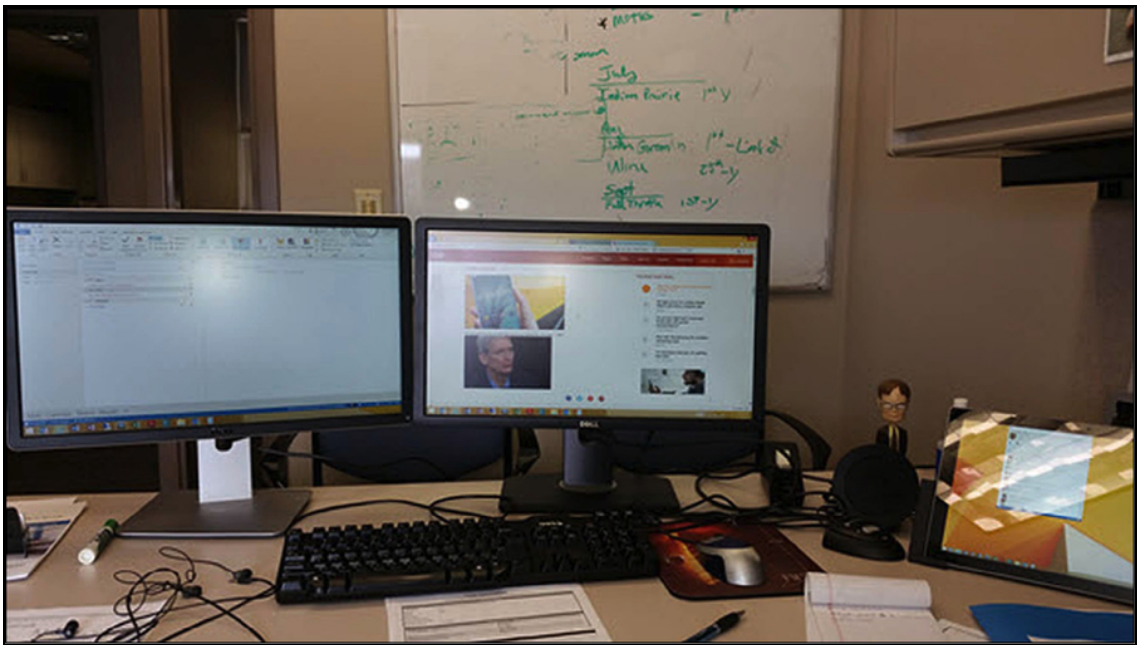


Figura 2.4 Quali informazioni potete trarre da questa immagine?

Che cosa notate? Che cosa potreste osservare come ingegneri sociali? Osservate i piccoli dettagli di questa semplice immagine.

- Potete vedere il tipo di ambiente di lavoro.
- Potete vedere il sistema operativo che usa questa persona.
- Potete vedere il suo tipo di tablet.
- Potete vedere che le piace una certa sitcom.
- Riuscite a capire quale browser usa e quale client di posta elettronica?
- Notate un segno che potrebbe rivelare altri dettagli sulla persona?
- Quali altri dettagli riuscite a individuare?

Questo è solo un rapido elenco, ma potrebbe esserci molto di più. Sulla base di questo, riuscireste a sviluppare un profilo sufficiente a elaborare una o due e-mail di *phishing* che potrebbero provocare con successo una risposta emotiva?

A volte, tuttavia, un'immagine o anche un'interazione con la persona non sono sufficienti. È qui che interviene l'OSINT tecnica a colmare questa lacuna.

OSINT tecnica

Prima di mettervi a scrivere una recensione terribile, dicendo al mondo quanto questo libro faccia schifo perché questo capitolo non conteneva un elenco completo di tutti gli strumenti noti per l'OSINT, lasciatemi dire una cosa.

Questo capitolo NON contiene un elenco completo di ogni strumento, processo e metodo di raccolta di OSINT con mezzi tecnici.

Ecco cosa posso dirvi: questo capitolo tratta gli strumenti e le tecniche che uso quotidianamente per la mia attività. Ci sono menti davvero fantastiche nel monto dell'OSINT che vi aiuteranno a scavare in profondità. Ecco due persone che ho avuto la fortuna di conoscere:

- *Nick Furneaux*: sono volato in Inghilterra per partecipare a un corso di quattro giorni di Nick ed è stato illuminante. È davvero sorprendente scoprire quello che si può fare con le API e capire come funzionano le applicazioni per *social media*. Il sito web di Nick è `www.csitech.co.uk`.
- *Michael Bazzell*: Michael è l'uomo da chiamare quando si tratta di scomparire dal Web, ma ha anche sviluppato una serie impressionante di strumenti per i professionisti dell'OSINT, che possono aiutarvi a scavare nei siti, nei *social media* e nei motori di ricerca. Trovate il suo sito web su `inteltechniques.com`.

Questi bravi ragazzi sono entrambi miei amici e ho seguito personalmente i loro corsi di formazione, i loro consigli e il loro aiuto. Posso dire con tutto il cuore che sono maestri dell'arte dell'OSINT

(sono senza vergogna: entrambi sono stati ospiti del *The Social-Engineer Podcast*; cercate *OSINT* per trovare gli episodi in questione).

Mi focalizzerò sul mondo OSINT e in particolare sui suoi usi pratici quotidiani per il lavoro che svolgo. Il tutto può essere suddiviso in quattro semplici argomenti: *social media*, motori di ricerca, Google e altri strumenti. Tratterò ciascuno di questi argomenti per darvi un'idea di come li utilizzo così che possiate usare tale conoscenza come base per approfondire l'argomento.

Social media

Nessun capitolo sull'OSINT sarebbe completo senza almeno una breve menzione del tema dei *social media*. Quello che mi fa specie è che ricordo un tempo in cui il solo leggere il diario di una sorella avrebbe comportato una sana dose di botte. Oggi i diari personali non solo sono online, ma la gente si offende se non li leggete, commentate e "mipiaciate".

I *social media* sono ormai parte della nostra esistenza quotidiana e sono qui per restare.

Ecco alcuni dati che stabiliscono un po' l'ordine di grandezza del fenomeno, secondo *We Are Social* (`https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates`). A gennaio 2019:

- la popolazione mondiale era di 7.676 miliardi di persone;
- gli utenti Internet erano un totale di 4.388 miliardi;
- c'erano 3.484 miliardi di utenti di *social media* attivi;
- c'erano 5.112 miliardi di utenti mobili;
- ci sono stati 3.256 miliardi di utenti di *social media* mobili attivi.

Come ingegnere sociale, questa è un'informazione importante. Prendiamo in considerazione alcune delle piattaforme più famose di

social media:

- *LinkedIn* Con oltre 590 milioni di utenti, LinkedIn comunica di voi le seguenti informazioni.
  - La vostra storia lavorativa.
  - Dove avete conseguito i vostri titoli di studio.
  - Quale istituto superiore avete frequentato.
  - Club e risultati accademici in cui siete coinvolti.
  - Persone che possono testimoniare le vostre capacità.
- *Facebook* Con i suoi oltre 2,23 miliardi di utenti, Facebook racconta a tutti le seguenti informazioni.
  - Qual è la vostra musica preferita.
  - Quali sono i film che preferite.
  - A quali associazioni appartenete.
  - Quali sono i vostri amici.
  - Come è composta la vostra famiglia.
  - Dove e quando andate in vacanza.
  - Quali cibi preferite.
  - I luoghi in cui avete vissuto.
  - E molto, molto altro ancora.
- *Twitter* Con i suoi 326 milioni di utenti, Twitter dice di voi le seguenti cose.
  - Che cosa state facendo adesso.
  - Quali sono le vostre abitudini alimentari.
  - Dove vi trovate esattamente.
  - Qual è il vostro stato emotivo (nei limiti di 280 caratteri).

Potrei andare avanti, ma sono sicuro che vi siete fatti un’idea. Solo questi tre *social media* possono fornirvi moltissime informazioni sui vostri obiettivi. Oserei dire che, a partire da qui, potete crearvi un profilo abbastanza completo del vostro obiettivo.

Curiosità

Nell'Episodio 87 di *The Social-Engineer Podcast,* abbiamo parlato con James Pennebaker. Aveva realizzato uno strumento (`www.analyzewords.com`) in grado di analizzare l'account Twitter di una persona in base alla lingua utilizzata. L'abbiamo applicato all'account Twitter di Michele (`@SultryAsian`) ed è stata valutata "spacey Valley Girl with an upbeat, in-the-moment style", ovvero qualcosa come "provinciale ingenua con uno stile ottimista e attuale". Onestamente, sono scoppiato a ridere quando l'ho letto, perché Michele, nella vita reale, è tutta il contrario, ma quello era esattamente il modo in cui voleva essere rappresentata sui social media.

La valutazione di una persona sulla base dei *social media* non deve essere confusa con lo sviluppo di un vero profilo psicologico. Come dice l'aneddoto divertente, ci sono persone che comunicano online in un modo e di persona in un altro. Nonostante questo, per un ingegnere sociale i *social media* sono comunque preziosi, perché molti attacchi si basano proprio sulla personalità "online": imparare a comunicare con quell'aspetto dell'obiettivo può aiutare ad avere successo.

Con centinaia di piattaforme di *social media* e miliardi di utilizzatori, i *social media* rappresentano una vera miniera di dati per gli ingegneri sociali. Uno dei modi migliori per strappare informazioni dalle piattaforme di *social media* prevede l'impiego dei motori di ricerca, argomento del prossimo paragrafo.

I motori di ricerca

Internet è in continua evoluzione, e offre sempre nuovi e migliori metodi per raccogliere informazioni nei suoi yottabyte di dati. Questi continui cambiamenti possono essere comodi per molte persone, ma possono anche diventare un problema per gli ingegneri sociali, perché un motore di ricerca che funziona oggi potrebbe non funzionare domani.

Ricordo quando uscì per la prima volta Spokeo. Lo usavo quasi quotidianamente ed è stato una fonte straordinaria di informazioni.

Aumentando la sua popolarità, è aumentato anche il numero di annunci pubblicitari. Poi cominciò a fornire le informazioni a pagamento, e tali informazioni erano sempre meno affidabili.

Ora, non sto dicendo che Spokeo non sia utile, ma in quanto ingegnere sociale professionale, il mio tempo è denaro e se devo sempre verificare su un'altra fonte ogni fatto che scopro, ciò mi può costare un lavoro.

Nel mio primo libro, e poi in molti altri libri successivi, ho scoperto che includere lunghi elenchi di strumenti è sostanzialmente inutile per il lettore. Capita spesso che:

- il giorno stesso in cui il libro viene pubblicato, tali strumenti sono obsoleti e quindi i suggerimenti per il loro uso diventano inutili per i lettori;
- nascono nuovi strumenti, migliori;
- tutte le combinazioni possibili dei primi due punti.

Invece di darvi un elenco di siti web e strumenti, voglio guidarvi nell'esecuzione di un'OSINT su un obiettivo. Certamente menzionerò siti web e strumenti da usare, ma il focus sarà più sul modo in cui pensare e procedere come ingegneri sociali.

Il nostro "obiettivo" è il mio buon amico Nick Furneaux (e spero resti tale anche dopo la pubblicazione di questo libro). Nota bene: non c'è nessuna cattiva intenzione nei confronti di Nick. Lo sto semplicemente utilizzando per dimostrare che anche per una persona molto consapevole, molto scrupolosa e molto attenta alla sicurezza, Internet conserva segreti per coloro che sanno dove cercare.

"d0xing the Furneaux"

Che cosa significa *d0x*? È un termine da hacker che significa "elaborare un documento su un obiettivo, contenente dettagli circa la

vita personale dell'obiettivo". Questi dettagli vengono spesso utilizzati per attaccare ulteriormente l'obiettivo, per umiliarlo o per perpetrare altri crimini.

In questo caso non abbiamo nessuno di questi scopi. Voglio solo mostrarvi la potenza dell'OSINT e come possa essere utilizzata. Spesso, inizio con le porte di `pipl.com`.

Pipl (che si pronuncia *people*) è un sito che descrivo un po' come il "figlio" delle Pagine bianche e dei *social media*. La cosa fantastica di questo sito è che potete effettuare una ricerca per nome, per nome-utente, per soprannome e per qualsiasi altro dettaglio che possiate conoscere sul vostro obiettivo.

Basta accedere al Web per scoprire subito che l'account Twitter di Nick è `nickfx`. Vediamo che cosa riusciamo a trovare utilizzando `pipl.com` con quel soprannome. Date un'occhiata alla Figura 2.5.

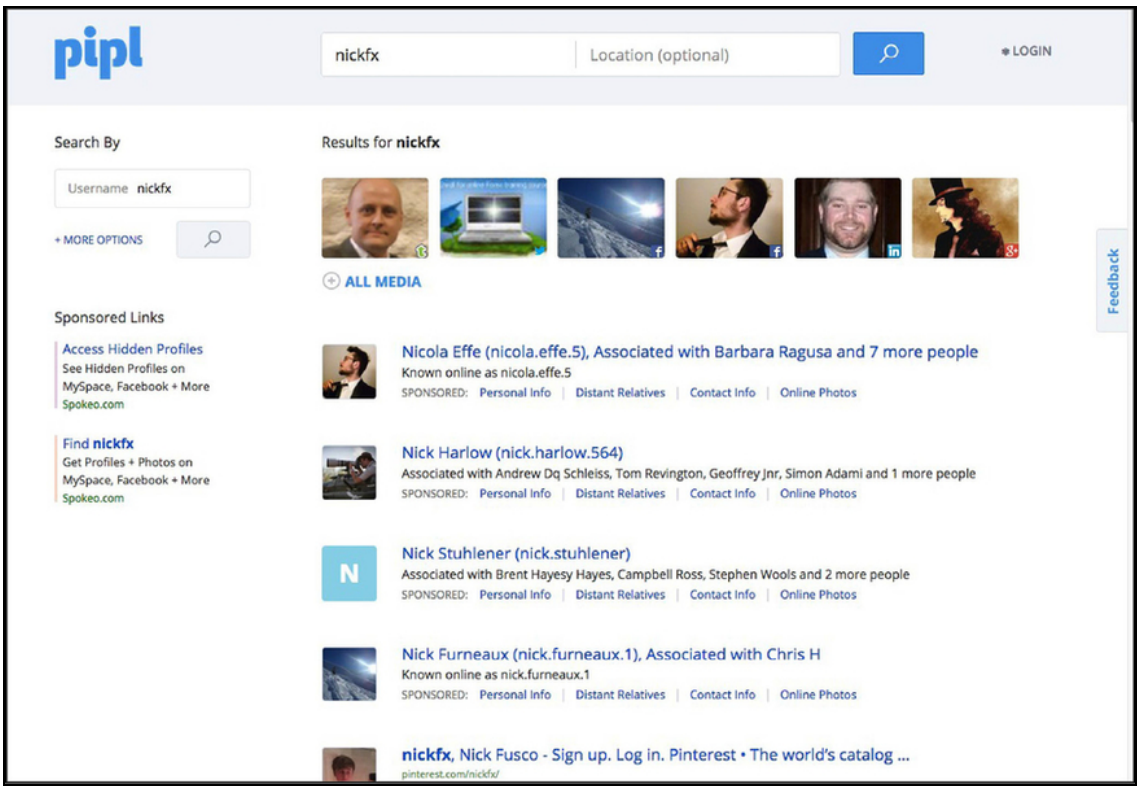


Figura 2.5 Lo vedete?

Con una rapida occhiata, potete vedere l'aspetto di "Nick" e solo quattro righe in basso, trovate Nick Furneaux, associato a Chris H (chissà chi sarà…) e il suo nome-utente.

Prima di arrivare a questo risultato, vediamo che cosa succede scegliendo l'immagine che sappiamo essere di Nick. Il risultato è rappresentato nella Figura 2.6.

Con un semplice clic, abbiamo la conferma di aver trovato il tipo giusto e anche la sua posizione. È l'OSINT: ora sappiamo dove abita.

Ora, tornate indietro di una pagina, ai risultati, e fate clic sul quarto link in basso. Che cosa scoprite? Date un'occhiata alla Figura 2.7.

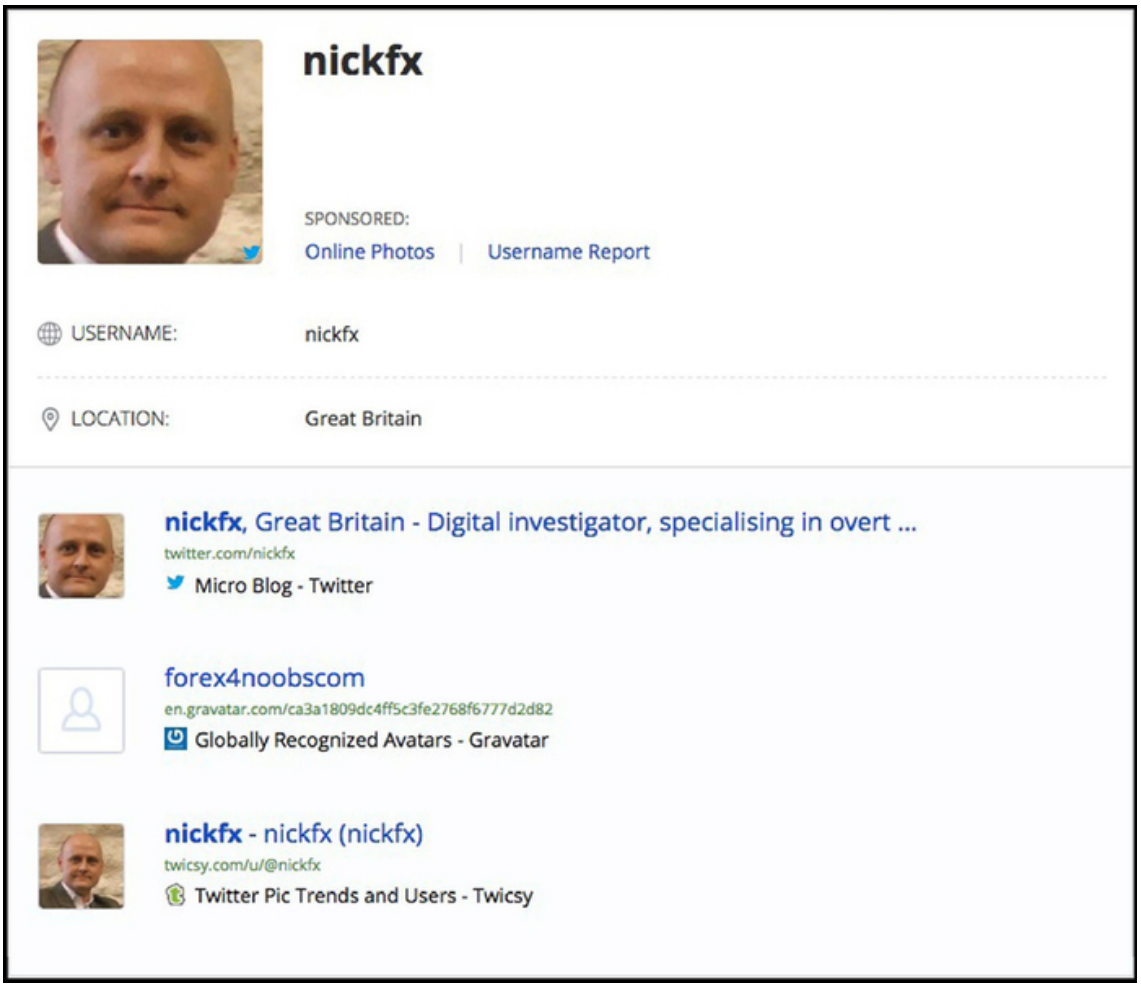


Figura 2.6 La conferma.



Figura 2.7 Ancora più OSINT!

Abbiamo già un po' di OSINT, vero? Una pagina di Facebook e un hobby che non conoscevo di Nick: gli piace lo snowboard. E deve proprio andare d'accordo con quel Chris H: sembra essere ovunque!

Quando faccio clic sul link di Facebook, ottengo ancora più OSINT.

- Vive a Bristol, Gran Bretagna.
- Posso vedere un elenco dei suoi amici.
- Trovo anche un nuovo nome-utente: `nick.furneaux.1`.

Tornando su `pipl.com`, inserisco il suo nome e la sua residenza a Bristol, Gran Bretagna, e ottengo ulteriori dettagli su di lui.

- L'impiego precedente.
- Il profilo LinkedIn.
- Ancora un altro nome-utente.
- Dove è andato a scuola.

Con solo una manciata di clic, ho già una buona quantità di informazioni su Nick, sicuramente utili per sviluppare un profilo su di lui. Posso scoprire anche altre informazioni?

Successivamente, passo sul sito `webmii.com`. L'obiettivo di WebMii è quello di aiutarvi a scoprire la visibilità online delle persone. La ricerca di "Nick Furneaux" restituisce i risultati che vedete rappresentati nella Figura 2.8.

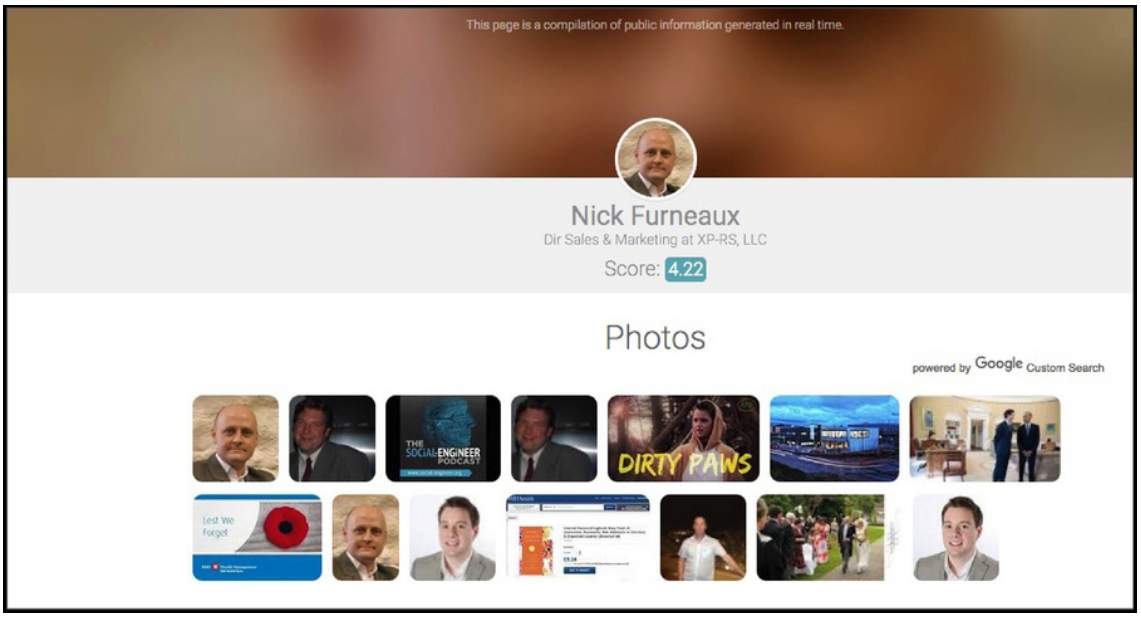


Figura 2.8 Molte più informazioni su Nick.

Noto subito un paio di cose: il punteggio di visibilità di Nick è 4,22 (non molto, visto che il massimo è 10). Ma facendo clic sul risultato vedo *quando* è particolarmente visibile (Figura 2.9). In termini di OSINT, le volte in cui Nick è stato più popolare devono suscitare il mio interesse: voglio scoprire che cosa è successo nella sua vita in quei momenti.

Tornando all'immagine rappresentata nella Figura 2.8, ci sono alcuni altri dati da raccogliere.

- La prima immagine ci riporta a Twitter.

- La terza immagine ci porta a un podcast in cui Nick è stato intervistato. È il podcast *The Social-Engineer Podcast* e ho sentito dire che è davvero notevole (ma quanto sono spudorato).
- Molte altre immagini rimandano alle pagine LinkedIn del Canada e non riguardano il Nick Furneaux cui siamo interessati
- La quinta immagine è strana: un giovane con una specie di cappuccio. Che cosa sarà mai?

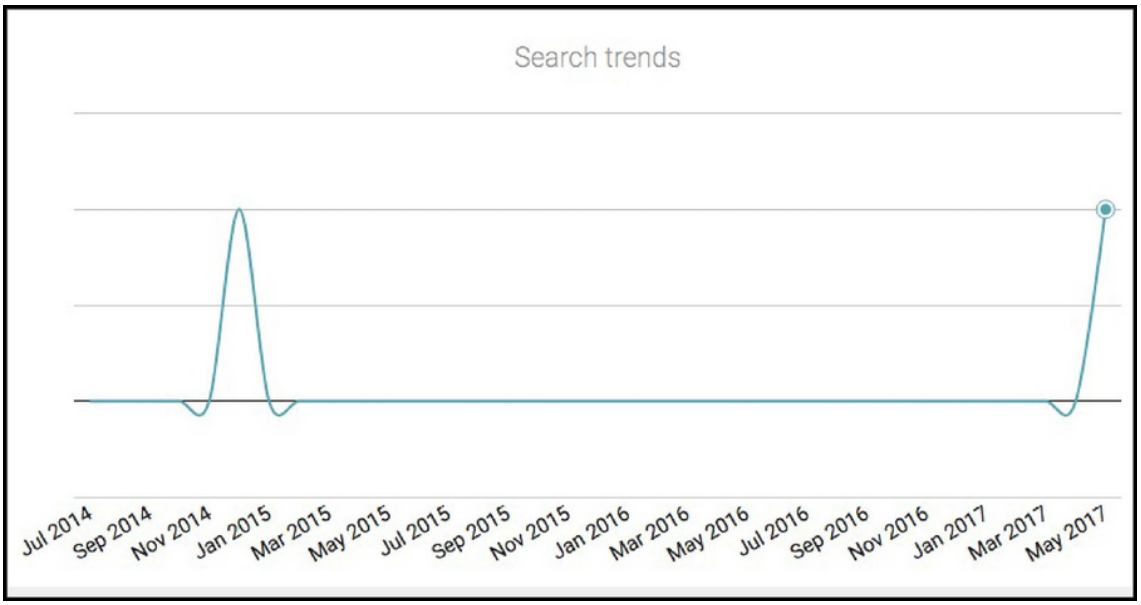


Figura 2.9 Quando è stato più popolare Nick?

Facendo clic su quel quinto link vado a un videoclip realizzato da una società chiamata AFB Productions. Faccio clic sul pulsante *More* e vedo quello che è rappresentato nella Figura 2.10.

Il video sembra essere stato realizzato da un tizio di nome Toby Furneaux (stesso cognome, quindi) e l'autista nel video è nientemeno che Nick Furneaux. Ovviamente, questa scoperta apre nuove possibilità nell'indicarci chi sia questo Toby e che cosa sia la AFB. Non ci vuole molto (due o tre clic) per rendersi conto che Toby è il figlio di Nick e che gestisce una piccola casa di produzione chiamata Any Future Box (AFB).

Un buon ricercatore OSINT includerebbe tutti questi dettagli nelle proprie informazioni, perché spesso i membri della famiglia (specialmente i figli dell'obiettivo) sono ottime risorse in termini di vettori d'attacco.

Osservate nuovamente la Figura 2.8. Mi sono imbattuto in quella foto di Nick in diversi punti. Questa immagine potrebbe portare a più risorse, quindi prendo l'URL effettivo dell'immagine e lo carico in una ricerca di immagini, che potete eseguire seguendo questi passaggi.

1. Fate clic destro sull'immagine.
2. Fate clic su *Visualizza l'immagine* (o *Apri l'immagine in un'altra scheda*).
3. Fate clic destro sull'immagine isolata e selezionate dal menu rapido l'opzione *Copia l'indirizzo dell'immagine*.
4. Su `www.google.com` fate clic su *Immagini*.
5. Fate clic su *Incolla immagine per URL* e incollate l'URL dell'immagine che avete copiato nel passaggio 3.

Dovrebbe apparire una pagina simile a quella rappresentata nella Figura 2.11.

Oltre a vedere che usa molto questo stesso ritratto, scopro che Nick ha anche una pagina Blogspot e ha scritto anche su una pagina di medicina legale. Seguendo il link della pagina di medicina legale, trovo un'intervista a Nick di alcuni anni fa e al termine di quell'intervista è indicato il suo indirizzo e-mail e l'URL del suo sito web.

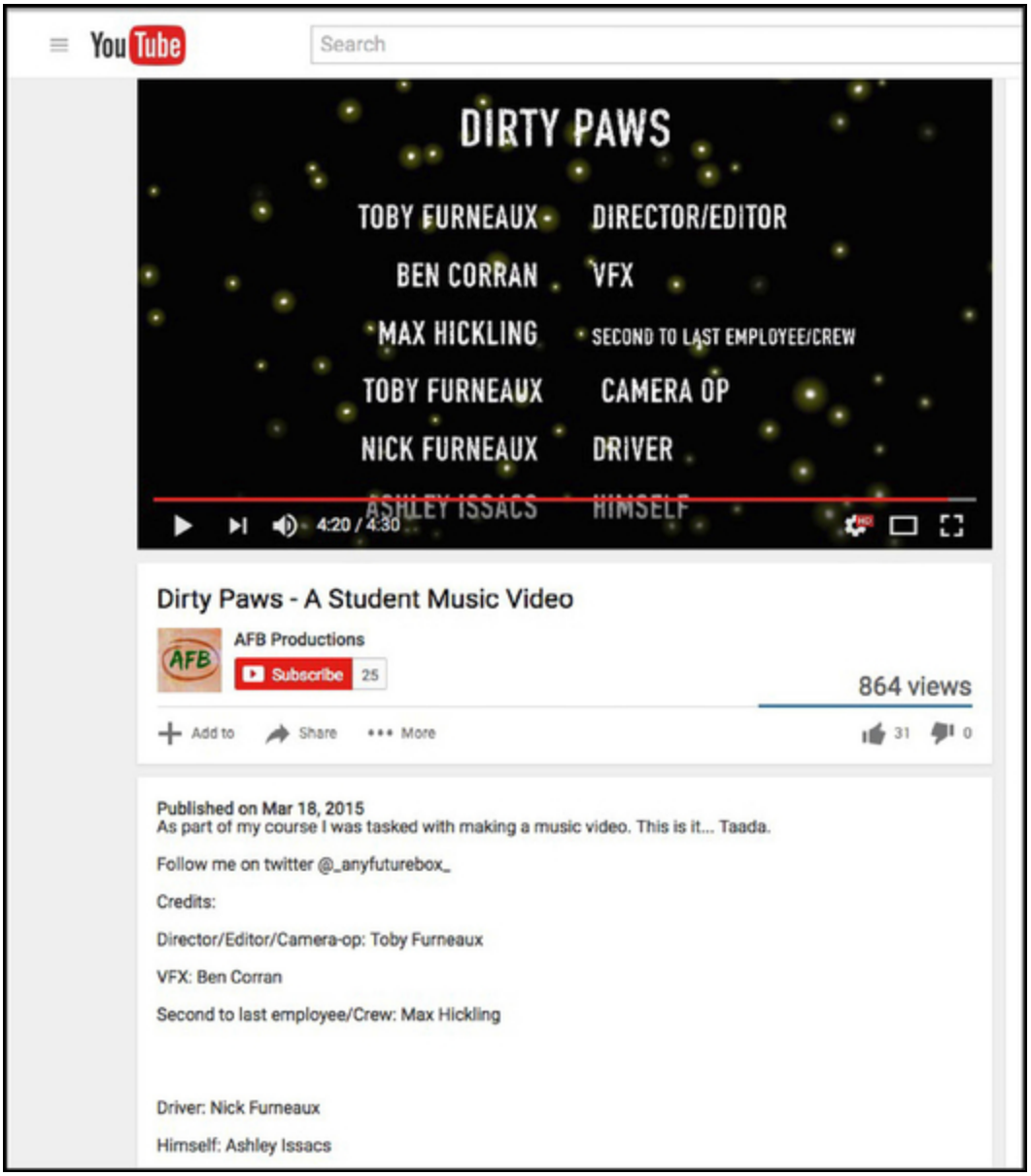


Figura 2.10 Ancora più OSINT!

Con una rapida ricerca WHOIS del nome di dominio del sito web di Nick, ottengo quello che è visualizzato nella Figura 2.12.

Nick ha usato questo sito web per molto tempo e la sua scadenza è a breve. Intelligentemente, Nick ha reso privato il suo dominio. Questo significa che non ci sono informazioni nel record: solo il nome dell'azienda, che già conosciamo, e il fatto che è un cittadino britannico.

Note sull'OSINT

Esistono diversi modi per eseguire una ricerca WHOIS. Se usate Linux o Mac, potete farlo direttamente dal terminale, digitando `whois nome-dominio` (sostituendo a `nome-dominio` il vero dominio). Oppure potete usare un sito web gratuito. Ce ne sono diversi tra cui scegliere, ma quello che uso più spesso è `http://www.whois.net`.

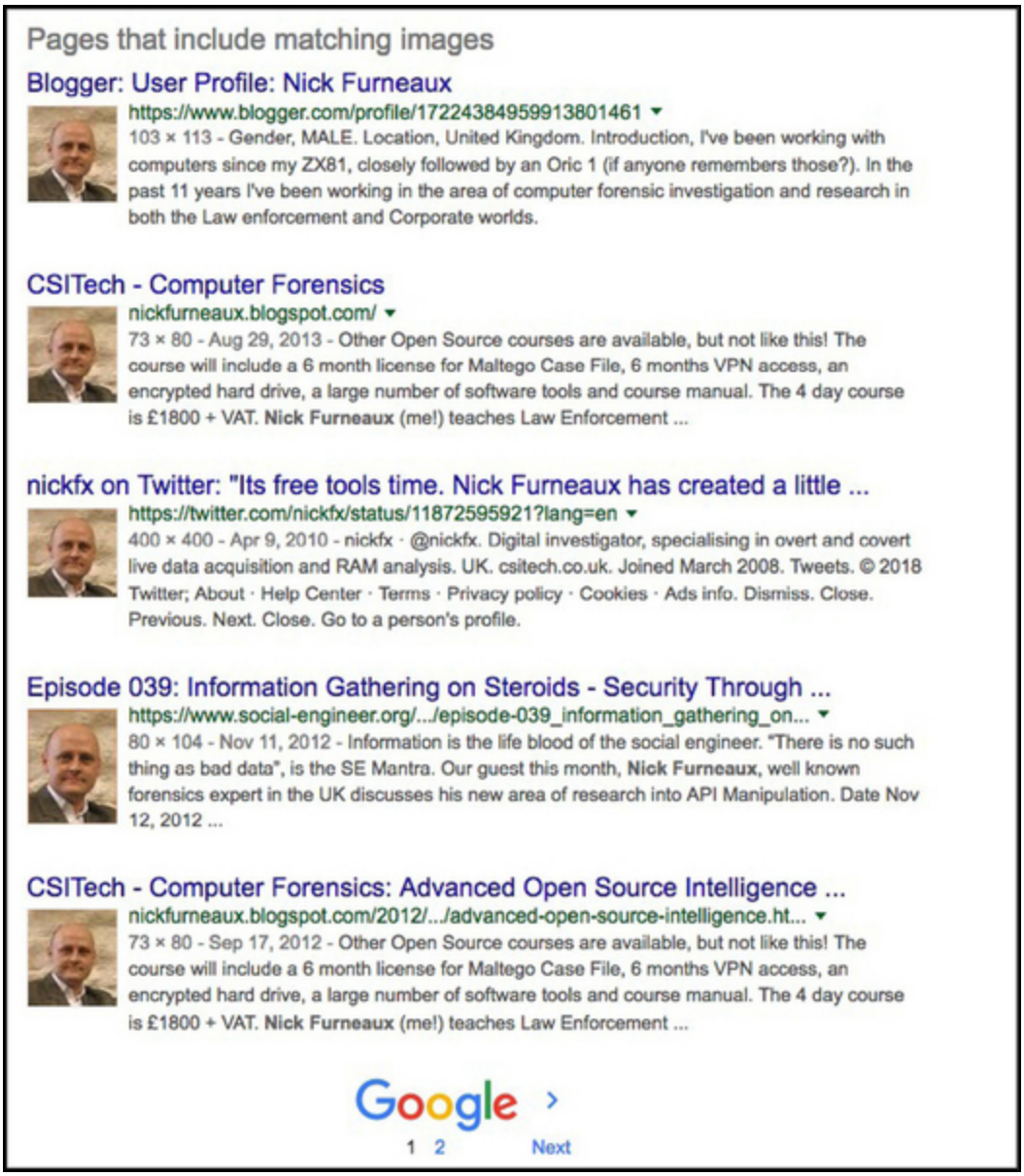


Figura 2.11 Un mucchio di informazioni su Nick.

Il metodo di raccolta delle informazioni che vi ho appena delineato è molto comune nel mondo dell'ingegneria sociale, perché con pochissimi clic permette di scoprire molte informazioni utili su un obiettivo.

Certo, non ho trovato un link alle password di Nick né alle sue foto private (grazie a Dio), ma ho trovato abbastanza informazioni che potrebbero essermi davvero utili nel caso volessi attaccare Nick con un attacco di *phishing* o *vishing*.

È tutto qui? Assolutamente no. Per fare davvero OSINT occorre salire sul ring del campionato mondiale di Pesi massimi.

Entrare in Google

Google. La sola parola fa gongolare di felicità un ingegnere sociale. Ok, ok… un'immagine piuttosto inquietante, lo ammetto. Quindi mettete da parte l'idea del gongolare e pensate più a un silenzioso ghigno di felicità.

Perché? Google è come un oracolo onnisciente. Sa tutto quel che avete fatto, lo salva e perfino lo mette da parte se cercate di cancellarlo (per sicurezza, per il "non si sa mai").

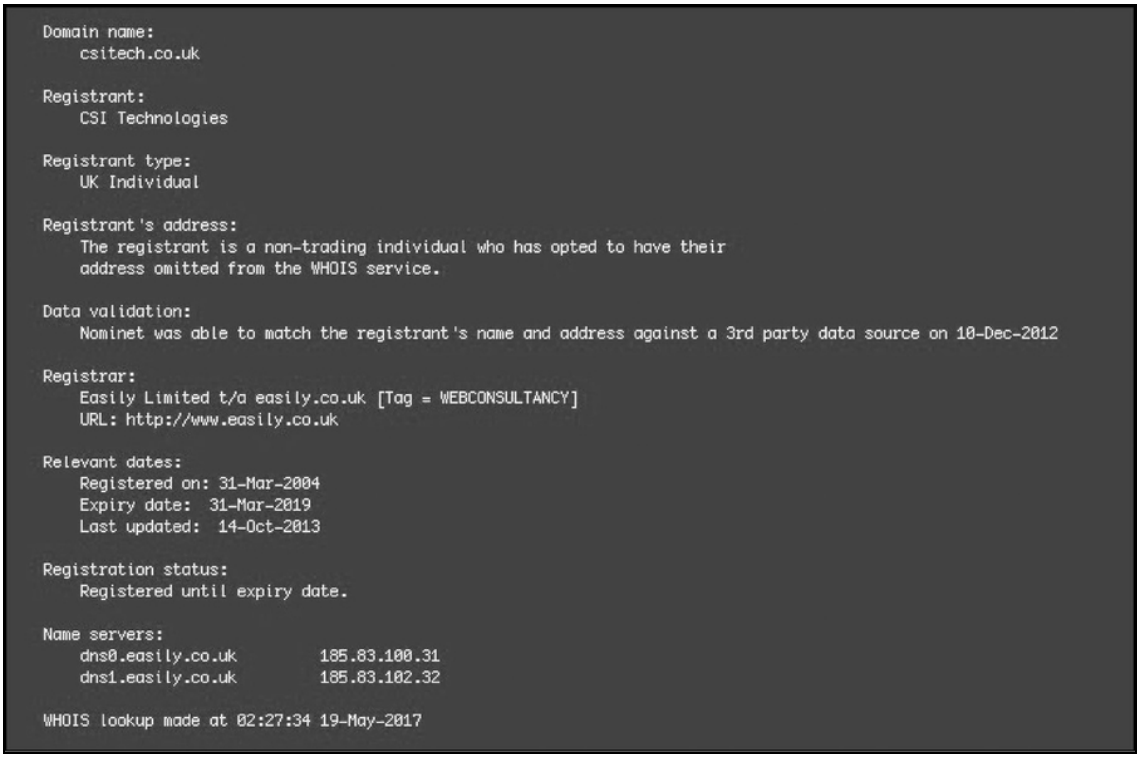


Figura 2.12 L'output di WHOIS.

Note su Google

Google è potente. Possiede circa l'88% della quota di mercato nella pubblicità legata alle ricerche. Secondo Google, il motore di ricerca indicizza più di 100.000.000 di gigabyte di siti web (`www.google.com/search/howsearchworks/crawling-indexing`).

Con tutta questa potenza e con miliardi di pagine web indicizzate, come può un piccolo ingegnere sociale trovare quei minuscoli frammenti di dati di cui ha bisogno? Prima di rispondere, devo spiegarvi brevemente come funziona Google (e qualsiasi altro motore di ricerca, del resto).

Rivelazione dei misteri dei motori di ricerca

Non c'è davvero nessun mistero da rivelare in questo paragrafo. Il titolo è volutamente fuorviante. Probabilmente avete già capito come funzionano i motori di ricerca, ma nel caso non lo sapeste, ecco una spiegazione molto semplice e veloce. I motori di ricerca usano piccoli

frammenti di codice chiamati *spider*. Gli *spider* “si insinuano” (io non faccio questo genere di cose) attraverso ogni pagina web aperta e memorizzano tutto ciò cui sono autorizzati ad accedere. Alcuni file, come `robots.txt`, impediscono a uno *spider* di indicizzare determinate aree, ma la maggior parte delle altre aree viene indicizzata e memorizzata.

Quanto viene trovato viene inserito in un database che, all’inserimento di un termine nella casella di ricerca, fornisce risultati come quelli che potete vedere nella Figura 2.13.

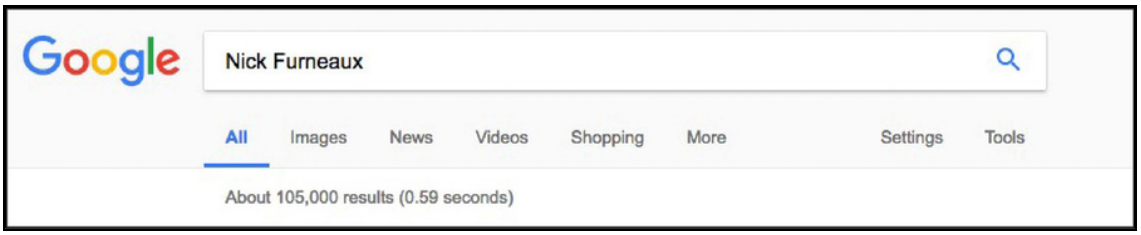


Figura 2.13 Nick Furneaux, ancora lui….

Permettetemi di sottolineare alcune cose chiave nella Figura 2.13. Innanzitutto, la ricerca ha restituito 105.000 risultati in poco più di mezzo secondo. Come può Google cercare 30 miliardi di pagine web in mezzo secondo? Ricordatevi che queste pagine sono state memorizzate in un database, il che consente di velocizzarne la ricerca.

Eseguire una ricerca in 105.000 pagine web non è solo improbabile ma, molto probabilmente, impossibile. Quindi, vi parlerò degli operatori.

Gli operatori

Google ha creato una serie di termini di ricerca denominati *operatori* che restringono le ricerche. Pensate alla differenza tra una lente di ingrandimento e un microscopio. Entrambi gli strumenti avvicinano un oggetto che desiderate ispezionare, ma se volete

davvero entrare nei dettagli, è meglio ricorrere a un microscopio. Questi operatori sono “il microscopio” della ricerca web.

I seguenti due siti web elencano tutti gli operatori utili per Google (e anche alcuni di Yahoo! e Bing):

- `https://support.google.com/websearch/answer/2466433?hl=en&ref_topic=3081620`;
- `www.googleguide.com/advanced_operators_reference.html`.

Per comodità, ecco un elenco degli operatori più utili.

- `intext`: cerca quel che segue l’operatore, all’interno nel testo della pagina web o del documento in questione. Per esempio, se digitate `intext: csitech`, Google cercherà tutte le occorrenze di quella parola.
- `site`: limita i termini di ricerca al sito indicato. Per esempio, se digitate `site: csitech.co.uk`, Google limita la ricerca solo a quel dominio, ignorando quanto si trova al suo esterno.
- `inurl`: questo operatore può sembrare simile all’operatore `site`, ma limita la ricerca a qualsiasi URL contenente il termine di ricerca digitato. Se digitate `inurl: csitech.co.uk`, la ricerca includerà anche qualsiasi sito web che abbia il termine `ccistech.co.uk` nel suo URL. Per esempio, se esistesse un sito chiamato `forensicsmag.com/csitech.co.uk/interviews`, verrebbe considerato da una ricerca con `inurl` ma non da una ricerca con `site`.
- `filetype`: limita la ricerca al tipo di file indicato.
- `cache`: cerca la versione memorizzata del dominio, del file o dell’oggetto elencato.
- `info`: fornisce informazioni sul dominio indicato.

Come in molte cose che riguardano il software, esistono delle regole. La ricerca su Google non è diversa.

- Dovete specificare l'operatore, seguito da un due punti e dal termine da cercare, senza spazi. Con `site:whitehouse.gov`, per esempio, limitate la ricerca al sito `whitehouse.gov`. Se invece scrivete `site: whitehouse.gov`, limiterete la ricerca al solo spazio che segue i due punti (`:`), il che non è molto efficace.
- Il trattino (`-`) specificato prima di un operatore rimuove i risultati dalla ricerca. Per esempio, se desiderate trovare tutti i riferimenti a `csitech`, ma senza considerare quelli nello spazio `.com`, potete provare questa ricerca per limitare i risultati: `inurl:csitech.co.uk –site.com`.
- Se il termine di ricerca contiene più parole e desiderate includerle tutte nella ricerca, dovete utilizzare le virgolette. Per esempio, se voglio cercare Nick Furneaux, posso provare `intext:"Nick Furneaux"` per includere sia il nome sia il cognome nel mio `intext` di ricerca.
- Secondo Google (`https://support.google.com/gsa/answer/4411411#requests`), esiste un limite al numero di termini di ricerca consentiti. Il valore predefinito è 50 e il limite massimo è 150. Ma, onestamente, chi avrebbe mai bisogno di cercare più di 100 termini di ricerca?

Credetemi, ci sono molti più termini di ricerca e chicche oltre a quelle che ho indicato qui. Google è uno strumento davvero potente e potrei scrivere interi volumi per approfondire ogni suo piccolo dettaglio. Ma torniamo alla nostra attività di OSINT. Procediamo con alcuni esempi e vediamo che cosa riusciamo a trovare.

Limitare per avere successo

Quando ho interrotto la mia ricerca di informazioni su Nick Furneaux all'inizio di questo capitolo, stavo già creando un bel profilo su di lui. Google può confermare le mie conclusioni e fornire ulteriori informazioni?

Avevo trovato alcune informazioni, come il suo nome e il soprannome che usa su almeno un *social media*. Che cosa succede se li metto insieme per vedere che cosa si riesce a trovare? Digitando `intext:"Nick Furneaux" intext:nickfx` nella casella di ricerca di Google si ottiene quanto è rappresentato nella Figura 2.14.

In meno di un secondo, ho ottenuto 206 risultati sul mio obiettivo. Una delle funzionalità di ricerca su Google è la possibilità di vedere le immagini correlate alla ricerca. Facendo clic sul link *Altre immagini per*, trovo alcuni risultati interessanti. In questo caso, le immagini possono portarmi a pagine che parlano di Nick.

Ma conosco già molte di queste informazioni su Nick, quindi vediamo che cos'altro riesco a trovare. Cambio i termini di ricerca in `intext:"Nick Furneaux" intext:UK`. I risultati sono rappresentati nella Figura 2.15.

Il primo risultato mi dice che insegna a Bristol. L'ultimo risultato fornisce il nome di un'azienda della quale Nick potrebbe ancora far parte, così come la sua data di nascita e persino un indirizzo a – indovina un po' – Bristol.

La pagina include anche un elenco di familiari o amici con i quali potrebbe collaborare in quell'azienda. è una miniera di informazioni.

Cambiare lo `"UK"` della ricerca precedente in `"Bristol"` ci porterà a informazioni come il codice postale e persino alcuni nomi di altri membri della famiglia che potrebbero vivere con lui.

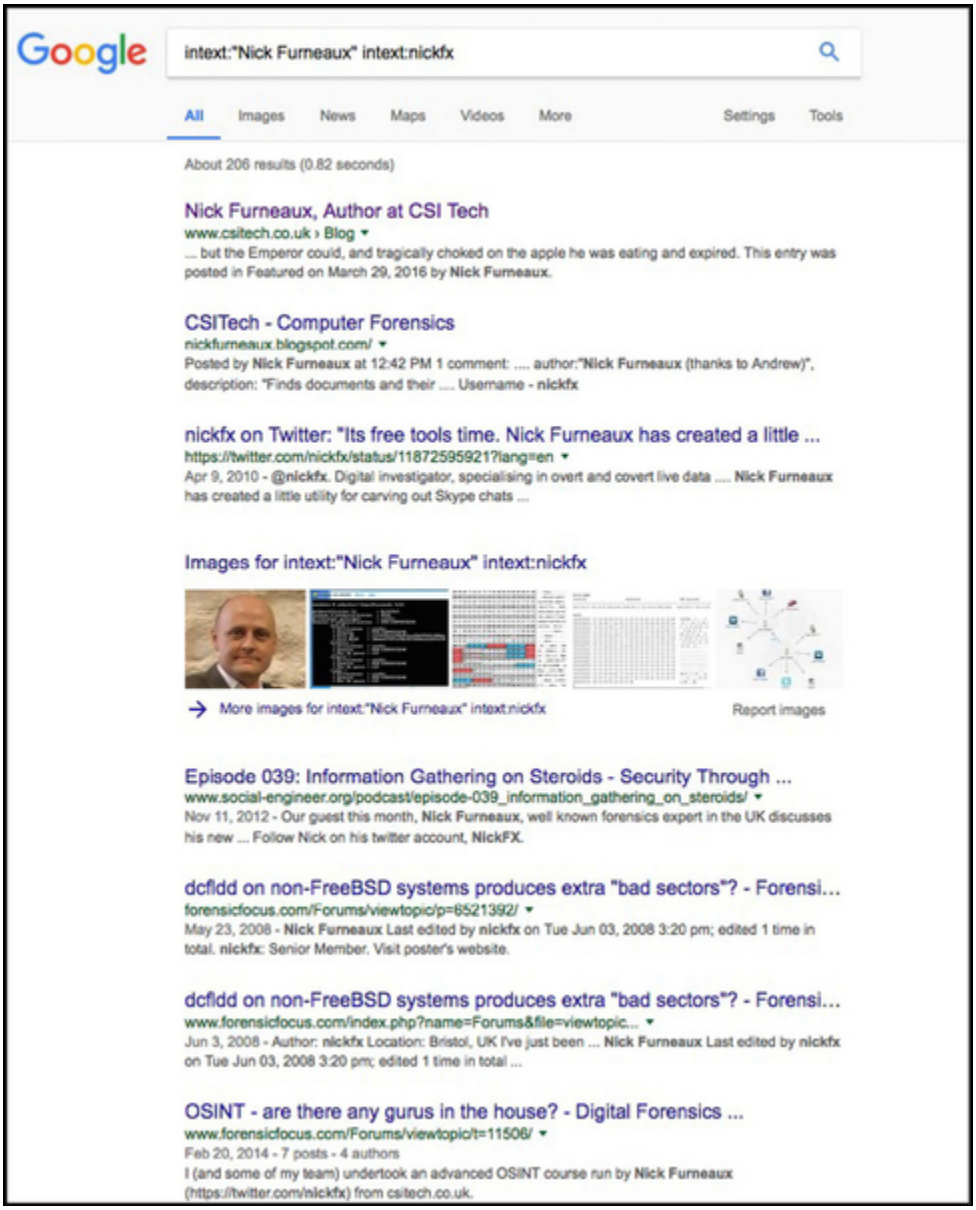


Figura 2.14 Da 0 a 206 in 0,82 secondi netti.

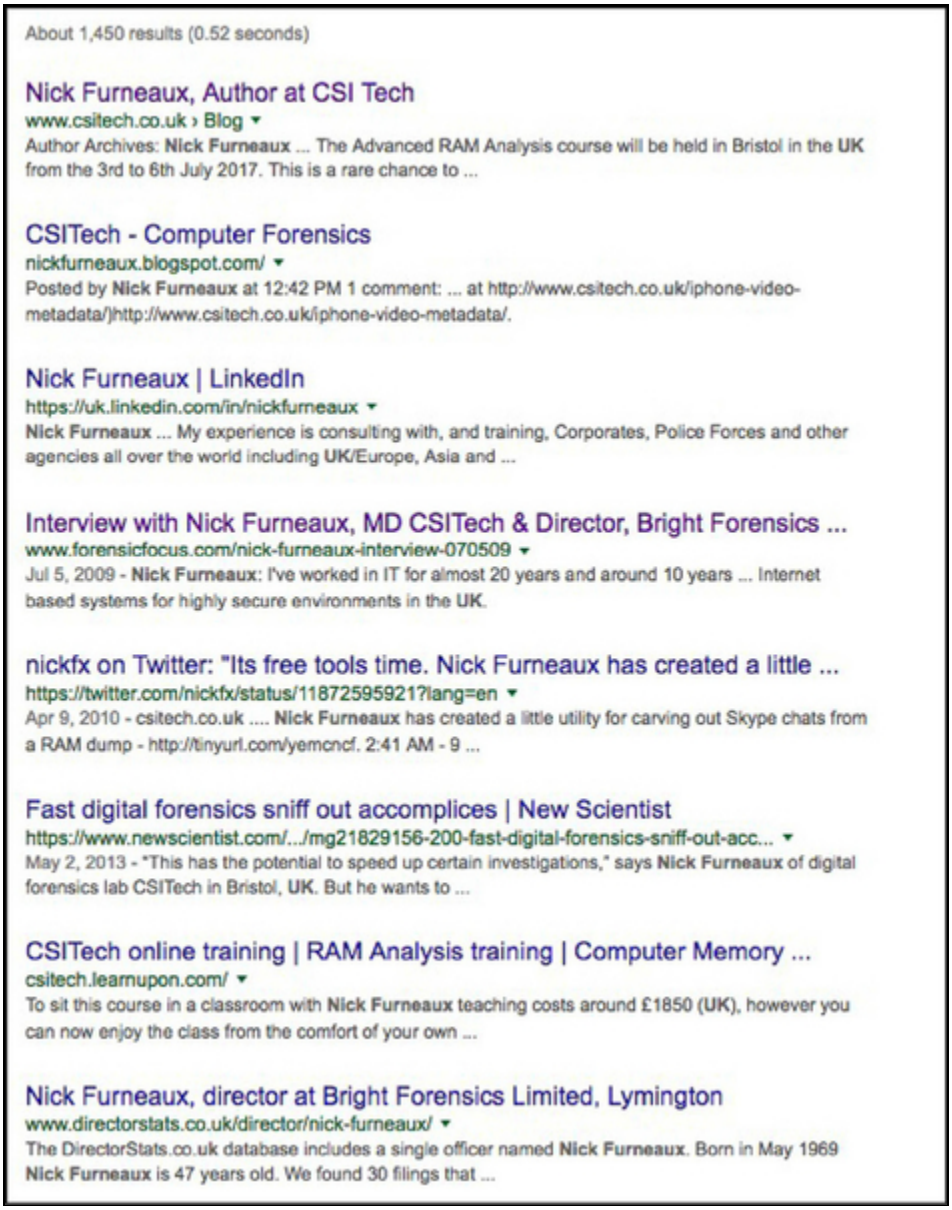


Figura 2.15 Ci stiamo solo scaldando, Nick…

Ecco un ultimo esempio prima di proseguire. Quale pensate possa essere il primo risultato della seguente ricerca Google?

intext:”Nick Furneaux” site:linkedin.com intext:Bristol

Il primo risultato che ho ottenuto è stata la pagina LinkedIn di Nick. Usando gli operatori di Google, potete specificare piccole informazioni tratte dalle vostre ricerche precedenti per continuare a cercare fino a quando non trovate l’informazione di cui avete bisogno.

Voglio mostrarvi qualcosa di più della potenza di Google, ma dal momento che Nick è ancora mio amico (o almeno lo era l'ultima volta che ho controllato), intendo allontanare l'attenzione da lui e generalizzare un po' le ricerche.

Non dovrebbe essere "privata"?

Avete mai sentito parlare delle chiavi private RSA? Una chiave RSA si basa su un algoritmo proprietario. Si presenta in due parti: la chiave pubblica, che permette di identificarla, e la chiave privata, che sblocca il regno.

Secondo questa definizione, le chiavi private RSA vengono utilizzate per stabilire una connessione sicura.

Quindi, potreste pensare che cercando le chiavi private RSA, non ne trovereste neanche una, giusto? Ma usando la seguente ricerca

BEGIN (CERTIFICATE|DSA|RSA) filetype:key

si ottengono oltre 3.000 risultati, come potete vedere nella Figura 2.16.

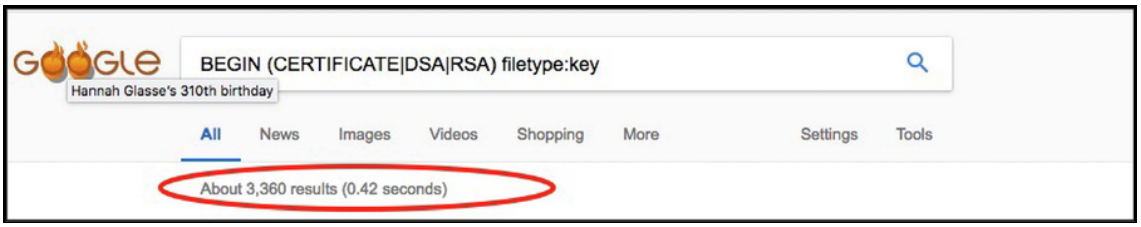


Figura 2.16 Perché, allora, chiamarla privata?

Ma è classificata come confidenziale

Spesso, gli enti governativi contrassegnano i documenti con determinate classificazioni per indicare se possono essere divulgati. Contrassegni come "classified" e "top secret" di solito indicano che i documenti non sono destinati al pubblico. Presumerete che non sia possibile trovarne alcuno online (non credo che vogliate sapere quello che dicono delle persone che presumono troppo…).

Ma dal momento che mi piace trascorrere la mia vita fuori dalle mura di una prigione, diciamo solo che vogliamo vedere se ci sono documenti contenenti password, le quali dovrebbero essere confidenziali, non è vero?

Che cosa succede se cerco `site:gov.ir intext:password filetype:xls`? In teoria questa ricerca dovrebbe produrre i risultati a qualsiasi dominio `gov.ir` e cercare solo i file `.xls` contenenti la parola *password*. I risultati sono rappresentati nella Figura 2.17.

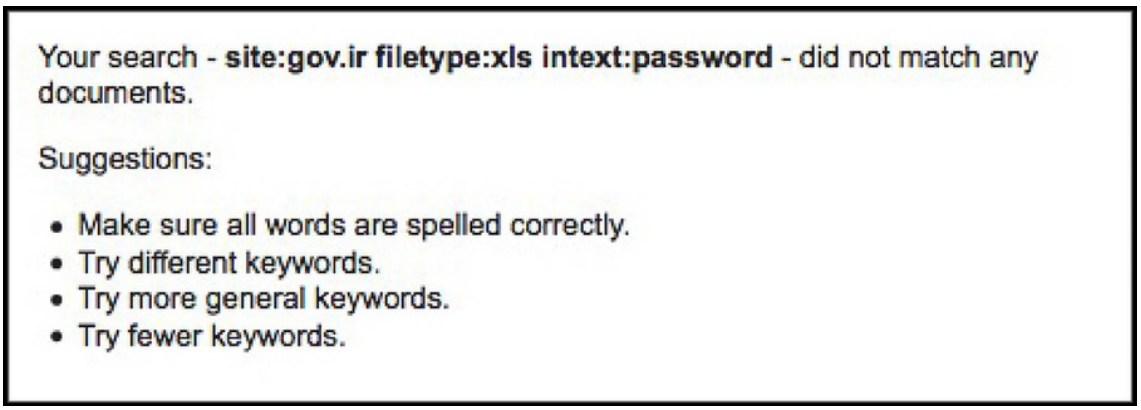


Figura 2.17 Che cosa è andato storto?

Mm, non è giusto. Perché mai un documento in un server governativo iraniano dovrebbe avere al suo interno la parola inglese *password*? Ah, ma che cosa succede se provo a usare `translate.google.com` per tradurre la parola *password* in persiano? Aiuta? La Figura 2.18 mostra il risultato.

Qui si vede la vera potenza di Google. Non ho bisogno di conoscere il persiano o di eseguire ricerche in persiano. Basta solo chiedere di cercare quella parola e così sono riuscito a trovare i documenti che cercavo.

Webcam: forse è il caso di smetterla di ballare in mutande in camera

C’è stato un vero boom: tutti volevano possedere una webcam. Vengono usate per monitorare i bambini, le baby-sitter, gli animali domestici, per sicurezza e molto altro ancora.

Molte di queste sono state vendute con impostazioni predefinite, il che le rendeva vulnerabili e aperte. A volte il software venduto con le webcam lasciava molto a desiderare. Facili da utilizzare? Sì, anche per i malintenzionati.

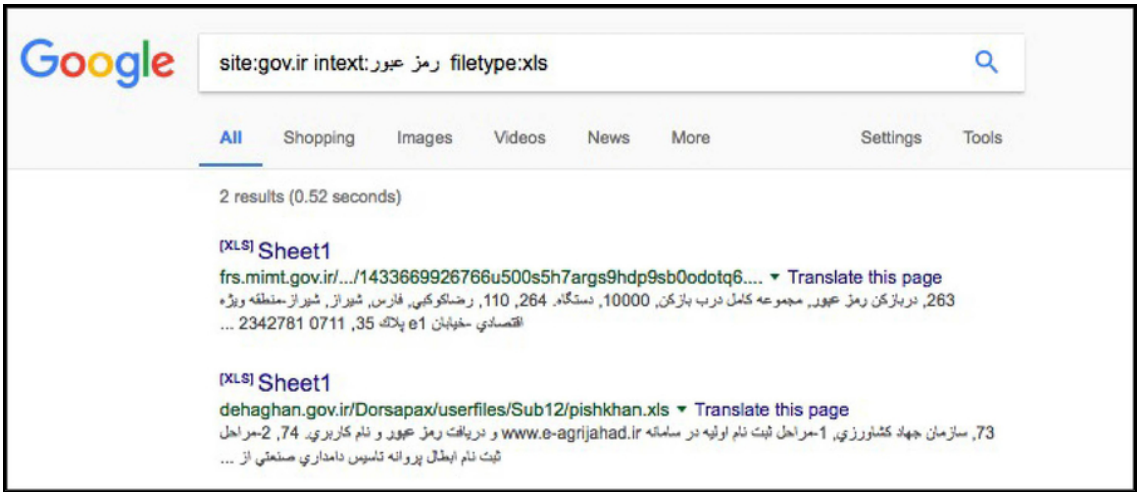


Figura 2.18 Ricerche Google multilingue.

Uno di questi software era webcamXP. Come indica il suo nome, è predisposto per funzionare sotto Windows XP, Vista, 7, 8, 9, 10, Server 2003, 2008 e 2012. Secondo il sito web, l’ultimo aggiornamento del software risale al 2016. Quindi non dovrebbe essere più troppo popolare oggi, giusto? Quindi una ricerca eseguita oggi non produrrebbe un granché di risultati, giusto?

Giusto?!

Così, ho cercato `intitle:"Webcam 7" inurl:8080 -intext:8080`. E il risultato lo vedete nella Figura 2.19.

Certo, molte di queste webcam sono concepite proprio per essere online e per essere viste dal pubblico. Trasmettono angoli di strada o ruscelli o aree boschive. Ma ci sono anche persone che installano le

webcam per uso personale e le lasciano aperte in giardino o anche in casa. Il punto è che se queste webcam non sono ben protette, qualsiasi persona con un minimo di abilità può osservarvi e non lo scoprireste mai.

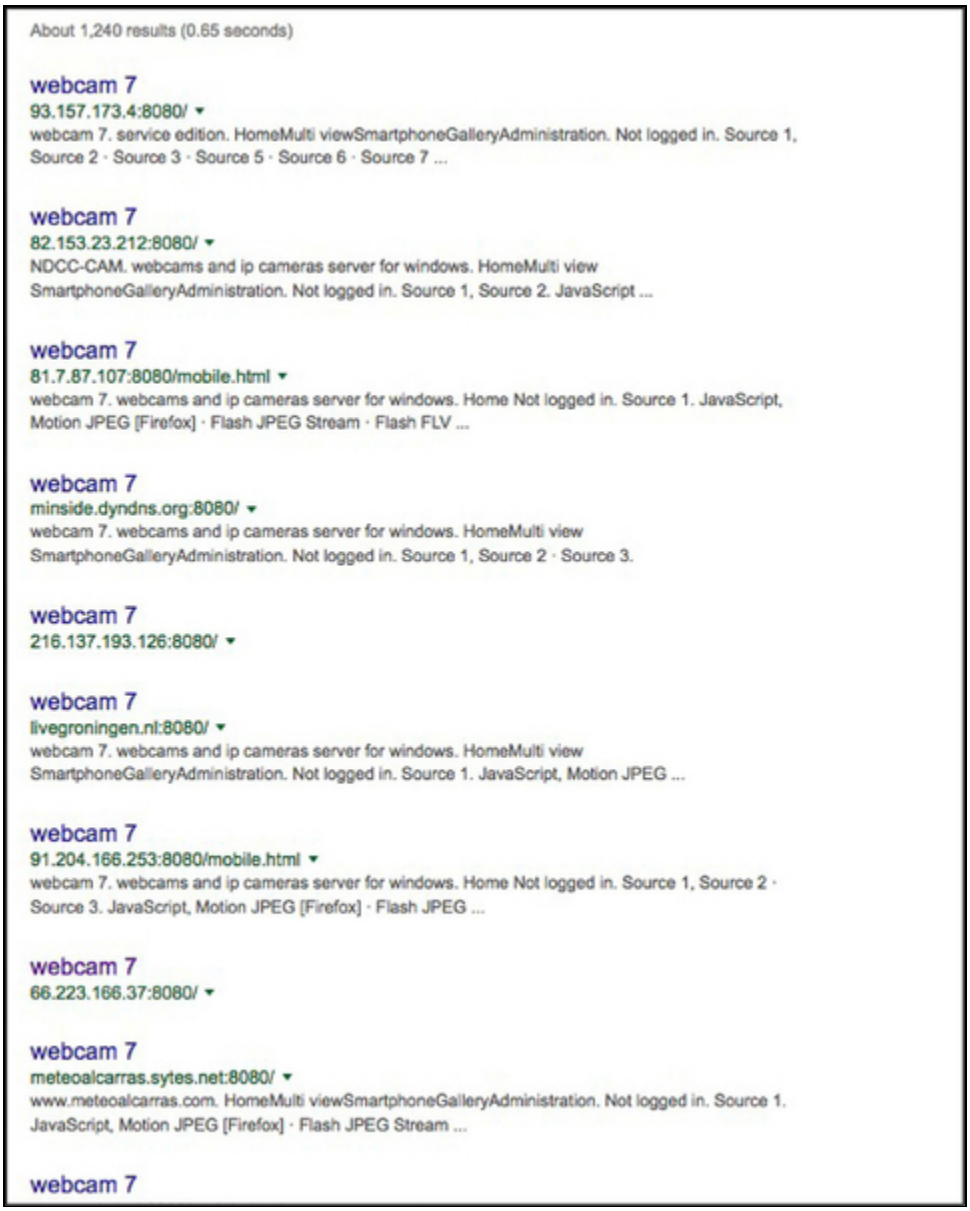


Figura 2.19 Webcam a bizzeffe!

Altre fonti di intelligence

Di solito quando arrivo a questo punto, chi mi ascolta reagisce con un misto di orrore e curiosità su cos'altro sia possibile ottenere con una ricerca Google. Non voglio elencare ogni ricerca Google che ho fatto, ma vi posso dire alcune delle cose che ho scoperto con facilità usando solo ricerche Google.

- La webcam di un tizio che osservava crescere le sue piante di marijuana.
- Le foto private dei telefonini di alcuni tizi.
- Le directory di musica e film condivisi di alcuni tizi.
- Vari documenti contenenti password, date di nascita e numeri di previdenza sociale.
- File contenenti migliaia di numeri di carte di credito.
- Database SQL pieni di informazioni.
- Libero accesso alle webcam del traffico.
- Libero accesso alle reti elettriche e ai sistemi di controllo.
- Vari punti di diffusione di immagini di pedofilia.

Ma vi assicuro che l'elenco potrebbe andare avanti, e anche molto.

Altre due cose

Questo paragrafo potrebbe riempire, da solo, un intero libro. Ma prima di procedere e concludere questo capitolo, non farei il mio dovere se non menzionassi altre due cose.

I robot sono fantastici

Da bambino, desideravo avere un *robot*. Pensavo che R2D2 sarebbe stato il migliore amico che potessi mai avere. Ma in questo caso, non sto parlando di quel tipo di *robot*. Mi riferisco al file `robots.txt`.

Che cos'è un file `robots.txt`? È un semplice file che i proprietari di siti web usano per indicare agli *spider* o ai *robot* che eseguono la

scansione dei siti dove possono accedere e dove no. Per esempio, non è raro incontrare istruzioni `Disallow` in un file `robots.txt`, che indicano che ai *robot* non è permessa la memorizzazione cache di una tal cartella. Per esempio, la Figura 2.20 mostra il file `robots.txt` del sito `whitehouse.gov`.

Ora provate a pensare come un ingegnere sociale. Che cosa vi dice il file rappresentato nella Figura 2.20?



```
User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
Disallow: /experiments/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
Disallow: /?q=experiments/
```

Figura 2.20 Notate quanti Disallow!

Potete vedere quali directory esistono, e anche a quali directory non dovete fare accesso, né voi né la cache di Google.

Inoltre, file come `mysql` o `pgpsql` forniscono indicazioni del tipo di tecnologia utilizzata sul vostro sito.

Ora, se questo fosse un mio vero obiettivo (e *non* lo è, ripeto, *non lo è*), andrei su ognuna di queste directory per vedere se tutto è stato configurato correttamente e per verificare che non ci autorizzi a entrare senza autorizzazione. Verificherei quei log e quei file, se sono accessibili, per vedere se c'è qualcosa di mal configurato nei server.

Una volta ho svolto un lavoro per un'azienda di medie dimensioni. È stato il raro tipo di test alla "fate tutto quello che riuscite a fare e vedete che cosa potete trovare, quindi attaccateci senza ritegno". Iniziai con un po' di OSINT e di ricerche Google e trovai nel loro file `robots.txt` che avevano un'istruzione `Disallow` relativa a una directory chiamata `admin`.

Solo per controllare, digitai `www.company.com/admin` e, con mio grande stupore, entrai senza credenziali! La directory conteneva l'archivio privato dei file dell'amministratore delegato e sembrava che lo usasse per condividere quei file dei quali avrebbe avuto bisogno in viaggio. Conteneva contratti, dati bancari, una foto del suo passaporto e numerosi altri dettagli riservati.

Trovai un contratto che era stato firmato da soli due giorni. Acquistai un dominio quasi identico al vero nome dell'azienda, preparai un'e-mail per chi aveva firmato il contratto e inviai al CEO un file infetto e un'e-mail che diceva: "Non sono sicuro di aver inviato il contratto firmato, ma ho una domanda sulla Sezione 14.1a. Potrebbe considerare il problema e farmi sapere?".

Entro 15 minuti, l'amministratore delegato aveva ricevuto l'e-mail, l'aveva aperta ed era stato violato. Stava rispondendo a un indirizzo

falso, e mi diceva che il contratto non si apriva e continuava a bloccarsi. Un test di penetrazione (*pen-test*) che doveva durare una settimana, era terminato in sole tre ore.

Chiamai l'amministratore delegato (CEO) e la nostra conversazione andò più o meno così.

CEO: Buongiorno.

Io: Ciao Paul. Sono io, Chris dei Social-Engineer. Volevo parlarti del *pen-test*…

CEO: Ha! Così presto, Chris? Pensavamo di essere più solidi.

Io: Bene, Paul, ho già il tuo passaporto, la tua data di nascita, le tue carte di credito, l'accesso ai vostri conti bancari e a una shell remota con le credenziali di amministrazione della rete. Ho pensato di doverti chiamare e vedere se desideri davvero che continui per tutta la settimana?

CEO: Andiamo! Stai inventando! Hai iniziato a lavorare appena un paio d'ore fa. Dimmi, chi è quell'ingenuo che ha fatto clic e ci ha fregato? Devo dirgliene quattro.

Io: Ehm, Paul… (*deglutii, non sapevo se potessi pronunciare proprio la battuta che avevo in mente*) Io non ci andrei giù troppo pesante; è un tipo piuttosto in gamba.

CEO: Ah sì? E chi è?

Me: Paul, sei tu.

Gli spiegai ogni dettaglio e lui capì subito che cosa fosse successo. Questo particolare *pen-test* ha avuto successo in gran parte per colpa di un file `robots.txt` e di una directory mal configurata.

È tutta una questione di meta, baby

Secondo l'*Oxford English Dictionary*, con *meta* si definisce "riferimento a se stessi o alle convenzioni del proprio genere;

autoreferenziali”. Quindi, i metadati sono letteralmente dati sui dati. Fa un po’ pensare al film *Inception*, vero?

Mi spiego più semplicemente. I metadati sono informazioni su un oggetto che trovate nell’ambito di una ricerca. Molte volte, questi dati forniscono informazioni piuttosto interessanti, molte delle quali potrebbero non essere state inserite intenzionalmente.

Diciamo che conduco una ricerca Google molto benigna per trovare i file `.doc` che contengono informazioni sulle password. Mi imbatto in questo piccolo documento chiamato `FinalPasswordPolicy`. Che cosa mi riveleranno i metadati? Date un’occhiata alla Figura 2.21.

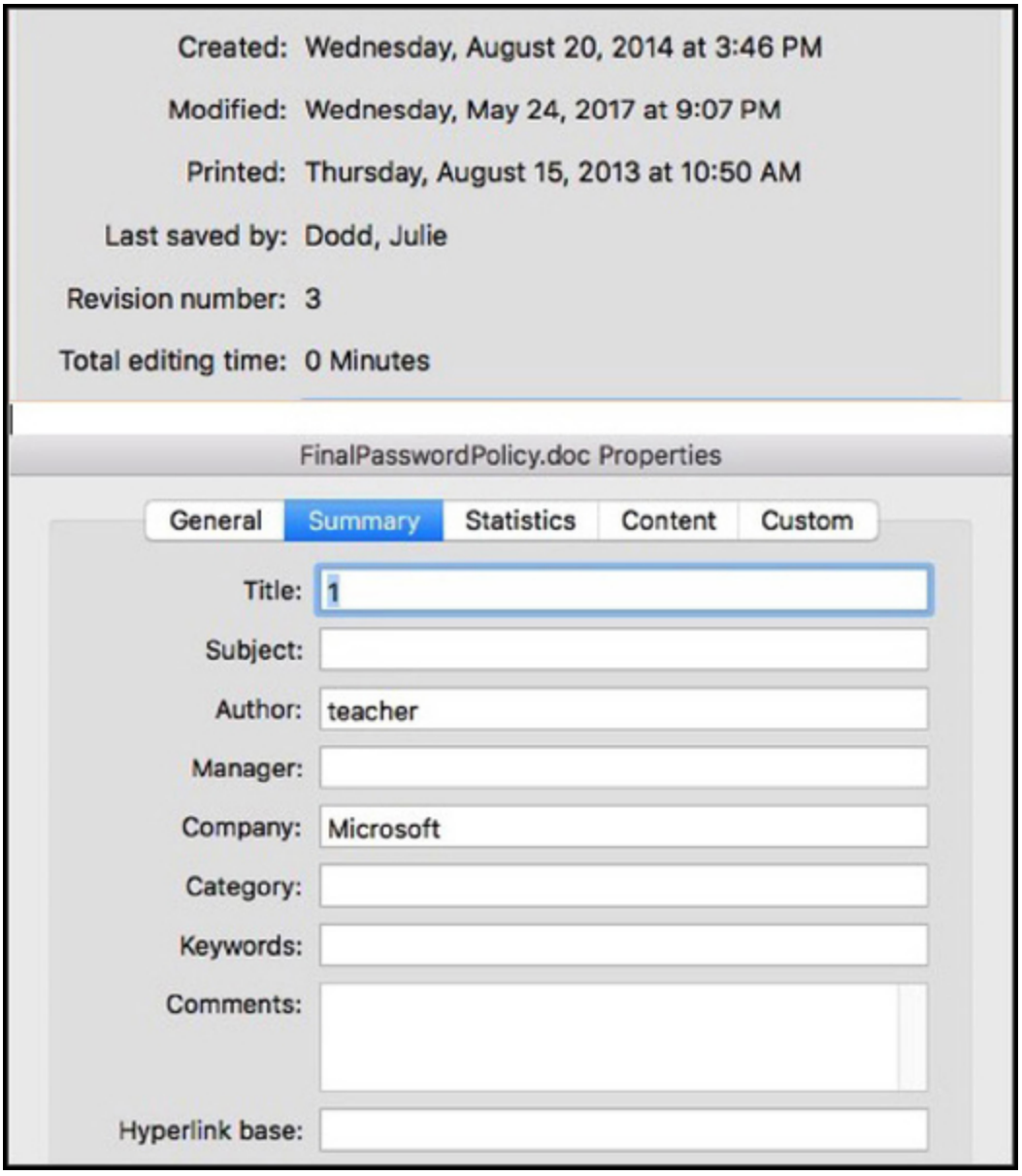


Figura 2.21 Metadati: vedete quello che ho fatto?

Questi metadati forniscono di un file la data e ora di creazione, l'ultima persona che l'ha salvato, il nome/titolo dell'autore, il numero di revisioni del file e alcune altre informazioni che non è il caso di menzionare qui. Potreste pensare: "E allora?".

Bene, già solo il nome e il tipo di un documento può essere un'informazione preziosa per un ingegnere sociale. Pensate: che cosa succederebbe se un ingegnere sociale dovesse trovare una nuova

policy delle risorse umane che avete appena rilasciato? I metadati rivelano quando è stata rivista l'ultima policy (in questo caso, non aveva neanche un mese), chi l'ha scritta e quando è stata rilasciata. Naturalmente, il documento conterrebbe anche tutti i dettagli della policy. Non pensate che un'e-mail di *phishing* che sembri provenire proprio da chi ha scritto la policy e che, apparentemente, includa un aggiornamento della policy riceverà qualche clic?

Date un'occhiata alla Figura 2.22.



Figura 2.22 "No, cioè… in che senso?"

A prima vista potreste pensare: "Ok. Quindi pensi di fregare qualcuno con un buono sconto per una salsa piccante?". La risposta è no, ma date un'occhiata ai metadati, presentati nella Figura 2.23.

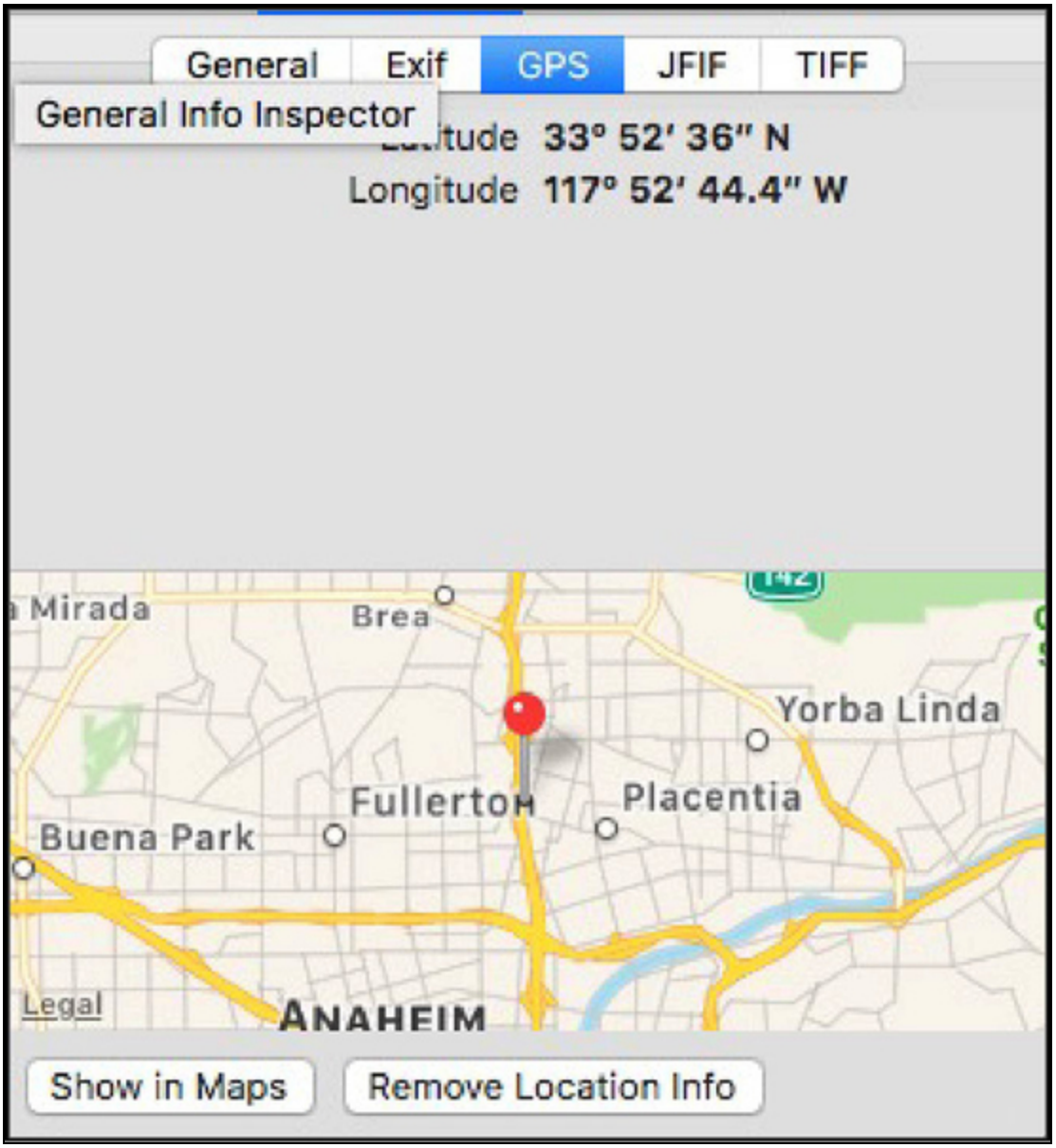


Figura 2.23 La risposta è …

Quando trovate online una foto apparentemente innocua, i metadati vi forniscono informazioni sul tipo di fotocamera, la data, l'ora e le coordinate GPS in cui è stata scattata. Inserendo queste coordinate in Google Maps… be', guardate la Figura 2.24.

La mappa punta al parcheggio del ristorante Pepe, che sembra essere un grande consumatore di quella marca di salsa piccante.

Quindi, un tipo ha usato lo smartphone per scattare una foto. Il suo smartphone aveva il GPS acceso e disponibile all'app della fotocamera, la quale ha incorporato tutti i metadati nel file della fotografia. Quando ha caricato l'immagine sulla sua pagina *social media*, il file conteneva tutte queste informazioni, ora disponibili per tutti.

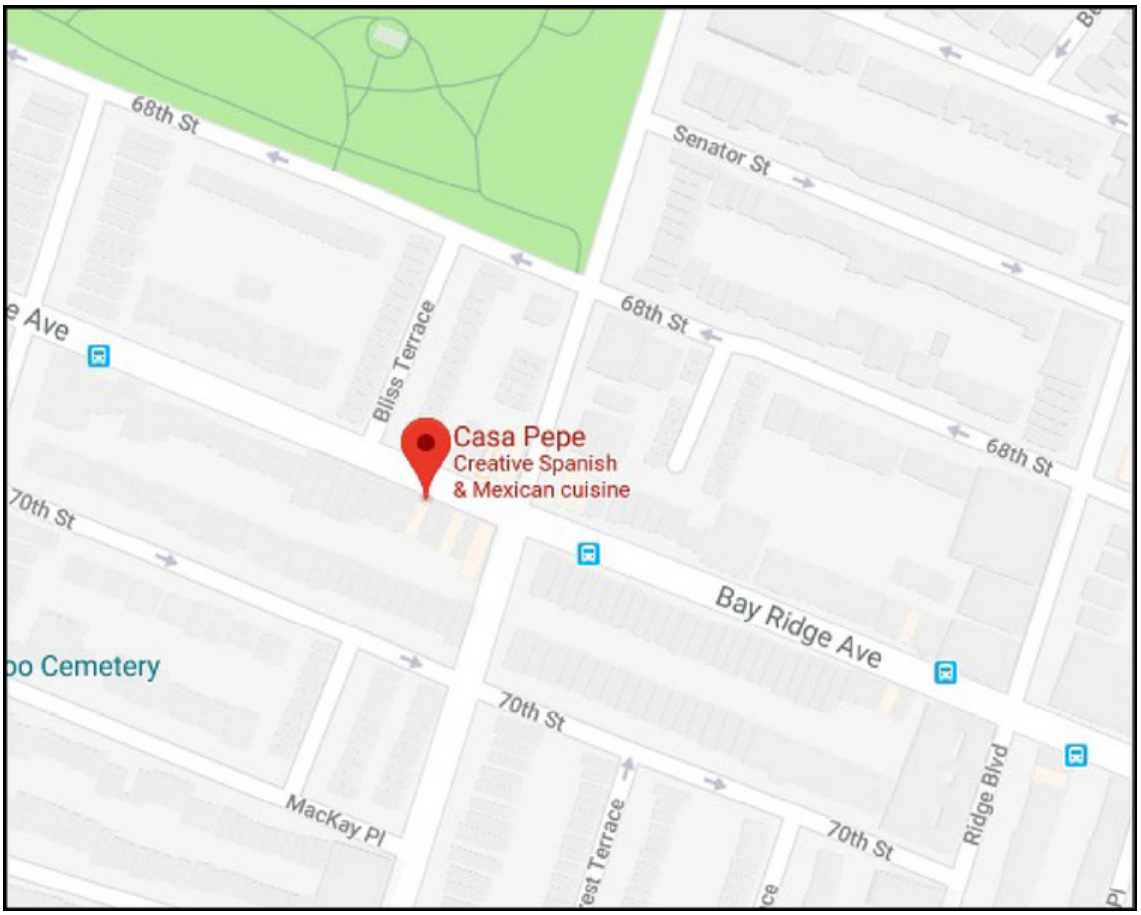


Figura 2.24 … direi piuttosto "succosa"!

Riuscite a valutare le implicazioni? Immaginate di non essere a cena da Pepe con i vostri amici, ma:

- amministratori delegati di una grande società di servizi oggetto di attacchi a livello nazionale;

- segretari di un miliardario, con informazioni sulle sue banche e i suoi meccanismi di trasferimento;
- vostra figlia quindicenne che si fa foto indecenti.

Ora cominciate a comprendere le implicazioni? Indipendentemente dallo scenario che avete in mente, questa informazione facilmente accessibile può diventare pericolosa.

Ho svolto un lavoro con il mio team in cui ci era stato assegnato il compito di eseguire un'indagine OSINT e di attaccare un obiettivo di alto livello nel campo della Difesa. L'obiettivo non era quello di violare quel personaggio, ma di verificare il suo livello di resistenza all'invito a intraprendere un'azione che non avrebbe dovuto intraprendere. Per scopi didattici, dovevamo registrare tutte le chiamate fatte e tutti i clic.

Una leggera attività di OSINT ci portò alle sue pagine nei *social media*. Ci imbattemmo nel suo account e scoprimmo che era un prolifico tweeter e che adorava usare il suo nuovo iPhone con il GPS acceso. Perché questo è così importante? Twitter ci permise di tracciare la sua posizione per tutto il giorno, mentre twittava da ogni luogo in cui si trovava. Nel giro di poche ore, sapevamo quanto segue:

- il posto in cui amava ordinare il caffè ogni mattina;
- la palestra in cui andava prima di tornare a casa;
- due dei suoi ristoranti preferiti;
- il suo indirizzo di casa;
- quanto odiasse il traffico cittadino.

C'era anche molta più OSINT, ma le informazioni dell'elenco precedente diventarono cruciali per i nostri attacchi. Innanzitutto, trovammo un dominio che era quasi identico (tranne una lettera) al dominio della sua palestra. Creammo una e-mail che diceva che stavamo aggiornando tutti gli account e che i dati della sua carta di

credito non risultavano validi. Gli domandammo di “accedere per inserire i dati della sua carta di credito”, cosa che lo ha spinto a fare clic molto rapidamente.

Sapendo che la pagina avrebbe prodotto un messaggio 404, aspettammo fino a quando non vedemmo il clic e poi lo chiamammo al telefono. La conversazione andò più o meno così:

Chiamante: Buongiorno. è il signor *Smith*?

Obiettivo: Sì, sono io. Chi parla?

Chiamante: Sono Sarah della Cold Gym. Le abbiamo appena inviato un’e-mail per l’aggiornamento del nostro sistema, ma quell’e-mail aveva un URL errato, quindi volevamo scusarcene. Posso inviarle un nuovo link o, se preferisce, posso prendere direttamente il numero della carta di credito e aggiornarla al volo. Che cosa preferisce?

Obiettivo: Nessun problema, Sarah, ecco il mio numero di carta.

Chiamante: Grazie mille, signor *Smith*! Ci rivediamo stasera!

Questo attacco funzionò perché sfruttava argomenti familiari, ed è stato credibile. Con solo un po’ di OSINT, un *phishing* e una chiamata, avevamo un clic, un numero di carta di credito e altri cinque vettori pronti nel caso in cui ne avessimo bisogno.

I metadati sono potenti e molto utili per un ingegnere sociale, quindi suggerisco di controllarli per ogni file che ricavate da un’attività di OSINT.

Ciò può essere scoraggiante, soprattutto quando si ha a che fare con un gran numero di file. Personalmente, per semplificare questo lavoro, cerco di utilizzare strumenti come FOCA (`www.elevenpaths.com/labstools/foca/index.html`) e Maltego (`www.paterva.com/web7`).

Anche se ho promesso di non approfondire troppo l’uso di questi strumenti, ritengo sia imperativo almeno trattare brevemente questi e altri due strumenti utili, cosa che farò nel prossimo paragrafo.

Strumenti del mestiere

Come ho detto nel Capitolo 1, ho deciso di non concentrarmi troppo sugli strumenti, perché cambiano con troppa frequenza.

Tuttavia, ci sono quattro strumenti che sono rimasti nella mia cassetta degli attrezzi negli ultimi cinque o dieci anni e ho pensato che sarebbe stato sbagliato da parte mia non menzionarli nemmeno. Sebbene questi strumenti siano rimasti in circolazione per molto tempo, hanno subito modifiche all'interfaccia e alle funzionalità. Se dovessi dedicare troppo tempo a esaminare ogni loro funzionalità, le informazioni sarebbero obsolete già nel momento in cui acquisterete questo libro. Vi indicherò, invece, i siti web di tali strumenti, dove potete ottenere tutorial e aggiornarvi con i loro sviluppi. Questo sarà un tour veloce, ma è una parte essenziale e imperdibile del puzzle che stiamo componendo.

SET

Ricordo di aver chiacchierato con il mio buon amico David Kennedy. Gli stavo raccontando del mio desiderio di avere uno strumento che mi permettesse di eseguire il phishing di qualcuno e di inviargli automaticamente un carico utile, per sottrargli le credenziali o clonargli la pagina web. La risposta di Dave fu: "Penso di poterlo fare".

Neppure ventiquattro ore dopo aveva un prototipo. Da quel momento in poi, Dave si occupò di quello che è stato chiamato SET, *Social Engineers Toolkit*, come se fosse una missione.

Sviluppa sempre nuovi aggiornamenti – quasi quotidianamente – e offre funzionalità che fanno sembrare ingenue tutte le mie piccole idee. è uno strumento incredibile che al momento ha oltre due milioni di download.

Potete scaricarlo, insieme alle istruzioni, da: https://www.trustedsec.com/social-engineer-toolkit-set/.

IntelTechniques

D'accordo, questo non è davvero uno "strumento" di per sé, ma più una raccolta di sorprendenti motori di ricerca raccolti dal mio buon amico Michael Bazzell.

Michael è un esperto in vari campi, ma ce ne sono due che davvero conosce in tutti i dettagli: trovare persone su Internet e nascondervi dalle persone che vi cercano su Internet. Una volta Michael mi disse che per acquistare beni da Amazon, avrei fatto bene a creare una società fittizia in Messico, così da fare in modo che i dati delle carte di credito non rimandassero a me.

Michael ha creato un'incredibile raccolta di strumenti per la ricerca di qualsiasi cosa: account di *social media*, numeri di telefono, indirizzi IP e persino immagini. Potete trovare questi strumenti su https://inteltechniques.com/menu.html e vi suggerisco di dedicare un po' di tempo a quel sito.

FOCA

FOCA è l'acronimo di Fingerprinting Organizations with Collected Archives. Nel lontano DEF CON 18 nel 2010, un piccolo gruppo di hacker brasiliani ha rilasciato uno strumento che ha gettato lo scompiglio in Internet.

A oggi, non c'è *nient'altro* come FOCA nel mondo. è uno strumento per Windows che ha attraversato alti e bassi nel corso degli anni. A un certo punto ho smesso di usarlo, perché per un po' di tempo non sono state emesse nuove versioni e non c'era modo di contattare la persona che se ne occupava (e lo strumento non è *open-source*).

Poi quelli di ElevenPaths sono subentrati nello sviluppo del progetto. Hanno prodotto un aggiornamento e lo hanno pubblicato sul loro sito web all'indirizzo `https://www.elevenpaths.com/labstools/foca/index.html`. Purtroppo, FOCA è ancora solo per Windows, ma se non utilizzate Windows, vale la pena di creare per lui una macchina virtuale.

La velocità con la quale FOCA trova file e vi estrae metadati utili è sorprendente. Provatelo.

Maltego: il "nonno" di tutti gli strumenti

A costo di sembrare interessato a pubblicizzare Maltego, dico che *adoro* questo strumento. Ma davvero! Quelli di Paterva fanno qualcosa che si vede raramente: producono uno strumento incredibile, rilasciando una versione limitata gratuita (che però è altrettanto incredibile) e mantenendo sempre aggiornata la versione commerciale, che quindi è sempre proiettata in avanti e molto usabile.

Che cos'è Maltego, vi chiederete? È uno strumento che vi aiuta a raccogliere dati da fonti online producendo un grafico interattivo per visualizzarli. Può aiutarvi a catalogare, registrare, investigare e creare collegamenti con fonti di intelligence pubbliche.

Maltego rende il mio lavoro molto più semplice di quanto lo sarebbe altrimenti e lo strumento è anche facile e perfino divertente da usare. Inoltre, quelli di Paterva (la società che produce Maltego) offrono incredibili video e corsi di formazione. Infine, Maltego è disponibile per ogni piattaforma.

Potete provarlo e scaricarlo direttamente dal sito web di Paterva all'indirizzo `www.paterva.com/web7/downloads.php#tab-2`. Vi suggerisco di iniziare con Maltego Classic.

Riepilogo

La conoscenza è certamente potere e non esiste fonte di conoscenza migliore sui vostri obiettivi dell'OSINT. Seguendo i principi di questo capitolo, esercitandovi e affinando le vostre abilità, potrete diventare veri maestri e scovare su Internet anche i dettagli nascosti più minuti.

Avete svolto tutto l'OSINT. Avete catalogato, raccolto e documentato ogni informazione in modo articolato. Pensate di aver trovato l'elemento che sarà il vostro vettore e ora dovete iniziare a preparare il vostro pretesto. In quale modo l'analisi dei dati che avete trovato e la ricerca degli indicatori chiave relativi allo stile di comunicazione del target vi saranno utili? Questo è l'argomento del prossimo capitolo.

Profilare le persone attraverso la comunicazione

> Per comunicare in modo efficace, dobbiamo renderci conto che siamo tutti diversi nel modo in cui percepiamo il mondo, e usare questa conoscenza come guida per comunicare con gli altri.
> - *Tony Robbins*

Quando scrissi *Social Engineering: The Art of Human Hacking* (Wiley, 2010), parlai a lungo con Chris Nickerson, proprietario di Lares Consulting, di modellazione della comunicazione. È piuttosto in gamba e ha una profonda conoscenza dell'argomento.

Mi ha davvero aiutato ad approfondire l'argomento e a capire alcuni dei modi in cui la comunicazione viene utilizzata nell'ingegneria sociale. In buona sostanza, potete ridurre la modellazione della comunicazione ai seguenti elementi chiave:

- c'è sempre una fonte;
- c'è un messaggio;
- c'è un canale;
- c'è un ricevitore.

In assenza di uno di questi elementi, non si ha comunicazione. I modelli di comunicazione Shannon-Weaver e Sender-Message-Channel-Receiver (SMCR) di Berlo impiegano principi simili.

Approfondimenti

Nel 1947, Claude Shannon e Warren Weaver svilupparono il modello di comunicazione Shannon-Weaver, “il padre di tutti i modelli”. Quindici anni dopo, David Berlo ampliò questo modello e creò lo strumento di modellazione delle comunicazioni SMCR. Successivamente, D. C. Barnlund unì e semplificò questi strumenti, sviluppando un modello di comunicazione valido ancora oggi. La teoria di Barnlund è inclusa nel Capitolo 4 del libro *Communication Theory*, *Second Edition* (Routledge, 2008).
Ecco il riferimento: https://www.taylorfrancis.com/books/e/9781351527538/chapters/10.4324%2F9781315080918-5.

Indipendentemente dal modello con il quale avete familiarità, una delle cose che ho appreso nel corso degli anni è che non è importante quale modello impiegare. Lo so, lo so: alcuni di voi probabilmente sentiranno l’impulso di bruciare questo libro, ma ora vi spiego perché sostengo questo.

Se applicate i principi di questo libro allo stabilire un legame, all’influenza, alla profilazione della comunicazione e così via e la persona con la quale state comunicando riceve il messaggio, tutto funzionerà. Se applicate questi principi nel modo in cui la persona con la quale state comunicando desidera essere coinvolta, la comunicazione andrà esattamente come desiderate.

Sì, mi rendo conto che è un’affermazione audace e non voglio dire che la cosa sia semplice.

Può essere complicato. Spesso, ci dobbiamo arrivare a modo nostro. Per esempio, io sono un comunicatore molto diretto. Per questo motivo non mi dispiace quando qualcuno mi fa notare che quello che ho fatto non era il modo migliore (però dovete dirmi come migliorare). Tendo a comunicare in questo modo anche con gli altri, il che può causare dei problemi quando comunico con una persona che non apprezza la sincerità.

Non è facile cambiare al volo profilo di comunicazione, anche se per alcune persone è più facile che per altre. Il problema nasce quando

ci sentiamo a nostro agio e rilassati, perché il nostro cervello tende a scatenare tutte quelle reazioni chimiche che vogliamo indurre nel nostro obiettivo e quelle reazioni possono farci ricadere nella nostra "zona di comfort".

Permettetemi di illustrarvelo in questo modo: vi ricordate quando da giovani (o da adulti) avete provato per la prima volta qualcosa di nuovo? Un nuovo tipo di cibo, per esempio. Quando i miei figli erano piccoli, io e mia moglie li incoraggiavamo ad assaggiare sempre qualcosa almeno una volta. Non dovevano per forza farselo piacere o finirlo, ma dicevamo loro che non potevano esprimere un giudizio se *non* lo assaggiavano.

Un anno andammo a Hong Kong. Ci recammo in un ristorante e mia figlia notò nel menu un piatto che la incuriosiva: era indicato come "Whole Pigeon" (piccione intero) e mi chiese di provarlo. Il mio primo pensiero fu quella di dirle: "Davvero? Quello stupido uccello?". Ma mi ricordai della nostra idea di incoraggiare i bambini ad assaggiare cose nuove.

Mia figlia ordinò il piccione, poi mi guardò e disse: "Bene papà, e tu che cosa provi, di nuovo?". Mi ero sempre sentito incuriosito dai cetrioli di mare, anche se non ero sicuro di volerli mangiare. Ma sembrano innocui, giusto?

La Figura 3.1 mostra mia figlia mentre mangia il suo piccione, ma non ho un'immagine che possa mostrarvi che cosa successe quando mangiai il cetriolo di mare. Sostanzialmente si tratta di grosse lumache che vivono nell'oceano, quindi usate la vostra immaginazione.



Figura 3.1 Sì, c’era anche la testa del piccione.

Che cosa ha a che fare questo aneddoto sulle abitudini alimentari della mia famiglia a Hong Kong con la modellazione della comunicazione? Bene, non appena assaggiai quella cosa così “diversa” (ma direi, piuttosto, disgustosa), andai alla ricerca di qualcosa di molto, molto più “domestico”. Perché? Perché era familiare e confortevole.

La comunicazione ha un funzionamento molto simile. La prima volta che si esce dalla zona di comfort per provare qualcosa di nuovo, ci si può sentire a disagio e sentirsi spinti a rientrare nella zona di comfort, specialmente se l’esperienza non è gradevole. Tuttavia, è importante non rimanerci, nella zona di comfort. Più provate qualcosa, più è probabile che essa entri a far parte del vostro arsenale di strumenti.

Curiosità
Ho provato i cetrioli di mare per quattro volte e ogni singola volta erano disgustosi come la prima. Questo fatto non riguarda la modellazione della comunicazione, ma ho pensato che vi avrebbe fatto piacere saperlo.

Per aiutarvi a padroneggiare la comunicazione come ingegneri sociali, in questo capitolo tratterò i seguenti componenti chiave:

- imparare a capire che cosa pensa una persona quando la avvicinate;
- conoscere il sistema DISC;
- imparare a modellare il vostro stile DISC;
- usare il sistema DISC a vostro vantaggio.

Nei prossimi capitoli del libro, alcune tecniche sono indipendenti le une dalle altre, mentre in questo capitolo tutte le tecniche sono legate fra loro e sono importanti. Cominciamo col cercare di capire quello che una persona pensa durante l'approccio.

L'approccio

Quando tengo il mio corso avanzato di cinque giorni di ingegneria sociale, inevitabilmente molti allievi hanno un problema in un campo ben preciso: l'approccio.

Sono quei primi secondi cruciali di interazione tra voi e uno sconosciuto che stabiliranno il tono di tutto il resto dell'interazione. Vi racconto un episodio particolarmente imbarazzante per chiarire questo punto.

Un giorno, al termine di una lezione, mi trovavo con il mio buon amico Robin Dreeke e un gruppo di allievi. Mi sfidarono a mostrare loro come fosse "facile" approcciare un perfetto sconosciuto. Sentendomi piuttosto euforico a causa di tutta la positività della lezione, della dopamina che scorreva a fiumi avendo insegnato tutto il

giorno e della scarica di adrenalina dell'imminente successo, ero pronto a usare la mia eccezionale abilità per mostrare loro quanto fosse facile essere ingegneri sociali.

Circa sette o otto di noi stavano in piedi nell'atrio discutendo su come avrei condotto l'approccio e Robin disse che mi avrebbe scelto l'obiettivo. Io sono alto 1,90 e Robin scelse un uomo di statura più modesta. Seduto dietro di me l'avrei letteralmente sovrastato. Era accomodato su una seggiola intento a leggere mentre aspettava qualcuno.

Ora, immaginate la scena e considerate quale poteva sarebbe l'approccio migliore per me. Da dietro? Diamine no! L'avrei spaventato. Ponendomi direttamente di fronte? Neanche: avrebbe dovuto alzare lo sguardo, tendendo il collo e quel disagio non lo avrebbe predisposto a una buona conversazione. Voi cosa fareste? Pensateci un attimo.

Ebbene, dopo che Robin mi ebbe indicato l'obiettivo, mi voltai senza pensarci e dissi (nel mio forte accento newyorkese): "Ehi, come va?! Posso farti una domanda veloce?".

Il tipo era rimasto talmente sorpreso dal modo in cui mi sono voltato e dalla mia introduzione rumorosa che si poggiò troppo indietro sulla sedia, perse l'equilibrio e cadde. Mi precipitai al suo fianco, imbarazzato e temendo che si fosse fatto male. Senza riflettere, gli dissi: "Lascia che ti aiuti". Era molto più leggero di quanto mi aspettassi e presi sia lui che la sedia, ma applicai troppa forza e lo mandai in avanti, steso sul pavimento.

Lui alzò lo sguardo e urlò: "Lasciami in pace! Ma che *diamine* hai in testa?!" (lui in realtà non utilizzò esattamente la parola *diamine* e la rabbia nella sua voce era estrema).

Mi voltai e dissi: "Sono davvero desolato, signore". Tornai nell'atrio vergognandomi, mentre il gruppo di allievi mi prendeva in giro. Robin

se la stava ridendo di gusto, tanto da avere le lacrime agli occhi: ero sconfitto.

Anni di esperienze come queste, con tonnellate di storie di questo tipo, mi hanno aiutato a definire qualcosa che ha letteralmente cambiato il modo in cui visualizzo le comunicazioni. Che cosa pensate si aspetti una persona con la quale state per comunicare affinché possa sentirsi a proprio agio e rilassata? Pensateci.

Immaginate di essere per strada e di vedere qualcuno che sta camminando proprio verso di voi e sta pensando di interagire con voi. Che cosa pensate in quel momento? Le mie esperienze mi hanno aiutato a identificare i seguenti quattro pensieri.

- Chi sei?
- Che cosa vuoi?
- Sei una minaccia?
- Quanto ci vorrà?

Quando vi avvicinate a qualcuno, se riuscite a rispondere a queste quattro domande entro i primi 5 o 10 secondi, potete cambiare il modo in cui procederà l'intera interazione. Questa informazione prepara il terreno per molte parti di questo libro, quindi metti un segnalibro in questa pagina perché vi farò riferimento spesso. Questi quattro fattori entrano in gioco anche nei seguenti argomenti, che tratto nei prossimi capitoli.

- Il vostro pretesto (Capitolo 4).
- Le prime parole pronunciate (Capitolo 5).
- Il linguaggio del corpo e le espressioni facciali (Capitolo 8).

Il grafico della Figura 3.2 vi aiuterà a ricordare questi quattro punti.



Figura 3.2 Questi quattro punti sono cruciali per le comunicazioni.

Non sto dicendo che ogni essere umano pensi a quelle domande con quelle esatte parole ogni volta che qualcuno gli si avvicina, ma queste solo le preoccupazioni, i pensieri o i timori tipici di una qualsiasi persona. Se voi (come “mittente” della comunicazione) siete in grado di rispondere a questi quattro punti già durante l’approccio, metterete il destinatario a proprio agio e gli permetterete di rilassarsi.

I truffatori conoscono bene questi fatti e usano varie tecniche per far rilassare il loro obiettivo prima di giungere a fare richieste (il vero scopo dell’interazione). Capire questo fatto non solo vi renderà più efficaci come ingegneri sociali, ma vi aiuterà anche a proteggervi quando qualcuno cercherà di usare queste tecniche contro di voi.

Il primo passo è comprendere qual è il vostro stile di comunicazione. È qui che facciamo la conoscenza di uno strumento di profilazione della comunicazione molto semplice, ma potente.

Il sistema DISC

William Moulton Marston nacque nel 1893. Conseguì la laurea ad Harvard a soli 22 anni, tre anni dopo conseguì la laurea in legge alla Harvard Law School e solo tre anni dopo la laurea in psicologia, sempre ad Harvard. Poi trovò lavoro come insegnante presso la American University.

Durante i suoi anni di studio ad Harvard, compì ricerche sulla relazione esistente fra il mentire e la pressione arteriosa. Nel 1915 costruì una macchina per misurare le variazioni di pressione arteriosa di un soggetto sottoposto a interrogatorio.

Nel 1917 Marston pubblicò le sue scoperte e da quello – come avrete indovinato – nacque il poligrafo. Negli anni Venti e Trenta, fu molto attivo come docente e consulente del governo. Era l'unico, a quel tempo, a interessarsi non tanto alla psicologia patologica, quanto al comportamento di un'intera popolazione di persone.

Nel 1928 pubblicò un libro intitolato *Emotions of Normal People* e nel 1931 ne pubblicò un altro intitolato *Integrative Psychology: A Study of Unit Response*. Fu da queste opere che Marston elaborò il sistema DISC. Stava cercando dei modi per misurare l'energia dei comportamenti e della consapevolezza. Anche se non ideò il test di cui parlo in questo capitolo, sviluppò un modello che poi applicò lavorando per la Universal Studios nel 1930. Volevano effettuare la transizione dal cinema muto a quello sonoro e il lavoro di Marston fu fondamentale per trovare i gesti e le espressioni facciali più naturali.

Curiosità
Marston era un grande sostenitore dei diritti delle donne e del potere alle donne. Da giovane, mentre studiava i classici greci e latini, si interessò alla fusione tra quegli studi e i diritti delle donne. Sono state queste passioni a portare Marston a sviluppare l'eroina Wonder Woman, grazie alla quale nel 2006 è stato inserito nella Comic Book Hall of Fame.

Il lavoro di Marston ha cambiato il modo in cui oggi guardo all'ingegneria sociale. Sono in molti a cercare di capire come profilare

psicologicamente qualcuno in modo veloce, ma trovo particolarmente efficace, quantomeno per me, l'approccio semplice di Marston. Non sono uno psicologo, quindi non sono in grado di capire il vostro profilo psicologico. Ma sono un ingegnere sociale, quindi per me capire come comunicate è come avere la chiave di un lucchetto.

Che cos'è il sistema DISC?

DISC è un acronimo. Si usano vari descrittori diversi, ma questi mi sembrano i più appropriati.

- *D*: diretto, dominante.
- *I*: influencer.
- *S*: di supporto, sostenitore.
- C: coscienzioso, conforme.

Ognuno di questi punti descrive il modo in cui viene rappresentato lo stile. Spesso, il sistema DISC viene rappresentato graficamente. Io uso quella mostrata nella Figura 3.3.

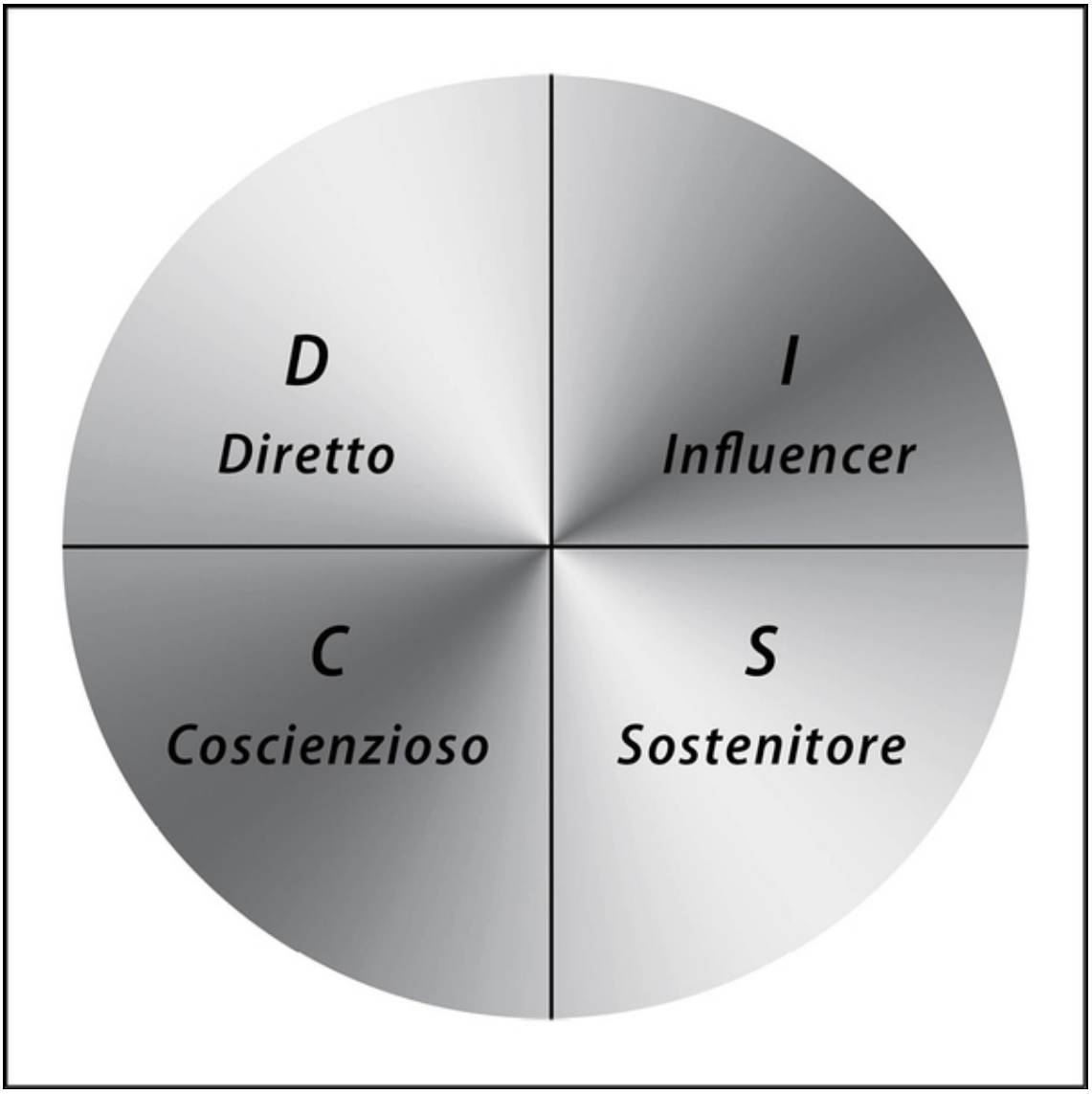


Figura 3.3 Definizione del sistema DISC.

Ognuno di questi stili di comunicazione è rappresentato in modo specifico, e ci aiuta a prevedere i comportamenti. Usando il sistema DISC, scoprirete che le persone sono prevedibilmente differenti.

Diciamo che avete a che fare con un comunicatore *D*, diretto. Un comunicatore diretto può essere chiassoso e rumoroso; ma un altro può essere più tranquillo e più fermo; un terzo potrebbe essere una via di mezzo fra i due. Ma nonostante queste differenze, tutti comunicano in modo diretto e schietto. Di conseguenza, se riuscite a profilare

rapidamente la persona, potete adattare il vostro stile di comunicazione per influenzarla meglio.

Ci sono sempre alcune domande su questo argomento che sorgono durante i miei corsi. Ecco due delle più comuni.

- *Domanda*: “Come faccio a sapere qual è il mio stile preferito?”. Bella domanda, ma non esiste una risposta semplice, quindi me ne occupo nel prossimo paragrafo.
- *Domanda*: “Posso adottare più stili? O un mix di due stili?”. Sì, tutti noi abbiamo dei punti di forza in più di uno stile, ed è possibile essere particolarmente abili in più di uno stile. Alcune persone si collocano all’intersezione fra due stili, ed è anche possibile cambiarli un po’ nel corso del tempo.

Anche se questo metodo di valutazione è molto accurato, tenete presente che qualsiasi valutazione come questa non è sempre efficace al 100% (almeno secondo me). È soggetta ad adattamenti in base al modo in cui una persona risponde e alla situazione specifica.

Penso che questo sia uno degli strumenti che dovrete adottare come ingegneri sociali professionisti e che vi aiuterà ad avvicinarvi veramente alle abilità dei veri professionisti.

Prima di addentrarci nel modo in cui usare il sistema DISC come ingegneri sociali, introduco quella che forse è la parte più importante di questo libro: capire qual è il vostro stile di comunicazione.

Conoscere se stessi è l’inizio della saggezza

Questo titolo non è uno strano enigma; è un concetto fondamentale per capire davvero come funziona la profilazione della comunicazione. Prima di poter diventare maestri nella comunicazione con gli altri, è essenziale che capiate prima di tutto voi stessi. Mi spiego.

Uno chef ha vari coltelli in cucina. Coltelli da 10, da 20 e da 25 cm. Ognuno ha una forma e un peso differente e ha un utilizzo differente. La Figura 3.4 mostra vari tipi di coltelli. Quale coltello pensate sia il migliore per aprire un cavolo?

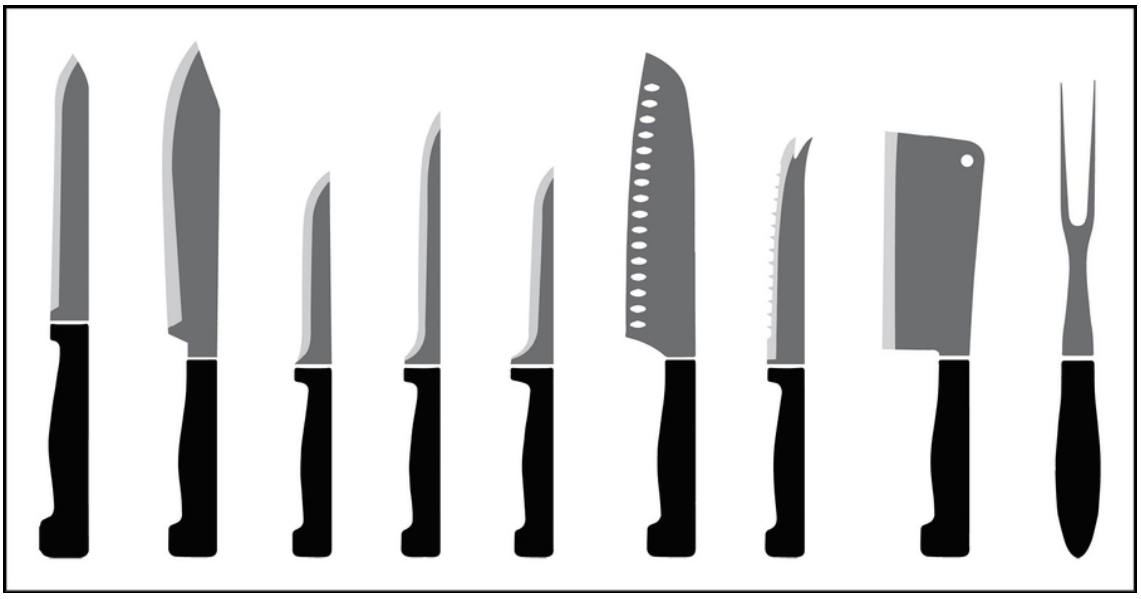


Figura 3.4 Scegliete accuratamente.

Io sceglierei il sesto coltello, perché ha il peso necessario per tagliare un vegetale coriaceo e ha la lunghezza necessaria per attraversarlo tutto, facilitando quindi il taglio per le braccia e il polso. Ho però visto alcune persone scegliere il quarto o il quinto coltello per tagliare il cavolo e indovinate che cosa è successo? Dopo pochi minuti, avevano le mani e i polsi doloranti – senza parlare del rischio di tagliarsi. La conoscenza dello strumento migliore per un certo lavoro, del suo utilizzo corretto e dei suoi punti di forza e di debolezza, permette di scegliere lo strumento più adatto al lavoro.

Il sistema DISC è un po’ la stessa cosa. Alcuni profili funzionano meglio per svolgere determinati compiti rispetto ad altri. Conoscere il vostro stile può aiutarvi a farvi capire meglio quali sono i vostri punti di forza e quali le vostre debolezze. Può aiutarvi a imparare a comunicare con maggiore chiarezza i vostri pensieri e le vostre

intenzioni. Può anche aumentare notevolmente la vostra possibilità di non essere rifiutati dalla persona con la quale state comunicando, che, come ingegneri sociali, è una parte molto importante del vostro lavoro.

Vi sono alcuni modi in cui posso aiutare gli altri a conoscere il proprio stile di comunicazione dominante, ma principalmente mi baso su uno strumento di valutazione DISC, che aiuta la persona in questione a conoscere facilmente se stessa. Ma un attimo! Prima di precipitarvi sul browser per cercare “valutazione DISC gratuita”, lasciate che vi dica perché questa potrebbe non essere la migliore soluzione.

Molte valutazioni online che ho visto all’opera utilizzano un metodo imperfetto. Propongono una frase e poi vi chiedono di rispondere a una serie predefinita di domande riguardanti quella situazione. Ecco un esempio.

Immaginate di essere il capo di Chris e che lui si sia rivoltato contro di voi. Che cosa dovreste fare?

- Licenziarlo in tronco.
- Fare una battuta sull’accaduto e andare avanti.
- Convocarlo e spiegargli in dettaglio perché quello che ha fatto è sbagliato.
- Cercare di aiutarlo a capire perché il suo atteggiamento non è positivo per il team.

Il problema di domande come questa in una valutazione DISC è che potreste non avere alcun contesto in base al quale rispondere. Che cosa succede se non avete mai avuto sottoposti? Che cosa succede se non avete mai dovuto gestire una persona dal carattere ribelle? Ci sono troppe variabili che rendono questa domanda una pessima domanda e che possono portare a risultati inaccurati.

Se state cercando un test di valutazione, vi incoraggio a cercarne uno che vi fornisca delle scelte fra più parole e che vi chieda di

scegliere quella che ritenete più affine e quella che ritenete più distante da voi, e che non si accontenti dello scenario del test. Ecco un esempio.

Dal seguente elenco di parole, *scegliete* quella che vi descrive di più e quella che vi descrive di meno. Anche se non provate sentimenti molto forti nei confronti di queste parole, una vi descriverà di più e una di meno, a seconda del vostro atteggiamento personale.

PIÙ	MENO
Logico	Logico
Serio	Serio
Obbediente	Obbediente
Indipendente	Indipendente

Con le frasi, siete costretti a immaginare una situazione che non avete mai vissuto, il che può essere davvero difficile per molti. Questo è il motivo per cui preferisco consigliare valutazioni che utilizzano coppie di parole. Questo tipo di valutazioni offre un risultato più accurato.

Spesso chiedo ai miei allievi di rispondere a ciascuna domanda pensando al modo in cui si comportano *al lavoro*, che spesso è molto differente da quello che adottano a casa. Di conseguenza, ottengo una rappresentazione coerente e onesta del loro profilo di comunicazione.

Sfortunatamente, non posso predisporre un test di valutazione DISC per ogni lettore di questo libro, quindi devo essere un po’ creativo nell’aiutarvi a capire quale possa essere la sua efficacia.

Osservate la Figura 3.5.

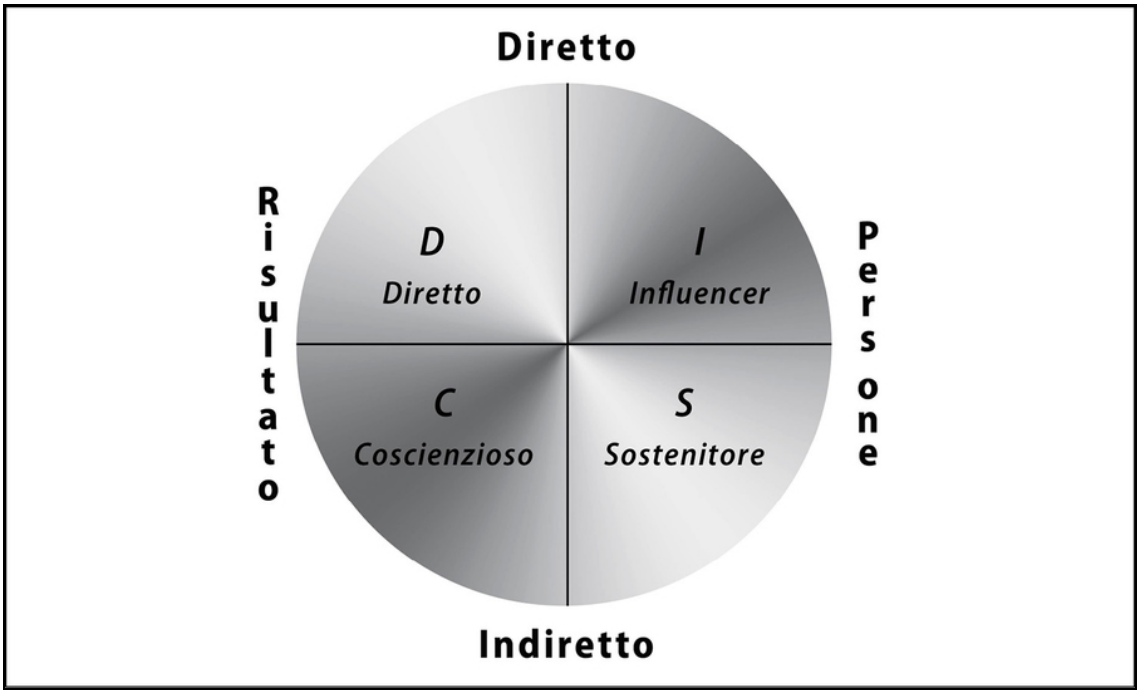


Figura 3.5 Comprendere DISC.

Mentre vi concentrate sulle parole poste all'*esterno* del cerchio (ignorando per il momento le parole che si trovano all'interno del cerchio), rispondete onestamente a queste due domande.

- Nel vostro stile di comunicazione siete più diretti o indiretti? *Fermi un attimo!* Prima di rispondere, devo ricordarvi che non vi sto chiedendo che cosa pensate che *gli altri* pensino di voi. Vi sto chiedendo di valutare onestamente se vi sentite più diretti o più indiretti. Arrivate al punto rapidamente o vi prendete tempo? Avete un problema con l'essere diretti o vi piace? Ora, in base alle vostre risposte, scrivete "Diretto" o "Indiretto" come stile di comunicazione.
- Siete più orientati al risultato o alle persone? Quando siete impegnati in un lavoro, vi concentrate più sullo svolgerlo o più sulle persone che vi aiuteranno a farlo? In base alla vostra risposta a questa domanda, scrivete "Risultato" o "Persone".

Se dovessi fare io questo test, scriverei “Diretto” e “Risultato”. Nella Figura 3.5, lo spicchio tra Diretto e Risultato è quello con la D: *Diretto*. Vedete quanto è veloce il test?

Ora provate a valutare voi stessi. Come è andata? Per maggiori dettagli, osservate la Figura 3.6.

Usando me stesso come esempio, mi colloco nella sezione *D* e trovo che sono diretto, orientato ai risultati, deciso, con forza di volontà e forte. Queste parole mi descrivono perfettamente (perfino troppo). Ma qual è il significato di ciò?

Io preferisco adottare uno *stile di comunicazione* diretto. Ricordate: questo non è un profilo psicologico, ma solo un profilo di comunicazione. E capire qual è il proprio significa poter vedere più chiaramente dove poterlo modificare per influenzare meglio il vostro obiettivo.

Ora che avete risposto alle due domande del test, dovreste avere una valutazione piuttosto precisa di voi stessi. Ma che cosa significa questo quando si tratta di profilare altre persone? E come potete usare questa informazione?

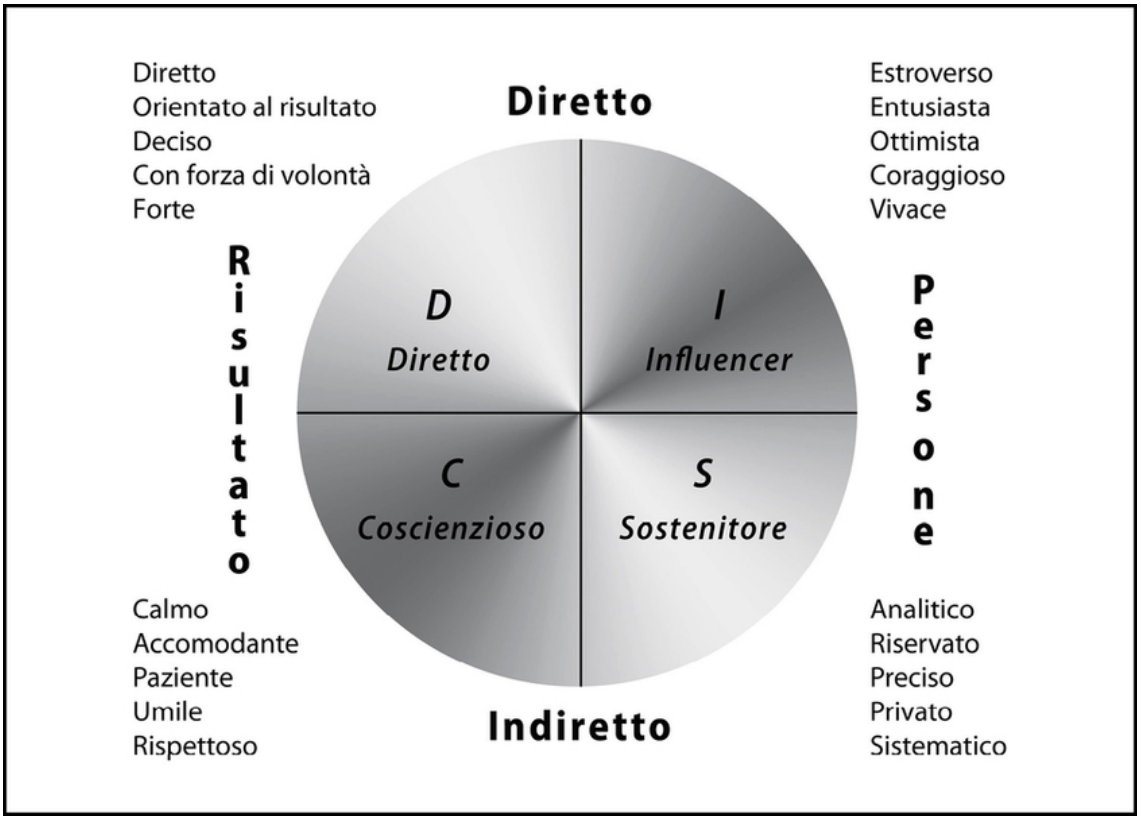


Figura 3.6 Il sistema DISC in dettaglio.

Sfruttare il sistema DISC

Il profilo DISC è talmente efficace che il mio team lo adotta per i *social media*, le chiamate vocali e persino per le foto, con un'accuratezza allarmante.

Robin Dreeke mi ha raccontato la storia di un profilo che costruì su un obiettivo usando solo una sua foto. Ecco come è andata.

La foto mostra una via trafficata di città. Si è appena verificato un incidente d'auto. Niente di grave, solo un parafango ammaccato. La strada è piena di gente che corre verso le due vetture per vedere se stanno tutti bene. L'obiettivo volta la schiena all'incidente, senza guardare, le spalle rilassate e le mani in tasca. Questo è tutto.

In base alla descrizione della scena, dove lo collochereste sul diagramma DISC?

Pensate alle domande che vi ho posto. Sulla base della descrizione che vi ho appena fatto della foto, l'uomo è più orientato al risultato o alle persone? È davvero impossibile dire che sia "orientato alle persone", vero? Quindi, la risposta sembrerebbe essere che è orientato al risultato.

È diretto o indiretto? Mentre tutti gli altri si stanno concentrando sull'incidente, mostra una decisa mancanza di immediatezza. Robin ha supposto che fosse una persona indiretta.

Questo collocherebbe l'obiettivo nel segmento in basso a sinistra, *C*, nel grafico della Figura 3.6: un tipo analitico, riservato, preciso, privato e sistematico. Si stava dirigendo da qualche parte e quell'incarico aveva la precedenza su qualsiasi altra cosa. Il suo linguaggio del corpo non mostrava né estroversione né forza, il che lo collocava ancor più accuratamente nella regione *C*.

Questo ha finito per essere il profilo scelto da Robin e se leggete il suo libro *It's Not All About "Me": The Top Ten Techniques for Building Quick Rapport with Anyone*, scoprirete esattamente come è andata a finire (suggerimento: ha avuto successo).

Ho formato persone in modo che imparassero a svolgere questo tipo di valutazioni in pochi minuti, concentrandosi solo sui quattro aspetti del sistema DISC e collocando la persona nel quadrante giusto. Ma che cosa succede se non potete rispondere perfettamente a tutte le domande?

Mettere all'opera il sistema DISC

Immaginate di non poter dire se l'obiettivo è orientato al risultato o alle persone, ma di sapere che è più diretto che indiretto. Potete ancora

comunicare efficacemente con lui se è una persona diretta, anche se rientra nella categoria dei Coscienziosi o dei Sostenitori.

Lo stesso varrebbe se sapeste che rientra nella categoria Risultato e non nella categoria Persone. Potete comunicare con lui applicando le categorie *D* o *C* meglio che applicando la categoria *S*. Vedete come funziona?

Ecco un piccolo test. Date un'occhiata alla pagina Twitter del nostro vecchio amico Nick Furneaux, su `https://twitter.com/nickfx?lang=en`.

NOTA

Nick non è molto prolifico in termini di tweet. Per questo motivo, potreste dover riflettere un po' per svolgere questo esercizio.

SUGGERIMENTO

È importante non perdersi nei retweet, in questo caso. I retweet non offrono un quadro preciso dello stile di comunicazione della persona. Tendo a considerare solo i media e i tweet che una persona pubblica da sé.

Diresti che Nick è un tipo più concentrato sul risultato o sulle persone? Provate a leggere i suoi tweet e a scoprire dove puntano i suoi commenti. Li leggo e penso che miri al *risultato*, ne sono sicuro. Ora… il suo stile è diretto o indiretto? Hmm… questo sembra un po' più difficile.

Date un'occhiata ai post che pubblica. Vedo messaggi molto diretti sulle *cose*, ma non sulle persone. Questo mi conferma che Nick è più un *D*.

Anche se non riuscite a inquadrare qualcuno al 100%, è sufficiente avvicinarsi all'idea. Nel caso di Nick, potete vedere che è sicuramente focalizzato sul risultato piuttosto che sulle persone. Così supponete che potrebbe essere un *D* o un *C*.

Un altro segreto è controllare i descrittori usati dalla persona. Tornate alla Figura 3.6 e guardate i descrittori associati a *D* e a *C*. Quali parole descrivono meglio quello che trovate nei tweet di Nick? È

più diretto, energico e orientato ai risultati? O è più preciso, privato e sistematico?

Dopo aver letto questi tweet, certamente vedo più un *D* che un *C*. Questo significa che Nick è al 100% un comunicatore di tipo *D*? Non esattamente: a volte le persone comunicano in un certo modo a seconda di dove, come e con chi stanno comunicando. Per esempio, quando insegno, tendo a comunicare più come un *I* che come un *D*. È meglio per me, meglio per gli allievi e meglio per tutti coloro che sono coinvolti. Se volete influenzarmi, dovete scoprire in quale modo comunico nel contesto in cui state cercando di influenzarmi.

Siete confusi? Non pensateci troppo. Ricordate: questa è una freccia della vostra faretra, che vi aiuta ad avvicinarvi all'obiettivo nei primi istanti della conversazione.

Tornando al nostro esempio: ora che avete profilato Nick come un *D*, come potete utilizzare queste informazioni a vostro vantaggio? Per rispondere a questa domanda, dovete prima capire come comunicare all'interno di ogni stile, indipendentemente dal fatto che si parta da una posizione di autorevolezza.

Il comunicatore D

Se state per comunicare usando il pretesto dell'autorevolezza:

- siate diretti e schietti;
- stabilite confini netti;
- siate brevi e concisi
- rispondete al *cosa*.

Se state per comunicare usando un pretesto più sommesso:

- sottolineate il *cosa*, non il *come*;
- fornite opzioni, ma date risalto al risultato;
- concentratevi sulla logica;

- accordatevi su fatti e posizioni, non solo sulla persona.

Il comunicatore I

Se state per comunicare usando il pretesto dell'autorevolezza:

- siate amichevoli e rilassati;
- permettete all'altra persona di condurre la discussione;
- aiutate a tradurre in azione le loro idee;
- rispondete al *chi*.

Se state per comunicare usando un pretesto più sommesso:

- sottolineate quanto c'è di nuovo e speciale;
- indicate i vantaggi e gli svantaggi;
- non dominate;
- citate "esperti" e testimonianze.

Il comunicatore S

Se state per comunicare usando il pretesto dell'autorevolezza:

- siate sistematici e obiettivi;
- siate rilassati e amichevoli;
- usate la coerenza e rispondete al *perché*;
- definite chiaramente che cosa state chiedendo.

Se state per comunicare usando un pretesto più sommesso:

- siate pazienti;
- ponete domande basate sul *come*;
- concentratevi sulla squadra.

Il comunicatore C

Se state per comunicare usando il pretesto dell'autorevolezza:

- siate dettagliati;
- siate affidabili;
- siate riconoscenti;
- rispondete a domande basate sul *come*.

Se state per comunicare usando un pretesto più sommesso:

- utilizzate dati e statistiche;
- fornite logica e fatti;
- ponete l'accento sull'affidabilità.

Utilizzando le descrizioni di ciascuno di questi stili di comunicazione, fate un po' di esercizio. Supponendo che Michele sia *I* e che io sia *D*, che cosa devo cambiare in me per influenzare Michele? Potete svolgere questo esercizio anche pensando al vostro stile e decidere che cosa avete bisogno di modificare per influenzare Michele.

Dovrei essere breve, concreto e pertinente, ma Michele preferisce uno scambio amichevole, con un dare-e-prendere, che non sia eccessivamente dominante. Vedete dove sorgono i problemi? Devo assicurarmi di poter creare un pretesto che mi permetta di colpire quei punti che accontenteranno Michele e mi permetteranno di influenzarla. Per essere un buon *influencer*, dovete pensare soprattutto a quello che l'altra persona pensa quando comunica e meno al modo in cui preferite comunicare voi.

Comprendere i limiti

Tutto questo funziona comunicando di persona, al telefono, in una e-mail o sui *social-media*. Avete solo bisogno di capire lo stile di comunicazione dell'obiettivo, il vostro sistema di consegna e il risultato che volete trarre dalla comunicazione. Da lì in poi, tutto è più facile.

Non pensiate che si tratti di un qualcosa di magico. Ci sono molti fattori che possono contribuire al successo o pregiudicarlo. Solo perché avete profilato l'obiettivo, lo avete valutato correttamente e avete creato un messaggio che lo stimolerà nella sua zona preferita di comunicazione, questo non significa che avrete sempre successo. Basta un malessere, uno stress, un intenso carico di lavoro e molti altri fattori per influenzare le capacità di comunicare in modo efficace con qualcuno. Avete bisogno di prove sul fatto che ci siano dei limiti? Pensate ai vostri figli (o ai figli delle persone che conoscete).

Mia figlia mi può sciogliere il cuore in un nanosecondo. Nonostante la sua capacità apparentemente sovrumana di farmi fare quasi tutto quello che vuole, quando sono sotto stress oppure ho troppe cose da fare, posso essere molto meno paziente e gentile con lei di quanto non lo sia normalmente. Il mio metodo di comunicazione cambia, e questo succede a tutti coloro che hanno a che fare con circostanze esterne.

La pratica rende perfetti, quindi non arrendetevi se non riuscirete ad avere successo la prima ventina di volte. Quando riuscirete a farcela, vi sorprenderete della sua efficacia.

Ecco un'altra storia: quando è stato pubblicato il mio primo libro, mi è stato chiesto di autografarlo. Non me l'aspettavo e rimasi sorpreso della fila di persone che aveva acquistato il mio libro e ora voleva il mio autografo.

Molte persone hanno detto molte belle cose del mio libro e di me. Sono state quanto meno esagerate. Un giorno un giovane mi si avvicinò e mi parlò per un minuto di come il mio libro gli avesse cambiato la vita. Lo aveva aiutato in alcuni momenti difficili e gli aveva persino dato un avviamento al lavoro. Ero talmente sopraffatto, che ricordo chiaramente di aver pensato tra me e me: "Sarà vero o è solo un altro degli scherzi di Dave? Perché mai qualcuno dovrebbe dirmi queste cose sul mio libro?". Gli elargii un piccolo sorriso, lo

ringraziai e gli restituii il libro autografato. Era molto deluso, ma le persone dietro di lui stavano aspettando, così sono andato avanti. Altre quattro o cinque persone si sono aggiunte alla fila e il giovane se ne stava in piedi di lato, e il suo linguaggio del corpo diceva chiaramente che era infelice.

Un altro giovanotto si fece avanti e mi consegnò la sua copia del libro perché la firmassi e mi disse: “È un bel libro, ma ci sono tre o quattro cose che ritengo veramente sbagliate e poi ha citato Wikipedia quattro volte. Non è corretto per un autore”. Lo guardai, gli feci un grande sorriso e gli chiesi di sedersi accanto a me al tavolo, in modo che quando la fila si fosse calmata, mi potesse mostrare dove pensava che avessi sbagliato, nel libro.

Mentre si avvicinava al tavolo per sedersi accanto a me, il primo giovane tornò di corsa. Era ovviamente molto arrabbiato. Mi indirizzò un paio di imprecazioni e mi disse: “Mi sono seduto ad ascoltarla e le ho detto quanto il suo libro ha cambiato la mia vita; le ho detto di essere un suo ammiratore e lei mi ha mandato via come se non le importasse!!!! Ora questo tizio le si avvicina, le dice che il suo libro fa schifo e diventa il suo migliore amico ???!?! E che c…!”.

In quel momento, sinceramente, non sapevo cosa rispondere. Ero sopraffatto dalla sua rabbia, ma lo capivo. Mi scusai e gli chiesi di venire a sedersi per discuterne, ma era troppo sconvolto e così uscì davvero arrabbiato.

Molto più tardi, dopo essermi ripetuto mentalmente all’infinito tutta la scena capii chiaramente cosa fosse successo. Quel giovane era un *I* e stava comunicando con me come farebbe un *I*: in modo energico, estroverso, vivace, amichevole e così via. Il suo stile di comunicazione *I* era talmente intenso che io, un forte *D*, non sapevo come riceverlo, e così tagliai corto e lo congedai. Ma quando il secondo giovanotto mi

sfidò e mi disse come potevo migliorare, il suo stile risuonava in me e volevo saperne di più.

Che cosa avrei potuto fare per risolvere il problema? O, meglio ancora, che cosa avrei dovuto fare per evitare che insorgesse quel problema?

La risposta è: comunicare allo stesso livello della persona. Quando il primo giovanotto si avvicinò con le sue lodi, avrei dovuto:

- chiedergli quale parte del libro l'avesse davvero aiutato;
- fargli i complimenti in modo sincero e realistico.
- ascoltarlo attivamente e poi rimandare la conversazione a un secondo tempo, poiché la fila era lunga.

Queste cose lo avrebbero fatto sentire considerato e speciale, e invece si è arrabbiato perché si è sentito escluso. La morale è che anche quando sbagliate, prendetevi il tempo per riprodurvi in testa l'accaduto e per vedere che cosa potete imparare dai vostri errori.

Riepilogo

DISC è uno strumento potente, che vi può aiutare a stabilire un contatto e a far sì che il vostro obiettivo si fidi di voi e desideri aiutarvi. Imparate a leggere rapidamente la volontà delle persone, e poi imparate ad applicare il vostro profilo e ad adattare il vostro stile in modo da poter comunicare più facilmente con il vostro obiettivo.

Non complicate troppo questo processo. Anche il solo riuscire a collocare una persona entro uno spicchio del cerchio DISC aumenterà drasticamente le vostre possibilità. È importante ricordare che il sistema DISC non è "magico". Non diventerete grandi esperti di modellazione della comunicazione umana da un giorno all'altro (magari mai).

Ma questo non deve essere il vostro obiettivo. Il vostro obiettivo dovrebbe essere quello di focalizzare la conversazione sulla persona – non su voi stessi – e mantenere fluide nella vostra circolazione sanguigna quelle due sostanze chimiche che ho menzionato nel Capitolo 1 (la dopamina e l'ossitocina). In questo modo, conquisterete la fiducia altrui e stabilirete legami, il che renderà più semplice il vostro lavoro di ingegneri sociali.

A questo punto, potreste dire: "Wow, questa è sostanzialmente una ricetta per trasformare le comunicazioni in vere e proprie armi".

Non sbagliate. Per nulla. Il fatto è che molte cose che non erano destinate a essere usate come armi, spesso sono state usate come tali. Un esempio? Le automobili.

Ho un'auto che mi piace molto. Adoro guidarla. è l'auto che ho sempre desiderato e adesso è mia. Quando Audi produsse la vettura, non credo che abbia pianificato che fosse coinvolta in tanti incidenti con omissione di soccorso. Ma secondo un rapporto del 2016 della AAA Foundation for Traffic Safety, oltre l'11% di tutti gli incidenti d'auto sono con omissione di soccorso.

Qual è il punto? L'auto può essere bellissima, divertente da guidare e può portarti in tanti posti. Ma può anche essere un'arma mortale. Dipende dalla persona e da come la usa. Lo stesso vale per il DISC.

Il mio mantra in Social-Engineer e durante i nostri cinque giorni di formazione è semplice: "Fate in modo che si sentano meglio dopo avervi incontrato".

Se tenete in mente questa cosa, le abilità che imparerete in questo libro non solo vi aiuteranno a difendervi e a individuare i malintenzionati, ma vi aiuteranno anche ad avere successo come professionisti dell'ingegneria sociale.

Quando profilate lo stile di comunicazione di una persona, non cercate dei modi per sfruttarla o per manipolarla. Cercate piuttosto dei

modi per modificare il *vostro* stile, in modo da poter comunicare con loro al loro livello, in modo da renderli felici.

Fate pratica di quello che avete appreso in questo capitolo con i familiari e gli amici, prima di dedicarvi davvero all'ingegneria sociale. Una volta che avrete dimostrato di essere sulla strada giusta con i modelli di comunicazione, cominciate a inserire nella comunicazione piccole richieste di azioni che volete far svolgere al vostro obiettivo. Fate qualche prova.

Quando le cose funzioneranno, potrete passare al prossimo argomento, che vi porterà al livello successivo: il pretexting.

Impersonare chiunque

> Tutto quello che potete immaginare è reale.
> - *Pablo Picasso*

Se potessi, aprirei questo capitolo con la sigla di *Mission: Impossible*. Avete presente? Purtroppo, non abbiamo ancora imparato a incorporare la musica nelle pagine di un libro. Ma almeno vi ho evocato quel motivo musicale, che è il più appropriato per questo capitolo.

Diventare chiunque vogliate essere – quello che in ingegneria sociale è chiamato *pretexting* – sembra qualcosa di fantastico. Alcuni definiscono il pretexting usando parole meno simpatiche, come *menzogna*, *falsità* e altro. Tuttavia, mi piace definirlo in termini più generali. Il modo in cui lo spiego in *The Social Engineering Framework* sul sito internet della mia azienda (`www.social-engineer.org/framework/influencing-others/pretexting`) è il seguente:

> Il pretexting si definisce come la pratica di presentarsi come qualcun altro, al fine di ottenere informazioni private. È qualcosa di più di creare una menzogna; in alcuni casi occorre creare un'intera identità completamente nuova e poi utilizzare tale identità per manipolare la ricezione delle informazioni. Il pretexting può anche essere usato per impersonare qualcuno in attività e ruoli che non hanno mai fatto. Inoltre, il pretexting non è un'unica soluzione valida per ogni situazione. Un ingegnere sociale dovrà sviluppare molti diversi pretesti nella propria carriera. E tutti avranno una cosa in comune: la ricerca.

In un lavoro, dovetti entrare in sette diversi magazzini e decisi di impersonare un ispettore degli estintori. In un altro lavoro, dovevamo

entrare nel centro direzionale e nella sala corrispondenza di una società, quindi finsi di essere un addetto al controllo dei parassiti. Per un altro lavoro, dovetti accedere al centro operativo della sicurezza e al centro operativo di rete dell'azienda, quindi inizialmente finsi di essere stato invitato per un colloquio di lavoro, ma dopo aver ottenuto l'accesso all'edificio, dovetti cambiare ruolo, così mi sono trasformato in un manager che veniva da fuori. Mi sono anche presentato come capo del personale e come incaricato del supporto telefonico. Potrei continuare a lungo, ma mi avete capito: ho assunto vari ruoli.

Il punto è che non esiste un pretesto adatto a tutte le situazioni, ed è per questo motivo che il presente capitolo è così importante. La maggior parte del capitolo spiega i principi del pretexting e come sia possibile applicarli a qualsiasi situazione, che si tratti di ingegneria sociale via telefono, e-mail, *social media* o di persona. Vi accompagno attraverso un lavoro che ritengo utile per spiegare tutti questi principi.

In questo capitolo descrivo i seguenti principi:

- pensare in base al risultato che su vuole ottenere;
- usare la realtà e la finzione;
- sapere fino a dove arrivare;
- evitare i vuoti della memoria a breve termine;
- ottenere il supporto necessario per il pretexting;
- impersonare il pretesto.

Il pretexting può essere una delle parti più divertenti del lavoro, ma anche una delle più pericolose. Se non applicate attentamente questi principi, le conseguenze possono essere anche drammatiche. Vi racconterò alcune storie di successi e fallimenti.

Sapere come eseguire un pretesto è di vitale importanza nella carriera di un professionista dell'ingegneria sociale. Può davvero fare la differenza tra il successo e il fallimento nel lavoro.

I principi del pretexting

Prima di approfondire ciascuno dei principi, voglio parlarvi di una tecnica che ha aiutato molti aspiranti ingegneri sociali: la recitazione o improvvisazione.

In molte città si tengono corsi di recitazione o di improvvisazione che chiunque può frequentare per un paio di fine settimana. Molti dei suggerimenti che vi propongo in questo libro vengono insegnati in quei tipi di corsi, i quali però possono darvi qualcosa che un libro non può fare: l'esperienza.

Un corso di recitazione o di improvvisazione può insegnarvi a uscire dalla vostra zona di comfort, a entrare nel personaggio e ad apprendere tutto quello che è necessario per pianificare e impersonare con successo un pretesto sul campo. Tuttavia, anche con alle spalle un buon corso di recitazione o improvvisazione, è comunque necessario conoscere i sei migliori consigli per imparare a impersonare un pretesto. Iniziamo con il primo.

Principio 1 – Pensare in base al risultato che si vuole ottenere

L'ispettore degli estintori, l'addetto al controllo dei parassiti, il direttore del personale: questi sono solo alcuni dei pretesti che ho menzionato. Come ho determinato quale personaggio utilizzare in ogni luogo e per ogni obiettivo?

Tutto inizia con un'attività di OSINT, nella quale analizzo i dettagli della persona o dell'azienda e raccolgo informazioni, notizie, hobby, simpatie, antipatie, eventi e così via (cose che analizzo più in dettaglio nel Capitolo 2). Questi dati possono dirmi molto sul pretesto sul quale dovrei concentrarmi. Ma c'è un'altra informazione chiave che determinerà quale pretesto mettere in campo: il risultato. Capire quello

che sto cercando di ottenere è ancora più importante della conoscenza dell'entità nella quale sto cercando di infiltrarmi. Ve lo illustro raccontandovi una storia che chiamerei "Avventura al 18° piano".

Sono stato assunto per accedere al 18° piano di un edificio sicuro. L'edificio era di proprietà di una società immobiliare che *non* era il mio cliente (lavoravo per conto di una società di contenuti audio online). L'unico piano al quale mi è stato permesso di accedere per questo test era il 18°. Generalmente, questa azienda non prevede appuntamenti estemporanei. Gli ascensori sono tutti controllati da badge. E il quartier generale dell'azienda era in un altro Stato.

Nella fase di OSINT, il mio team aveva raccolto poche informazioni sui nomi e le identità dei dipendenti dell'azienda che lavoravano all'interno dell'edificio che rappresentava l'obiettivo. Tuttavia, trovammo il nome di un manager dell'azienda, più alcuni dei contenuti che il manager aveva realizzato. Inoltre, individuammo su un file server alcuni documenti che l'azienda non aveva alcuna intenzione di rendere pubblici: una checklist della sicurezza, alcune newsletter di comunicazioni interne, del materiale di marketing sui prossimi progetti e vari altri documenti.

Sulla base di queste informazioni, quale vi sembrerebbe un buon pretesto? Pensateci un attimo prima di leggere. Cercate di immaginare almeno un pretesto.

Forse avete pensato a un riparatore di ascensori? Questo vi darebbe la possibilità di entrare nell'ascensore senza l'allarme di sicurezza. Forse avete pensato a un rappresentante inviato dal quartier generale dell'azienda per condurre una verifica a sorpresa in un ufficio? O forse pensavate a qualcos'altro.

Ecco alcuni dettagli che vi aiuteranno a costruire il pretesto: la mia missione, se fossi riuscito a penetrare nell'edificio e a raggiungere il 18° piano, era quella di realizzare video e scattare fotografie di uscite e

ingressi. Dovevo scattare foto a qualsiasi computer non bloccato e cercare di ottenere immagini di documenti o progetti non pubblici.

Dati tutti questi dettagli, dovevo assicurarmi che il mio pretesto mi offrisse la possibilità di girovagare fra computer e scrivanie e dovevo avere con me una macchina fotografica o poter usare una telecamera nascosta per scattare le foto richieste.

Un riparatore di ascensori sarebbe stato un pessimo pretesto per svolgere questa missione. Mi avrebbe permesso di entrare nell'edificio? Sì, ma non di avvicinarmi ai miei obiettivi.

Come rappresentante del quartier generale sarei riuscito a entrare nell'edificio, accedere al piano e anche agli uffici, ma avrei avuto delle limitazioni. Avrei avuto bisogno di sapere chi lavorava in quell'ufficio, in modo che la mia "visita a sorpresa" potesse essere fruttuosa.

Dalla checklist della sicurezza che avevo trovato sul file server, avevo scoperto che questa azienda aveva rigorose linee guida sul controllo delle porte che davano sulle scale. Non venivano mai sbloccate. In effetti, non c'erano nemmeno maniglie sulle porte, dalla parte della tromba delle scale.

Usando queste informazioni, ho sviluppato come pretesto un consulente della sicurezza per conto terzi. A causa di un problema riscontrato in un'altra filiale, ero stato inviato a fare rapidi controlli di 15 minuti sulle uscite, per garantire che venissero seguite le politiche di sicurezza. La mia visita non era stata preannunciata, quindi lo staff dell'ufficio che stavo visitando aveva ragione a essere colto di sorpresa e si sentiva spinto a gestire le cose correttamente senza alcun preavviso. Per garantire al cliente la realizzazione della missione, avevo bisogno di registrare l'intero evento sulla mia macchina fotografica.

Vedete come avere obiettivi specifici permette di caratterizzare meglio il pretesto? Avere tutti i dettagli mi permise di sviluppare una

parte del pretesto che poi mi aiutò a raggiungere tutti i risultati prefissi senza suscitare allarme. Forte, vero?

Armati di questa informazione, saltiamo al secondo principio, dove vi darò maggiori dettagli sull'"Avventura al 18° piano".

Principio 2 – Usare la realtà e la finzione

Questo principio può essere facilmente definito spiegando quanto sia più facile ricordare il pretesto scelto se lo si fonda sulla realtà, per voi e per l'obiettivo. Con questo, voglio dire che dovreste provare a usare frammenti della vostra vita reale e usare conoscenze che già avete in vostro possesso o che potete facilmente assimilare. Dico spesso che penso che una delle relazioni più difficili da falsificare sia quella padre-figlia. Non ho capito questa relazione fino a quando non ho avuto mia figlia. Il modo in cui parlo di lei e le emozioni che provo sono quasi impossibili da fingere, penso. Se non avessi una figlia ma avessi bisogno di costruire un legame con un obiettivo che invece ce l'ha, sarebbe pericoloso per me scegliere un pretesto che avesse una falsa figlia. Ma posso sempre avere una nipote, giusto?

L'idea è che il vostro pretesto dovrebbe basarsi su fatti, emozioni e conoscenze che già possedete o che potete facilmente fingere. Tornando ad alcuni dei pretesti proposti nel paragrafo precedente, conosco pochissimo gli ascensori e il loro funzionamento, quindi fingermi un riparatore di ascensori avrebbe probabilmente portato a un fallimento se solo mi avessero interrogato.

Inoltre, tendo a scegliere un nome al quale posso facilmente rispondere. Alcuni riescono a rispondere a un nome che non è il loro, ma la maggior parte sceglie di adottarne uno che hanno già usato o con il quale sono stati chiamati o che sia una variante del loro vero nome.

Questo è probabilmente ovvio, ma in generale, cerco di adottare personaggi maschili per l'ingegneria sociale in loco, di persona. Ma

impersono come pretesto una donna quando opero online, sui *social media* e persino nell'ingegneria sociale telefonica.

> **Curiosità**
> Molte aziende adottano come politica il fatto che il personale di supporto tecnico non deve mai mettere in discussione il genere del chiamante. Così, quando chiama qualcuno di nome "Sally" ma ha la voce di Barry White, non bisogna fare domande. Si rischia di offendere l'interlocutore, che magari ha solo una voce insolita. Sapendo questo, ho usato i nomi Christina, Christine e Laurie nei miei contatti telefonici.

In termini di credibilità per l'obiettivo, dovreste provare a basare il vostro pretesto su qualcosa che manterrà il vostro obiettivo in quell'*alpha mode* (ricordate la discussione sull'*alpha mode* nel Capitolo 1).

Se l'argomento è familiare all'obiettivo – ovvero se le parole, i titoli e il contesto sono quelli previsti – allora avete maggiori probabilità di lasciare l'obiettivo in *alpha mode*, in modo che non si accorga del potenziale pericolo.

Per la mia "Avventura al 18° piano" stavo usando un documento che avevo trovato tramite l'OSINT. Non dovevo apprendere nuove competenze, quindi mi trovavo nella zona di realtà non solo per i miei obiettivi, ma anche per me.

A volte, però, iniziando a pianificare la realtà, potreste avere problemi a cercare di non eccedere.

Principio 3 – Sapere fino a dove arrivare

Sapere fin dove spingersi – senza eccedere – è molto importante. Nelle mie lezioni, trovo spesso allievi che per i loro pretesti vogliono costruire intere vite. Alcuni vogliono essere dettagliati al punto da ricordarsi che cosa hanno mangiato alla festa del loro 11° compleanno.

Quando si tratta di decidere quanti dettagli creare, tenete a mente che le persone si preoccupano solo di quello che devono fare per completare il "contratto sociale" che avete creato.

Mi spiego. Nel mio pretesto di ispettore della sicurezza per l'"Avventura al 18° piano", che cosa pensate interessasse di me agli obiettivi?

In questo caso, non importava loro del nome dei miei figli, dei miei cani o quello che avevo mangiato per colazione. A loro importavano solo le quattro domande che ho menzionato nel Capitolo 3.

- Chi sei?
- Che cosa vuoi?
- Sei una minaccia?
- Quanto ci vorrà?

Pensiamo a cosa un obiettivo vorrà sapere subito sul mio pretesto.

D: Chi sei?

R: Sono un ispettore della sicurezza, mi ha inviato l'azienda per fare un controllo *molto* rapido per garantire l'applicazione di tutte le politiche.

D: Che cosa vuoi?

R: Ho solo bisogno di circa 15 minuti del vostro tempo per fare questo controllo veloce.

D: Sei una minaccia?

R: Mi hanno chiamato per un'urgenza, ma nessuno è nei guai.

D: Quanto ci vorrà?

R: Speriamo meno di 15 minuti.

Il resto sono solo dettagli in più dei quali l'obiettivo non ha alcun bisogno, che non lo interessano. Questo significa che potete essere impreparati? Affatto. Dovreste comunque essere preparati a rispondere ad alcune informazioni di base sul vostro "personaggio" nel caso in cui

il vostro obiettivo ve le chieda. Quindi, ho sviluppato un pretesto che aveva le seguenti caratteristiche.

Sono Phil Williams, sono un ispettore della sicurezza e ho 40 anni. Ho un figlio. Sono sposato. Non ho animali domestici, ma amo i cani e i gatti. Ho una vita piuttosto monotona: vado a lavorare e vado a casa. Ho vissuto a *X* per *tot* anni.

Con quel pretesto di base, quali dettagli ho bisogno di sapere per essere sicuro di riuscirci?

- Il nome di mia moglie.
- Il nome di mio figlio.
- L'età di mio figlio.
- La regione in cui abito.
- La città in cui vivo.
- Il mio ruolo professionale e il lavoro che svolgo per l'azienda

Fondamentalmente questo è tutto. Forse ci sono un paio di curiosità che vale la pena pianificare, ma per la maggior parte, queste basi sono tutto quello che potrei dover rivelare di me.

Lasciate che vi faccia un esempio di una persona che esagerava davvero con il pretexting: una volta stavo lavorando con uno studente per un compito. La sera prima aveva fallito l'approccio con un estraneo e per aiutarlo a ricostruire la fiducia in se stesso dopo quel fallimento, andammo nell'atrio dell'hotel, in modo che potessi vederlo all'opera con uno sconosciuto. Il mio scopo era quello di osservarlo, per vedere che cosa sbagliasse e offrirgli consigli utili per "aggiustare" il pretesto.

Lo studente si avvicinò a una donna e cominciò bene. Aveva un sorriso caloroso ed era davvero amichevole. La donna iniziò a interessarsi e vidi il suo linguaggio del corpo diventare caldo e amichevole con i fianchi rivolti verso di lui (per saperne di più sul

linguaggio del corpo consultate il Capitolo 8). Lo studente chiese alla donna da dove venisse. Gli rispose con un sorriso: “Da Philadelphia”.

Disse: “Oh, davvero? è sorprendente, anch’io!”. Sfortunatamente, nulla era più lontano dalla realtà. Mentre lo ascoltavo pronunciare quelle parole, ho visto il suo “treno” iniziare a rallentare.

La donna rispose: “Beh, è incredibile! E dove vivi?”.

Lo studente si rese conto di aver appena esagerato, e alla grande. Lui rispose: “Umm, sai quel coso a forma di campana…”. La sua voce si spense, perché sapeva che stava per fare una pessima figura.

“La campana?”, chiese lei. “Intendi la Liberty Bell?”.

“Sì, è proprio quello che intendevo…”, disse timidamente.

“Prima di tutto, non so a che gioco tu stia giocando. Che cosa significa ‘quel coso a forma di campana’? Nessuno a Philly chiamerebbe la Liberty Bell un ‘coso a campana’. In secondo luogo, non c’è neanche una casa vicino alla campana. Questa conversazione è finita”. Si voltò e se ne andò.

Lo studente si avvicinò a me e disse: “Ecco. È così che sono andate le mie ultime due serate”.

Gli domandai di descrivermi in dettaglio come fossero andate queste ultime due serate. Mentre descriveva le conversazioni, il problema mi divenne più chiaro: accettava semplicemente qualsiasi cosa dicesse l’obiettivo, senza pensare al fatto che potesse sostenerlo o meno.

Gli feci una lezione sulla *tribe mentality* (che discuterò in dettaglio nel Capitolo 5), il che vuol dire che aveva bisogno di far parte della tribù alla quale apparteneva l’obiettivo e questo lo avrebbe automaticamente accettato.

Per vostra informazione

Non dovete attendere fino al Capitolo 5 per conoscere la verità sulla *tribe mentality*; eccone una breve descrizione. La *tribe mentality* si riferisce al fatto che dovete inserirvi nel gruppo (la “tribù”) delle persone che state avvicinando. Può trattarsi del vostro stile di abbigliamento, della lingua, della cultura o di altri aspetti

delle vostre caratteristiche. Come ingegneri sociali, è preferibile tentare di inserirsi nella loro tribù invece di provare a farli entrare nella vostra.

Questa esperienza dello studente è una buona lezione sui pretesti per tutti. È importante avere una certa conoscenza dei dettagli del pretesto scelto. Nell'incontro fra lo studente e la donna di Philadelphia, sarebbe bastato, per entrare a far parte della sua tribù, cambiare una sola frase, dicendo qualcosa come: "Philadelphia? Ho sentito dire che è un bel posto da visitare. Non ci sono mai stato. Quali sono i posti che più ti piacciono di Philadelphia?". Questo le avrebbe comunicato che la stava ascoltando, che era interessato e che voleva saperne di più, invece di fingere una conoscenza che non aveva.

Padroneggiare questo concetto può fare una grande differenza nel successo del pretesto. Dopo aver avuto successo con il contatto iniziale, le persone con le quali interagite inizieranno a fornirvi dei dettagli. Tutti quei dettagli possono essere difficili da ricordare e questo ci conduce al quarto principio.

Principio 4 – Evitare i vuoti della memoria a breve termine

Succede a tutti: si incontra qualcuno per la prima volta, si avvia una buona conversazione e poi, al momento dei saluti, non si ricorda più il suo nome. Non è bello: si dà l'impressione di essere poco interessati a quella persona.

Ho scoperto che sono più le persone che hanno difficoltà a ricordare questi dettagli di quante invece li memorizzano. Questo è il motivo per cui questo paragrafo è così importante. E non ispirerete certo fiducia se a metà conversazione estrarrete un taccuino per controllare i dettagli della vostra storia. Ancora peggio se la persona con la quale state parlando scopre che state prendendo nota dei dettagli di cui vi parla.

Abbiamo tutti sentito suggerimenti del tipo: “Ripetete il nome quante più volte potete nei primi 20 secondi della conversazione e non lo dimenticherete”. Questo suggerimento funziona, ma non sempre ha senso ripetere continuamente il nome di una persona dopo averlo sentito. Quasi mi immagino la scena: mi incontrate per la prima volta e: “Ah, Chris, Chris, Chris… sì Chris… Allora si chiama Chris. Bene, Chris, di che cosa stavamo parlando, Chris?”.

Umm… raccapricciante. Per favore, non fatelo quando mi incontrerete.

Detto questo, trovo che utilizzare il nome di una persona in qualche modo (che però sia significativo) può aiutare a ricordarlo. In “Avventura al 18° piano”, mentre entravo nell’edificio e andavo dritto verso l’ascensore, una donna della sicurezza mi fermò. Alzò una mano e disse: “Scusi, dove sta andando?”.

Mi fermai, sapendo che sarei dovuto entrare in relazione con lei: “Oh, mi dispiace, signora”. Tesi la mano e le dissi: “Sono Phil Williams dal quartier generale di *[nome dell’azienda, che preferisco non divulgare]*. Abbiamo un ufficio qui al 18° piano”.

Controllò un elenco che aveva su un blocco e poi disse: “Mi dispiace, signor Williams. Non trovo il suo nome nell’elenco dei visitatori approvati oggi”.

“Ha perfettamente ragione. Il mio nome lì non c’è. Mi dispiace… Sono stato così maleducato. Come si chiama?”, dissi osservando il suo cartellino. “Claire, piacere di conoscerla”.

Dopo una breve pausa: “Vede, Claire, si è verificato un incidente in una delle nostre sedi locali a causa di alcune politiche di sicurezza che non sono state seguite a dovere e sono stato mandato a ispezionare i nostri uffici per assicurarmi che vengano seguite tutte le politiche stabilite dal regolamento. Deve trattarsi di visite a sorpresa, altrimenti come possiamo garantire che i risultati siano corretti?”.

“Capisco”, disse Claire.

“E una delle sezioni di questo rapporto riguarda la sicurezza del front-desk. Sono contento di avere il suo nome, così posso riferire che ha seguito perfettamente tutte le procedure. Claire è il suo nome e… come si scrive il cognome?”. Mentre lo dicevo, estrassi la penna, guardai i miei appunti e scrissi il nome sul taccuino.

Senza attendere un istante, disse: “Farclay. F-A-R-C-L-A-Y”.

“Ok, signora Farclay. Ha fatto un’ottima impressione in questo controllo, un ottimo inizio. Grazie. Spero che la mia visita a sorpresa termini con il massimo dei voti”.

Poi fece qualcosa di inatteso. Disse: “Bene, signor Williams, che ne dice se la mando al 18° piano col mio badge, così che possa vedere se il controllo a sorpresa produce risultati positivi?”.

“Claire! Posso chiamarti Claire?”. Lei annuì e così continuai: “Claire, sei un genio! Questa è una grande idea”.

Con orgoglio, accompagnò il suo nuovo amico (me) verso l’ascensore e usò il suo badge per aprire le porte e per spedirmi direttamente al 18° piano. La ringraziai e le dissi: “Ci rivediamo tra 15 minuti”.

Qual è stata la mia chiave, in questa situazione?

- Usare il nome della guardia un paio di volte, in modo rapido.
- Dare al mio pretesto un motivo per scrivere tutto.

Per quanto mi riguarda, anche se queste tecniche facciano meraviglie, non sempre sono pratiche. Per questo motivo, dovete avere anche altri metodi nel vostro arsenale. Io adotto vari tipi di tecniche.

- *Il biglietto da visita*: scambiare biglietti da visita con un obiettivo è un ottimo modo per ottenere tutti i suoi dettagli. Ma non iniziate da lì. Aspettate di aver costruito un minimo di relazione o il momento di congedarvi.

- *Dispositivi di registrazione*: a volte registro l’audio e il video degli incarichi dal vivo e l’audio degli incarichi telefonici, per assicurarmi di catturare tutti i dettagli. Può essere un ottimo strumento, ma assicuratevi di avere il permesso dell’azienda prima di registrare qualcosa o qualcuno dentro i loro locali.
- *Un partner*: trovo utile che qualcun altro lavori insieme a me, in modo che tale persona possa aiutarmi a ricordare certi dettagli mentre magari mi concentro su altre cose.

Tutte queste idee sono utili per registrare i dettagli di sicurezza per il rapporto che seguirà, mentre non sono molto utili per ricordare quegli stessi dettagli, mentre vi trovate nel bel mezzo di una missione.

Ecco alcuni suggerimenti.

- *Pratica*. Ogni volta che potete, fate pratica ricordando i dettagli di luoghi e momenti che *non* fanno parte del vostro lavoro: riunioni di famiglia, feste, riunioni d’ufficio, chiamate commerciali e quando siete impegnati con qualcuno.
  Sfidate voi stessi a ricordare elementi come il colore della camicia di una persona, il tipo di gioielli che indossava, il loro nome e cognome o altri dettagli che normalmente non vi interessano.
  Per esperienza, la memoria funziona un po’ come un muscolo. Più la esercito più si rafforza.
- *Leggere*. Ho scoperto che trascorrere un po’ di tempo a leggere un libro aiuta la memoria. Non vi consiglio nessun libro in particolare: basta leggere qualcosa che non si trovi su un display. Non ho fondamenti scientifici per confermare questo suggerimento, ma posso dirvi che più tempo trascorro a esercitare il cervello, più “funziona” quando ne ho bisogno. Per migliorare la mia capacità di ricordare i dettagli ho anche dedicato del tempo a risolvere dei problemi matematici.

Il mio consiglio finale per questo paragrafo è: quando vi prendete una breve pausa, concedetevi qualche minuto per registrare i vostri pensieri. Io lo faccio in due modi: scrivendo i dettagli che devo ricordare o utilizzando un'app di registrazione vocale dello smartphone.

Dopo che Claire mi ebbe spedito al 18° piano, nell'ascensore estrassi il telefono e avviai l'app di registrazione per registrare tutti i dettagli che riuscivo a ricordare. Questo ha due scopi: innanzitutto mi aiuta a stendere il rapporto, successivamente; ma soprattutto trovo che quando pronuncio i dettagli ad alta voce, ho più facilità a ricordarli, più tardi.

La mia registrazione è stata qualcosa come:

Claire Farclay. Circa 1,50 cm, bionda, guardia di sicurezza di corporatura media. Camicia bianca, distintivo, pantaloni neri. Badge sul petto, a sinistra. Immagini di due cani al banco della sicurezza. Ho estratto il taccuino. Ho costruito il legame lodando il fatto che ha seguito le procedure. Per mandarmi al 18° piano ha usato il badge bianco che aveva fissato a un cordino retrattile sul fianco destro. Codice inserito nell'ascensore: 4381.

Ricordo ancora quei dettagli a memoria anche se l'"Avventura al 18° piano" è avvenuta più di due anni fa. Ecco quanto può essere allenata la memoria.

La quinta freccia da aggiungere alla vostra faretra per il successo del pretexting è il *supporto*.

Principio 5 – Ottenere il supporto necessario per il pretexting

Voglio che vi fermiate a riflettere sul pretesto che sto usando in questo capitolo: un controllo di sicurezza per una società. Ora

rispondete alle seguenti domande:

- Che cosa indosserebbe un controllore della sicurezza?
- Quali strumenti o attrezzi avrebbe un controllore della sicurezza?
- C’è qualche conoscenza speciale che un controllore della sicurezza dovrebbe avere?

Le risposte a queste domande sono alla base di questo paragrafo. Consideriamole ciascuna separatamente, in modo da poter vedere chiaramente il ruolo di questo principio.

D: Che cosa indosserebbe un controllore della sicurezza?

R: Ho scoperto che questi controllori generalmente indossano divise color cachi o blu, una camicia abbottonata, scarpe da ginnastica o stivaletti antinfortunistici. E sono puliti.

D: Quali strumenti o attrezzi avrebbe un controllore della sicurezza?

R: Nella mia ricerca, ho scoperto che hanno macchina fotografica, telefono, taccuino, penne e pennarelli, carta, una checklist e talvolta un metro a nastro (a seconda del lavoro).

D: C’è qualche conoscenza speciale che un controllore della sicurezza dovrebbe avere?

R: La risposta a questa domanda potrebbe rimandare ad altre domande. Come auditor di sicurezza devo capire se funzionano gli estintori? Devo capire se funzionano le porte antincendio, gli allarmi o altri aspetti dell’edificio? O è accettabile che io sia lì solo per controllare i punti di una checklist? Inoltre, che cosa dovrei sapere della società alla quale sto cercando di accedere? Che cosa dovrei sapere della società alla quale sto fingendo di appartenere?

Una volta sono stato in un edificio con Michele, e una guardia di sicurezza alla quale avevo dato un biglietto da visita falso mi chiese dove vivessi, perché non aveva mai sentito parlare della mia società. Non mi aspettavo quella domanda, così indicai verso ovest, dicendo: “Oh, vivo da quella parte”.

La guardia mi rispose: “Nella zona industriale? Dove avete trovato casa?”.

Mi resi conto che stavo per essere scoperto, quindi dissi: “Oh, intendevo dopo la zona industriale. Sa quel quartiere che si trova oltre?”.

La guardia mi rispose, rispettosamente: “Mi dispiace, signore. Non sono uno stupido: vuole convincermi che il suo biglietto da visita recita ‘a conduzione familiare da 20 anni’ e lei non sa nemmeno in che zona abita?”.

Il mio grave difetto, in questo caso, fu la scarsa conoscenza della zona del mio pretesto, cosa che mi avrebbe consentito di rispondere alle domande in modo più intelligente.

Non avrei potuto prevedere che mi avrebbe fatto questa domanda, così la guardia sicuramente ha svolto ottimamente il suo lavoro, essendone a conoscenza, ma io non ho più ripetuto lo stesso errore. Da quel momento in poi, se avessi avuto in mano un biglietto da visita che diceva che vivevo lì da qualche tempo, mi premunivo delle informazioni di supporto pronte a dimostrarlo.

Più spesso, però, preferisco facilitarmi il compito, quindi per il mio pretesto dichiaro di essere nuovo nella zona o di venire da fuori città. Questo mi dà la possibilità di non dover sapere tutto sul luogo in cui mi trovo.

In “Avventura al 18° piano” scoprii che prendere appunti mi permette non solo di entrare nella parte, ma anche di avere tutto ciò di cui avrò poi bisogno per supportare la mia registrazione dettagliata. Poiché mi comportavo come previsto, Claire non aveva alcun motivo di dubitare delle mie azioni.

E questo ci porta all’ultimo principio: *l’esecuzione*. Seguendo i cinque principi precedenti, l’ultimo dovrebbe essere il più facile da mettere in atto.

Principio 6 – Impersonare il pretesto

Per impersonare il pretesto non basta applicare i primi cinque principi. Nell'esecuzione del pretesto entrano in gioco nervi, eventi imprevisti e anche i "jolly": altri esseri umani. Questo significa che può succedere di tutto.

Faccio questo lavoro da oltre un decennio e sono ancora nervoso, ogni volta, che si tratti di entrare in un luogo o di prendere in mano il telefono o di inviare un'e-mail. Avrò dimenticato qualcosa? Mi prenderanno? Fallirò? Queste domande si susseguono sempre nella mia mente mentre mi accingo a entrare in azione.

Le seguenti "cose" mi aiutano a impersonare il pretesto più facilmente:

- fare pratica;
- stirarsi e fare un bel respiro;
- comunicare;
- *non* seguire un copione.

è importante ricordarsi che, pur con tutta la preparazione a monte ci sono sempre le incognite: l'addetto molto scrupoloso, la guardia troppo zelante, la porta imprevedibilmente chiusa. In altre parole, dovete essere pronti a essere flessibili.

Fare pratica

Se si tratta di un'e-mail di *phishing*, mi assicuro di inviarla a me stesso e ad alcuni colleghi per trarne un *feedback*. Chiedo anche ai miei colleghi di fare clic sul link o di aprire il documento, per accertarsi che tutto funzioni correttamente. Se si tratta di *vishing*, mi assicuro di avere sul desktop tutto il supporto necessario in termini di rumori di sottofondo, informazioni e dettagli. Faccio anche una chiamata di prova, per assicurarmi che il mio trucco funzioni. Se si

tratta di *SMiShing*, mando il messaggio a un altro smartphone o a me stesso per assicurarmi che sia formattato correttamente e che il link funzioni. E se sto impersonando qualcuno in un edificio, mi esercito con le battute di apertura e mi assicuro di avere i miei dati solidamente fissati in mente, prima ancora di salire in macchina. Mi accerto inoltre che tutte le mie fotocamere e ogni altro apparecchio o strumento funzioni.

Come mi disse Paul Kelly, un assistente di Paul Ekman (che ho presentato nel Capitolo 2): "Solo la pratica perfetta rende perfetti". Esercitatevi a fare le cose nel modo giusto, per consentire alla vostra memoria muscolare di entrare in azione.

La pratica può fare la differenza tra il successo e il fallimento. In uno dei miei incarichi, dopo essere arrivato sul posto e aver preso la mia attrezzatura dal bagagliaio, accesi la fotocamera e scoprii che aveva le batterie scariche. Dovetti usare la fotocamera del cellulare. Ricordo che mentre svolgevo la missione tutto quello a cui riuscivo a pensare era se il mio telefono avrebbe funzionato, se avrebbe continuato a registrare, se era troppo evidente che andavo in giro impugnando il mio telefono in modo un po' strano.

Stirarsi e fare un bel respiro

Potrebbe sembrare sciocco, ma dedico alcuni istanti a fare respiri profondi e stretching. Inoltre, in base a quanto sono nervoso, posso mettermi per qualche istante in una bella posa di forza, per "caricarmi" prima di impersonare il pretesto e condurre l'attacco. Per informazioni sulle pose di forza, consultate il Capitolo 8.

Comunicare

Da buon professionista dell'ingegneria sociale, mi assicuro di comunicare in modo adeguato con il mio cliente. Per esempio, il

giorno prima di avviare una campagna di *phishing*, comunico al mio contatto che sto per condurre l'attacco (naturalmente, se devo eseguire un test di penetrazione in completa "black-box", comunico queste informazioni solo dopo il completamento). Lo stesso per le campagne di *vishing*. Questo è particolarmente importante quando devo impersonare qualcuno. Mi assicuro che il mio contatto sappia quando si svolgerà l'attacco, in modo che, in caso di complicazioni, possa sempre far contattare qualcuno.

Sono stato scoperto durante una missione. Beh, questo non è del tutto vero: il cliente ha voluto che *dopo* aver compiuto la missione di penetrazione, comunicassi alla sicurezza che ero un *pen-tester*. Dissi ripetutamente al cliente che questa era una pessima idea, ma lui ha insistito. Andò più o meno così:

Dopo aver oltrepassato con successo la sicurezza come addetto alla riparazione del compattatore di rifiuti e dopo aver avuto accesso all'intera struttura senza sorveglianza, me ne stavo andando e dissi: "Signore, prima di andarmene devo dirle che il mio nome non è Paul come dice il mio tesserino. Mi chiamo Chris e sono quello che voi chiamate *pen-tester*. Ero incaricato di mettere alla prova la sicurezza del vostro edificio e l'applicazione delle politiche di controllo degli accessi".

Mentre parlavo vidi la guardia di sicurezza cambiare espressione e la sua mano correre al teaser. Mi disse: "Tu saresti *cosa*? Sto per essere licenziato?".

Cercai di calmarlo dicendo: "Signore, qui non viene licenziato nessuno. Questo era solo un test, per aiutare la sua azienda ad adottare nuove politiche, con lo scopo di migliorare la sicurezza".

Ma lui aveva già impugnato la radio e stava chiamando il capo della sicurezza e in più aveva già premuto il tasto per bloccare le uscite, così che non potessi fuggire.

Arrivò il capo della sicurezza. L'uomo che avevo appena ingannato spiegò la situazione in modo molto dispregiativo e arrabbiato. Cercai di intervenire e la guardia mi disse: "Nessuno ti ha interpellato, Paul o Chris o qualsiasi sia il tuo nome".

Dissi: "Ho in tasca una lettera che dovreste leggere". Consegnai loro la mia lettera "Uscite gratis di prigione", come mi piace chiamarla. Questa lettera viene scritta dall'azienda per la quale lavoro per descrivere chi sono, che cosa sto facendo e per dire che ho il permesso di farlo. Fornisce anche un paio numeri di persone da contattare come riscontro della mia storia.

Dopo aver letto la lettera, il capo della sicurezza disse: "E come faccio a sapere che anche questa lettera non sia finta? Eh, Chris?".

"Beh, questa è un'ottima domanda. E, a essere sincero, non potete saperlo. Ma basta chiamare uno di questi numeri e tutto vi verrà chiarito", dissi con la voce più gradevole che potessi sfoggiare.

"Io *non* chiamo nessuno di questi numeri. Per quel che ne so io, questo potrebbe essere il numero di un tuo complice nel furgone parcheggiato qui fuori" (ricordo che pensai: "Accidenti, *questa è una buona osservazione e anche una grande idea per il futuro. Grazie signor capo della sicurezza*").

Continuò: "Io chiamo solo qualcuno che conosco in azienda". Prese il telefono e compose un numero. Snocciolò la storia e poi chiese: "Tu ne sai qualcosa?".

Sentii la voce all'altro capo del telefono dire: "Io non so nulla di questo test di penetrazione. Chiama la polizia".

Venni scortato e poi rinchiuso in un ripostiglio (non sto scherzando). Per fortuna, nella fretta, le guardie mi avevano lasciato il cellulare e il grimaldello. In pochi minuti ero uscito dal ripostiglio, avevo aperto la porta dell'ufficio e me ne stavo seduto in corridoio, intento a chiamare il mio contatto per dirgli di risolvere il problema *subito*! E per fortuna

l’avevo chiamato la sera prima per assicurarmi che fosse in sede. Qualche minuto più tardi, tutto era stato chiarito e me ne stavo andando libero e illeso.

Come dimostra questa storia, dovete assicurarvi di comunicare con le persone giuste, dicendo le cose giuste, al momento giusto. So che questo è un concetto molto vago, ma solo perché i requisiti e le regole cambiano in base al lavoro, all’attività e al cliente. Alcuni clienti richiedono un controllo maggiore rispetto ad altri. Ricordate che siete professionisti, e che quindi dovete assicurarvi che i vostri clienti siano soddisfatti.

Non seguire un copione

Questo consiglio è rivolto principalmente a coloro che rientrano nel tipo *C* del grafico DISC, che hanno bisogno di accumulare molti dettagli e di programmare ogni passo (il Capitolo 3 tratta in dettaglio il profilo DISC e che cos’è un tipo *C*). Usare un copione, sia per il *vishing* sia per impersonare qualcuno, toglie dinamismo all’operazione. Vi garantisco che nulla andrà mai esattamente come avete pianificato. Avere la capacità di essere dinamici vi garantisce un vantaggio e una maggiore probabilità di successo.

Riepilogo

Vi suggerisco di dedicare del tempo a rivedere i sei principi del pretesto, in modo da poterli perfezionare. Ricordatevi che ogni principio ricade poi su quello successivo e vi aiuterà a essere più efficaci.

Pianificare le vostre missioni in modo efficiente può aiutarvi a trovare pretesti basati sulla realtà che mantengano l’obiettivo in *beta mode* (fate riferimento alla ricerca di Langer, nel Capitolo 1). Usare la

realtà invece della pura finzione faciliterà il vostro compito di impersonare il pretesto e vi renderà più credibile per l'obiettivo. Avere un pretesto saldamente fondato sulla realtà vi aiuterà a determinare quanto lontano vi potete spingere in quel particolare compito, in modo che il vostro impegno sia al giusto livello: né troppo né troppo poco. Una certa semplicità faciliterà anche la memorizzazione non solo delle caratteristiche del vostro pretesto, ma anche delle informazioni che vi verranno fornite. La pianificazione aiuta a decidere quale abbigliamento, quale attrezzatura e quale dotazione tecnologica dovete avere per "essere" il vostro pretesto. Se ne studiate bene le caratteristiche, vi sarà più facile impersonare il pretesto.

Ricordate che la scelta del pretesto può facilitare o pregiudicare la vostra missione. Immaginate di andare in un'azienda, con completo elegante e valigetta 24 ore. Questo sarebbe l'abbigliamento tipico di un addetto alla riparazione dei compattatori di rifiuti?

Questo esempio può anche essere estremo, ma è per farvi capire il concetto. Se iniziate a percepire che la vostra copertura sta saltando, *diventerete* nervosi. E il nervosismo pregiudicherà la vostra fluidità nel parlare, la capacità di memorizzare e anche la capacità di pensare velocemente.

Il pretesto, se ben impersonato, aiuta a rispondere alle quattro domande di cui vi ho parlato nel Capitolo 3: chi sei, che cosa vuoi, sei una minaccia e quanto ci vorrà. Ma quelle domande hanno anche un altro scopo, che affronteremo nel Capitolo 5 e che ha a che fare con la costruzione del legame.

Come cercare di farsi accettare

> Una relazione è la capacità di entrare nel mondo di qualcun altro, è farlo sentire capito, è fargli capire che avete un forte legame che vi unisce.
> - *Tony Robbins*

OilHater era il *nickname* di una persona che detestava veramente l'industria petrolifera. Quest'uomo, molto colto e che parlava in modo fluente, spiegava in modo articolato su blog e forum quanto il *fracking* fosse terribile per l'ambiente e come avrebbe rovinato il pianeta per le generazioni future. Mentre i suoi post acquisivano popolarità e lui acquisiva *follower*, la rabbia era sempre più evidente nei suoi post.

NOTA

I nomi utilizzati in questo esempio sono stati modificati, per motivi di sicurezza.

Dopo mesi di costruzione di una sua reputazione, OilHater iniziò a pubblicare minacce violente. I suoi post iniziarono a parlare di far saltare in aria gli impianti di *fracking*, per fermare questi attacchi a Madre Natura. Menzionava anche alcune stazioni di *fracking* di alcune aree del Texas che avrebbe voluto colpire.

A questo punto, Paul iniziò a comparire in tutti i forum in cui si parlava dei pericoli del *fracking*. Paul era padre di due bambini piccoli ed era seriamente preoccupato. Un gigante petrolifero aveva iniziato a condurre attività di *fracking* nella sua zona e voleva sapere come proteggere i suoi figli da ogni pericolo.

I forum erano pieni di persone che offrivano a Paul consigli utili su cosa fare e come proteggere la sua famiglia dai danni alle risorse

idriche e al suolo. Paul continuava a postare sui forum, ponendo domande tipiche di una persona inesperta.

Un giorno, OilHater rispose a un messaggio di Paul dimostrando una vasta conoscenza e correggendo alcuni post errati di altri membri del forum. E Paul ringraziò OilHater per averlo aiutato a capire alcune informazioni confuse che aveva ricevuto da altri post. Paul poi si complimentò per l'approfondita conoscenza di OilHater, chiedendogli se avesse lavorato per l'industria petrolifera, perché sembrava a conoscenza di molte cose.

OilHater spiegò di essere solo un cittadino molto preoccupato, che aveva passato ore e ore a studiare i danni che l'industria petrolifera stava causando. Paul chiese se potesse inviargli un messaggio privato con alcune domande personali. Durante quella conversazione privata, Paul fornì alcune informazioni a OilHater: che era del Texas e che era preoccupato per la sua zona e gli chiese se vi intravedesse i pericoli che aveva menzionato nelle sue precedenti risposte.

OilHater rispose che sapeva tutto di quella zona e di quanto fosse pericolosa. Paul continuò a chiedere che cosa avrebbe potuto fare. OilHater forniva risposte sempre più rabbiose e anche Paul si sentiva più arrabbiato. Paul continuò a considerare OilHater un esperto di questi argomenti e continuò a sottoporgli domande.

Paul era scandalizzato dal fatto che non si potesse fare nulla per fermare le operazioni di *fracking* e per salvare i suoi figli. Disse scherzosamente in una conversazione: "Sembra che l'unico modo per fermarli sia farli saltare dalla faccia della terra. Peccato che non possiamo farlo".

OilHater rispose: "Non esserne così sicuro".

Paul gli chiese che cosa intendesse, ma OilHater tacque per un po'. Paul continuò a postare nei forum, scrivendo di quanto fosse sconvolto

del fatto che l’area in cui viveva in Texas era sotto l’assedio dall’industria petrolifera.

Dopo circa una settimana, OilHater inviò un messaggio privato a Paul, dicendogli che aveva un piano per aiutarlo a fermare il *fracking* nella sua zona e per aiutare i suoi figli. Paul, eccitato, rispose che era disponibile, ma non sapeva che cosa potesse fare.

OilHater gli disse che il piano l’aveva, ma non era certo che Paul volesse aiutarlo. Poi disse: “Potrebbe essere pericoloso”.

Paul disse qualcosa del tipo: “Potrei anche correre dei rischi per salvare i miei figli. Che cos’hai in mente?”.

OilHater dichiarò: “A volte occorre sporcarsi le mani per mettere fine a un pasticcio. Non sei d’accordo?”.

Paul rispose: “Certamente. Non voglio che i miei figli si ammalino di cancro o anche peggio, e che poi quei truffatori si arricchiscano sulla sofferenza dei nostri figli”.

OilHater rispose: “Ti ricordi che l’ultima volta ti ho detto che l’unico modo per fermarli sarebbe stato quello di farli saltare in aria? Ci stiamo assicurando che per un po’ la smettano col *fracking*”.

Paul disse: “Adesso sono curioso! Non ho mai fatto nulla di simile, ma i miei figli non meritano tutto questo. Che cosa hai in mente? Cosa possiamo fare?”.

OilHater disse: “Conosci Peg’s Diner, in centro?”

Paul rispose: “Sì, ci vado spesso”.

OilHater disse: “Possiamo incontrarci lì giovedì sera alle 19:30?”.

Paul rispose: “Sì, certo. Ma come ti riconoscerò?”.

OilHater disse: “Vieni al ristorante e siediti a un tavolo nell’angolo più lontano. Indossa un cappellino da baseball. Mi avvicinerò io”.

Paul oppose un po’ di resistenza, e disse: “Scusa, ma mi sembra un po’ strano. Posso sapere come ti chiami? Io sono Paul Wilcox e abito al 123 di Main Street. Voglio solo sapere con chi ho a che fare”.

“Certo, mi dispiace di essere così reticente”, rispose OilHater: “Sto solo usando una linea anonima. Mi chiamo Robert Moore. Ti incontrerò da Peg alle 19:30”.

Alle 19:30 di quel giovedì sera, Robert Moore non incontrò Paul Wilcox, ma un rappresentante delle forze dell’ordine, il quale si assicurò che i suoi piani non venissero portati a compimento.

Se non l’avete ancora indovinato, quel Paul Wilcox ero io. Questo progetto di tre settimane e mezza definisce l’essenza stessa di questo capitolo, ovvero come la costruzione di un legame con il vostro obiettivo può creare una relazione di fiducia. Per il resto di questo capitolo, farò riferimento a questo racconto come all’“Operazione Petrolio”.

Questo capitolo si basa sui 10 principi che Robin Dreeke delineò nel suo libro del 2011: *It’s Not All About “Me”: The Top Ten Techniques for Building Quick Rapport with Anyone*. Anche se Dreeke parlava delle comunicazioni quotidiane, vi mostrerò come applicare questi principi all’ingegneria sociale.

Prima di introdurre i 10 principi, ho bisogno di spiegare un po’ quello che mi permise di costruire un legame nell’Operazione Petrolio. è una cosa semplice, ma anche così profonda che, se non si procede correttamente, è molto probabile che si finisca per fallire.

La tribe mentality

Come ingegneri sociali, prima ancora di poter iniziare a costruire un legame, dovete stabilire che fate parte della tribù del vostro obiettivo. Una *tribù* è semplicemente tutto ciò che identifica un determinato gruppo: può essere uno stile di abbigliamento, una serie di attività, un atteggiamento o un interesse condiviso. La comunanza tra i membri del gruppo crea la “tribù”. Per affermarvi come membro della tribù, dovete capire quali aspetti dovete rispecchiare per farne parte.

Può essere più facile immaginare come funziona ripensando al liceo. Gli abiti che indossavate vi identificavano subito con la vostra tribù.

Esiste un video intitolato *The Tribe Mentality – The Bystander Effect* (https://vimeo.com/265364702), che dimostra quanto sia importante per noi far parte della giusta tribù. Nel video, un attore indossa abiti da lavoro e giace a terra; chiede aiuto nelle stazioni della metropolitana più trafficate, piene di gente affaccendata. Durante una sessione a Londra, l'attore è rimasto a terra per oltre 20 minuti prima che qualcuno lo soccorresse.

Prima di cominciare a giudicare tutti coloro che sono passati davanti all'attore senza soccorrerlo, pensate allo scenario. Un uomo in jeans, t-shirt e giubbotto, sdraiato a terra nel bel mezzo di una stazione della metropolitana chiede aiuto tenendosi lo stomaco. Ora provate a rispondere alle quattro domande introdotte nel Capitolo 3 dal punto di vista di una persona che passi davanti a questo attore, senza sapere che è un attore.

- *Chi è questa persona?* Semplicemente, non lo sapete. Magari è un tossicodipendente. Magari è un truffatore. Sta davvero male? E se vi contagiasse?
- *Che cosa vuole da me questa persona?* Magari vuole dei soldi. E magari volete veramente aiutarlo, ma siete in ritardo per la riunione. Magari quest'uomo vuole solo che vi fermiate, per potervi rubare il portafoglio (o i reni).
- *Questa persona rappresenta una minaccia?* Che cosa succede se quest'uomo è un ladro o un tossicodipendente e, quando vi inginocchiate per aiutarlo, vi accoltella al fegato? E se è davvero malato, magari contagioso.
- *Quanto tempo mi farà perdere?* Quest'uomo è senza soldi, quindi la cosa potrebbe richiedere del tempo. Che cosa succede se dovete portare quest'uomo all'ospedale e vi ci vuole tutto il giorno?

Ci sono molti ragionevoli motivi per cui un passante, non essendo in grado di rispondere a queste quattro domande, eviterebbe di abbassare le difese per aiutare l'attore. Successivamente, però, lo scenario del video cambia un po'. Lo stesso attore indossa un completo e giace a terra. Indovinate in quanto tempo viene soccorso? Circa sei secondi. Quando le persone che si sono fermate per aiutarlo sono state intervistate, hanno detto cose del tipo: "Beh, era in giacca e cravatta, quindi volevo aiutarlo" e "Doveva sentirsi davvero male per accasciarsi a terra con indosso un completo".

L'unica cosa che è cambiata nella situazione era il tipo di abbigliamento, ma questa singola modifica ha fatto in modo che i passanti rispondessero diversamente alle famose quattro domande:

- *Chi è questa persona?* è uno di noi e ha bisogno di aiuto.
- *Che cosa vuole da me questa persona?* Ha bisogno di aiuto e dovrei aiutarlo, perché è uno di noi.
- *Questa persona rappresenta una minaccia?* Ovviamente no, perché è ben vestito.
- *Quanto tempo mi farà perdere?* Non importa, perché è uno di noi e ha bisogno del mio aiuto.

L'abito e il luogo collocano l'attore nella tribù giusta per ottenere l'aiuto necessario. La mentalità della tribù è davvero così forte. Pensateci: non è cambiato nulla che potesse fornire risposte più chiare a tre delle quattro domande. I passanti non possono sapere chi è l'uomo a terra, quanto tempo sia necessario per aiutarlo o se è una minaccia. Sanno solo che ha bisogno di aiuto.

Nello scenario dell'Operazione Petrolio, io ero un cittadino preoccupato, diventato sempre più arrabbiato e carico di odio nei confronti di un'industria che anche l'obiettivo odiava. Più conoscenze mi sono state fornite, più rabbia e disperazione ho esibito, e questo mi ha "iscritto" alla stessa tribù di OilHater.

Sia l'Operazione Petrolio sia il video *The Tribe Mentality* supportano la forza del pretesto che ho trattato nel Capitolo 4. Il pretesto aiuta tremendamente a collocarti nella tribù giusta. Una volta entrato nella tribù, ci sono 10 principi per la costruzione del legame che possono fare in modo che il vostro obiettivo parli con voi per tutto il tempo che volete.

L'ingegneria sociale per la costruzione del legame

Come definireste un legame? Quando pongo questa domanda ai miei allievi, ricevo vari tipi di risposte. Molti usano parole e frasi come "sviluppare una relazione", "fiducia" e "far sentire l'altro a proprio agio". Mi piace molto la definizione di legame che uso da alcuni anni e che ho messo insieme da varie definizioni: *costruire un ponte di comunicazione basato sulla fiducia e su interessi comuni.*

Costruire un ponte è per me una bella immagine mentale e i 10 principi trattati in questo capitolo puntano proprio a questo. Consentono alla persona con la quale si interagisce di sentirsi a proprio agio mentre si attraversa quel "ponte" per entrare nella sua tribù. Prima di raccontare il retroscena su come sono nati i 10 principi, dovete capire perché la fiducia è così potente.

La molecola morale

Nell'Episodio 44 di *The Social-Engineer Podcast*, ho avuto il privilegio di avere ospite Paul Zak. Come ho detto nel Capitolo 1, ha scritto il fantastico libro *La molecola della fiducia: all'origine della prosperità economica e sociale* (Scuola di Palo Alto, Milano 2015). In questo libro, Zak parla della sua ricerca sull'ossitocina. Per molti anni, l'ossitocina è stata ignorata dai ricercatori, ma Zak ha deciso di

scoprire come viene rilasciata nel flusso sanguigno e che cosa succede quando ciò accade.

Zak ha trovato molte ragioni per cui l'ossitocina viene rilasciata nel flusso sanguigno, e tutte hanno a che fare con la fiducia e le emozioni coinvolte. Un aneddoto di cui ha parlato in questo podcast riguarda un periodo in cui è stato vittima di una classica truffa chiamata *Pigeon Drop*. Da giovane, Zak lavorava in una stazione di servizio. Un giorno, un cliente riferì di aver trovato una scatola di gioielli in bagno. Mentre questo "buon cittadino" consegnava la scatola a Zak perché potesse metterlo nel cassetto degli oggetti smarriti nella stazione di servizio, squillò il telefono. Al telefono c'era un uomo che diceva freneticamente di aver perduto una scatola di gioielli. Il chiamante era così entusiasta di aver ritrovato i gioielli da offrire una ricompensa di 200 dollari a chi li avesse recuperati.

L'uomo che aveva trovato i gioielli disse che non poteva aspettare il proprietario e i soldi della ricompensa, perché aveva un importante colloquio di lavoro. Così, il chiamante suggerì quella che sembrava essere una soluzione straordinaria: Zak poteva semplicemente prendere 100 dollari dalla cassa del distributore e darli a colui che aveva trovato i gioielli. Al suo arrivo, con la ricompensa, Zak poteva tenere 100 dollari per sé e rimettere in cassa i 100 dollari che vi aveva preso. Il truffatore fece così entrare Zak nella "tribù", fidandosi di lui in due modi: avrebbe tenuto una parte del premio in denaro per aver trovato i "gioielli" e avrebbe fatto una buona azione per qualcuno. E così è stato truffato da questo dinamico duo.

è solo quando Zak fece ricerche per il suo libro che si rese conto del meccanismo impiegato dal truffatore. Quando la persona al telefono aveva fatto sentire Zak come se facesse parte di un gruppo di persone di fiducia e speciali, il cervello di Zak aveva rilasciato ossitocina e il suo cervello aveva associato questa sensazione positiva al chiamante.

Quindi, quando il chiamante gli chiese di togliere dalla cassa 100 dollari da dare all'uomo che aveva trovato i gioielli, acconsentì felicemente.

Il potere della fiducia può far sì che una persona faccia qualcosa che istintivamente sa che non sarebbe la cosa migliore da fare.

Quando applicate i 10 principi per la costruzione del legame trattati in questo capitolo, si induce il cervello (il vostro e quello dell'obiettivo) a rilasciare ossitocina. Questo rilascio fa sentire l'obiettivo fiducioso nei vostri confronti. La cosa che mi stupisce della ricerca di Zak è che questi sentimenti possano anche tornare in un secondo tempo, anche solo pensando o occupandosi del motivo per cui l'ossitocina è stata rilasciata (anche in voi, se avete avuto successo nello sviluppo di un legame con il vostro obiettivo).

Un'altra sostanza chimica importante è il neurotrasmettitore chiamato dopamina. Come hanno notato René Riedl e Andrija Javor in un articolo intitolato *The Biology of Trust: Integrating Evidence from Genetics, Endocrinology, and Functional Brain Imaging* (in "Journal of Neuroscience, Psychology, & Economics", 2012, http://psycnet.apa.org/buy/2011-27428-001), la dopamina è il principale neurotrasmettitore associato al meccanismo di ricompensa. L'articolo rileva inoltre che la combinazione di dopamina e ossitocina è fondamentale per la creazione di relazioni sociali. In sostanza, la dopamina e l'ossitocina contribuiscono a tutti quei processi che creano un legame di fiducia e rafforzano le interazioni sociali.

Capite ora l'importanza di comprendere il ruolo della dopamina e dell'ossitocina? Se imparate a usarle correttamente nella creazione del legame e della fiducia, potete costruire un ponte tra voi e il vostro obiettivo. Sviluppare quella relazione farà sì che il vostro obiettivo si senta felice (e fortunato di avervi incontrato) il che, ovviamente, garantirà un legame più forte.

I 10 principi per la costruzione del legame

Per l'Episodio 20 di *The Social-Engineer Podcast* mi trovavo fuori città per un allenamento. Mi sistemai in albergo per registrare il podcast, ma l'ospite che avevo contattato aveva disdetto all'ultimo momento e questo avrebbe rovinato il piano di registrare sempre un nuovo episodio ogni secondo lunedì del mese. Pensai… "Chi è già stato presente in passato, è stato un ospite di successo e posso chiamare anche all'ultimo momento?".

Scrissi al mio amico Robin Dreeke una breve e-mail, gli raccontai la situazione e gli chiesi se potesse intervenire. Rispose velocemente con un: "Ma sì, certo. Di quale argomento vuoi parlare?".

Senza pensarci, esclamai: "Delle migliori tecniche per costruire un legame con chiunque".

Disse: "Dammi un'ora per mettere insieme i pensieri".

Un'ora dopo, registrammo un podcast che non solo è diventato leggendario, ma ha condotto alla scrittura del primo libro di Robin. Questi sono i 10 principi di Robin trattati nel podcast e trattati nel suo libro.

- Usare vincoli temporali artificiali.
- Controllare la comunicazione non verbale.
- Usare un ritmo di conversazione lento.
- Impiegare i temi della simpatia e dell'assistenza.
- Sospendere l'ego.
- Dare fiducia agli altri.
- Porre domande sul come, sul perché e sul quando.
- Sfruttare un equivoco.
- Impiegare l'altruismo reciproco
- Gestire le aspettative.

Il libro di Robin tratta in dettaglio ciascuno di questi principi. Io li analizzo dal punto di vista del professionista dell'ingegneria sociale e, quando possibile, li relaziono all'Operazione Petrolio.

Usare vincoli di tempo artificiali

Un vincolo di tempo è semplicemente un limite di tempo nel corso di qualsiasi relazione con un'altra persona. L'aggiunta della parola "artificiale" sta solo a significare che siete voi a stabilire quel limite di tempo che, in verità, non esiste. Perché questo è importante per un ingegnere sociale? Pensate alla quarta domanda alla quale dovete rispondere per il vostro obiettivo: quanto tempo ci vorrà?

Il vincolo di tempo artificiale risponde a questa domanda. Il vostro limite di tempo artificiale può essere assolutamente inventato e falso, ma deve essere credibile. Quando sviluppate un vincolo di tempo, dovete considerare i seguenti fattori.

- Se il vincolo di tempo è troppo breve o troppo artificiale, non regge il gioco. Per esempio, considerate questa semplice domanda: "Posso parlarti un secondo?". Qualsiasi persona con la quale parlate saprà che "un secondo" non è un vincolo di tempo reale, quindi la vostra richiesta perde validità.
- Il vincolo di tempo deve anche essere realistico per il pretesto che avete scelto di usare. Per esempio, se considerate una persona in fila al supermercato, esiste un vincolo di tempo intrinseco: la lunghezza della coda. E non c'è bisogno di faticare troppo per creare un vincolo di tempo: vi basta restare all'*interno* del vincolo di tempo già esistente.

In Operazione Petrolio, ho potuto utilizzare i vincoli tipici della messaggistica privata sui forum come una sorta di vincoli temporali. Se avessi incluso una lunga diatriba sulle mie "sensazioni personali", il

mio obiettivo avrebbe dovuto leggere tutto prima che io potessi sviluppare un legame. Mantenendo i miei messaggi brevi e puntuali, ma emotivi, ho potuto limitare il tempo necessario affinché l'obiettivo rispondesse, quindi OilHater non si è sentito sotto pressione e coinvolto fino a quando non abbiamo costruito un legame. Più la conversazione si è fatta personale e coinvolgente, più i messaggi sono diventati lunghi.

Controllare la comunicazione non verbale

Questo principio è semplice da comprendere, ma difficile da attuare senza la pratica. Controllare la comunicazione non verbale significa che il linguaggio non verbale del corpo deve corrispondere al comportamento del pretesto impersonato.

Supponete di trovarvi ai grandi magazzini con vostro figlio. Mentre state facendo shopping, una persona vi si avvicina in modo un po' frettoloso e vi dice: "Devo andare alla festa di mio nipote e sto facendo tardi. Lui ha circa la stessa età di vostro figlio. Ho dimenticato di comprargli un regalo. Può dirmi che cosa piace ai ragazzi di quell'età?".

Mentre immaginate questa scena, rispondete a questa domanda: dove dovrebbe guardare la persona che vi ha avvicinato? Dimenticate per un attimo che possa essere un attacco di ingegneria sociale.

Questa persona dovrebbe guardare vostro figlio? No, assolutamente no. Una persona che guardasse intensamente vostro figlio probabilmente vi farebbe accendere tutti gli allarmi sul linguaggio non verbale e vi metterà automaticamente sulla difensiva.

La persona dovrebbe guardare voi? Sarebbe meno inquietante, ma non è del tutto congruente con quello che vi sta dicendo. Potrebbe sembrare troppo aggressivo.

Avrebbe più senso che la persona guardasse verso gli articoli o verso l'uscita, perché è di fretta. E così il suo linguaggio non verbale concorderebbe con quello che sta dicendo.

Quando il vostro linguaggio del corpo, non verbale, corrisponde a quanto state dicendo, l'obiettivo è in grado di rispondere alla terza domanda: "Sei una minaccia?". Questo consente di costruire correttamente il legame.

Qui si vede il motivo per cui ho detto che questo principio è difficile da attuare: faccio questo mestiere da più di dieci anni e sono ancora molto nervoso prima di ogni lavoro *vishing* o impersonificazione che svolgo. Se siete come me (e come la maggior parte delle altre persone), il nervosismo vi renderà tesi. E questa tensione vi irrigidirà i muscoli. Se il pretesto che avete scelto non prevede tensione o pressione, la vostra comunicazione non verbale non sarà allineata con lui (nel Capitolo 8 spiego questo concetto in modo più dettagliato).

In sostanza, è difficile trattenere le emozioni cercando di mantenere il realismo del pretesto scelto, almeno per tutti coloro che non sono sociopatici. E poiché sto scrivendo questo libro non per i sociopatici ma per coloro che aspirano a diventare professionisti dell'ingegneria sociale, il controllo dei segnali non verbali potrebbe non essere sempre facile.

Curiosità
Anche i sociopatici hanno una coscienza, secondo Michael Tompkins, psicologo presso il Centro di cura della salute mentale di Sacramento. Ma la coscienza di un sociopatico è debole. Un sociopatico può facilmente giustificare un torto che compie, sempre che vada a suo vantaggio, e in più gli manca l'empatia, che è uno degli elementi chiave delle comunicazioni umane.

Non vi suggerisco di predisporre la comunicazione non verbale per la vostra missione, ma di riflettere bene su quello che sarebbe normale per il pretesto scelto e di tenerlo bene in mente prima di proseguire.

Questo consiglio non vale solo per l’ingegneria sociale, ma anche per qualsiasi attività di *vishing*. Una cattiva postura può portare a tensioni muscolari delle corde vocali o della laringe, che possono influire sulla qualità della voce e caricarla di tensione. Se la vostra postura è errata e siete troppo tesi, questo può facilmente emergere nel tono di voce e pregiudicare la costruzione del legame.

Nell’Operazione Petrolio, potevo non preoccuparmi di questo principio.

Usare un ritmo di conversazione lento

Che cosa succede se cercate di parlare troppo velocemente di un argomento che non conoscete o che non vi piace? Iniziate a balbettare e a inciampare sulle parole. Inoltre, potreste ritrovarvi a usare espressioni come “ehm” e altre brevi parole di riempimento. Questo induce chi vi ascolta a dubitare delle vostre conoscenze e della vostra sincerità.

Tuttavia, se parlate troppo lentamente, chi vi ascolta potrebbe pensare che non conosciate quello di cui state parlando o che siate condiscendenti. Dovete trovare un equilibrio tra troppo veloce e troppo lento.

Come potete determinare la velocità perfetta con la quale parlare durante una missione? Semplice:

- Ritmo.
- Velocità.
- Volume.
- Tono.

Cercate di ascoltare e di adattarvi alla persona con la quale state comunicando. Le reazioni dell’interlocutore su questi quattro fattori vi daranno indicazioni su come dovreste comunicare.

AVVERTIMENTO

Quando dico che dovreste prestare attenzione a queste caratteristiche verbali dell'altra persona, *non voglio dire* che dovreste cercare di imitare il suo accento. E non importa quanto pensiate di essere bravi a imitare l'accento, a meno che disponiate di un maestro di dialettica a vostra disposizione per aiutarvi a perfezionare le piccole sfumature. Non provateci nemmeno. Essere sorpresi a imitare (male) un accento pregiudica il legame, ed è anche offensivo. Tuttavia, potete provare a utilizzare espressioni colloquiali che possono farvi sembrare un "locale". Imparare il gergo locale può aiutarvi a mimetizzarvi mentre usate questa tecnica per individuare la velocità perfetta.

Questo è un altro principio da tenere presente come ingegneri sociali e si sposa bene con l'ultimo principio. Non solo dovete considerare le caratteristiche verbali del vostro obiettivo, ma dovete anche assicurarvi che corrisponda al vostro pretesto. Se il pretesto deve avere un colloquio di lavoro, probabilmente sarà stressato. Non sareste credibili se foste calmi e se parlaste in modo rilassato.

Impiegare i temi della simpatia e dell'assistenza

Esiste un affascinante studio chiamato *Mirror Neuron and Theory of Mind Mechanisms Involved in Face-to-Face Interactions: A Functional Magnetic Resonance Imaging Approach to Empathy*, condotto dai ricercatori Martin Schulte-Ruther, Hans J. Markowitsch, Gereon R. Fink e Martina Piefk (`www.ncbi.nlm.nih.gov/pubmed/17651008`). Discute l'effetto che una richiesta di assistenza basata sull'empatia ha su un altro essere umano. Lo studio sottolinea come il semplice fatto di vedere qualcuno che sta effettuando una richiesta emotiva può attivare aree del cervello legate alle esperienze personali di sofferenza emotiva.

In altre parole, se la richiesta di solidarietà o assistenza viene gestita correttamente, la persona sottoposta a test manifesterà una forte

connessione emotiva con tale richiesta. Questa connessione fa sì che per quella persona sia praticamente impossibile rifiutare l'aiuto.

I marketer lo sanno bene, ed è per questo che molte campagne includono immagini e/o musica di sottofondo che evocano certe emozioni, insieme alle richieste. Sorprendentemente, il meccanismo funziona anche se non ci si trova faccia a faccia con l'obiettivo. Anche se la connessione è più potente quando vengono coinvolte le espressioni facciali, questo non è obbligatorio per innescare la connessione emotiva richiesta. Basta la voce o una vivida descrizione per indurre il soggetto a immaginare una scena e a scatenare una risposta empatica.

Questo principio è molto efficace per gli ingegneri sociali. Nel corso della storia, truffatori, *scammer*, *phisher* e, ancor più tragicamente, serial killer hanno usato i temi della solidarietà e dell'assistenza per convincere il loro obiettivo a fare cose che non avrebbero dovuto fare.

Ecco un suggerimento che si applica un po' a tutti i principi, ma che è particolarmente rilevante per questo: il livello dell'assistenza che richiedete deve essere commisurato al livello di legame che avete stabilito. Se un tipo che avete appena incontrato e il vostro migliore amico vi chiedono di aiutarli a spostare dei mobili, quale richiesta pensate di onorare con maggiore probabilità? Probabilmente sceglierete di aiutare il vostro amico, perché il livello di legame che avete con una persona aiuta a prendere decisioni e a dedicare tempo ed energie ad aiutarlo. Se qualcuno con il quale non avete alcun legame vi fa una richiesta di assistenza troppo personale o esagerata, ottiene l'effetto contrario: non costruisce un legame ma vi insospettisce.

Consentitemi di usare l'Operazione Petrolio per aiutarvi a fissare questi punti. All'inizio, la mia richiesta di solidarietà e assistenza si limitava semplicemente ai miei post sui forum e a richieste di aiuto per capire il *fracking*, perché ero preoccupato per i miei figli. Questa

richiesta non era rivolta al mio obiettivo: era una semplice richiesta di aiuto.

Dopo che OilHater si è dimostrato la fonte di informazioni “più esperta” sull’argomento, iniziai a rivolgergli richieste di assistenza più dirette. Più parlavamo e più cresceva il nostro legame, e più le mie richieste diventavano dettagliate e personali. Alla fine, sono stato in grado di applicare un derivato molto potente di questo principio, definito “ingegneria sociale inversa”. In altre parole, non occorre applicare i principi dell’ingegneria sociale per guadagnare il rispetto: il legame che avevo costruito con OilHater praticamente lo costrinse a fidarsi sempre più di me e a darmi sempre maggiori informazioni.

Zak disse che l’effetto dell’ossitocina (la molecola della fiducia) diventa più intenso quando fate sentire all’obiettivo che può fidarsi di voi. È questa fiducia che stabilisce il legame. È molto potente, ed è un fattore importante quando si è pronti a fare una richiesta all’obiettivo. Sono stato in grado di applicare questo principio durante l’Operazione Petrolio, e quando alla fine OilHater mi ha creduto abbastanza da chiedere il mio aiuto, quando il suo livello di fiducia ha raggiunto un punto in cui ha iniziato a condividere con me le sue reali intenzioni, a quel punto il nostro “legame” era inciso nella pietra. Chiedendo continuamente a OilHater una sempre maggiore assistenza nel comprendere il problema e le potenziali minacce e poi accorrendo in suo aiuto quando ne aveva bisogno, avevo stabilito un legame molto forte con lui.

Sospendere l’ego

Questo principio del legame è così potente, se riuscite a dominarlo, che potrebbe essere inarrestabile. Ma non è facile da stabilire come si potrebbe pensare.

Per capire perché il dominio di questo principio può essere difficile, devo definire la sospensione dell'ego. Una vera sospensione dell'ego significa letteralmente mettere da parte il proprio ego – il bisogno di primeggiare, di essere corretti o di sembrare intelligenti – e il concetto stesso di giusto e sbagliato. Quando sospendete il vostro ego, mettete da parte tutto al servizio dell'altra persona e questo non è un qualcosa che si possa fingere con facilità.

Perché questo è un meccanismo così potente, ma così difficile da attuare? Spesso le persone si sentono deboli se devono ammettere di non sapere qualcosa. E come vengono raffigurate, spesso, le persone deboli? Nei media, nei film, nella musica e nelle altre forme di intrattenimento, le persone umili o mansuete spesso sono considerate vittime. Secondo me, queste percezioni generali complicano la sospensione dell'ego. Nessuno ama essere percepito come un debole.

Ecco un esempio per aiutarvi a capire perché è difficile fingere: siete in piedi in fila al supermercato e alle vostre orecchie giunge una conversazione: "Una persona assolutamente affidabile mi ha detto, che per curare le allergie, tutto quello che devi fare è lavarti la faccia con una miscela di latte, miele e acqua di sorgente, per tre volte al giorno".

Molte persone penserebbero che la dichiarazione non ha alcuna validità scientifica. Qual è stata la vostra reazione quando avete letto quella dichiarazione? Se avete pensato a qualcosa tipo: "Questa è una delle cose più stupide che abbia mai sentito" o "Certe persone sono proprio strane", allora non stavate applicando la sospensione dell'ego. Sospendere l'ego significa sentire i pensieri di qualcuno su un argomento e reagire con: "Questa è la loro opinione e hanno ogni diritto di averla; questo mi permette di cercare di capire il loro punto di vista".

La sospensione dell'ego vi richiede di prendere in considerazione i pensieri, le dichiarazioni, le opinioni altrui come sacrosanti diritti, a

prescindere dal fatto che siate d'accordo con loro. Significa anche avere la capacità di non essere d'accordo senza con ciò diventare offensivi.

Un esempio presidenziale

Un esempio davvero sorprendente di sospensione dell'ego è stato esposto dall'ex-presidente degli Stati Uniti Ronald Reagan. Durante la seconda parte della presidenza Reagan, molti organi di informazione misero in dubbio la sua capacità di far fronte a un altro mandato come presidente degli Stati Uniti, perché era "troppo vecchio".

Reagan avrebbe potuto discutere, argomentare o tentare di dimostrare che i suoi critici avevano torto usando validi argomenti. Tuttavia, discutere un argomento di contesa spesso può solo aggiungere nuova benzina sul fuoco. Più vi sforzate di combattere, più sembrate dimostrare le ragioni degli oppositori, almeno in chi la pensa come loro. Al contrario, il presidente Reagan decise di essere il primo a giocare sulla propria età, usando un umorismo autoironico. Faceva battute su se stesso del tipo: "Ricordo quando venne alla luce una faccenda eclatante e i reporter si precipitarono gridando: 'Giù gli scalpelli!'". Adottò questo tipo di umorismo nei discorsi e nelle conferenze stampa.

La stampa intendeva puntare sul fatto che Reagan fosse troppo vecchio per fare il presidente. Ma portando l'argomento alla ribalta, Reagan fu in grado di prendere il controllo della situazione, in modo da "disinnescare" ogni attacco che facesse leva sulla sua età. Invece di arrabbiarsi, sospese l'ego e usò l'umorismo per chiudere la bocca agli oppositori.

In Operazione Petrolio sono stato in grado di applicare il principio della sospensione dell'ego agendo come se non avessi alcuna conoscenza del *fracking* e dell'industria petrolifera (anche se onestamente non dovetti fingere troppo…). Inoltre, non mettendo in discussione quanto diceva OilHater su quanto fosse terribile, pericolosa e mortale l'industria del *fracking*, sospesi il mio ego e permisi a OilHater di diventare "il capo". Ogni volta che l'ingegnere sociale sospende il proprio ego e permette all'obiettivo di gonfiare il proprio, si genera un mix perfetto per costruire un legame di successo.

Un altro fattore nel successo dell'applicazione di questo principio è quello di avere una certa conoscenza dell'argomento e la capacità di

porre buone domande. Una combinazione di conoscenze limitate e buone domande aiuta l'obiettivo a continuare a essere dominante e consente all'ingegnere sociale di mettere in atto la sospensione dell'ego. Ho usato questo aspetto del principio in Operazione Petrolio chiedendo continuamente a OilHater ulteriori informazioni, per aiutarmi ad approfondire la conoscenza delle piccole nozioni che avevo. Questo ebbe l'effetto di gonfiare il suo ego mentre io sospendevo il mio.

Dare fiducia agli altri

Il prossimo principio va di pari passo con la sospensione dell'ego. In poche parole, per dare fiducia dovete complimentarvi o approvare le dichiarazioni, le decisioni e le scelte dell'altro. Quando qualcuno sente di aver conquistato la vostra fiducia, il suo cervello rilascia dopamina e ossitocina, che a loro volta vi permettono di creare un sentimento di fiducia e di legame.

Ricordate quando ho parlato dell'utilizzo dei temi della solidarietà e dell'assistenza? La regola che ho menzionato è estremamente importante per la fiducia: il livello di fiducia *deve* essere uguale al livello del legame.

Per ribadire questo punto, ecco la storia di un insuccesso epico. Quando ero relativamente alle prime armi con l'impersonificazione come professionista dell'ingegneria sociale, entrai in un edificio. La mia missione era superare l'ingresso e il controllo alla reception e poi ai controlli. Vidi che l'incaricata dei controlli aveva una decina di foto dei suoi figli, ma rivolte verso l'esterno, non verso di lei. Questo mi diceva che era orgogliosa della sua famiglia e che voleva che tutti la vedessero. Le foto erano delle vacanze e nelle foto tutti sembravano davvero felici.

Provai a pensare su due piedi e a immaginare il modo migliore per costruire un legame, ma quello che mi uscì di bocca fu terribile. Guardai una foto, la indicai e dissi: “Ha davvero delle belle figlie…”. Le mie parole mi si spensero in gola quando mi resi conto che le sue figlie avranno avuto 12 o 15 anni. Ero mortificato e vedevo che lei aveva inteso male le mie parole.

Si accomodò meglio sulla sedia con un’espressione fra il sorpreso e il preoccupato, mentre le montava la rabbia. Mi guardò e disse: “Grazie”, ma con un tono severo, non educato. Poi aggiunse: “Chi è e che cosa vuole?”.

Mentre la guardavo, probabilmente ho esibito tutta una collezione di espressioni facciali: shock, spavento e disgusto… Poi dissi: “Oh, ho dimenticato una cosa in macchina. Torno subito”. Ma non tornai più: dovetti inviare un altro membro del team e in un altro giorno per completare la missione.

Oltre ad aver toccato un argomento massimamente delicato, non ero neanche lontanamente al livello di legame che mi permettesse di fare i complimenti alle sue figlie. Per conquistare la fiducia sarebbe stato meglio dire: “Wow, che bella vacanza. Dove siete stati?”. O anche: “Che bella foto. A volte dimentico di catturare questi bei momenti con i miei figli”.

In altre parole, in una conversazione iniziale con l’obiettivo, il vostro livello di legame sarà praticamente zero. Pertanto, il vostro dare fiducia non dovrebbe essere troppo personale.

SUGGERIMENTO

Assicuratevi di tener conto delle barriere culturali quando dovete dare fiducia sotto forma di regali o complimenti. Potete davvero rovinare un legame se attraversate un confine culturale in modo inappropriato. Allo stesso tempo, capire che cosa può essere importante per il vostro obiettivo può aiutarvi a scegliere la giusta forma di elogio.

Ricordate quando ho detto quanto sia potente la concessione della fiducia quando si mescola con la sospensione dell'ego? Questo perché quando voi sospendete l'ego e consentite all'altro di espandere il proprio, gli si dà fiducia. Quel sentimento di fiducia può creare un legame e quando una persona si sente degna di fiducia, il suo cervello rilascia di nuovo le sostanze chimiche del benessere (la dopamina e l'ossitocina) e voi ne siete la causa.

In Operazione Petrolio, sono stato in grado di utilizzare continuamente il senso di fiducia con i seguenti mezzi:

- ho sospeso il mio ego;
- ho dato fiducia all'obiettivo;
- mi sono complimentando per le sue conoscenze;
- ho ascoltato i suoi consigli e ho chiesto chiarimenti;
- ho accettato la sua idea per "risolvere" il problema.

Più davo fiducia (coi dovuti modi) a OilHater, più forte è diventato il legame tra noi.

Porre domande sul come, sul perché e sul quando

Perché le domande "come", "perché" e "quando" sono così potenti nella costruzione di un legame? Perché le risposte a queste domande non possono limitarsi a un sì o a un no.

Già questo dovrebbe aiutarvi a capire perché la fiducia è così importante. Ricordate che date fiducia a qualcuno quando chiedete il loro parere e poi ascoltate la sua risposta.

> **AVVERTIMENTO**
> Quando usate domande a risposta aperta, è fondamentale che poi ascoltiate la risposta. Nulla pregiudica di più la fiducia di qualcuno che vi sta dando la sua opinione se voi sembrate annoiati o non prestate attenzione. Questo significa anche che non potete pensare alla prossima mossa mentre l'altro sta parlando.

Le domande a risposta aperta sono ottime per mantenere viva la conversazione. Molte volte, una breve pausa dopo una domanda e l'ascolto della risposta incoraggia l'altro a continuare a parlare.

Tuttavia, fate attenzione a non produrre raffiche di "perché". Fareste la figura del bambino di tre anni che chiede continuamente "Ma perché? E perché? Perché?". Per quanto siano carini, quando fanno così i bambini di tre anni non si dimostrano esattamente abili costruttori di legami.

In Operazione Petrolio, ho usato costantemente i come, i perché e i quando. Usavo frasi come "Perché il *fracking* è così dannoso per l'ambiente?" o "Come possiamo davvero impedirgli di danneggiare la mia casa?".

Questo tipo di domande ha permesso a OilHater di aprirsi e di offrirmi le sue conoscenze su questi argomenti. L'ascolto attivo è molto più facile da svolgere online che di persona, perché potete leggere le frasi più volte e assimilare le informazioni prima di rispondere. Tuttavia, è necessario faticare per essere ascoltatori attivi anche quando si comunica online. Per esempio, il mio amico Jim Manley si arrabbia con me quando mi invia un'e-mail di otto paragrafi per descrivermi un problema o una situazione, ma io leggo solo una o due frasi e poi rispondo con una domanda. Mi risponde immancabilmente con qualcosa del tipo: "LEGGI TUTTA LA E-MAIL, HADNAGY!!" (e… sì, ho censurato drasticamente il tono delle sue risposte). Se siete come me, dovrete fare pratica con l'ascolto attivo… anche nella scrittura.

In Operazione Petrolio, ho applicato l'ascolto attivo e ho usato domande aperte per far continuare a parlare l'obiettivo.

Sfruttare un equivoco

È un *qui pro quo*. Pensatela in questo modo: vi siete mai pentiti di un acquisto? Avete speso del denaro per qualcosa, e la cosa vi ha molto emozionato. Ma quando siete arrivati a casa e avete aperto la confezione, avete iniziato a pensare: “Ho davvero speso così tanto per questa cosa?”.

Questo rimorso è il risultato della sensazione che quello che avete ottenuto non valeva quanto avete dato. Uno dei peggiori errori che un ingegnere sociale può fare è insinuare nel suo obiettivo il sentimento del “rimorso del compratore”. In termini di ingegneria sociale, il rimorso del compratore si ha quando l’obiettivo pensa fra sé e sé: “Quel tipo, quello con cui ho avuto quella bella conversazione oggi… Hmm, ma come si chiamava? Di dov’era? Aspetta, io gli ho detto il mio nome e cognome, la data di nascita, gli ho mostrato la foto dei miei figli e anche la mia patente e… non so nemmeno come si chiama!”.

Quella conversazione mentale può creare paura e ansia nell’obiettivo, perché quello che vi ha dato non gli è sembrato equilibrato con quello che voi gli avete dato. Ora, prima di passare oltre, ho scritto “non gli è *sembrato* equilibrato” e non “non era equilibrato”. C’è un’enorme differenza tra queste due frasi.

Per una missione, mi trovavo in un negozio e mi sono avvicinato all’obiettivo, che era con suo figlio, un ragazzo. Mi assicurai di tenere lo sguardo rivolto verso gli scaffali ed esordii dicendo: “Mi scusi. Sto andando a una festa e sono molto in ritardo. Mia moglie vuole ammazzarmi, perché avrei dovuto acquistare un regalo per nostro nipote, che ha più o meno l’età di suo figlio. Che cosa piace ai ragazzi di questa età?”.

Con questo esordio, ho stabilito l’equivoco, fornendo all’obiettivo tutta una serie di informazioni:

- che sono sposato;

- che ho un nipote, quindi ho un fratello o una sorella con dei figli;
- che sono in ritardo;
- che sto andando a una festa;
- che non ne so nulla di ragazzi.

In una o due brevi frasi, ho comunicato al mio obiettivo molte informazioni. Nel momento in cui la missione è terminata, avevo quanto mi serviva della sua storia, e mi sono garantito che non avrebbe provato il rimorso del compratore, perché ormai "mi conosceva".

SUGGERIMENTO

Le informazioni che fornite non devono necessariamente essere reali (nome, numero di bambini e così via), *ma* ricordate sempre che più dettagli falsi producete, più ne dovrete ricordare. Per questo motivo, evitate di fornire dettagli eccessivi.

Nell'Operazione Petrolio, usai l'equivoco un paio di volte, ma soprattutto quando OilHater programmò il nostro incontro da Peg. Gli diedi il mio nome completo e indirizzo per stabilire il legame di fiducia e perché speravo che avrebbe ricambiato. Lo fece, il che mi permise di bloccare con successo un potenziale atto violento.

Impiegare l'altruismo reciproco

Pensate a questo principio in termini semplicistici. Un seghetto alternativo va avanti e indietro, avanti e indietro, ed è così che funziona il principio del legame. Esternate altruismo (in termini di parole e di azioni) dando qualcosa di importante all'obiettivo e l'obiettivo ricambia con qualcosa di suo.

Se aprite la porta a qualcuno mentre si sta dirigendo a un ingresso e ci sono due porte da attraversare, che cosa farà quasi sempre l'altro? Terrà la seconda porta aperta per voi. Questo è altruismo reciproco. Come applicare questo concetto all'ingegneria sociale? Se date qualcosa di valore a una persona, questa si sentirà in debito e vorrà

ricambiare la vostra generosità. *Ora ecco una domanda molto importante*: chi determina il valore del dono?

È il destinatario a determinare il valore, non voi. La connessione con quello che è importante per l'obiettivo può essere fatta tramite l'OSINT, l'osservazione o l'improvvisazione, ma in ogni caso non dovete supporre che perché voi apprezzate qualcosa, anche l'obiettivo lo apprezzerà. D'altra parte, se riuscite a trovare qualcosa che l'obiettivo apprezza veramente, i sentimenti che lo spingeranno a ricambiare saranno sufficientemente forti da costringerlo a ignorare molti protocolli di sicurezza.

Una volta entrai in un ufficio e mi avvicinai alla portineria. La donna sembrava in lacrime. Abbandonai un attimo la veste dell'ingegneria sociale e le dissi: "Tutto bene?".

Ero sinceramente preoccupato e lei se ne accorse, così rispose: "Sono venuta al lavoro stamattina indossando gli orecchini che mio marito mi ha regalato per il nostro decimo anniversario. Ha risparmiato due anni per comprarli e ora ne ho perso uno". E scoppiò di nuovo a piangere.

Dissi: "Beh, forse è sul pavimento" e mi chinai sul pavimento, iniziando a cercare. Anche lei fece altrettanto, mentre diceva: "Ho già controllato, ma credo che non sia una cattiva idea controllare di nuovo".

Il Sole entrò dalla finestra e vidi un piccolo luccichio sulla sua spalla. Dissi: "Probabilmente ha già controllato, ma vedo un luccichio proprio sulla sua spalla. Mi permette?".

Si sporse in avanti e io presi dal suo maglione un bellissimo orecchino di diamanti e glielo porsi. Le sue lacrime di dolore si trasformarono in gioia, mentre mi abbracciava e mi ringraziava così tante volte da finire per essere imbarazzante.

Poi disse: “Mi scusi. L’ho trattenuta per così tanto tempo. Come posso aiutarla?”.

In quel momento decisi di tornare in modalità “ingegnere sociale”, perché mi resi conto che qualsiasi richiesta avessi fatto in questo momento avrei avuto successo. “Be’, era così sconvolta, che non volevo farle troppa fretta. Sono in ritardo con un colloquio di lavoro, quindi mi scusi se prendo le mie cose e corro su”. Mi alzai, presi la borsa e le cartelle e mi avviai verso la porta. Camminai come se volessi attraversarla e, avvicinandomi, sentii il ronzio meccanico della porta che si apriva.

Il regalo che avevo involontariamente dato alla portinaia (trovando il suo prezioso orecchino dell’anniversario) valeva più del potenziale imbarazzo che avrebbe provato nel fermarmi, dato l’incontro importante cui dovevo partecipare, per qualcosa di così stupido come un protocollo di sicurezza.

Nell’Operazione Petrolio, ho usato l’altruismo reciproco in un paio di modi. In primo luogo, ho ascoltato e prestato fede alle conoscenze di OilHater. In secondo luogo, ero disposto a rinunciare a un po’ del mio tempo per incontrarlo e per occuparmi del problema. Entrambe le cose hanno costruito un legame di fiducia e questo ha condotto OilHater a prendere una decisione che *non* era nel suo migliore interesse.

Gestire le aspettative

Quando applicate questi principi, vedrete schiudersi porte che non avreste mai immaginato di aprire. È quasi come essere telepatici o maestri Jedi. Iniziate una conversazione e, prima che ve ne accorgiate, la persona vi sta raccontando la storia della sua vita. Il problema è *non usare* questi principi nella vita di tutti i giorni: dovete imparare a disattivare queste tecniche, a non essere sempre “attivi”. Un altro

problema è l’enorme mole di informazioni che riceverete sulle persone, il che può essere travolgente.

Il momento intermedio dell’instaurazione del legame è quello in cui dovete applicare di più questo concetto. Se la fiducia, la confidenza e il legame rilasciano dopamina e ossitocina nel vostro obiettivo, lo stesso accade a voi. Quando vi sentite bene, quelle stesse sostanze chimiche vengono rilasciate anche in voi e provate le stesse sensazioni positive, che possono indurvi a correre rischi inutili. Se vi spingete troppo oltre o se affrettate troppo le cose, potete rovinare il legame in un modo che potrebbe essere quasi impossibile da ricostruire.

L’altro lato della medaglia è la gestione delle vostre aspettative quando le cose non vanno come desiderate. Ricordate questo motto: “Lasciate che si sentano meglio per avervi incontrato”. Se notate che i vostri sforzi non sortiscono alcun risultato o, peggio ancora, fanno insorgere emozioni negative, è meglio accampare una scusa e andarsene piuttosto che proseguire. Non volete rovinarvi la reputazione di serio professionista della sicurezza solo perché il vostro bisogno di riuscita è più forte del vostro desiderio di lasciare che i vostri clienti si sentano bene.

Poiché questi principi funzionano tutti incredibilmente bene, può essere difficile imparare a non utilizzarli nella vita quotidiana quando non si sta lavorando. Non dovete trattare le persone come vostri strumenti. Una parte della gestione delle vostre aspettative è imparare che quando usate questi principi in un ambiente non professionale, dovete adattare il modo in cui comunicate.

Nell’Operazione Petrolio, dovetti gestire le mie aspettative perché ci sono volute quasi due settimane prima che OilHater rispondesse ai miei messaggi nei forum. Poi ci fu un periodo in cui tacque e dovetti pensare a come avrebbe reagito Paul. Anche se volevo che OilHater continuasse a scambiare messaggi con me, non avevo idea se fosse

sparito per sempre o solo per pochi giorni. Gestire le mie aspettative e avere pazienza ha portato a un risultato positivo.

La macchina del legame

Una delle domande che più spesso mi vengono rivolte su queste competenze è come metterle in pratica senza essere ingegneri sociali (per esempio, durante le esercitazioni), in modo che risultino più naturali quando dovranno essere impiegate in modo professionale. In questo paragrafo, vi do alcuni consigli su come fare pratica e perfezionare i 10 principi.

Usate gli amici e la famiglia

Non occorre aspettare di essere pronti per fare pratica. Scegliete un principio, per esempio la concessione di fiducia, e provate ad applicarla la prossima volta che vi riunite tutti insieme in famiglia. C'è quel cugino che non vedete da un po'; cercate di fargli un complimento sincero. Fate seguire una domanda personale, sulla sua vita, e ascoltate attivamente la sua risposta. Guardate come è disposto a rispondere.

Alla successiva riunione di famiglia o di lavoro, scegliete un altro principio, per esempio controllare la comunicazione non verbale, e prendete nota mentalmente dei diversi modi in cui le persone reagiscono in base a quanto le guardate. Nel corso del tempo, inizierete a sviluppare un kit di strumenti che funzionano e che non funzionano e inizierete a mettere in pratica questi principi anche senza pensarci attivamente.

Leggete

Ci sono molti libri (come quelli di Robin Dreeke), che parlano della costruzione di un legame. Potete trovare un elenco abbastanza completo su `www.social-engineer.org/resources/seorg-book-list`. Leggere dell'uso di questi principi li rafforzerà nella vostra mente e vi aiuterà a richiamarli quando ne avrete bisogno.

Prendete nota dei fallimenti

Quando le cose non funzionano come previsto e una conversazione prende una brutta piega, non cercate di negare la cosa e dimenticarla. Prendete invece nota di quello che è successo e perché.

Ho imparato più dai miei fallimenti che dai miei successi e, di conseguenza, i miei successi si basano proprio sui miei fallimenti. Imparare dai fallimenti e prenderne nota mi consente di insegnare meglio queste competenze e di essere un professionista migliore nel campo dell'ingegneria sociale.

Riepilogo

Questo capitolo vi ha insegnato a riconoscere, utilizzare e sfruttare le capacità di costruzione di un legame. Queste abilità sono potenti quando si comunica con altre persone e sono essenziali per diventare ingegneri sociali professionali.

Indipendentemente dal fatto che stiate svolgendo attività di *phishing*, *vishing*, *SMiShing* o stiate impersonando qualcuno, avete bisogno di queste capacità per trarre il massimo beneficio. Ma un'ultima nota: se è importante imparare a costruire il legame, è altrettanto importante imparare a disimpegnarsi senza rovinare il legame.

Ho notato che la fase di disimpegno tende a essere una delle abilità più difficili da acquisire da parte dei miei allievi dopo aver appreso i

principi del lavoro, perché questa fase ci fa sentire male. Il vostro obiettivo vi sta raccontando la storia della sua vita e vi dice tutto quello che volevate sapere (e anche alcune cose che non volevate sapere) e ora dovreste semplicemente andarvene via?

Beh, no. Dovete imparare a disimpegnarvi. E se avete seguito i 10 principi, disimpegnarvi vi sarà facile. Ecco un paio di esempi.

Se avete usato vincoli temporali artificiali, potete guardare l'orologio e dire: "Accidenti! Non posso credere che sia passato così tanto tempo. È così interessante che ho perso la cognizione del tempo *[fiducia]*. Sono veramente desolato, ma devo scappare *[sospensione dell'ego]*".

Se impiegate l'equivoco e la fiducia per costruire un legame, potete dire: "Sa una cosa? È talmente affascinante parlare con lei *[ulteriore convalida]* che ho dimenticato di comprare l'insalata per mia moglie/marito. Farò meglio a sbrigarmi *[conferma dell'equivoco, dando all'obiettivo ulteriori informazioni 'personali', ovvero che siete sposati e che stasera cenerete a insalata]*!"

Trovo utile pianificare alcune strategie di commiato in linea con il pretesto che sto usando. Questo mi dà modo di ribadire la fiducia e un modo gentile per sottrarmi alla situazione senza pregiudicare il legame costruito.

AVVERTIMENTO

Se iniziate a utilizzare le tecniche di costruzione del legame in un ambiente chiuso, per esempio un aereo, un treno o altri mezzi di trasporto pubblici, sappiate che avrete ben poche strategie di uscita. Per esempio, se ho bisogno di usare questi principi in aereo, di solito mi preparo un vincolo di tempo artificiale, che è più o meno questo: "Ho in mente di schiacciare un pisolino, così posso mettermi subito al lavoro quando atterro, ma prima volevo chiederle da dove viene?". Informando preventivamente la persona che *non* voglio impegnarmi in una lunga conversazione. Tuttavia, dopo molte volte in cui non ci sono riuscito ed essere stato bloccato a parlare con qualcuno per tre ore (o addirittura nove ore in un viaggio!) invece di ricorrere alla scusa del sonno (del quale avrei tanto bisogno), indosso le cuffie ed evito il contatto di sguardi.

Il legame vi collega ai vostri simili. Mentre vi legate a un numero sempre maggiore di persone, avete la possibilità di farle sentire meglio o anche peggio per avervi incontrato. In ogni scelta che fate nell'uso di queste abilità avete il potere di influenzare o manipolare la persona con la quale state parlando. Questo è il tema del Capitolo 6.

Sotto la mia influenza

Il segreto della mia influenza è sempre stato che è rimasta segreta.
- *Salvador Dalì*

Questo capitolo riguarda sia l'influenza sia la manipolazione, ma per ora voglio concentrarmi sull'influenza. Come definireste l'influenza?

Io la definisco come "convincere qualcuno a *voler fare* quello che voi volete che faccia". Questo significa che la persona è convinta di voler fare quello che volete voi, o almeno così lo ricorderà. Poiché la persona percepisce l'idea come propria, la considererà un'ottima idea e si impegnerà nel portarla a compimento.

Una delle più grandi menti su questo argomento è Robert Cialdini. Per decenni ha studiato, scritto e perfezionato l'arte dell'influenzare gli altri. Nell'Episodio 86 di *The Social-Engineer Podcast* ho avuto il privilegio di ospitare Bob (così chiese di essere chiamato). È stata una delle conversazioni più affascinanti che abbia avuto e da lui ho imparato davvero molto.

Bob ha scritto un libro, che uso ancora oggi, intitolato *Influence: i 6 segreti per farsi dire sì* (Mylife, Coriano di Rimini 2011). In questo libro, tratta i sei principi definibili, insegnabili e tracciabili dell'influenzamento. Per praticità, ho suddiviso i sei principi di Bob in otto principi.

In questo capitolo, per prima cosa definisco questi otto principi così come sono stati studiati e approfonditi da grandi menti come quella di

Cialdini. Dopo la definizione di ciascun principio, ne lego il concetto all'ingegneria sociale.

Dopo aver trattato ciascun principio, parlo del quadro di riferimento, che è strettamente legato all'influenzamento. In poche parole, il quadro di riferimento è il fondamento su cui si basano le vostre convinzioni, i vostri punti di vista e i vostri pensieri. Più avanti nel capitolo discuterò su come potete modificare il quadro di riferimento nel vostro obiettivo. Parlo anche di manipolazione, il cugino più oscuro e sinistro dell'influenzamento e poi riassumo il tutto, fornendovi alcuni consigli e indicandovi la strada per impadronirvi di questo straordinario talento.

Lezione di abilità

Nella mia carriera, ho avuto l'opportunità di usare le mie competenze per contribuire a rintracciare, fermare e arrestare persone che si rivolgono ai bambini. Un caso mi aiuta a definire l'influenzamento nel modo in cui ne ho parlato nell'introduzione del capitolo.

Per questa missione, che chiameremo Operazione Rent-a-car, dovevamo scoprire l'indirizzo di un tipo che sapevamo essere un trafficante di bambini. Le autorità avevano dimostrato il suo coinvolgimento con altri mezzi, ma il personaggio si era trasferito così tante volte che il suo indirizzo non era veramente noto. Sapevamo che stava noleggiando un'auto dopo un volo che lo aveva portato in una certa città. La missione era quella di scoprire il luogo dal quale aveva noleggiato l'auto e cercare di influenzare l'agente in modo che ci comunicasse il suo indirizzo.

Il mio pretesto? Ero il proprietario di un ristorante-pizzeria in città. Avevo trovato nel ristorante un iPad appartenente al nostro obiettivo e volevo restituirglielo, ma era bloccato. Sapevo che ottenere il suo indirizzo sarebbe stato difficile, quindi avevo in mente di offrire il pranzo all'incaricato del noleggio, in cambio di suggerimenti su come rintracciare il tipo.

C'è voluto del tempo, ma alla fine trovai l'agenzia di noleggio, che confermò che l'auto era stata effettivamente noleggiata da loro. Una parte della mia conversazione con l'incaricato al noleggio andò come segue.

NOTA

Per motivi di sicurezza, ho usato solo nomi di fantasia per l'incaricato al noleggio di auto e per il ristorante.

Io: Senta, mi trovo in un vicolo cieco, quindi ho una pizza gratis in cambio di una qualche buona idea che potrebbe avere in mente…

Incaricato: Adoro la sua pizza Big Tony! Che cosa posso fare per lei?

Io: Beh, vorrei spedire questo iPad direttamente al proprietario, ma non conosco il suo indirizzo. Che ne dice se io glielo porto e ci pensa lei a spedirglielo?

Incaricato: Tony, non posso. Sono veramente dispiaciuto, ma la nostra politica prevede che non siamo responsabili dei beni che rinveniamo all'interno delle vetture.

Io: Sì, questo ha perfettamente senso. Porc… Non so cosa fare. Che cosa dovrei fare, secondo lei, per farglielo riavere?

Incaricato: [*Ci pensa qualche istante, poi mi sussurra*] Guardi… non dovrei farlo, ma… e se io le dessi il suo indirizzo e così glielo spedisce?

Io: Steve, sei un genio! Perché non ci ho pensato? Sai cosa? Quando abbiamo finito, ti offro un buono da 25 dollari qui da noi.

Notate che per ben due volte nella conversazione, ho insinuato nell'incaricato l'idea che mi desse l'indirizzo, ma poi ho fatto il finto tonto invece di chiederglielo. Questo è un ottimo esempio di come, giocando con i principi di influenzamento, ho insinuato pensieri sul modo in cui ottenere l'indirizzo, per fare in modo che l'idea sembrasse provenire dall'obiettivo. Questo ha fatto sì che non dovessi convincerlo a fare quello che volevo facesse.

Negli argomenti di questo capitolo, noterete molte somiglianze con i principi del legame.

NOTA

Ho lanciato un'organizzazione senza scopo di lucro chiamata Innocent Lives Foundation (www.innocentlivesfoundation.org) che ha lo scopo di salvare i bambini dalle mani dei predatori. I membri della fondazione sono tutti professionisti della sicurezza che lavorano a stretto contatto con le forze

dell’ordine per scoprire persone che cercano di nascondersi in Internet e di adescare i bambini. Le competenze trattate in questo libro sono state ampiamente utilizzate per scoprire quei predatori e aiutare a salvare bambini.

Principio 1 – La reciprocità

Questo principio è molto simile all’altruismo reciproco nella costruzione di legami. Si basa sul modo in cui gli esseri umani si sentono spinti a ricambiare quando ricevono gentilezze o quando ricevono cose che gradiscono. Secondo Cialdini, anche se non vogliamo ciò che ci viene dato, il nostro cervello non si sente a suo agio fino a quando non sente di aver ricambiato la gentilezza. I marketer lo sanno bene e usano continuamente questo principio.

La reciprocità in azione

Pensate all’ultima volta che siete stati in un negozio di alimentari e avete ricevuto un campione gratuito. Il negozio o l’azienda di marketing che ha allestito l’idea del campione sa che la maggior parte delle persone è più incline all’acquisto del prodotto dopo aver ricevuto un campione gratuito.

Ma le persone sono anche più inclini a soddisfare una richiesta dopo un complimento.

Ero con mia moglie e mia figlia a Londra per lavoro. Avevamo acquistato biglietti economici premium per poter tornare a casa in relativa comodità. Come tre piccoli viaggiatori ubbidienti, arrivammo all’aeroporto con tre ore d’anticipo.

Avevo con me il carrello per i bagagli, ma le nostre debordanti borse erano in bilico, sull’orlo della distruzione. Mi stavo avvicinando al check-in quando un piccolo avvallamento nel pavimento fece cadere a terra tutte le nostre borse con un forte tonfo! Così pronunciai ad alta voce una battuta: “Incidente sulla M5!”.

A causa del mio forte accento americano, tutti gli inglesi sorrisero al pensiero di un americano che usava il nome di una strada inglese per scherzare. Una donna al check-in alzò gli occhi dal computer, sorrise e ci chiamò. Estrassi i passaporti per consegnarli e mia moglie iniziò a farle complimenti per la sciarpa.

Ora, mia moglie di lavoro non fa l'ingegnere sociale. È semplicemente un essere umano fantastico, bello e meraviglioso, che adora veramente il prossimo. Quindi, stava sinceramente complimentandosi con questa donna dicendole cose come: "Wow, che make-up perfetto" e "Adoro il modo in cui la sua sciarpa si abbina col colore degli occhi".

Osservavo questa interazione e vedevo l'atteggiamento non verbale di questa donna, che era semplicemente raggiante di orgoglio, felicità e ripiena di tutte le buone sostanze chimiche che un cervello può rilasciare. Immediatamente pensai: "Questo è il tuo momento, Chris, cala la tua richiesta".

Mentre consegnavo i passaporti, mi chinai su mia moglie e dissi alla donna: "La mia bellissima moglie e io saremmo curiosi di sapere: quanto costerebbe passare a una classe superiore per il volo di ritorno?".

Non scherzo: la signora al check-in iniziò a digitare freneticamente. Ci regalò tre biglietti di prima classe senza costi aggiuntivi, con accesso completo alla sala VIP per le tre ore di attesa.

Pensateci: qualche complimento preceduto da una battuta scherzosa e seguito da una richiesta. Un trionfo della reciprocità!

La mia idea della reciprocità è rappresentata nella Figura 6.1.

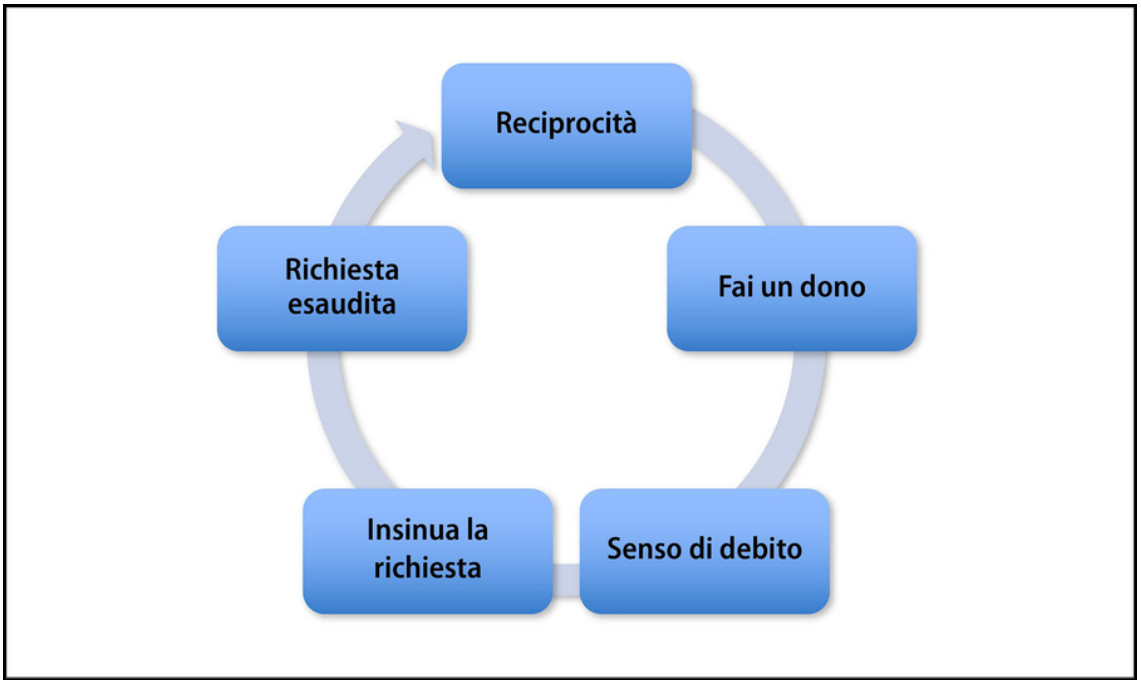


Figura 6.1 La reciprocità in azione.

La reciprocità funziona solo quando viene seguito questo percorso. Non potete insinuare troppo presto il comando o la richiesta. Potete "calare" la vostra richiesta solo dopo aver creato quel senso di debito, il quale aumenta la possibilità che la richiesta venga onorata.

La reciprocità nell'ingegneria sociale

Probabilmente avete in mente chissà quante idee su come usare il principio di reciprocità. Lasciate che vi dia un consiglio: il livello della richiesta che potete fare dipende dal valore percepito del regalo che avete fatto al destinatario.

Rifletteteci un attimo. Cialdini dice che l'obiettivo si sentirà in debito, indipendentemente dal fatto che desiderasse quel che gli avete dato. Se il destinatario reputa che il dono è di valore, si sentirà ancor più costretto a restituire un dono di valore uguale o maggiore.

Faccio parte di un piccolo gruppo di hacker che sono anche appassionati degustatori di whisky. Quando ci ritroviamo, a volte ci scambiamo delle bottiglie di whisky. Ognuno di noi porta qualcosa per gli altri, quindi ognuno di noi se ne torna a casa con qualcosa di differente, pensato dagli altri. Spesso stabiliamo un tema, in modo che non possa accadere che qualcuno di noi torni a casa con qualcosa che vale un centinaio di dollari, mentre qualcun altro se ne torni con qualcosa che vale molto di più. Questo tiene sotto controllo il principio della reciprocità, così che nessuno si senta troppo indebitato (o in credito).

In qualità di ingegneri sociali, è imperativo che per prima cosa scopriate che cosa può essere prezioso per la persona o l'azienda che è il vostro obiettivo. Dovete preparare il vostro pretesto avendo questo in mente. Se poi offrite all'obiettivo qualcosa di valore, avrete ancora maggiori probabilità di riuscita.

Per esempio, nella missione di cui vi ho appena parlato, l'Operazione Rent-a-car, scoprii abbastanza rapidamente che all'obiettivo piaceva veramente Tony's Pizza. Grazie a questo, ho offerto un pasto gratis in cambio delle sue meravigliose idee. Non dissi: "Se mi dai il suo indirizzo, ti regalo una pizza". Perché no?

La ragione è semplice: in quella fase non avevamo ancora costruito un legame. Chiedere l'indirizzo di un cliente prima di aver costruito un legame con l'obiettivo lo avrebbe indotto ad alzare tutte le difese, gli scudi e ad accendere l'allarme rosso.

Con l'offerta della pizza gratis, seguita dall'insinuazione di quello che volevo veramente, ho fatto in modo che l'obiettivo se ne "venisse fuori" con l'idea della quale, guarda caso, avevo bisogno.

Curiosità
Non volevo che l'incaricato andasse da Tony e non ricevesse il suo buono. Dopo aver riattaccato, chiamai subito Tony e acquistai per telefono il buono di 25 dollari a suo nome e gli dissi di scriverci sopra "da Tony".

Ecco un’altra situazione in cui utilizzai questo principio: dovevo incastrare col *phishing* un amministratore delegato. Durante la fase di OSINT, avevo scoperto che amava correre e iscriversi alle maratone. Lo scoprii perché aveva scattato tonnellate di *selfie* mentre correva le maratone.

La missione di *spear-phishing* era pagata da una società di marketing per una recente maratona alla quale aveva partecipato. Il messaggio diceva qualcosa del tipo: “Durante la recente maratona *Run for Kids* cui avete preso parte, abbiamo scattato alcune foto che vorremmo usare per attività di marketing e promozione. Abbiamo bisogno della sua approvazione per poter usare queste foto. Fate clic per vedere le foto e approvarle”. Se ricordo bene, l’amministratore delegato aveva fatto clic sul link meno di 60 minuti dopo aver ricevuto il messaggio.

Se trovate qualcosa che l’obiettivo apprezza veramente, esaudirà la vostra richiesta senza pensarci su due volte.

Principio 2 – L’obbligo

L’obbligo sembra molto imparentato alla reciprocità, ma con una piccola differenza. Mentre la reciprocità è il senso di debito a causa di un regalo o di qualcosa di valore che ha dato origine all’azione, l’obbligo è quello stesso senso, ma sulla base di norme sociali o comportamenti attesi.

L’obbligo in azione

Ho posto la seguente domanda agli allievi di tutto il mondo: se vi trovate in coda e permettete a un altro automobilista di passare davanti a voi, che cosa pensate sia obbligato a fare? Che cosa *deve* fare, secondo voi?

Gli allievi rispondono che l'automobilista deve alzare una mano o fare un cenno della testa, ovvero deve (è tenuto a) mostrare un certo livello di rispetto e apprezzamento per la gentilezza che ha appena ricevuto. Che cosa succede se non lo fa?

Ero a Washington, mi recavo a una riunione su una bellissima autostrada a quattro corsie e il traffico era costretto a confluire in una sola corsia, così si è formata una coda. Ero determinato a non lasciarmi prendere dal nervoso, così misi su della musica mentre procedevo piano piano. Altre macchine cercavano di confluire sull'autostrada da una rampa d'accesso e gli altri automobilisti non si sentivano troppo altruisti. Non permettevano agli altri di entrare nel flusso. Così rallentai un po' e lampeggiai per far passare il prossimo.

Mentre si piazzava davanti a me, lo guardai attraverso il suo lunotto, alla ricerca di un cenno della testa, di un cenno o di uno sguardo riconoscente, nello specchietto retrovisore. Non lo vidi, e mi sentii ribollire il sangue. La mia faccia divenne paonazza e la mia guida divenne più aggressiva. Iniziai a pensare: "Hanno fatto bene tutti gli altri, a non farti passare!", come se gli altri automobilisti avessero una sorta di sesto senso che aveva permesso loro di capire che questo automobilista era maleducato.

Costruii un'intera trama su questo arrogante spreco di carne umana che avevo davanti. Quando le corsie si riaprirono, pochi chilometri dopo, ero deciso a dirgli il fatto suo e a sorpassare il maleducato automobilista per mostrargli a chi aveva rubato la strada.

Pigiai l'acceleratore e tutti i sei cilindri della mia potente auto sportiva entrarono in azione. Come mi trovai accanto all'altro automobilista, lo guardai con disprezzo e vidi che… aveva solo un braccio. Credo di essere passato dalla rabbia alla vergogna in un secondo netto. Gli sorrisi, lo salutai e chinai la testa.

Che cosa voglio dirvi con questa storia terribilmente umiliante? Quando avevo visto che l'uomo non rispondeva al suo obbligo di ringraziarmi, mi ero sentito furioso. Solo quando vidi che aveva una ragione più che valida per non farlo compresi il mio errore di valutazione.

Provatelo la prossima volta che conversate con qualcuno. Quando vi pongono una buona domanda, non rispondete né fate cenni. Osservateli e basta. Se vi chiedono se state bene, rispondete semplicemente: "Sì".

Posso immaginarvi ridere o almeno sorridere al pensiero. Perché? Perché è difficile pensare all'idea di non soddisfare all'obbligo di rispondere a una semplice domanda.

Gli obblighi sono potenti, specialmente quando si riferiscono alle norme sociali. La Figura 6.2 presenta il ciclo dell'obbligo.

Come ingegneri sociali, vi troverete a giocare con queste reazioni attese. Ogni volta che mancate di farlo, riducete la possibilità di costruire un legame, perché l'obiettivo si chiederà perché non vi comportate in modo "normale".



Figura 6.2 L'obbligo in azione.

L'obbligo nell'ingegneria sociale

Gli ingegneri sociali usano le situazioni sociali per creare un senso di obbligo il quale spinga l'obiettivo ad agire sempre nel modo desiderato. Per esempio, è considerato scortese non tenere la porta aperta a una donna o a una persona che porta pacchetti o un carico, e gli ingegneri sociali utilizzano questo obbligo a loro vantaggio.

Per una delle mie missioni, mi sono caricato una pesante scatola piena di telefoni e parti di computer. Attesi l'ora di pranzo e mi avviai verso le porte del luogo in cui avrei dovuto entrare. Mentre mi avvicinavo, un'anima gentile mi disse: "Oh, ti tengo aperta la porta".

Come feci un passo dentro l'edificio, un impiegato molto severo lo riprese: "Dovresti chiedergli di mostrare il badge prima di farlo entrare!".

Dissi: “Ha perfettamente ragione. Questa scatola è davvero pesante. Ho il badge qui nella tasca dei pantaloni. Puoi tirarmelo fuori?“ poggiando il fianco sul tipo severo.

Subito si spostò: “Io la mano nella tua tasca non ce la infilo, caro!”

“Ops! Ma dove ho la testa?”, dissi imbarazzato. “Che situazione… questa scatola pesa meno di 25 chili. Me la terresti, mentre prendo il badge?”.

“Vai avanti, non ho tempo per queste cose!”, esclamò il ragazzo e uscì.

La porta mi era stata tenuta senza alcun obbligo. Così ho approfittato della politica di sicurezza richiamata dal tipo severo… per fingere di offrire la mia “tasca” per obbligo. Il tipo si sentì a disagio all’idea di infilarmi una mano in tasca e si sentì obbligato a farmi passare, senza verifica.

Questo scenario ha funzionato in più di un’occasione. Fino a quando un giorno, incontrai un’incaricata della sicurezza che mi disse: “In questa tasca?”, mentre allungava la mano verso la mia tasca anteriore destra.

Dissi: “Forse è nell’altra. Provi in entrambe”. Speravo che l’imbarazzo della situazione la facesse desistere, ma… niente. Allungò la mano nella mia tasca, tastò in giro, cosa che, a proposito, è stata molto imbarazzante sì, ma *per me*!

Dopo aver trovato solo le mie chiavi nella prima tasca, la donna disse: “Proviamo nell’altra tasca”. In quella tasca trovò il mio portafoglio e un coltellino. Mi guardò e disse: “Potrebbe essere nel portafoglio?”.

Dissi: “Non ne sono sicuro, forse”, anche se sapevo benissimo che non era nel mio portafoglio. Lo aprì di scatto e, proprio davanti comparve la foto di mia figlia. La donna vide la foto ed esclamò: “*Oh mio Dio*, che carina! Come si chiama?”.

Parlammo un quarto d'ora della mia famiglia, mentre lei teneva in mano il mio portafoglio, il mio coltellino e le chiavi, e io tenevo questa stupida scatola terribilmente pesante. Dopo circa 15 minuti, mi rimise tutto in una tasca e disse: "Beh, farebbe bene a segnalare lo smarrimento del badge alla sicurezza prima di mettersi nei guai. Ci vediamo". Detto questo mi lasciò andare. Avevamo sviluppato un legame e un'amicizia e ora si sentiva obbligata a fidarsi di me.

L'obbligo è un principio potente, che può facilitare molto il lavoro di un ingegnere sociale.

Principio 3 – La concessione

L'*Oxford English Dictionary* dà questo significato della parola inglese *concede*: "Ammettere o concordare sul fatto che qualcosa è vero, dopo aver negato o dubitato".

Ricordate, la definizione stessa dell'influenzamento è il fatto che se una persona pensa di aver prodotto un'idea, molto probabilmente penserà che si tratti di una grande idea! La concessione aiuterà l'obiettivo a portare a compimento la "sua idea" svolgendo l'azione che desiderate.

La concessione in azione

Nella zona in cui vivo, l'*American Society for the Prevention of Cruelty to Animals* (ASPCA) è molto efficace nell'usare la concessione per spingere a donare del denaro. Una chiamata di richiesta andrà più o meno in questo modo.

Chiamante: Buongiorno signor Hadnagy. Mi chiamo Carrie e la chiamo da parte della protezione animali di Montrose. Come sta il suo cane?

Io: [*Rispondendo e rendendomi conto che sto parlando di cose a me care e che sto sorridendo… Oh no, come faccio a fermarmi?*] Sta benissimo. È un po' avanti con gli anni, però.

Chiamante: Sono contenta che stia bene. Ed è bello parlare con un amante degli animali. E come amante degli animali, oggi ho bisogno del suo aiuto. Come sa, dobbiamo prenderci cura dei cani randagi della nostra zona. Vogliamo che ogni animale abbia una casa amorevole come il suo cane. Vorrebbe aiutarci?

Io: [*Pensando che mi è praticamente impossibile fermare quello che sta per accadere*] Beh, io amo gli animali. Di che tipo di aiuto avete bisogno?

Chiamante: [*Parlando con decisione e senza vacillare*] Oggi le chiediamo un aiuto economico e molte persone stanno donando circa 250 dollari per aiutarci.

Io: [*Sensazione di trionfo perché ho intenzione di chiudere la telefonata*] 250 dollari?! Wow, mi dispiace, ma non dispongo di quella somma. Mi piacerebbe aiutare, ma in questo momento non posso farlo.

Chiamante: Oh, ho capito. Sono tempi duri e sono un sacco di soldi. Che ne dice allora di aiutarci con soli 25 dollari?

Prima che me ne rendessi conto, avevo estratto la mia carta di credito. Analizziamo bene quello che è successo. Ho accettato, "concesso", alcune cose:

- che sono un amante degli animali;
- che ero disposto ad aiutarli;
- che volevo aiutarli, ma la prima somma era eccessiva.

Quando mi è stata offerta un'alternativa, non ho potuto dire di no. Che cosa sarebbe successo se la ragazza mi avesse chiesto fin da subito 25 dollari? La donazione avrebbe potuto concludersi a un livello molto più basso, mentre iniziando con un valore così alto, si era praticamente garantita più donazioni.

Gli interrogatori delle forze dell'ordine impiegano frequentemente questa tattica. Se riescono a far sì che un colpevole ammetta anche solo un minimo particolare, che "conceda" un fatto, poi gli sarà quasi impossibile ritrattare.

Considerate le seguenti due alternative. Il detective potrebbe chiedergli: "Ti trovavi al Lee Bar alle 23 durante la rapina?". Il colpevole potrebbe facilmente rispondere: "No, non ci sono mai stato". Al contrario il detective potrebbe chiedergli: "Ieri sera alle 23 che cosa hai visto della rapina al Lee Bar?". Al che il colpevole potrebbe rispondere: "Beh, non ho visto nulla. Era buio". Con questo tipo di risposta, il detective sa che l'interrogato era al Lee Bar alle 23: l'indiziato ha fatto una concessione! Rispondendo alla domanda, ammette (concede) di essere stato presente al bar a quell'ora.

La Figura 6.3 illustra il ciclo della concessione.

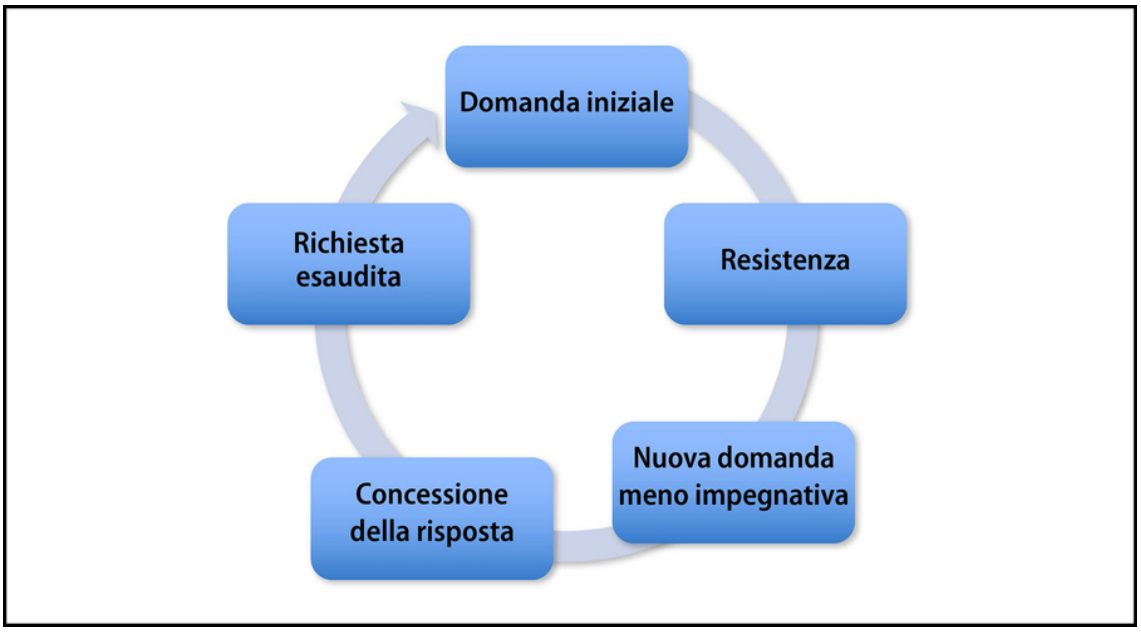


Figura 6.3 La concessione in azione.

La concessione nell'ingegneria sociale

Durante una missione di *vishing*, ci è stato assegnato il compito di ottenere il nome completo, il codice e il numero di previdenza sociale dei dipendenti. Sviluppammo due pretesti che ritenevamo solidi e poi iniziammo a chiamare i nostri obiettivi.

Le chiamate sarebbero andate in questo modo:

Io: Ciao, sono Paul dell'IT. Parlo con Sally Davis?

Obiettivo: Sì. Come posso aiutarla, Paul?

Io: Bene, ieri sera abbiamo riprogrammato il BIOS nel firmware per il sistema di gestione dei badge e abbiamo notato alcuni record mancanti. Ha avuto problemi a usare il suo badge stamattina?

Obiettivo: No, nessun problema, mi ha fatto entrare.

Io: Ottimo. Beh, è fortunata. Molti account hanno avuto problemi sia all'ingresso sia nell'uso delle stampanti. Devo verificare solo alcuni dettagli del suo account, per evitarle problemi. Ci vorranno solo pochi secondi, va bene?

Obiettivo: Certo, di che cosa ha bisogno?

Io: Solo il vostro nome, completo, il codice dipendente e il numero di previdenza sociale.

Obiettivo: Umm… Sono parecchie informazioni e anche riservate. Mi ripete il suo nome? Devo verificare.

Molte chiamate seguirono questo stesso schema e fallimmo in modo tragico. Così, mi sedetti a riflettere sui principi dell'influenzamento e apportai una modifica al pretesto. La seguente conversazione riprende subito dopo il momento in cui l'obiettivo mi dice di essere entrata senza problemi quella mattina.

Obiettivo: No, nessun problema, mi ha fatto entrare.

Io: Ottimo. Beh, è fortunata. Molti account hanno avuto problemi sia all'ingresso sia nell'uso delle stampanti. Devo verificare solo alcuni dettagli del suo account, per evitarle problemi. Ci vorranno solo pochi secondi, va bene?

Obiettivo: Certo, di che cosa ha bisogno?

Io: Innanzitutto, voglio assicurarmi che il suo nome sia scritto correttamente. Ho il vostro nome come S-A-E-L-L-L-Y…

Obiettivo: No, è sbagliato. Non c'è la "E" e poi solo due "L".

Io: Davvero? Per fortuna l'ho chiamata. Mi fa lo spelling anche del cognome, per verifica?

Da lì, procedevo chiedendo il dipartimento, confermavo l'indirizzo e-mail e quando arrivavo al codice del dipendente e al numero di previdenza sociale, l'obiettivo aveva già concesso di rinunciare a tutte queste informazioni e continuava. Questo ci diede un tasso di successo dell'84% per quella missione, e solo con una lieve variazione nel colloquio.

Come ingegneri sociali, ricordatevi che non dovete andare direttamente ai dati che vi servono. Partite dalle poche cose che già sapete, per costruire quei sentimenti che porteranno alla persona a concedervi il resto e a obbedirvi.

Principio 4 – La rarità

"Vendita straordinaria per fallimento!".

"I prezzi più bassi di sempre!".

"Solo dieci pezzi rimasti sul mercato!".

Perché queste affermazioni funzionano sempre su di noi? Se qualcosa viene dipinto come prezioso o raro, il suo valore aumenta. Quanto poteva essere prezioso un cupcake fra 20? E quanto è prezioso, invece, quell'ultimo cupcake?

La rarità in azione

Per una competizione DEF CON, ho avuto la fantastica idea di acquistare uno di quei fucili per dardi in schiuma e assumere un

“cecchino” che avrebbe sparato ai bambini nel SECTF4Kids (*Social Engineering Capture The Flag 4 Kids*) che teniamo ogni anno. Il concorrente avrebbe dovuto risolvere un indovinello e poi entrare in una stanza per inserire un tubo in una scatola, mentre un cecchino avrebbe cercato di colpirlo. Se il concorrente veniva colpito, doveva tornare fuori dalla stanza e ricominciare da capo.

Curiosità
Il concorso è andato incredibilmente bene e se volete sapere come la squadra di ragazzi ci ha sconfitto, dovrete chiedermelo di persona.

Il fucile che ho comprato era un Nerf CS6 Long Shot. Tra il momento in cui l’acquistai e qualche mese dopo il DEF CON, Nerf annunciò che non avrebbe più commercializzato quel modello. Lo stavano sostituendolo con un altro che, secondo molti, era di qualità inferiore.

Non avevo bisogno di due fucili, ne misi uno in vendita su eBay per i 99 dollari che lo avevo pagato. Il primo giorno, le offerte raggiunsero i 199, poi i 250, poi i 299 e infine i 340 dollari. Il prezzo di vendita finale fu di 410 dollari. Parlo di 410 dollari per un fucile di plastica che spara dardi di schiuma a 15 metri! Certo, aveva il mirino e quattro caricatori e noi gli avevamo apportato anche alcune modifiche, ma comunque…

Con 410 dollari si può comprare un fucile vero, quindi perché un fucile di plastica è stato acquistato da qualcuno a quel prezzo? Per rarità. Poiché quel modello di fucile non sarebbe stato più commercializzato e ora era unico, divenne estremamente prezioso.

Le aziende spesso producono prodotti, cibo, medicine, orologi, gioielli e oggetti di valore rari solo per aumentare il loro valore agli occhi dei consumatori. La Figura 6.4 mostra il ciclo della rarità.

La rarità nell’ingegneria sociale

In una missione, la nostra OSINT ci ha svelato gli account sui *social media* dell’amministratore delegato della società, dove aveva pubblicato post sulla sua prima vera vacanza dopo tre anni. Aveva portato la famiglia alle Bahamas. Aveva foto dei bagagli, della corsa all’aeroporto, della famiglia sull’aereo e una foto che diceva: “Ora iniziano due settimane di paradiso”.

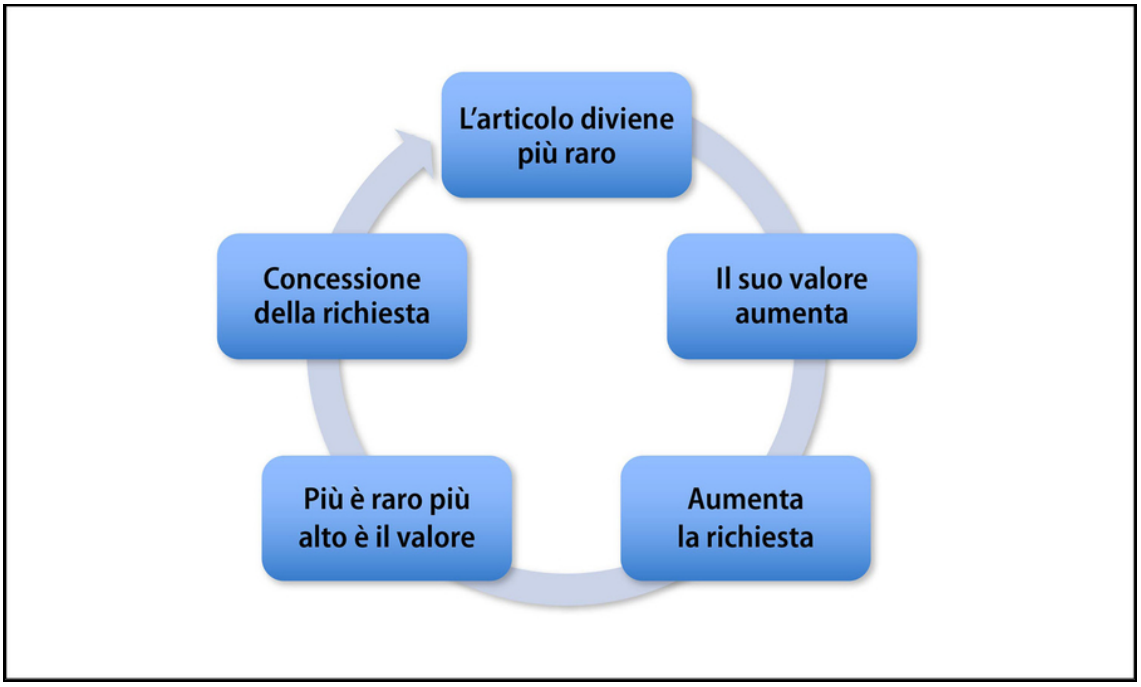


Figura 6.4 La rarità in azione.

Armato di queste sole conoscenze e del nome della sua società di supporto IT, che avevamo ottenuto tramite *dumpster diving* (immersione nel cassonetto della spazzatura), varcai la porta d’ingresso e avvicinai Jane in portineria. La nostra conversazione andò più o meno così.

Jane: Come posso aiutarla?

Io: Salve, sono Paul della XYZ. Jeff mi ha chiesto di venire e di occuparmi… [*osservando gli appunti e sfogliando le pagine come se*

stessi cercando qualcosa] … della lentezza sul suo desktop. Pensa di avere un virus.

Jane: [*guardando la sua agenda*] Paul, non vedo alcuna traccia di questo appuntamento di Jeff. Mi dispiace, ma dovrà ritornare.

Io: Guardi, Jane. Non so cosa dirle. Jeff mi ha chiamato e mi ha detto che sarebbe partito per le Bahamas per due settimane e di volerlo vedere sistemato per il suo rientro, altrimenti guai. Ho dovuto spostare altri quattro appuntamenti per essere qui oggi. E se devo spostare anche questo appuntamento, devo rimandarlo al mese prossimo. [*Breve pausa*] Per me non ci sono problemi. Mando una e-mail a Jeff e gli dico che si è dimenticato di dirglielo e che ora deve aspettare più di quattro settimane per ripararlo.

Io: [*girando i miei appunti verso Jane senza fare una pausa*] Per favore, firmi qui come conferma che sono venuto e che l'intervento ha dovuto essere rimandato a fra quattro settimane.

Jane: [*fermandosi un attimo a osservarmi*] Beh, in effetti si è lamentato del fatto che il suo computer era lento. Non voglio dirgli che tornerà fra quattro settimane. Dai, la lascio passare.

E con questo mi trovavo nell'ufficio dell'amministratore delegato, senza alcun controllo e potendo violare tutto ciò che era presente nell'edificio.

Rendendo prezioso (e quindi raro) il mio tempo, avevo aumentato il suo valore e l'importanza di prendere la decisione subito. La rarità del mio tempo fece pensare a Jane che allontanandomi avrebbe creato un problema maggiore per l'azienda. In tal modo l'azienda è stata completamente compromessa.

Come ingegneri sociali, potete applicare la rarità al tempo, alle informazioni o anche agli oggetti che il pretesto offrirà. La rarità renderà più prezioso ciò che offrite e influenzerà l'obiettivo, costringendolo a prendere decisioni basate su quel valore percepito.

SUGGERIMENTO

Spesso mi viene chiesto: “Quante persone hai fatto licenziare?”. Come professionista dell’ingegneria sociale, ritengo sia importante garantire che i miei risultati vengano utilizzati per scopi educativi e non per licenziare, a meno che, ovviamente, non trovi un dipendente che compie qualcosa di illegale o dannoso per la sua azienda. Quindi posso dire con orgoglio che è raro che qualcuno sia stato licenziato solo perché è caduto vittima di uno dei miei pretesti.

Principio 5 – L’autorità

Quando qualcuno, con il giusto tipo di autorità, fa certe affermazioni, altre persone le prendono molto sul serio. Ecco alcuni esempi:

- Se un tipo in camice bianco dice “Si cali i pantaloni”, si ascolta.
- Se un genitore, un insegnante o una guardia dice “Non toccare questo!”, si ascolta.
- Se il sergente istruttore o il comandante dice “Mettiti giù e fai venti flessioni!”, sicuramente si ascolta.

Tutte queste persone hanno una cosa in comune: hanno un’autorità su di voi. Ma che cosa stabilisce tale autorità? Quando entrate in una stanza, come potete dire chi ha l’autorità?

Osservate Ben nelle Figure 6.5 e 6.6. In quale foto pensate che stia mostrando maggiore autorità e perché?

Probabilmente pensate che Ben nella Figura 6.6 mostri più autorità e sicurezza. In entrambe le foto Ben indossa gli stessi vestiti, ha la stessa età ed è assolutamente lo stesso. Ma nella Figura 6.6, è in piedi con il petto in fuori, le mani intrecciate, il mento sollevato e nessuna espressione di paura sul volto. Tutto ciò indica una persona fiduciosa in se stessa e tale fiducia ci dice che la persona ha autorità. Di fatto, quando chiedo ai miei allievi che cosa indica loro l’autorità, elencano elementi come la sicurezza di sé, la voce alta, il petto in fuori, il mento

sollevato, un bel vestito, una personalità diretta e altre caratteristiche analoghe.

Che effetto ha l'autorità su di noi? Ci dà fiducia in quella persona, senza che debba dimostrare perché dovremmo obbedirle.



Figura 6.5 Che cosa vi dice l'espressione e il linguaggio del corpo?



Figura 6.6 Quali sono i segni di fiducia in se stessi?

L’autorità in azione

Uno degli studi più influenti su questo argomento è stato compiuto da Stanley Milgram. Nel 1963 Milgram esaminò le giustificazioni per i crimini di guerra pronunciate durante il Processo di Norimberga. Durante le udienze, la difesa usata era, il più delle volte: “Stavo solo

eseguendo gli ordini". Nello studio intitolato *Behavioral Study of Obedience*, Milgram delinea le sue scoperte.

Milgram ha voluto esaminare se anche semplici cittadini rispettosi della legge possano essere costretti da un'autorità a intraprendere un'azione che potrebbe portare al ferimento o addirittura alla morte di qualcuno. Naturalmente, l'esecuzione di questo tipo di ricerca presenterebbe enormi limiti. Come dimostrare che un certo numero di persone obbedirebbe o non obbedirebbe a una figura autoritaria che chiedesse loro di ferire un'altra persona?

Alcuni cittadini volontari presero parte allo studio di Milgram. Perché l'esperimento funzionasse, è stato detto loro che ci sarebbero stati uno studente e un insegnante e che i compiti erano casuali, ma in realtà tutti i volontari erano designati come insegnanti.

I volontari osservavano uno studente legato a una sedia con alcuni elettrodi fissati alla pelle. Ai volontari è stato detto che le risposte errate alle domande avrebbero provocato uno shock elettrico per gli studenti. Lo studente non ha mai davvero subito uno shock: era un attore che fingeva di ricevere la scossa.

All'insegnante (il volontario) è stata mostrata una grande scatola con vari interruttori a leva da 15 a 450 volt con incrementi di 15 volt. Ai volontari era stato somministrato uno shock elettrico da 45 volt, quindi avevano una certa percezione della realtà.

Poi un uomo con un camice bianco (l'autorità) sedeva come sovrintendente dell'insegnante, ponendo le domande. Quando lo studente sbagliava le risposte, la tensione aumentava e così l'intensità della punizione.

Se l'insegnante obiettava perché sentiva lo studente soffrire, l'uomo in camice era stato incaricato di dire solo due cose:

- "L'esperimento deve continuare, per favore continui";
- "Non c'è alcun danno permanente ai tessuti. Prego, vada avanti".

Non sembra molto convincente, vero? Ma questo studio ha dimostrato che il 65% degli “insegnanti” ha somministrato allo studente lo shock elettrico a 450 volt!

Provate a riflettere. Gli insegnanti erano persone normali, appartenenti alla classe lavoratrice. Non erano affatto sociopatici affetti da sadismo. Tuttavia, secondo lo studio di Milgram, 26 volontari su 40 (il 65%) hanno continuato ad aumentare la tensione fino a 450 volt e questo solo perché qualcuno dotato di autorità chiedeva loro di continuare.

La Figura 6.7 illustra il ciclo dell’autorità.

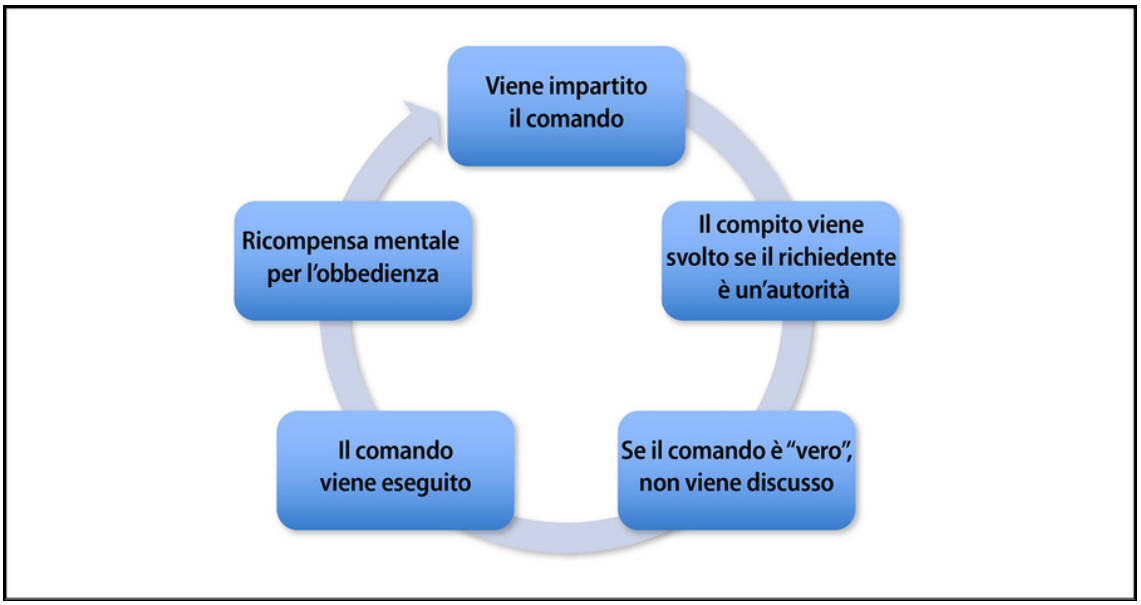


Figura 6.7 L’autorità in azione.

L’autorità nell’ingegneria sociale

Ho sempre faticato a far usare direttamente l’autorità ai miei pretesti nelle attività di ingegneria sociale. La ragione principale è perché spesso non ho le conoscenze necessarie, il che significa che vengo scoperto e fermato.

Tuttavia, a volte sono sufficienti l'autorità implicita o un trasferimento di autorità. Per una missione, trovai online un invito a un meeting per il consiglio finanziario del nostro target. Rientrava nell'ambito del nostro lavoro, così decisi di usarlo. Eseguimmo un'attività di OSINT su tutti i membri invitati al meeting e trovammo una donna che sembrava essere la figura autoritaria. Oltre a sembrare autorevole sui *social media*, nei siti di valutazione dei dipendenti era nominata in alcune recensioni come personaggio con il quale era difficile lavorare.

Così assegnai al numero di cellulare della mia complice il nome di questa donna (chiamiamola Sally Smith) e le dissi: "Quando mi vedi discutere con la guardia, scrivimi questo messaggio: 'Dove diavolo sei finito? Ti aspettiamo da 15 minuti! Sali subito!'".

Afferrai una pila di cartellette e documenti e provai a superare la sicurezza. Sapevo che sarei stato fermato, perché avevamo notato che la sicurezza era molto rigida. Andò così:

La guardia giurata disse energicamente: "Mi scusi signore! Dove sta andando?! FERMO!".

Mi fermai sul posto, mi voltai con uno sguardo arrabbiato e gli dissi: "Che cosa? Non mi hai visto uscire e andare alla macchina? Devo tornare alla riunione del consiglio finanziario al 14° piano. E devo salire subito".

"Mi dispiace, signore, ma io non l'ho vista passare. Per favore, mi mostri il badge", chiese la guardia, con un tono più confuso.

Sbuffai e: "Va bene, ma stia sicuro che darò il suo nome a Sally quando sarò salito e così le spiegherà il mio ritardo". Iniziai a controllarmi le tasche e poi dissi: "Non so, devo aver lasciato…". Poi arrivò la notifica del messaggio.

Estrassi il telefono e glielo mostrai. Nella schermata del messaggio campeggiava il nome "Sally Smith" e il messaggio sottostante diceva

“Dove diavolo sei finito? Ti aspettiamo da 15 minuti! Sali subito!”.

Dissi: “Ecco… vuoi che la chiami per spiegarle il motivo per cui sono trattenuto qui mentre tutta la sala riunioni aspetta queste carte? O forse dovrei dirle il nome della guardia che mi sta trattenendo?”.

Lesse il messaggio, mi guardò e disse: “Sono veramente dispiaciuto, signore. Davvero non l’avevo vista passare. Per favore, se possiamo dimenticare l’incidente, vada subito alla riunione”. “Se mi fai passare subito, posso dimenticare l’accaduto”. E grazie a quello stratagemma, ero nella fortezza e gironzolavo libero.

L’autorità, anche se non emanata direttamente da me, fece sì che la guardia compisse un’azione che era non nel suo interesse. L’autorità è un motivatore potente!

Principio 6 – La coerenza e l’impegno

Vogliamo tutti apparire coerenti, il che significa che vogliamo che ci sia un accordo tra quello che diciamo e quello che pensiamo di rappresentare. Questo è particolarmente vero quando ci impegniamo in qualcosa. Avete mai visto un bambino impegnarsi in una risposta che sa essere falsa? (“No, non ho rotto io quella lampada!”). Il bambino rimane coerente con la sua risposta iniziale, anche fornendogli prove schiaccianti della bugia.

Perché la coerenza è importante per noi? Vogliamo (o forse abbiamo bisogno di) sembrare coerenti, perché la coerenza è un segno di fiducia in se stessi e di forza.

La coerenza e l’impegno in azione

Vivo in una bella zona rurale, ma recentemente vi sono stati scoperti ricchi giacimenti di petrolio e gas. Ora stanno eseguendo il fracking,

pompando e scavando in tutta la contea. Di conseguenza, sulla mia strada sono comparsi molti camion.

Ho visto camion carichi di tonnellate di materiali sfrecciare sulla mia strada a 80 o 100 chilometri all'ora. I loro conducenti sono incuranti e pericolosi. Alcuni miei vicini iniziarono così a porre segni disegnati a mano nei loro terreni, per dire ai conducenti di rallentare, di curare la sicurezza e di fare attenzione ai bambini che vivono lì. Voglio però dire che se un mio vicino venisse a chiedermi di mettere uno di questi cartelli nel mio cortile, al posto dei bellissimi fiori di mia moglie o della mia fiammante macchina, dovrei declinare, anche se certamente voglio che i conducenti rallentino.

Nel 1966, i ricercatori Jonathan L. Freedman e Scott C. Fraser studiarono la coerenza e l'impegno e ne scrissero in *Compliance Without Pressure: The Foot-in-the-Door Technique* ("Journal of Personality and Social Psychology", settembre 1966, www.researchgate.net/publication/17217362_Compliance_Without_Pressure_The_Foot-in-the-Door_Technique). Andarono di porta in porta, chiedendo agli abitanti di un quartiere di porre cartelli di grandi dimensioni, ma scritti malamente, contenenti avvertenze sulla sicurezza della guida. I cartelli avrebbero bloccato la veduta dalla casa. I ricercatori scoprirono che l'83% di tutti i proprietari di case rifiutò di mettere tali cartelli in giardino.

Poi Freedman e Fraser modificarono solo leggermente la loro richiesta nel quartiere successivo e ottennero il 76% di accettazione! Esattamente: il 76% delle famiglie ha risposto positivamente! A che cosa fu dovuto questo cambiamento? A contenuti testuali migliori? A una grafica più attraente? Al pagamento di una somma? A un vero e proprio affitto dello spazio?

Assolutamente no. Il cambiamento è stato prodotto dalla dimensione del cartello. Nel secondo quartiere, prima chiesero ai proprietari di

case di applicare un adesivo da 8 centimetri alle finestre di casa, con lo stesso messaggio. Poi, alcune settimane dopo, tornarono e chiesero loro di installare il cartello, grande e brutto, nel loro cortile; e il 76% accettò.

Freedman e Fraser definirono questo approccio a “piede nella porta”. Una volta che avevano infilato un piede nella porta (il piccolo adesivo alla finestra), il proprietario della casa era più disposto a soddisfare le successive richieste (il grande cartello). Freedman e Fraser condussero numerosi studi e tutti con gli stessi impressionanti esiti. L’accettazione aumenta drasticamente quando la persona in questione accetta prima qualcosa di più piccolo.

Quando si fondono insieme l’accettazione e il principio di coerenza, si ottiene una forza inarrestabile. Fondamentalmente, vogliamo essere e apparire coerenti. Il nostro cervello non ama i conflitti interiori. Quindi, compiamo una scelta e poi la seguiamo, anche quando sappiamo di avere torto, perché ormai abbiamo scelto e preferiamo rimanere coerenti. Questo meccanismo è rappresentato nella Figura 6.8.

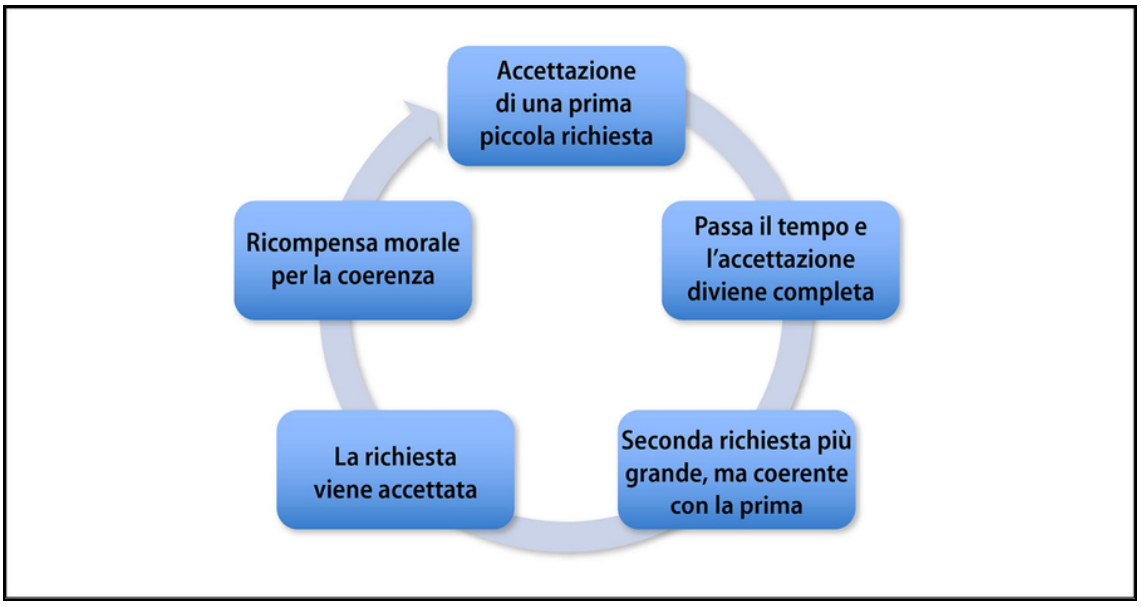


Figura 6.8 Accettazione e coerenza in azione.

NOTA

L’elemento temporale, per la coerenza e l’accettazione, non deve necessariamente estendersi su un lungo periodo; a volte bastano pochi secondi. Una volta che la persona si impegna con la prima richiesta, tenderà a mantenere la propria coerenza.

La coerenza e l’accettazione nell’ingegneria sociale

Una delle mie regole personali è quella di *non pregiudicare mai la correttezza del pretesto, a meno che sia davvero necessario*. Deve esserci una situazione davvero seria perché mi senta costretto a farlo. Questa regola è nata a causa della storia che sto per raccontarvi.

Ero stato incaricato di una missione multi-fase, nella quale dovevo accedere a una serie di cassonetti in un’area protetta. I cassonetti erano quelli in cui l’azienda gettava via la tecnologia obsoleta.

Per raggiungere i cassonetti, dovetti aggirare la sicurezza, dirigermi verso un’area protetta dell’impianto, ottenere l’accesso senza essere fermato e lavorare indisturbato cercando qualcosa di valore.

Avviai la fase OSINT con l’obiettivo di trovare la società che si occupava dei cassonetti. L’azienda che era il mio obiettivo applicava politiche molto rigide, che impedivano di svelare qualsiasi tipo di informazione sui loro fornitori, ma decisi di chiamare il reparto contabilità per cercare di ottenere quelle informazioni. La chiamata andò in questo modo.

Rapp. azienda: Buongiorno, sono Beth. Come posso aiutarla?

Io: Beth, sono Paul di Professional Dumpster. Siamo relativamente nuovi nella zona e stiamo cercando di estendere la nostra clientela locale. Posso inviarvi un breve preventivo?

Rapp. azienda: Salve Paul. Sì, accettiamo offerte da nuovi fornitori. Inviateci solo un prezzo per unità e, se il prezzo è accettabile, vi

richiederemo maggiori informazioni.

Io: OK, fantastico. Posso avere il suo indirizzo e-mail, per favore?

Rapp. azienda: Beh, non dovrà inviarlo a me, ma a vendors@company.com.

Io: Oh, capisco. Posso inviarle una copia per conoscenza. A volte mi dicono che il mio preventivo non è mai arrivato. Sono nuovo in questa attività e non sono molto esperto di tecnologie.

Rapp. azienda: Ah, ok. Il mio è beth.p@company.com.

Io: Beth, non so come ringraziarla. Ascolti… posso fidarmi di lei per qualcosa di un po' più personale?

Rapp. azienda: Certo, immagino di sì.

Io: Ho venduto un po' di tutto, ma i cassonetti sono un po' una novità per me e non so se me la cavo bene. Non sono nemmeno sicuro che i nostri prezzi siano competitivi.

Rapp. azienda: Mi dispiace, Paul. Deve essere difficile. Immagino… Invii il preventivo e mi assicurerò personalmente che venga considerato.

Io: Grazie davvero Beth. So che non sono cose da chiedere, ma posso sapere almeno chi è il mio attuale concorrente? [*Ormai si è impegnata ad aiutarmi, dandomi il suo indirizzo e-mail e avviando una conversazione. Ma il legame che ho creato è sufficiente per porre questa domanda?*]

Rapp. azienda: Paul, sa… [*Sospira e poi si ferma*] Mi piacerebbe, ma abbiamo una rigida politica in merito. Non voglio finire nei guai, ma davvero vorrei poterglielo dire.

Io: Ah, certo, ho capito Beth. È solo che sto veramente faticando. Che ne dite di questo: io dico alcuni nomi e lei dà un colpo di tosse quando sente il nome giusto: Superior Waste, Excellent Dumpster, Waste Management [*e qui Beth tossisce*]. Beth, spero che si rimetta presto – la sento un po' costipata!

Rapp. azienda: [*ridacchia*] Grazie, mi sento una cospiratrice. Buona fortuna a lei.

Con queste informazioni, sono riuscito a ottenere l'abito giusto, a ottenere l'accesso al luogo protetto e a trovare alcuni dischi rigidi e chiavette USB non distrutti che avrebbero potuto portare a una violazione su larga scala dell'azienda, se fossero caduti nelle mani sbagliate.

Giocare con il desiderio dell'obiettivo di rimanere coerente ai propri impegni, fisici o mentali, consente all'ingegnere sociale di facilitare l'accettazione di tutte le richieste successive.

Principio 7 – L'apprezzamento

Alle persone piacciono le persone come loro. E piacciono le persone alle quali piacciono. Per quanto sembri uno scioglilingua è importante capire il significato più profondo di queste due affermazioni.

Nel Capitolo 5 ho parlato della tribe mentality. Ora riflettete su questo elemento nel contesto della dichiarazione: "Alla gente piacciono le persone *come loro*". Se siamo simili, nella stessa tribù – confortevole e familiare – saremo apprezzati, accettati e considerati.

Ora, per affrontare la seconda affermazione, "Alle persone piacciono le persone alle quali piacciono", lasciate che vi ricordi di Zak e della sua ricerca sull'ossitocina cui ho accennato nel Capitolo 1. Qui si applica perfettamente. Se apprezzate qualcuno, o fate sentire a qualcuno che è apprezzato o degno di fiducia, tale persona non potrà fare a meno di ricambiare.

Prima che diciate: "Beh, è abbastanza logico", lasciatemi esporre alcune regole fondamentali.

- *L'apprezzamento deve essere sincero*. Non si può semplicemente simulare la simpatia e sperare che la cosa funzioni. Potrebbe

funzionare per i primi minuti, ma alla fine emerge e diventa evidente che l'apprezzamento non è reale e questo può pregiudicare la fiducia e il legame in modo irreparabile.

- *Non pensate che complimenti e apprezzamenti siano la stessa cosa*. Perché un complimento funzioni deve essere sincero e allo stesso livello del legame che avete costruito.
- *La comunicazione non verbale svolge un ruolo enorme in questo campo*. Quando i vostri segni non verbali sono autentici (ricordate la discussione sul controllo dei segni non verbali nel Capitolo 5?), allora è più facile che qualcuno si fidi di voi, si senta a proprio agio con voi e che quindi vi apprezzi.

Il tema ricorrente di tutti questi punti è che la vostra espressione di apprezzamento sia sincera. Il mio buon amico Robin Dreeke considera ogni persona come se operasse in un suo proprio reality show. Non deve apprezzare la vostra vita o le cose che fate, ma esprimere abbastanza interesse per scoprire la trama della vostra vita e come si dipana. Quel desiderio di scoprirlo è sincero e questa sincerità è evidente, il che gli consente di instaurare il senso di fiducia e il legame e di applicare l'influenzamento con maggiore facilità.

Per incoraggiare questo sentimento, potete cercare dei modi per elargire un complimento e rispecchiare il linguaggio del corpo e/o i segnali verbali (senza però imitarli "a pappagallo") per aiutare la persona a sentirsi accettata e positiva nei vostri confronti. La Figura 6.9 illustra il funzionamento del principio dell'apprezzamento.

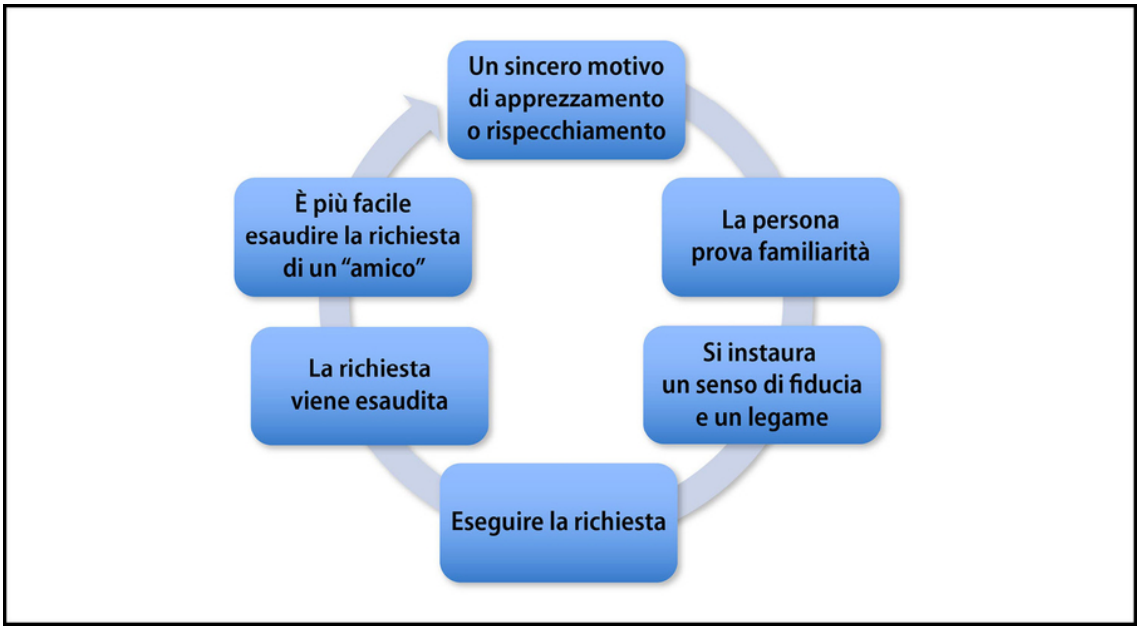


Figura 6.9 L'apprezzamento in azione.

L'apprezzamento e l'ingegneria sociale

In una missione, ho voluto dare supporto. Mentre mi dirigevo verso la porta d'ingresso, sapevo di non avere molto tempo per attivare un solido piano.

Un uomo stava uscendo dalla sua nuovissima Kia e si avviava a passo spedito verso la porta. Presi il suo ritmo e mi assicurai di essere a portata d'orecchio quando chiesi a un'altra persona che stava camminando verso la porta: "Ehi, sai di chi è quella Kia?". La donna alla quale mi ero rivolto si voltò e mi guardò perplessa, ma questo non importava. Mi interessava che il proprietario dell'auto rallentasse e si voltasse.

Mi guardò e disse: "È mia. C'è qualche problema?".

Allungai la mano e dissi: "Paul, del Personale". Feci una pausa abbastanza lunga, sperando che non fosse anche lui del Personale, poi ho proseguito: "Mi spiace, sono nuovo. Mia moglie e io stavamo

pensando proprio a quella macchina. Sono curioso di sapere che cosa ne pensa".

Questo è stato più che sufficiente. A quel punto voleva mostrarmi ogni sua caratteristica e parlarmene. Dopo una breve anteprima della vettura, gli dissi: "Ehi, sono in ritardo per la riunione. Ti dispiace se camminiamo mentre parliamo?".

"Niente affatto, Paul". Iniziammo a camminare, e mi parlò della garanzia, del comfort, del consumo e di molto altro ancora. Adorava la sua macchina.

Mentre ci avvicinavamo alla reception, dissi: "Credo che tu abbia fatto la scelta migliore possibile. Come sei diventato così esperto di macchine?". Con questa affermazione, non solo mi sono complimentato per la sua scelta, ma ho apprezzato le sue conoscenze. Così passò il suo badge e mi tenne perfino aperta la porta, senza pensarci.

A favore delle guardie, estrassi il portafoglio e lo picchiettai sul lettore di badge della porta e continuai a camminare in modo naturale. Questo tipo mi parlò della sua Kia per ben venti minuti, accompagnandomi all'ufficio del Personale. Quando arrivammo, mi disse: "Bene, eccoci qui: il tuo ufficio. Il mio interno è 4328. Se hai bisogno di altre informazioni, fammelo sapere".

Dissi: "Beh, credo proprio di aver bisogno del tuo aiuto per comprare l'auto. Ne sai così tanto! Posso chiamarti verso le 15, dopo la riunione?".

"Ma certo! Nessun problema! A risentirci, allora", e scomparve dietro l'angolo.

Ho fatto apprezzamenti su qualcosa che apprezzava e su di lui per le sue conoscenze. Queste due sole cose mi hanno permesso di superare la sicurezza, entrare nell'edificio ed eludere tutti i controlli di sicurezza.

L’apprezzamento è un principio potente che può, letteralmente e figurativamente, aprire molte porte per un professionista dell’ingegneria sociale. Se siete come me, la parte più difficile è imparare a interessarsi al punto che il vostro apprezzamento risulti sincero.

SUGGERIMENTO

Non dovete essere gentili e amichevoli, e poi diventare duri e indifferenti non appena avrete ottenuto quello che volete. Questo tipo di incongruenza del comportamento può far sì che il vostro obiettivo ne abbia una sensazione negativa.

Principio 8 – La prova sociale

Nel 1969, Robert O’Connor eseguì uno studio chiamato *Modification of Social Withdrawal Through Symbolic Modeling* (“Journal of Applied Behavior Analysis”, 1969, www.ncbi.nlm.nih.gov/pmc/articles/PMC1311030). I soggetti di questo studio erano bambini piccoli affetti da ansie sociali e che erano stati ritirati dalla scuola.

I bambini sono stati divisi in due gruppi. A quelli del Gruppo 1 venne mostrato un video che non conteneva alcun livello di interazione sociale. A quelli del Gruppo 2 venne mostrato un video di una ventina di minuti che presentava dei bambini in un ambito sociale e con risultati positivi.

I bambini del Gruppo 1 non alterarono il loro comportamento, mentre quelli del Gruppo 2 manifestarono un netto miglioramento nelle loro interazioni sociali. Non solo, ma anche quando O’Connor tornò sei settimane dopo per osservare i bambini, quelli del Gruppo 2 ora erano molto progrediti in termini di interazioni sociali.

O’Connor è stato in grado di modificare un percorso di vita potenzialmente lungo con un sostanziale ritiro sociale utilizzando

qualcosa chiamato *prova sociale*. Il video ha dimostrato ai bambini del Gruppo 2 che era buono, sicuro e persino utile essere più socievoli.

La prova sociale in azione

Un tempo c'era un divertente programma televisivo chiamato *Candid Camera*, nel quale veniva organizzato uno scherzo per mostrare i potenti effetti delle prove sociali su vari tipi di persone. Tre o quattro persone, attori che fingevano di non conoscersi, entravano in un ascensore e si voltavano verso la parte posteriore. Il soggetto ignaro alla fine si sarebbe conformato agli altri. In un caso, indussero perfino un giovane a compiere un giro completo e a togliersi il cappello, sempre usando solo prove sociali.

Ognuno di noi vuole essere come tutti gli altri. Alcuni di voi potrebbero obiettare di essere unici e di non rientrare davvero in alcun gruppo, ma anche questo, comunque, è un gruppo.

Quando ci sentiamo siamo persi, confusi o insicuri, generalmente osserviamo gli altri per vedere come si comportano, alla ricerca di indizi (prove sociali) di quello che dovrebbe essere anche il nostro comportamento.

Curiosità
Ho mostrato un video di *Candid Camera* durante una lezione a Las Vegas. Cinque dei miei allievi decisero di scoprire se funzionasse ancora oggi. Hanno fatto finta di non conoscersi e hanno provato il test per tre volte. In tutti e tre i casi, i soggetti si conformavano alla pressione del gruppo e si voltavano nella sua direzione.

La Figura 6.10 illustra il ciclo della prova sociale.

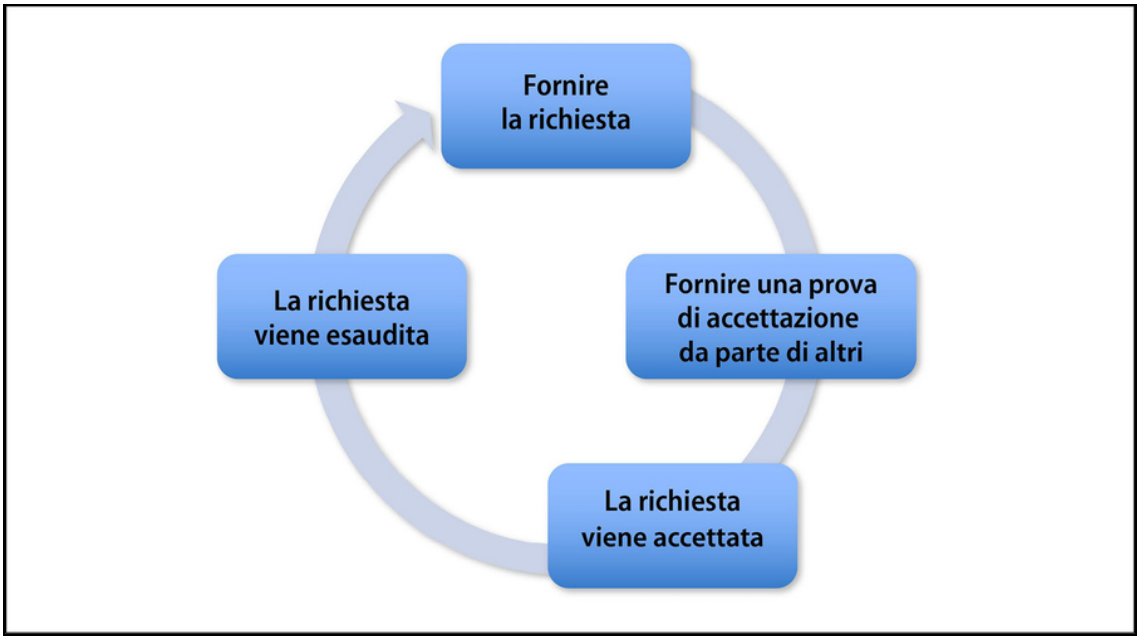


Figura 6.10 La prova sociale in azione.

La prova sociale nell’ingegneria sociale

Molto spesso, le persone non vogliono essere le prime a compiere un’azione. Tuttavia, l’uso della prova sociale aiuta il cervello delle persone a prendere la decisione di intraprendere un’azione con la quale non si sentono a proprio agio.

In una missione, dovevo accedere a un’area sicura di un edificio, così indossai il miglior abbigliamento tecnico da riparatore telefonico che riuscii ad approntare con un minimo preavviso. Invece di andare direttamente nella sede del mio obiettivo, entrai nell’azienda accanto. Entrai e mi presentai come Paul, tecnico telefonico della XYZ Telephone Company. Dissi di dover eseguire un’operazione di manutenzione e lasciai un biglietto da visita, ovviamente falso.

Ho eseguito l’operazione nelle due aziende poste ai lati del mio obiettivo. Poi andai nell’ufficio che era il mio vero obiettivo. Mi avvicinai alla reception e dissi: “Mi chiamo Paul. Stiamo rilevando una

fluttuazione nelle linee telefoniche, che sta causando blocchi telefonici e di Internet in zona. Devo controllare ogni azienda di questo blocco per verificare che non ci siano problemi nelle impostazioni di sistema". La donna all'ingresso voleva interrompermi, ma continuai a parlare osservando i miei appunti mentre dicevo: "Stavo parlando con Beth dell'azienda qui accanto, ma le loro linee sono risultate a posto. Anche nell'altra azienda Fred è stato contento che il test fosse regolare. Così, ho pensato che, visto che sono qui, mi basta eseguire i test sul vostro sistema per assicurarmi che il problema non sia qui".

Invece di guardarla, decisi di scarabocchiare delle note sul mio modulo, come per riordinare gli appunti delle altre due aziende. Con solo una lieve esitazione, la donna disse: "Oh, scommetto che l'avete fatto felice, Fred. Si lamenta sempre del servizio".

E con quello avevo superato la reception e venni accompagnato alla sala server.

Ho usato le prove sociali con i sondaggi, le e-mail di *phishing*, le chiamate di *vishing* e molto altro ancora. In una campagna di sondaggi, iniziavo ogni conversazione con un breve preambolo, seguito da: "Ho solo altre tre chiamate e poi ho finito la giornata. Per fortuna oggi sono stati tutti molto gentili". Poi snocciolavo le mie domande. Il più delle volte bastò solo applicare quella leggera pressione sociale, in parte perché le persone si sono sentite bene per il fatto di non essere le prime a darmi le loro informazioni. La prova sociale è stata uno degli aspetti più potenti dell'influenzamento che ho usato.

Influenza vs manipolazione

Come inizio a discutere i principi dell'influenzamento, di solito una delle prime domande è: "Alcune delle cose che ha fatto sembrano piuttosto manipolative: non è che influenzamento e manipolazione

siano la stessa cosa?”. L’influenzamento e la manipolazione sono simili, ma non vanno confuse.

Permettetemi di essere franco: quello che sto scrivendo qui è il mio punto di vista su questo argomento. Questo non significa che sia l’unico punto di vista possibile. In effetti, quando abbiamo avuto Cialdini sul podcast, ho appreso che la sua opinione su questo argomento differisce drasticamente dalla mia.

Definisco influenzamento “convincere qualcuno a voler fare qualcosa che vogliamo che faccia”. Definisco manipolazione “convincere qualcuno a fare qualcosa che vogliamo che faccia”. La differenza sta nel fatto che la manipolazione non si cura dei sentimenti dell’obiettivo. Mentre l’influenza tende a essere positiva nei suoi temi, la manipolazione esce, anche abbondantemente, da quel confine.

La manipolazione in azione

Credo che il modo migliore per illustrare il concetto dell’influenzamento rispetto a quello della manipolazione sia quello di raccontarvi una storia davvero imbarazzante per me, ma che è stata fondamentale in quanto ha cambiato la mia attività.

Quando decisi di diventare un professionista dell’ingegneria sociale, ero fermamente convinto di dover sempre vincere. L’idea che qualsiasi cosa non fosse una vittoria del 100% fosse un fallimento era come una sorta di principio per me. Questo pensiero mi ha spinto a non preoccuparmi troppo dei sentimenti del cliente o del suo staff, bastava che “vincessi”.

In una missione, mi è capitato di *non* vincere. Stavo perdendo. Gli obiettivi non facevano clic sulle mie e-mail di *phishing*. Mi chiudevano regolarmente in faccia le chiamate di *vishing*. Le chiavette USB che disseminavo venivano riconsegnate e non venivano mai inserite, indipendentemente da come le rendessi invitanti. E due

tentativi di *tailgating* (seguire da vicino una persona autorizzata all'accesso) e vari altri stratagemmi non hanno avuto successo.

Ero frustrato e non mi rendevo conto che questo sarebbe stato un ottimo momento per dire al cliente che la sua sicurezza era davvero efficace. Invece, mi sono sentito spinto a passare dal "lato oscuro". La società aveva una zona pranzo aperta, all'esterno. Avevo tentato di passare attraverso quelle porte, ma non ero riuscito a superare la sicurezza, anche se ho avuto libero accesso alla zona pranzo.

Il pretesto era così: ero Frank T., capo di un nuovo progetto dell'ufficio del Personale che consisteva nel raccogliere informazioni per un lancio nel settore sanitario. La mia segretaria, Marsha, era una ragazza madre, del tutto "esaurita". Ero in piedi a portata d'orecchio di un tavolo pieno di dipendenti quando Marsha si avvicinò a capo chino e mi porse una pila di fogli. Io li guardai e, con fare sprezzante, le dissi: "Che cos'è questa merda, sei un essere inutile…". Sbuffai sonoramente e le dissi: "Guarda, se anche un compito così semplice è troppo per te, forse è meglio che ti cerchi un altro lavoro, per sostenere te e tuo figlio! NON NE POSSO PIÙ DI TE!".

Poi lanciai i fogli sul tavolo e lasciai lì Marsha, lasciandomi dietro i documenti. Marsha si sedette e iniziò a piangere.

Vidi un ragazzo alterarsi per la scenata che avevo fatto, ma quando vide Marsha piangere, si rivolse a lei e le disse: "Stai bene? Di che cosa si trattava?".

Alzò lo sguardo per guardarlo, spaventata e nervosa e gli rispose: "Oh… mi scusi, mi dispiace tanto. Non volevo disturbarvi durante il pranzo. Sa come è fatto Frank. È solo stressato".

"Frank? Nessuno ha il diritto di trattarla così. Questo è ridicolo". E si sedette accanto a lei.

"No, non capisce. Ha problemi a casa e deve compilare questi moduli entro oggi, ma io me ne sono dimenticata. Ho pensato di

portarglieli durante la pausa-pranzo, ma si è arrabbiato. Verrò licenziata".

"Ma comunque non dovrebbe parlare con te in questo modo… È da…".

Lei lo interruppe, per difendere il suo aggressore: "No, è giusto. Me lo merito. Dovevo averlo finito per la settimana scorsa. È colpa mia. È davvero un brav'uomo e ha corso un rischio per me".

"Giusto o no, dammi quelle carte!". L'uomo, il suo salvatore, si alzò, si incamminò verso ogni tavolo e disse: "Questo lavoro deve essere terminato entro oggi, ma voglio che sia finito prima di pranzo. Quando avrete finito, consegnatelo a questa nostra graziosa collega".

Indicò Marsha, che ora sorrideva e lo ringraziava per aver salvato il suo lavoro ed essere stato così gentile.

Il manager non aveva ancora finito di parlare che tutte quelle persone in sala da pranzo avevano cominciato a scrivere: avevamo decine di moduli con nomi completi, date di nascita, ID interni, numeri di previdenza sociale, indirizzi di casa, indirizzi e-mail, numeri di telefono e ogni altra informazione personale.

Certo, ho vinto, ma a quale prezzo? Quando tutti hanno scoperto che quello era stato solo un abile stratagemma, pensate che ne abbiano tratto un insegnamento? E quale sarebbe stata la lezione? Che è sbagliato comportarsi da esseri umani? Che non bisogna provare empatia? Questa non è una buona lezione.

Poiché avevo usato la manipolazione, in quell'azienda divenni "il tipo che aveva maltrattato la segretaria". Vi dico una cosa: non solo non avevo offerto nessuna lezione utile, ma a tutt'oggi non ho più ricevuto altro lavoro da quell'azienda.

I principi della manipolazione

Sebbene siano negativi, anche la manipolazione ha i suoi principi:

- aumento della suscettibilità;
- controllo ambientale;
- rivalutazione forzata;
- esaurimento delle energie;
- punizione;
- intimidazione.

Anche solo i nomi dovrebbero far capire perché sono elementi così negativi, ma c'è uno studio che penso spieghi ancora meglio perché non mi piace usare questi principi.

Nel 1967, Martin Seligman e Steven F. Maier dell'Università della Pennsylvania condussero uno studio per determinare come funzionavano alcuni di questi principi. Impiegarono come soggetti di test dei cani per vedere come avrebbero accettato delle circostanze incontrollabili. Seligman e Maier pubblicarono i risultati in un articolo intitolato *Learned Helplessness* ("Journal of Experimental Psychology", maggio 1967, http://homepages.gac.edu/~jwotton2/PSY225/seligman.pdf).

In sostanza, hanno legato i cani in vari modi – sia da soli sia in gruppo – e poi hanno somministrato loro uno shock elettrico. In alcuni casi, i cani dovevano capire che c'era un pannello che, se premuto, poteva fermare la scossa. Ma in altri casi, il pannello non faceva nulla. Quei cani impararono che, poiché non c'era nulla che potessero fare per fermare la punizione, dovevano accettarla come parte della vita e restavano lì a mugolare dal dolore, senza tentare di fuggire.

Per quanto sia inquietante leggere di questo studio, esso contiene in sé un aspetto importante per comprendere i principi della manipolazione. Molto spesso il soggetto accetterà qualcosa che teme, che è doloroso o che sa essere negativo semplicemente perché non vede altra possibilità. La paura e la rabbia sostituiscono la capacità del cervello di pensare razionalmente, il che lascia le decisioni nelle mani

delle emozioni. Come professionisti dell'ingegneria sociale, eliminando la possibilità di pensare in modo logico, nella maggior parte dei casi si rimuove anche la possibilità di offrire un momento educativo. Quando l'obiettivo scopre che le sue paure sono state usate solo per un test, sviluppa emozioni talmente negative da obbligarlo a non voler ricevere più alcuna lezione da voi.

Scegliere fra influenzamento e manipolazione come ingegneri sociali

Chi intende svolgere la professione dell'ingegnere sociale, vorrà assicurarvi che il cliente possa trarre insegnamenti dal suo impegno. Questo significa che è molto meglio influenzare che manipolare.

Tuttavia, prima di decidere che non esistono situazioni in cui si debba ricorrere alla manipolazione, lasciate che vi dica di alcuni casi in cui la impiego e senza alcun rimorso.

In Innocent Lives Foundation, a volte abbiamo la necessità di utilizzare la manipolazione per raggiungere i nostri obiettivi. Quando cerchiamo di scovare le reti di pedofili o individui che commettono crimini orribili, sfruttiamo qualsiasi possibilità.

Uso la manipolazione anche quando lavoro su attacchi al Paese. Molto spesso, quando il mio team protegge beni o infrastrutture pubbliche, impieghiamo sia l'influenzamento sia la manipolazione per garantirci ogni possibilità di successo.

Un'altra situazione in cui utilizzo la manipolazione è quando è richiesta da un cliente. Generalmente, ciò accade quando la posta in gioco è molto alta, per esempio quando il cliente è un grande istituto finanziario, uno stato o un'organizzazione di supporto alle infrastrutture che deve mettere alla prova tutti i livelli di sicurezza. A volte un cliente dice di aver bisogno che il mio team ricorra alla manipolazione anziché all'influenzamento per mettere sotto forte

stress i protocolli. In genere, questa richiesta viene avanzata dopo che abbiamo condotto altri test e dobbiamo procedere a un livello successivo. Quando però eseguiamo questi test aggiuntivi, ci assicuriamo sempre che sia ben chiaro lo scopo e che ci sia una lezione da apprendere.

Per esempio, uno dei nostri clienti ha avuto bisogno di noi per sottoporre a test il loro personale avanzato del supporto telefonico. L'azienda proteggeva dati del valore di milioni di dollari e il cliente voleva assicurarsi che il supporto telefonico resistesse agli attacchi che avrebbero potuto subire nel mondo reale.

Dopo un paio di tentativi condotti usando l'influenzamento, decidemmo di impiegare un pretesto che coinvolse due agenti di sesso femminile del mio team di ingegneria sociale.

L'Agente 1 chiamava il dipartimento e richiedeva alcune informazioni per completare una busta paga utilizzando una scusa molto credibile.

Agente 1: Ciao, sono Sarah, della XYZ. La persona che si occupava delle buste paga è stata licenziata e questa volta devo fare io gli stipendi. Settimana prossima dovrei partorire, è il mio primo figlio, e devo terminare il lavoro entro la fine della settimana.

Supp. tel.: Congratulazioni! Che emozione! Nessun problema: posso aiutarla. Devo solo verificarla e poi posso resettare l'account e farla accedere.

Agente 1: Eccellente, grazie. Ohi!

Supp. tel.: Tutto bene, Sarah?

Agente 1: Non so. Ho appena avuto una strana fitta. Probabilmente è solo lo stress. Va bene, facciamo questa cosa, così posso procedere. Di che cosa ha bisogno?

Supp. tel.: Ok, ho bisogno del suo numero di codice e del suo PIN.

Agente 1: Signore, come le ho detto, l’incaricata è stata licenziata e non so quale PIN usava. Lo ha resettato e ora ho bisogno di tornare sul suo account.

Supp. tel.: Oh, Sarah, mi dispiace tanto, ma io…

Agente 1: [*simulando il travaglio e lasciando cadere il telefono*] Oh mio Dio, oh mio Dio, mi si son rotte le acque!

Supp. tel.: Sta bene? Signora? Tutto bene?

Agente 1: [*urlando a un finto collega*] Vieni a prendere il telefono e tu [*come se parlasse a un altro collega*] CHIAMA IL 118!

Agente 2: pronto, chi è?

Supp. Tel.: Oh mio Dio. Salve, sono Steve della QRS. Stavo assistendo Sarah con l’account delle paghe, ma penso che abbia bisogno di aiuto. Vada pure.

Agente 1: [*urlando da lontano*] Se riattacchi quel telefono, ti licenzio! Prepara gli stipendi o la settimana prossima NESSUNO verrà pagato!

Agente 2: [*sotto forte stress*] Oh, Steve, ho solo bisogno di accedere al conto, poi Sarah si lascerà portare in ospedale.

Sorprendentemente, Steve diede il numero di conto e tutte le informazioni di cui avevamo bisogno.

Inventiva? Sì, molta. Manipolazione? Assolutamente! Ma la società aveva espressamente chiesto di determinare se il suo supporto telefonico era in grado di resistere a ogni pur fantasioso tipo di attacco proveniente dal mondo reale che potesse essere escogitato da un vero hacker e abbiamo scoperto che cosa avrebbe o non avrebbe funzionato sul personale.

Non intendo fornire un elenco esaustivo di quando sia il caso di utilizzare la manipolazione, ma vi ho spiegato alcune cose che dovete sempre considerare se pensate di fare il mestiere dell’ingegnere

sociale. Userete la manipolazione? E se sì, quando? E fin dove vi spingerete?

I principi dell'influenzamento e della manipolazione funzionano con la maggior parte degli esseri umani non psicopatici e nessuno di noi può trascorrere troppo tempo nel "lato oscuro" senza poi rischiare di perdersi. È impossibile entrare nel fango e non sporcarsi. Trovo utile parlare con il mio team alla Innocent Lives Foundation dopo aver usato la manipolazione, per assicurarmi che si sentano a posto e che non ne siano rimasti troppo colpiti. La fondazione ha uno psicologo dedicato al personale proprio per garantire che le nostre persone lavorino in un ambiente sano e sicuro, nel quale possano anche scaricare il peso mentale di qualsiasi negatività.

Riepilogo

Se volete conservare anche solo una cosa importante da questo capitolo, fate che sia questo: siete esseri umani (e anch'io lo sono). L'influenzamento, chiaro e semplice, funziona. Funziona sui vostri obiettivi e funziona anche su di voi. È impossibile fermarlo, è irresistibile.

L'influenzamento, se usato correttamente, è gratificante e può alterare i comportamenti e le interazioni. Se riuscirete ad applicare con efficacia l'influenzamento e la capacità di stabilire un legame, sarete davvero inarrestabili.

Le persone *vorranno* raccontarvi tutto di loro. *Vorranno* fidarsi di voi. *Vorranno* essere vostri amici e darvi una mano. Questo è un grande potere e se non state attenti, può dare alla testa e potreste abusarne.

Tenetevi sotto controllo, ricordandovi costantemente perché avete scelto questo tipo di professione. Io mi ripeto costantemente le seguenti cose.

- Lo sto facendo per proteggere la sicurezza dei miei clienti.
- Lo sto facendo perché sono bravo a farlo.
- Lo sto facendo per aiutare gli altri a conoscere questo pericoloso vettore d’attacco.
- Lo sto facendo per provvedere alla mia famiglia e ai miei dipendenti.

Queste responsabilità giocano un ruolo fondamentale nell’essere un vero *professionista* dell’ingegneria sociale. E il fatto di ragionare in questo modo *influenza* le mie decisioni a vantaggio dei miei clienti, dei miei dipendenti e di me stesso.

I principi dell’influenzamento e della manipolazione trattati in questo capitolo vengono usati quotidianamente da operatori di marketing, pubblicitari, venditori, organizzazioni che cercano donazioni o nuovi associati e da molti altri. Perché non dovremmo usare questi stessi principi anche per aiutare i nostri clienti a capire quanto possano essere pericolosi le mani di un esperto truffatore o ingegnere sociale?

Dedicate del tempo a leggere e rileggere questo capitolo e scegliete un principio alla volta sul quale lavorare. Provate ad applicare quel principio in ufficio o con la vostra famiglia, sempre in modo benevolo. Man mano che ve ne impadronirete, diventerà un elemento del vostro arsenale comunicativo, un’altra freccia nella faretra, che vi renderà ingegneri sociali ancora migliori.

Ho altre due frecce da offrirvi per la vostra faretra. Il prossimo capitolo vi aiuterà a sfruttare le competenze di cui vi ho parlato negli ultimi due capitoli.

Realizzare la propria opera d’arte

L’arte e la scienza hanno il loro punto d’incontro nel metodo.
- *Edward George Bulwer-Lytton*

Ho deciso di tornare, momentaneamente, al tema dell’arte del mio primo libro, Social Engineering: The Art of Human Hacking (Wiley, 2011) per definire chiaramente perché questo capitolo è così importante. Dopo aver modellato il piano delle comunicazioni, costruito il pretesto e appreso le tecniche per stabilire il legame e per influenzare siete pronti per partire, e quindi dovete essere in grado di mettere tutto in azione. È qui che l’arte incontra la scienza del quadro di riferimento e della sollecitazione.

Come dice il conte Edward George Bulwer-Lytton, politico e scrittore britannico del XVIII secolo, il *metodo* è il luogo in cui l’arte e la scienza si incontrano e si incrociano l’una con l’altra. Questo capitolo spiega come, in quanto professionisti dell’ingegneria sociale, possiate imparare l’arte di usare la sollecitazione e il quadro di riferimento con precisione scientifica.

Quando iniziai a lavorare in una cucina, il capo chef (il mio capo) mi consegnò un sacchetto di sedano e mi disse: “Fai una julienne”. Essendo alle prime armi, non avevo proprio idea di cosa intendesse. Dopo pochi secondi, che mi sembrarono un’eternità, mi disse: “Non hai proprio idea di cosa sto parlando, vero?”.

Feci un cenno e, dopo 60 secondi, lo chef aprì il sacchetto e preparò il sedano come nella Figura 7.1.



Figura 7.1 Una perfetta julienne di sedano

“Ah, tagliato a bastoncini”, dissi come se fossi l’uomo più intelligente del mondo. Iniziai col primo gambo – preciso e lento – mentre lo chef mi osservava. Disse: “Bel lavoro; ora ho bisogno di due sacchetti fatti così”.

Sentendomi fiducioso, tentai di imitare la sua velocità. Per non urtare la sensibilità di nessuno, non pubblicherò l’immagine del mio originale tentativo di preparare una julienne di sedano e… dita.

Probabilmente vi starete chiedendo che cosa c'entri questa storia con il tema di questo capitolo. Cucinare è un'arte, ma c'è anche della scienza dietro il modo in cui si usano gli strumenti – il modo in cui si impugna il coltello può anche pregiudicare le tue possibilità di lavorare come un vero chef. Capire l'arte di come rendere gustoso il cibo è molto importante per uno chef, così come capire come preparare il cibo (in genere senza lasciarci troppe dita) in un modo che migliori il piatto. Mescolare l'arte della preparazione del cibo e la scienza del combinare il tutto a formare un piatto crea un perfetto equilibrio.

NOTA

Nel corso degli anni, mi sono tagliato le dita così tante volte da sembrare una creazione del Dr. Frankenstein, ma nella mia carriera e hobby di chef, non ho mai servito a nessuno frammenti di dita in un piatto. Ho pensato che vi facesse piacere saperlo.

Questo capitolo è concepito con l'idea di fondere l'arte e la scienza del quadro di riferimento e della sollecitazione, per portare le abilità apprese nei primi sei capitoli a un livello superiore. Applicando correttamente ciò che apprenderete in questo capitolo, dovreste essere in grado di ottenere almeno una stella Michelin in ingegneria sociale.

Le regole dinamiche del quadro di riferimento

Pensate alla vostra casa e a come è strutturata. Guardandola dall'esterno, una stanza vi sembra separata rispetto alle altre? Avete un salotto di forma strana o è un classico rettangolo? La struttura dell'abitazione – come sono disposte le pareti, dove sono collocate le finestre, qual è la posizione delle porte e così via – è determinata dal progetto della casa. In altre parole, il modo in cui vedete e percepite la vostra casa si basa sul modo in cui è stato realizzato il quadro di riferimento.

Il quadro di riferimento nella comunicazione non è così diverso. Penso che il quadro di riferimento, ovvero il modo in cui qualcuno osserva e poi reagisce a una determinata situazione, sia in gran parte basato sulla vita del soggetto e sulle sue vicissitudini. E quei frame, o punti di vista, possono essere modificati in base all'esperienza di vita.

Quando avevo 16 anni, il surf e lo skateboard erano tutta la mia vita. Per quanto mi riguardava, non c'era nient'altro per cui valesse la pena di vivere. Un esempio di come possa essere dinamico il quadro di riferimento viene proprio da questo periodo della mia vita.

Un giorno, caricammo le nostre tavole da surf sul portapacchi di due auto, ammassate una sull'altra e guidammo nel cuore della notte dalla costa occidentale alla costa orientale della Florida. Avevamo sentito che era in arrivo una tempesta e volevamo correre sulle sue onde.

Arrivammo alle 5 di mattina. Il Sole sarebbe sorto dopo un'ora e mezza. Scaricammo le nostre tavole e le passammo con la cera. Avevamo ancora una mezzora prima che il Sole fosse abbastanza alto da permetterci di vedere chiaramente le onde, ma eravamo ansiosi e avevamo 16 anni, quindi decidemmo di gettarci nel buio per catturare la prima onda, non appena fosse sorto il Sole. Potevamo sentire le onde infrangersi sulla riva e in lontananza scorgevamo anche la sagoma di alcune grandi onde in arrivo.

Uno per uno, tutti e sei andammo incontro alle onde e ci mettemmo in fila. Aspettammo nell'acqua, dondolando su e giù e aspettando che il Sole sorgesse. Dopo pochi minuti, sentimmo quello che sembrava essere un gran colpo di fucile.

Non ci facemmo troppo caso, perché il suono sembrava piuttosto lontano e non sembrava minaccioso. Iniziai a sentire un odore pungente, così mi rivolsi a uno dei miei amici e dissi: "Ehi, è la marea rossa?".

La marea rossa è un periodo dell'anno in cui c'è un intenso proliferare di alghe che uccide i pesci e molte altre forme di vita. Il loro odore è piuttosto sgradevole. Ma il mio amico rispose: "No, è troppo presto, non so di che cosa si tratta…".

Solo pochi minuti dopo, il Sole era salito sull'orizzonte e vedevamo arrivare le meravigliose onde che ci preparavamo a cavalcare. Vedemmo anche un gruppo di pescatori su un molo piuttosto vicino a noi che gettavano in acqua esche per gli squali! I colpi di fucile che avevamo sentito erano dei pescatori, che sparavano agli squali che emergevano. Quindi io e i miei amici eravamo immersi in una "zuppa di pesce" per squali. Da idioti scoppiammo a ridere ma eravamo davvero in pericolo.

Guardai in basso e vidi una grande ombra passare sotto la mia tavola. Non sono mai stato bravo a misurare le cose, così non posso dirvi esattamente quanto fosse grande, ma di certo era più grande della mia tavola.

Io e i miei amici ridemmo ancora di più, uscimmo da quella "zuppa" e cavalcammo qualche grande onda. A 16 anni, il mio quadro di riferimento era solo il surf e gli squali non significavano molto per me.

Ripensando a quella situazione, quasi trent'anni dopo, il mio quadro di riferimento è sicuramente cambiato. Tremo al solo pensiero anche se mi trovo lontano dall'acqua, dalle esche per squali e dalla tavola da surf. Ma quando a 16 anni salivo sulla mia tavola, non avevo paura di niente: vivere pericolosamente faceva parte della mia vita. Ora, con due figli, un'attività e tanta voglia di vivere, la sola idea di trovarmi in acque piene di esche e infestate dagli squali mi riempie di terrore. E mi vien voglia di costruire una macchina del tempo per tornare indietro nel tempo e prendere a calci nel sedere un certo sedicenne.

Le mie esperienze di vita, la mia età e il mio assetto interiore sono tutti elementi che costituiscono il mio quadro di riferimento. Questo

concetto è troppo importante per passare oltre. *Il quadro di riferimento è dinamico, non statico*.

Il quadro di riferimento è una caratteristica del funzionamento del nostro cervello. La nostra mente reagisce all'intero contesto di una situazione e non alla sola situazione isolata. Ecco alcuni esempi:

- La Luna sembra più grande quando è all'orizzonte rispetto a quando è nel bel mezzo del cielo. Questo perché il nostro cervello reagisce al contesto (alla posizione) di un oggetto, anche se la Luna ha sempre le stesse dimensioni apparenti.
- Per i nostri vecchi cani, non usiamo il verbo uccidere; diciamo che li sopprimiamo. Questo è un quadro di riferimento che usiamo per tentare di allontanare da noi una circostanza dolorosa.
- Nel 1974, Elizabeth Loftus dimostrò l'essenza del quadro di riferimento in uno studio che prevedeva un semplice cambio di parole in una frase. Dopo aver mostrato a qualcuno il video di un incidente d'auto, gli pose due domande.
  - A che velocità procedevano le auto quando sono entrate in contatto?
  - A che velocità procedevano le auto quando si sono scontrate?

La prima domanda ha sempre suscitato in risposta una velocità inferiore rispetto alla seconda (potete leggere di questo studio in: www.simplypsychology.org/loftus-palmer.html).

In uno studio del 1986 condotto da David A. Snow, E. Burke Rochford Jr., Steven K. Worden e Robert D. Benford, intitolato Frame Alignment Process, Micromobilization, and Movement Participation (www.jstor.org/stable/2095581?seq=1#page_scan_tab_contents), i ricercatori hanno definito i seguenti quattro diversi aspetti del quadro di riferimento.

- Costruzione di un ponte.

- Amplificazione.
- Estensione.
- Trasformazione.

Voglio che pensiate alla *costruzione di un ponte fra quadri di riferimento* dal punto di vista di un ingegnere sociale. Mentre vi avvicinate a un'azienda vedete una guardia di sicurezza. Il suo quadro di riferimento è chiaramente quello di mantenere tutti gli estranei all'esterno della proprietà. Il quadro di riferimento di un ingegnere sociale è quello di guadagnare l'accesso all'edificio.

Non sarebbe professionale che l'ingegnere sociale andasse dalla guardia di sicurezza e dicesse: "Salve, ho bisogno di entrare per rubare alcune cose e seminare il caos". Anche se siete professionisti e pen-tester, non potreste dire: "Guardi, sono un professionista della sicurezza e sto cercando di aiutare la sua azienda a proteggere gli accessi. Se mi fa entrare posso hackerare i vostri server".

Quindi, che cosa costruisce quel ponte tra il quadro di riferimento vostro e quello della guardia? Riuscite a pensare a qualcosa di cui ho già parlato e che potrebbe colmare questa distanza? Un indizio è rappresentato nella Figura 7.2.

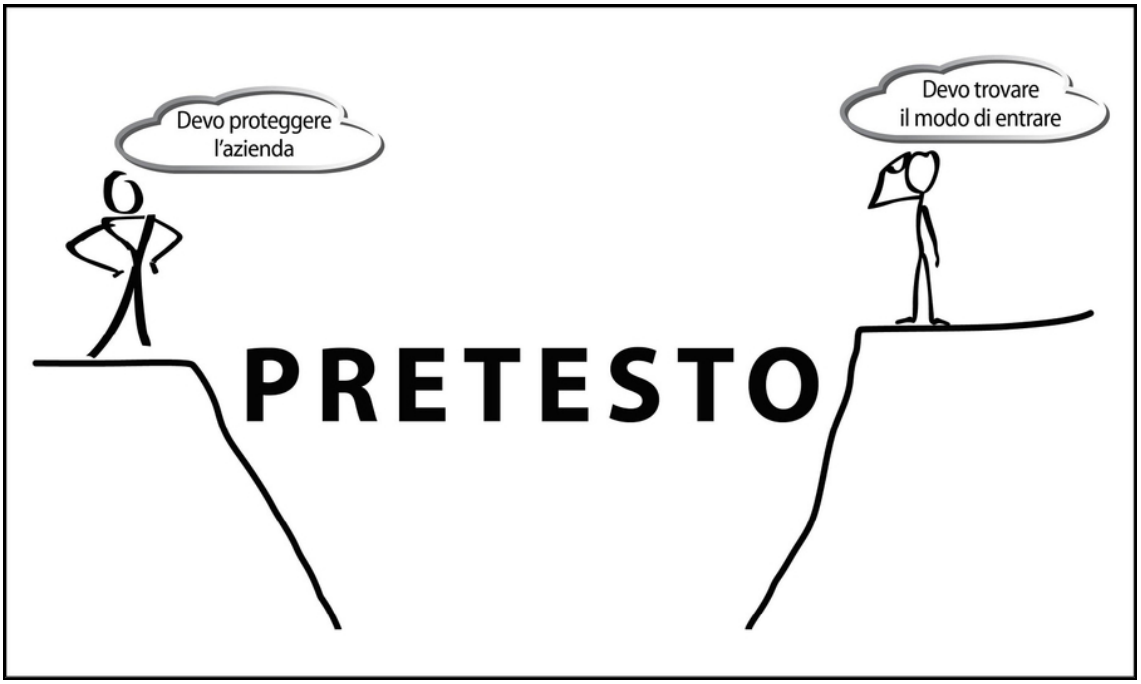


Figura 7.2 Il pretesto colma il divario fra i quadri di riferimento.

Il pretesto ha proprio lo scopo di colmare il divario e di aiutarvi a modificare il quadro di riferimento dell'obiettivo in modo che accetti quello che dite e fate. Tutti i dettagli di cui dotate il vostro pretesto – quello che portate con voi, il vostro aspetto e così via – aiuta a "piegare" il quadro di riferimento, ma c'è di più.

Nel 2004, George Lakoff scrisse il libro Non pensare all'elefante (Fusi orari, Roma 2006). In quel libro, definisce le quattro regole del quadro di riferimento. Queste quattro regole sono essenziali per imparare a padroneggiare quest'arte. Io ho solo adattato le quattro regole di Lakoff all'ingegneria sociale.

Regola 1 – Tutto quello che dite evoca il quadro di riferimento

Per comprendere meglio questa regola, dovete capire come la nostra mente lavora per visualizzare le cose sotto forma di immagini. I più

grandi maestri e narratori usano le parole proprio per evocare immagini nei vari punti delle loro storie. Ecco un esempio di come lo stesso evento possa essere raccontato in due diversi modi.

- Storia 1 Mentre ero seduto sulla mia tavola da surf, vidi una grande onda venirmi incontro. Mi sono sdraiato e ho spinto, ma l'onda si è infranta e mi sono ritrovato sott'acqua a chiedermi quanto fosse grande lo squalo che avevo visto.
- Storia 2 Il Sole occhieggiava all'orizzonte e i suoi raggi lambivano l'acqua, e mi riscaldavano il viso. Un'onda, alta come un palazzo, incombeva su di me. La sua forza emanava dalla velocità e dal filo dell'onda. Il suo apice schiumoso piombò su di me come un leone in carica.
  Mi sdraiai sulla mia tavola e la sospinsi verso la cima. Scavavo nell'acqua usando ogni fibra del mio corpo. L'acqua, pur fluida, aveva la consistenza del cemento.
  L'onda sollevò la mia tavola con una forza sovrannaturale. Passai da un istante all'altro dal fondo alla cima di un ottovolante. A stenti stavo in piedi, mentre la tavola fremeva e batteva sull'acqua. Quando mi voltai, vidi solo il labbro dell'onda, prima che mi schiaffeggiasse come un ladro infuriato.
  L'onda mi travolse, e sott'acqua trattenni il fiato, immaginando quel nero proiettile di carne dello squalo che piombava su di me. Fra panico e ipossia raggiunsi la superficie. Afferrai la tavola, le dita tremanti, e remai fino a riva.

Entrambe le storie raccontano lo stesso evento, ma quale vi aiuta davvero a immaginarvelo? Quale vi aiuta a sentirvi più presenti nella storia? Ecco perché questa regola è così importante. A volte le parole che scegliamo dal nostro vocabolario quotidiano possono creare immagini mentali offensive per l'obiettivo. Come professionista dell'ingegneria sociale, trovo che non solo riesco a essere più efficace,

ma riesco a conservare più clienti se faccio attenzione a non usare un linguaggio offensivo.

Per non rendere volgare questo libro, non produrrò la lunga lista di parole che potrebbero essere offensive, ma vi presento solo alcune linee guida sulle cose da evitare.

- Battute razziste Anche sotto forma di battuta, gli insulti razzisti non sono divertenti. In più correte il rischio di essere etichettati come ignoranti.
- Battute sul genere o sul sesso Hanno lo stesso effetto degli insulti razziali: sono degradanti e pregiudicano la costruzione di legami.
- Imprecazioni Trovo che anche se il mio obiettivo utilizza un linguaggio volgare, posso evitare di farlo per rispetto di coloro che ascoltano la conversazione. Spesso, evitando di usare lo stesso linguaggio dell'obiettivo, posso anche cambiare il loro modo di usare quel linguaggio.
- Funzioni corporee Queste parole scatenano forti sentimenti di disgusto e, pertanto, dovrebbero essere evitate.

Pensate alle parole che usate nel vostro vocabolario quotidiano e poi decidete se potrebbero evocare nell'obiettivo una delle sette emozioni di base: rabbia, sorpresa, paura, disgusto, disprezzo, tristezza o felicità. Quindi decidete se quell'emozione è positiva o negativa. Se è potenzialmente negativa e pericolosa, evitate di impiegare quella parola.

SUGGERIMENTO

Nel mio campo svolgiamo "test di penetrazione". Naturalmente si tratta di un'attività che presta il fianco a una sfilza di allusioni. Tuttavia, fin troppo spesso, ho sentito qualcuno che aveva completato un pen-test dire: "Mi sono fatto quel server". Considerando la frequenza con la quale qualcuno è vittima di violenza sessuale, trovo di cattivo gusto questa affermazione. Sentire un professionista della sicurezza descrivere il proprio lavoro come uno stupro potrebbe evocare, in chi magari è stata vittima di una violenza sessuale, il

trauma che ha subito. Quindi… non usate termini volgari per descrivere il vostro lavoro!

Regola 2 – Le parole definite nel quadro evocano il quadro

L’altra sera camminavo in veranda e, in un angolo illuminato, ho visto una creatura in una ragnatela. Stava avvolgendo un insetto in un bozzolo, per cibarsene in seguito.

Che cosa vi ho appena descritto? Probabilmente la scena rappresentata nella Figura 7.3.



Figura 7.3 Nel caso ve lo stiate chiedendo, sì, è un ragno. Foto per gentile concessione di Artyangel, https://pixabay.com/en/Spider-fly-web-insect-2683918/.

Il punto è che non ho avuto bisogno di usare la parola “ragno” per evocare in voi l’immagine del ragno. Mi è bastato descrivere il ragno e il vostro cervello lo ha automaticamente immaginato.

Come professionista dell’ingegneria sociale, il mio pretesto vi induce automaticamente a pensare al lavoro che dico di dover fare da

voi. Ma posso anche sollecitare il giusto quadro emotivo descrivendo una situazione, invece di ricorrere a minacce.

In un caso, inviai a un cliente un phishing che suonava più o meno così.

Il 4 gennaio, la sua automobile è stata fotografata mentre attraversava l'incrocio XCV431 senza rispettare il cartello stradale di Stop. È stata emessa una contravvenzione che non è stata pagata. Il mancato pagamento può comportare ulteriori provvedimenti. Può presentare un reclamo o verificare l'esito del pagamento sul nostro portale sicuro www.pleaseclickthisnowsoicanhackyou.com.

(Ovviamente, l'URL aveva una composizione più convincente) Notate che non ho avuto bisogno di minacciare un arresto, né di minacciare gravi sanzioni. Ho appena evocato a parole quanto era necessario per innescare le emozioni di curiosità e timore, offrendo però al destinatario la speranza che ci fosse una via d'uscita (e lui, sì, ha fatto clic).

Regola 3 – Negazione del quadro di riferimento

Immaginate la seguente scena: a un mio allievo avevo assegnato il compito di ottenere da una persona alcune informazioni personali: il nome completo, la data di nascita e un breve curriculum. Anche se l'allievo era nervoso per la mia presenza da osservatore, la conversazione iniziò abbastanza bene e, dopo un minuto, stava andando così.

Allievo: Buongiorno, mi darebbe una mano? Mi stavo chiedendo che cosa comprarle per un regalo e cercavo una bella idea. [*L'allievo ha impiegato una bellissima affermazione di convalida: un'idea per un regalo di compleanno per la moglie.*]

Obiettivo: Certo, nessun problema. Veramente però dovrei… [*Stava per dire "andare", ma fu interrotta dall'allievo.*]

Allievo: [*tendendo la mano*] Piacere, sono Tom, Tom Smith. [*Usò un bel ritmo naturale, per sollecitare l'obiettivo a rivelare il suo nome.*]

Obiettivo: Ah, piacere di conoscerla, Tom. Mi chiamo Sarah.

Allievo: Piacere di conoscerla, Sarah. Posso chiederle il cognome?

Obiettivo: E perché vuole saperlo?

Allievo: Oh, nessun motivo, solo curiosità. A ogni modo, come festeggia il suo compleanno? È nata a luglio?

Obiettivo: Ehi, Tom, è stato un piacere conoscerla, ma non credo di volerle dare tutte queste informazioni. Mi scusi.

Allievo: Nessun problema, Sarah, non sono certo qui a *fregare* lei o qualcun altro!

A quell'ultima affermazione, l'obiettivo si allontanò fisicamente dal mio allievo, guardò l'orologio, disse che era in ritardo e se ne andò.

Che cosa ha sbagliato? Io la chiamo *negazione del quadro di riferimento*, ovvero menzionare proprio il pensiero al quale volete che obiettivo non pensi, inducendolo in pratica a pensare proprio a quello.

Qual è l'unica cosa che non volete che il vostro obiettivo pensi quando lo impegnate in un attacco di ingegneria sociale? Che non pensi che lo *state fregando*!

Se non volete che lo pensino, non dovete dire cose come:

- "Non sto cercando di fregarla!".
- "Non sto cercando di entrare!".
- "Non le invierei mai un'email di phishing".
- "Non sono mica un truffatore!".

Tutti questi sono esempi di negazione del quadro di riferimento. Ogni volta che ci opponiamo al quadro di riferimento, lo neghiamo. E ricordate la Figura 7.2: il loro quadro di riferimento è proteggersi.

Cercate dei modi per ampliare o migliorare il quadro di riferimento usando il vostro pretesto, l'abbigliamento o altri strumenti, offrendo quindi all'obiettivo la possibilità di fugare ogni domanda o dubbio.

Regola 4 – Fare in modo che l'obiettivo pensi al quadro di riferimento, rafforza il quadro di riferimento stesso

Ogni volta che induciamo qualcuno a pensare a un quadro di riferimento, rafforziamo quel quadro di riferimento. Qualsiasi sia, lo rafforziamo. Per esempio, i genitori hanno la possibilità di rafforzare nei propri figli quadri di riferimento positivi o negativi, come in questi esempi:

- "Sei talmente stupido!".
- "Non sei un granché in campo".
- "Farai mai una cosa giusta?".
- "Sei un bel tipo: carina e intelligente!".
- "Hai la possibilità di realizzare qualsiasi cosa tu abbia in mente".
- "So quanto è difficile, ma so anche che puoi farcela!".

Come professionisti dell'ingegneria sociale, potete rafforzare i quadri di riferimento con le parole, l'abbigliamento e il pretesto che scegliete.

In una missione di vishing che stavamo svolgendo, il nostro pretesto era che stavamo chiamando dal reparto IT e il sistema di controllo dei badge si era danneggiato nel corso della notte. Il nostro obiettivo era ottenere il nome completo, la data di nascita, il codice interno e altri dettagli dei dipendenti che eravamo stati incaricati di chiamare. Andò più o meno così:

Obiettivo: Buongiorno, sono Bob. Come posso aiutarla?

Ingegnere sociale: Buongiorno Bob, sono Paul dell'IT. La scorsa notte si è danneggiato il sistema di controllo dei badge e ci hanno segnalato circa 100 account malfunzionanti. E lei è uno dei fortunati. Ha avuto problemi all'ingresso, oggi?

Obiettivo: No, ha funzionato. Con chi parlo?

Ingegnere sociale: Sono Paul, Paul Williams dell'IT. Lavoro con Tony R. Look, ci vorrà solo un minuto. Come sa, la registrazione degli accessi è legata direttamente al calcolo dello stipendio, quindi vogliamo correggere gli errori al più presto.

Obiettivo: Ah certamente! Di che cosa avete bisogno?

Ingegnere sociale: Devo verificare solo il vostro nome completo. Può scandirmelo?

Obiettivo: Davvero? È un semplice S-M-I-T-H. Non troppo difficile.

Ingegnere sociale: Wow, allora per fortuna ho chiamato. Qui all'IT abbiamo Robert Jones per questo interno. Chissà cosa sarebbe successo nel calcolo degli stipendi. Probabilmente quando è stato lanciato l'algoritmo che è andato in errore, ha provato a ricollegare le tabelle e ha disallineato i database. [I*n pratica dissi qualcosa che non significava nulla, ma immaginavo che Bob, contabile, avrebbe accettato questa "spiegazione"*.]

Obiettivo: Sì, non vorrei che qualcun altro si prendesse il mio stipendio. Possiamo controllare anche il resto?

Da lì in poi è bastato dare false indicazioni e conferme per ottenere il nome completo, la data di nascita, il codice interno e anche le ultime quattro cifre del suo codice di previdenza sociale. Le mie parole e il mio pretesto avevano rafforzato il mio quadro di riferimento, quindi l'obiettivo ha ceduto facilmente.

Mantenete concentrato l'obiettivo sul vostro quadro di riferimento, con le prime parole, e il passaggio alla fase successiva sarà molto più facile. La chiamiamo *sollecitazione*.

La sollecitazione

Come definireste la sollecitazione?

Io la definisco come “ottenere informazioni senza richiederle”. In sostanza, la sollecitazione somiglia a una normale conversazione, ma il professionista la guida in direzione ben precisa per ottenere determinate informazioni senza mai chiederle.

La sollecitazione ha alcune regole e principi naturali, che portano al successo. Ognuno di questi è efficace da sé, ma quando gli elementi vengono combinati, padroneggiando l’arte della conversazione, un professionista dell’ingegneria sociale può rappresentare una forza che è bene non sottovalutare.

Mentre leggete delle quattro regole di sollecitazione, tenete in mente un argomento importante: se è fatta bene, la sollecitazione dovrebbe sembrare una normale conversazione, senza forzature, con l’obiettivo.

Appelli all’ego

Nel Capitolo 5 parlo di sospensione dell’ego; questo principio è l’esatto contrario. In questo caso, dovete rifocalizzarvi sull’ego dell’obiettivo anziché considerare il proprio.

Che cos’è l’ego? L’*Oxford English Dictionary* lo definisce come “Il senso di autostima di una persona”. È importante capirlo, perché quando capiamo questo fatto, possiamo pensare che il nostro compito sia quello di gonfiare l’ego dell’obiettivo, ma non è quello che intendo. Sto dicendo che dovete fare appello al suo ego.

Nel fare appello all’ego dell’obiettivo dovete tenere in mente le tre seguenti cose:

- dovete usare la sincerità;
- dovete avere il giusto livello di legame;
- dovete essere realistici.

Supponete che non vi abbia mai incontrati prima. Vi vedo, mi avvicino e vi dico: “Wow, lei è una delle persone più attraenti che abbia mai visto”. Se poi provassi ad avviare una conversazione, che cosa potreste pensare? Probabilmente una o più delle seguenti cose:

- “Vaff…!”.
- “Che cosa vuoi da me?”.
- “Ok, dov’è la fregatura?”.
- “Certo che lo sono. Sparisci!”.

Qualunque cosa pensiate in quel momento, è dovuta al fatto che quell’appello al vostro ego non è stato fatto con sincerità, con realismo e in linea con il livello di legame che abbiamo stabilito, quindi non produrrà una buona sollecitazione.

Ecco una storia vera, accaduta a mia moglie, che è una delle migliori sollecitatrici che abbia mai visto all’opera. Eravamo a New York. Avevo portato lei e la famiglia a vedere il mio vecchio quartiere. A un certo punto eravamo in metropolitana in direzione centro. Se avete mai preso la metropolitana, sapete che la gente se ne sta per i fatti suoi. Non è maleducata, ma neanche amichevole. Ognuno ha il suo posto e si sente stressato o stanco. Ognuno sta per conto suo e pensa agli affari suoi.

Mia moglie era seduta di fianco a una donna anziana afroamericana che sembrava volesse dormire un po’ prima di scendere. Mia moglie si sporse, toccò la sua sciarpa per sentire la consistenza del materiale e disse: “Wow, è veramente bello e morbido. Posso chiederle dove l’ha acquistato?”.

Ora: eravamo in metropolitana, a New York, e mia moglie aveva attraversato di punto in bianco confini personali, etnici e spaziali. Eppure, le due fecero amicizia in pochi secondi. Perché? Qual è stato il suo appello all’ego?

Non solo mia moglie ha convalidato il gusto della donna su un capo di abbigliamento, ma l'aveva pregata di dirle dove l'aveva trovato. E questa non era una truffa: mia moglie era davvero interessata, e quella sincerità era palese.

Grazie a questo è nata una conversazione di una ventina di minuti su dove trovare ottimi vestiti a New York. Per quanto mi sentissi infastidito, perché mi rendevo conto che così avrei speso più soldi, non potei fare a meno di ammirare mia moglie, osservarla e imparare mentre mi insegnava a essere un maestro nel campo della sollecitazione.

Ora, come potete diventare maestri come Areesa? Qual è l'ingrediente segreto? Ecco alcuni suggerimenti:

- lei ama davvero gli altri e si interessa sinceramente a loro;
- le sue intenzioni sono altruiste;
- lei è un tipo adorabile e ha un grande sorriso.

Ma che cosa potete fare se non siete un'amorevole, amichevole, adorabile, sorridente piccola donna asiatica come mia moglie?

In primo luogo, fate pratica osservando alcune cose degli altri, a partire dalla vostra famiglia. Quando tornate a casa dal lavoro domani, prendete nota delle cose: vostra figlia ha lavato i piatti? Vostro figlio ha portato fuori la spazzatura? Hanno fatto i compiti? Anche vostra moglie ha avuto una giornata lunga e stressante?

Provate semplicemente a dire qualcosa del tipo: "Wow, ho notato che i piatti erano già fatti quando sono tornato a casa. Grazie!". Oppure: "Ehi, tesoro, sembri stanca. Tutto bene oggi?".

Poi osservate che cosa succede. Il linguaggio del corpo della persona si rilasserà, e poi si aprirà e diventerà più amichevole e loquace. Perché? Perché l'avete considerata e avete fatto appello al suo ego.

Dopo aver fatto pratica in famiglia, provate fuori casa, con estranei. Sarà molto più difficile. Dovrete osservare senza essere inquietanti e condurre il vostro approccio sulla base di tutte le lezioni apprese nel Capitolo 5. Poi potrete iniziare a fare appello al loro ego.

Immaginate questo scenario: siete dietro il vostro obiettivo in coda da Starbucks. Il soggetto è un maschio, alto, approssimativamente di 34 anni. È ben vestito e ha uno stile da figlio di papà, ma nerd. Lo vedete estrarre un iPhone nuovo di zecca e scrivere un messaggio. Con questa sola informazione, quale potrebbe essere l'appello all'ego che escogitereste per avviare una conversazione? Pensateci per un attimo prima di continuare a leggere.

Io proverei con qualcosa del genere: "Mi scusi. Ho visto che ha il nuovo iPhone. Stavo pensando di prenderlo anch'io. Si trova bene?".

Se ha appena speso 1.000 dollari per un telefono, avrà certamente un'opinione. Indipendentemente dall'opinione che vi darà, potrete confermarla e fare appello al suo ego con un: "Wow, grazie, mi è stato davvero utile. Non sono mai stato bravo con queste decisioni, ma lei mi ha convinto. Mi chiamo Chris, Chris Hadnagy…" e allungo la mano per stringere la sua.

E così può iniziare una conversazione.

Interesse reciproco

Al giorno d'oggi gli argomenti interessanti sono davvero molti. E molti di questi sembrano non solo dividere le persone, ma causare vere e proprie spaccature nella società. Alcuni di questi argomenti così polarizzanti possono dare origine a una tale passione che alcune persone possono addirittura diventare violente se non concordate con loro.

È importante che un professionista dell'ingegneria sociale non solo capisca bene questo concetto, ma che abbia la capacità di mettere da

parte i propri pensieri su questi temi, per trovare un interesse reciproco.

Permettetemi di fare un esempio tratto dalla mia esperienza. Non vi dirò come la penso. Immaginate la situazione come se voi foste lì.

Ero all'ingresso di un palazzo di uffici. Avevo il compito di cercare di entrare e trovai un gruppo di persone in piedi attorno a un televisore. Era accaduto un fatto terribile: una sparatoria a scuola. C'erano bambini morti e feriti. Lo sparatore si era ucciso. Una situazione davvero orribile.

Un uomo disse: "Se fossi stato lì, e avessi avuto la mia pistola, l'avrei freddato prima ancora che potesse finire il primo caricatore".

Un'altra persona rispose: "Questo è il problema! Finché sarà così facile comprare un'arma, queste cose continueranno ad accadere!".

Come immaginate la gente si stava dividendo in due fazioni ben delineate. L'atmosfera era tesa e tutti si sentivano in dovere di dire la propria opinione sull'argomento. Una donna alzò lo sguardo su di me e, senza nemmeno chiedere chi fossi, mi disse: "Ha sentito la notizia? Questo è davvero terribile".

Risposi: "No, la sto sentendo adesso. È veramente terribile. Ha la famiglia o degli amici in quella zona?".

"Grazie a Dio, no", rispose lei. Poi, senza nemmeno un fiato, disse: "Ma è tutto a posto. Bill ha la soluzione: distribuirà pistole a tutti quanti e così torneremo al selvaggio West".

Bill, che ormai era fisicamente turbato, disse: "Molto meglio la tua idea: sederci in cerchio a cantare e pregare, mentre uccidono i nostri figli".

Ahia. La cosa stava sfuggendo di mano. Mi resi conto che non era più il caso di comportarsi da ingegneri sociali: però potevo tentare di disinnescare la situazione. Poiché entrambi i loro commenti erano rivolti a me, quando Bill ebbe finito di parlare, entrambi si fissarono

l’un l’altro e poi fissarono me, quasi a dire: “Allora? Tu da che parte stai?”.

Sapendo che se mi fossi schierato mi sarei alienato metà del gruppo, dissi: “Oh, Signore! Chissà quelle povere famiglie. Ho due figli. Non riesco proprio a immaginare che cosa significhi ricevere la notizia che uno di loro è stato ucciso. Questo è davvero un giorno triste”.

All’improvviso la spaccatura si ricompose. Non c’era più distanza fra loro. Si guardarono l’un l’altro e non si ricordavano più di essere pro o contro le armi. La cosa riguardava i nostri figli. E non importa se le pistole ti piacciono o le detesti: sul fatto che sia terribile che dei bambini vengano uccisi a scuola siamo tutti d’accordo.

Quando il vostro compito è quello di applicare l’ingegneria sociale a un gruppo grande o piccolo e l’argomento potrebbe essere scabroso o le persone non sono esattamente gradevoli, cercate un terreno comune. Di solito potete trovare qualcosa che vi permetterà di essere tutti concordi e di dare inizio a una conversazione.

L’esempio precedente è molto serio, ma funziona anche per situazioni non così tragiche. Ecco alcuni argomenti che possono aiutarvi ad avviare una conversazione su una base comune.

- Meteo – Soprattutto se c’è brutto tempo (una tempesta di neve, troppa pioggia, troppo caldo/freddo) il meteo può fornire numerosi argomenti per rompere il ghiaccio rapidamente.
- Tecnologie – Chiedere all’obiettivo consigli tecnologici su qualcosa in suo possesso (smartphone, portatile, smartwatch e così via) e che avete notato può essere un ottimo modo per avviare un discorso.
- Bambini – Finché fate domande senza superare il livello di legame che avete stabilito – e vi limitate a domande generali sui bambini, non sui loro figli in particolare – questo argomento può davvero far parlare le persone.

- Animali – La gente ama parlare (e condividere foto) dei propri animali domestici.
- Sport – Anche se non tutti sono interessati allo sport, se notate qualcuno che indossa la maglia o il cappellino di una particolare squadra, questo può essere un ottimo argomento. Sempre che non diciate qualcosa come “Ah, tifoso dei Cowboy? Come mi dispiace…”. No, questo non è un buon inizio.

Vi suggerisco di evitare argomenti come la politica, l’assistenza sanitaria, la religione, qualsiasi scelta profondamente personale e qualsiasi notizia di carattere violento. Questi argomenti hanno il potere di produrre grandi spaccature tra voi e il vostro obiettivo.

Attraverso l’osservazione dell’obiettivo e di quello che lo circonda (tramite un’attività di OSINT o l’osservazione fisica), trovate un argomento che possa essere di interesse reciproco, quindi utilizzate tale argomento per avviare una conversazione.

Dichiarazioni deliberatamente false

Il principio della dichiarazione deliberatamente falsa è così potente che dovete metterlo alla prova. Che cosa pensate quando siete in coda in un negozio di alimentari e sentite qualcuno dire un qualcosa che sapete essere falso?

Ho sentito e visto di tutto, da quelli che fanno versi di disappunto o di falsa approvazione a quelli che correggono un perfetto sconosciuto.

Perché le persone reagiscono in questo modo? Perché sentiamo il bisogno di avere ragione e di correggere tutto quello che c’è di sbagliato. Quando sentiamo qualcosa che “sappiamo“ essere sbagliato, generalmente tentiamo di correggerlo, anche se questa è solo la nostra opinione. A seconda di chi siamo, di dove ci troviamo e della nostra

passione per l’argomento, potremmo permettere alle nostre idee di uscire allo scoperto.

Ecco un esempio che mi ha davvero sorpreso per quanto funzionò. Ero seduto in un ristorante con Robin Dreeke e ci eravamo accordati su una conversazione, per vedere come avrebbe funzionato una dichiarazione deliberatamente falsa. Era un piccolo ristorante, con i tavoli l’uno vicino all’altro. Ed era normale che i commensali sentissero tutte le conversazioni altrui.

Robin mi disse, a voce piuttosto alta: “Ehi, ma hai letto quell’articolo del ‘Times’ che dice che oltre l’80 percento delle persone usa come PIN del bancomat la propria data di nascita?”.

Questo studio in realtà non esiste, l’articolo cui faceva riferimento Robin era falso e spero davvero che questa statistica in realtà sia ben lontana dalla realtà.

Risposi: “No, non è vero. Io uso una combinazione della data di nascita mia e di mia moglie, per cui è 0411”.

Robin disse: “Beh, io penso che sia vero, perché anch’io faccio così”.

Poi rimanemmo entrambi in silenzio per un paio di secondi e, proprio al momento giusto, la coppia accanto a noi andò avanti e il marito disse: “Le dico sempre di non usare la sua data di nascita per il PIN, ma lei mi dice che è facile da ricordare”. Sorprendentemente, sua moglie rispose: “Beh, come si fa a non ricordare 0660, giusto?”.

Wow, davvero questa donna ci aveva appena dato – a noi perfetti sconosciuti in un ristorante – il PIN della sua bancomat? Vorrei poter dire che la cosa si è fermata lì. Ma non è così! L’uomo dall’altra parte del nostro tavolo si rivolse alla donna con la quale cenava e disse: “E tu che PIN usi?”.

E lei, senza esitazione, rispose: “La mia banca mi permette di usare sei cifre, così posso usare tutta la data di nascita di mia figlia: 031192”.

La cameriera che ci stava servendo e che aveva sentito il discorso intervenne: “La mia banca mi permette di scegliere una parola, che scrivo usando il tastierino. Mio figlio ha chiamato il nostro cane Samson, quindi uso quello”.

Eccoci qui, seduti in un ristorante, a raccogliere date di nascita, nomi di animali domestici e, ahinoi, anche i PIN delle bancomat e il tutto grazie a una dichiarazione deliberatamente falsa.

Ero così innamorato di questo principio che iniziai a usarlo ovunque e anche a insegnarlo. Poi ho avuto un allievo che mi ha insegnato qualcosa. Raccontai questa storia a lezione e lui disse: “Wow, mi è venuta un’idea. Voglio provare alcune cose”.

Più avanti, durante la lezione, lo stavo osservando in pubblico mentre interagiva con alcuni obiettivi. Si avvicinò a una donna seduta a un tavolo intenta a mangiarsi una ciotola di fragole. Senza presentarsi, senza stabilire un legame, ebbe questa conversazione.

Allievo: Ehi, le piacciono le fragole. Forse è nata a febbraio!

Obiettivo: Umm, no, in realtà sono nata a luglio.

Allievo: Wow, il mese del “4”! Proprio il giorno della festa?

Obiettivo: No, l’11. Ma perché? [*E gli riservò uno sguardo confuso.*]

Allievo: No, niente, interessante. Arrivederci.

E poi se ne andò. Dissi tra me e me: “Non può funzionare una seconda volta”. Ma si avvicinò a un perfetto sconosciuto dopo l’altro ed elargì loro le false dichiarazioni più strane immaginabili. E ogni volta, l’obiettivo gli cedeva le informazioni richieste.

Il difetto di questo metodo è che non genera alcun legame. Così, dopo l’“attacco”, i suoi obiettivi rimanevano sconcertati e si chiesero che cosa fosse appena successo. Sicuramente non si sono sentiti meglio dopo averlo incontrato.

Fate attenzione con le dichiarazioni deliberatamente false e utilizzate le seguenti linee guida.

- Usare troppe volte di seguito delle dichiarazioni deliberatamente false può rendervi inaffidabili e questo può pregiudicare la fiducia che il vostro obiettivo ripone in voi.
- Non confondete le dichiarazioni deliberatamente false con la negazione del quadro di riferimento. Se non volete che l'obiettivo pensi che sta per essere fregato, non menzionate "fregare" nella dichiarazione deliberatamente falsa.
- La dichiarazione deliberatamente falsa funziona molto meglio dopo aver costruito un certo livello di legame con l'obiettivo.
- La dichiarazione deliberatamente falsa deve avere attinenza con la realtà. Se il mio allievo si fosse avvicinato alla prima donna e avesse detto: "Ehi, le piacciono le fragole. Amerà anche gli aquiloni!", non sarebbe andato da nessuna parte; avrebbe generato solo confusione, non il bisogno di correggere.

Vi sfido davvero a provare le dichiarazioni deliberatamente false. Vi stupirete di come funzionano e della quantità di informazioni che ne trarrete.

Avvicinarsi a un perfetto sconosciuto e chiedergli il suo PIN, la sua data di nascita o altre informazioni personali accenderà (il più delle volte) tutti i tipi di allarmi che può avere in testa. Ma usando una dichiarazione deliberatamente falsa, potete ottenere tutti questi dettagli direttamente in un'innocente conversazione.

Equivoci e dichiarazioni deliberatamente false

Ho impiegato il metodo del mio allievo in una missione di sollecitazione e funzionò alla grande. Andai avanti: "Ah, il 12 agosto. È divertente: anche mia sorella è nata in agosto".

Giocare sugli equivoci aiuta l'obiettivo a sentirsi a proprio agio dopo quello che vi ha appena detto, dietro sollecitazione. Aggiunsi: "Mia nonna diceva che i nati ad agosto sono tipi artistici e creativi. Ha forse un qualche talento musicale?".

Con una risatina la donna rispose: “No, veramente me la cavo di più con la matematica. Per questo faccio la contabile. Credo che non sempre le nonne abbiano ragione, vero?”.
Dissi: “Ah, immagino di no. Ma non diciamoglielo. La mia nonna italiana le pizzicherebbe l’orecchio e ci urlerebbe dentro!”.
La donna rispose: “Oh, so come funziona. La mia famiglia viene dall’Irlanda. Loro non pizzicano, mollano pugni!”.
“Ohi! Sembra… una cosa… divertente. E così ha un bel cognome irlandese?”. Pensai che questo potesse essere un grande passo per ottenere ancora più informazioni personali.
“Non c’è niente di più irlandese del mio nome: Mary O’Donnell”, disse, con una marcata cadenza irlandese.
Risposi: “Oh, ma che bell’accento. Purtroppo, io ho perso tutto il mio italiano, tranne per le parolacce”.
“Bene, potrebbero tornare utili!”.
Notate come, con una dichiarazione deliberatamente falsa e un equivoco, sono riuscito a ottenere il suo nome completo, la sua data di nascita, il suo lavoro e altri dettagli della sua vita e della sua famiglia.

Conoscere le cose

Non confondete la conoscenza con il “so-tutto-io”. Sono due cose completamente diverse. Avere conoscenze sugli argomenti che tratterete con il vostro obiettivo può essere molto utile durante il colloquio di sollecitazione. È tempo di parlarvi di un altro fallimento, un fallimento sul lavoro.

La mia società era stata incaricata di ottenere l’accesso alla sala server di un’università. Nell’osservare l’edificio in cui si trovava la sala server, notammo che un professore sarebbe entrato nell’edificio all’incirca alle 7. Nessun altro era nell’edificio in quel momento, quindi pensammo che sarebbe stato il momento giusto per ottenere l’ingresso. Le porte utilizzavano tutte serrature RFID e, poiché si trattava di un lavoro di ingegneria sociale, pensammo di provare prima di tutto con una tecnica che facesse leva sulle persone.

Eseguimmo la nostra OSINT sul professore e scoprimmo che aveva scritto un articolo che aveva a che fare con la fisica quantistica con alcune altre parole delle quali non sapevamo nulla. La mia infinita saggezza e la mia grande abilità (tranquilli, è sarcasmo) mi suggerirono di memorizzare il nome della pubblicazione e così il mattino dopo, pensai di attaccare bottone col professore.

Mentre camminava velocemente verso l'edificio, il mio piano era quello di iniziare la conversazione partendo dalla sua pubblicazione: avremmo camminato insieme verso l'edificio e, dopo esserci salutati, mi sarei diretto alla sala server.

Iniziai: "Buongiorno. Mi chiamo Paul Williams. Lei è il professor Smith, giusto?".

"Sì, sono io. Come posso aiutarla?", chiese il professore, senza smettere di camminare verso l'edificio.

"Volevo dei chiarimenti sull'articolo che ha scritto sulla fisica quantistica", dissi mentre snocciolavo il titolo della pubblicazione con grande facilità.

Dopo una leggera pausa, disse: "Va bene. Quali chiarimenti?".

Oh no! Il mio cervello andò in fuorigiri. Come ho fatto a non pensare a questa parte? Camminavamo ancora verso la porta, che però ora sembrava trovarsi a chilometri di distanza. Provai a pensare a una qualsiasi cosa intelligente da dire, ma la mia migliore risposta fu: "Ehm, quindi, che cosa l'ha spinta a scrivere quell'articolo?". La mia voce si spense, sprofondando nell'incertezza.

Per la prima volta da quando l'avevo avvicinato, il professore si fermò, si voltò verso di me e mi disse: "Non so a che gioco stai giocando, figliolo, ma torna da me quando lo avrai letto, l'articolo". Poi si voltò e camminò ancora più decisamente verso la porta.

Certo, avrei anche potuto leggerlo, l'articolo, ma anche se lo avessi letto decine di volte, dubito che avrei potuto trovare anche solo una o

due domande intelligenti sull'argomento. Oppure avrei potuto trovare qualcuno che ne capisse qualcosa, perché mi aiutasse a formulare domande intelligenti. Tuttavia, nessuna di queste soluzioni avrebbe facilitato le cose. Il modo più semplice sarebbe stato per me usare un pretesto che si adattava alle mie reali conoscenze. Forse avrei potuto essere un allievo che voleva seguire le lezioni di questo professore e che voleva sapere quali articoli o libri leggere per seguire meglio le lezioni.

Per cominciare a parlargli, avrei dovuto conoscere l'università, i corsi, gli insegnanti e i programmi di studio. Il fatto di avere queste conoscenze non vuol dire che avrei dovuto riversargliele addosso solo per dimostrare la mia buona fede, ma avere queste conoscenze avrebbe reso più credibile il mio modo di parlare e le cose che avrei detto. In questo modo, se mi avesse posto una domanda tipo: "In quale corso ti trovi ora?", avrei potuto rispondere correttamente e andare avanti.

Più credibili siete, più l'obiettivo si convincerà che siete chi dite di essere.

Uso delle domande

Le domande sono una parte naturale della conversazione. Dal momento in cui iniziamo a parlare, utilizziamo delle domande per inviare e ricevere informazioni. Questo è il motivo per cui, per ogni buona sollecitazione, è essenziale comprendere quali sono i quattro diversi tipi di domande, e imparare a usarli. Questo è l'argomento del presente paragrafo.

Le domande sono elementi potenti della comunicazione. Non appena sentiamo una domanda, il nostro cervello inizia a formulare una risposta. Anche se questa risposta non viene mai pronunciata, non possiamo evitare di formulare una risposta.

Un uso abile delle domande coinvolge l'obiettivo nella conversazione. Ogni tipo di domanda può essere utilizzato da un esperto di ingegneria sociale per sollecitare all'obiettivo sia informazioni sia emozioni.

Per aiutarvi a capire come utilizzare i diversi tipi di domande nell'ambito dell'ingegneria sociale, ecco una storia tratta dalla mia esperienza. La chiamerò Operazione OfficeSpace.

Il mio compito era quello di accedere al sedicesimo piano di un palazzo di uffici, ma l'azienda che occupava quel piano non possedeva l'intero edificio. Mi venne in mente un pretesto: ero stato inviato dall'azienda per condurre un'ispezione a sorpresa per vedere se venissero seguite le politiche di sicurezza dello spazio di lavoro, come il fatto di mantenere sbloccate le uscite di sicurezza.

Ho basato il pretesto su un po' di notizie di OSINT che avevamo trovato sulle nuove politiche e sulle critiche sulla stampa che questa azienda aveva ricevuto per le sue criticabili condizioni di lavoro. L'azienda si era impegnata pubblicamente a risolvere tali problemi e aveva affermato di aver inviato chiari messaggi a tutte le sedi locali, con le istruzioni da seguire.

Realizzai un badge col logo aziendale e l'indicazione "Safety Inspector" ben in vista nella parte superiore. Armato di appunti, fotocamera e altri strumenti, varcai l'ingresso e passai davanti al banco di sicurezza.

La donna dietro il banco si alzò in piedi e mi chiese: "Mi scusi, signore, dove sta andando?".

Rallentai appena e risposi: "Al sedicesimo".

"Umm, si fermi, per favore. Devo chiederle il codice, dal momento che il suo badge non funziona nell'ascensore".

"Ah sì? Mi dispiace. Mi lasci spiegare. Qual è il suo nome, signora?".

“Alicia Smith”, disse lei indicando il suo badge.

“Piacere di conoscerla, Alicia. Lavoro al sedicesimo per la ABC Corporation, e a causa di alcuni recenti incidenti in alcune delle nostre strutture, sono stato incaricato di compiere delle ispezioni a sorpresa. Le sedi, quindi, non sono state avvertite della mia presenza. Ha sentito parlare dei problemi che abbiamo avuto sulle condizioni di lavoro dei dipendenti?”.

Scrollò le spalle, ma rispose: “Sì, l’ho sentito dire”.

“Ok, allora sa quanti problemi abbiamo avuto. Sono sicuro che il vostro datore di lavoro si prende cura di voi, e questi controlli sono tutti volti a dimostrare che le cose sono a posto, ma la mia deve comunque essere un’ispezione a sorpresa per essere efficace”.

“Ok, capisco. Penso sia una buona cosa che una società prenda questa faccenda così sul serio. La accompagno all’ascensore e la invierò al sedicesimo piano”. E così stavo camminando verso gli ascensori, in compagnia della mia nuova alleata.

Mi fermai e chiesi: “Alicia, alcuni ascensori richiedono il badge anche per uscire. Quale tipo di sistema di sicurezza avete negli ascensori?”.

“Oh, che stupida. L’avevo quasi dimenticato. Sì, abbiamo appena installato questo nuovo sistema di sicurezza e ha bisogno di un badge anche per uscire. Devo solo registrarla come visitatore. Attenda qui”. Tornò di corsa alla scrivania per prendermi un badge in bianco e poi mi mandò su.

Uscii dall’ascensore al sedicesimo piano e alla mia sinistra e alla mia destra c’erano delle porte di vetro. Vidi alla mia destra una segretaria seduta e lei mi guardava con uno sguardo sempre più curioso. Mentre mi avvicinavo alla scrivania, sapevo che mi avrebbe fatto qualche domanda; volevo prevederla, e così dissi: “Salve. Sono Paul dalla sede centrale”. Estrassi il mio badge e glielo mostrai

brevemente, ma non ero sicuro di averlo reso credibile, così estrassi la penna e sfogliai gli appunti". Questo è l'ufficio 43211, giusto?", chiesi come se questo fosse un appunto su un ordine di lavoro.

"Ehm, sì Paul. Perché è qui? Non c'è nessuna visita in programma", disse, con un'espressione molto confusa.

"Non è una visita programmata: questa è un'ispezione a sorpresa. Dopo i problemi del mese scorso con la OSHA [l'ente americano per la sicurezza e la salute sul lavoro, NdT], dobbiamo assicurarci che il nostro spazio di lavoro sia stato sensibilmente migliorato. Avete ricevuto quel memo interno, giusto?".

Lei annuì con la testa e disse: "Sì. Mi è stato chiesto di stamparlo e di assicurarmi che tutti ne avessero una copia fisica".

"Bene, bene: allora un OK sulla prima casella". Passai alla seconda pagina e feci un segno su una casella, per poi dire: "Grazie! Mi ha molto facilitato il lavoro! Vorrei scrivere il suo nome, per segnalarla per aver seguito le indicazioni. Come si chiama?".

"Beth. Beth Simons".

"Eccellente, Beth. Per quanto siate scrupolosi, sono sicuro che abbiate alcune aree che richiedono un'attenzione particolare. Dove dovrei iniziare?".

Guardò verso una zona e disse: "Credo che siamo tutti in regola qui, ma non ne sono sicura. Non vorrei mettere in difficoltà qualcuno".

"Ho capito, Beth. Grazie per la sua sincerità. Inizio il mio giro. La avviserò personalmente quando avrò finito". Dopo di che potei girare per tutto l'ufficio senza sorveglianza.

Domande a risposta aperta

Come immaginate, una domanda a risposta aperta non indirizza chi la riceve verso una specifica direzione, ma invece gli permette di rispondere fornendo esclusivamente la sua opinione. Le domande a

risposta aperta, in generale, non possono essere risolte con un semplice sì o no. Una domanda a risposta aperta consente all'obiettivo di decidere quante informazioni fornire. Questo significa un rafforzamento e anche una conferma per la persona coinvolta e può aiutare a costruire un legame. Una domanda a risposta aperta è qualcosa del tipo: "Qual è il ristorante che preferisce in città?". Al contrario, "C'è un buon ristorante vicino a questo hotel?" non lo è. Entrambe sono domande valide, ma la prima sollecita informazioni che vi consentiranno di profilare l'obiettivo in modo più approfondito. Le parole che usate in una domanda suscitano emozioni e quelle emozioni influenzano la risposta che ricevete. Una domanda a risposta aperta incoraggia l'obiettivo a coinvolgere le proprie conoscenze, attitudini, credenze, opinioni e sentimenti.

Il successo di queste domande dipende in gran parte dal modo in cui voi, come ingegneri sociali, utilizzate l'ascolto attivo e indirizzate le domande con lo scopo di ottenere informazioni utili. Questo è un dettaglio importante da capire, così che, quando formulerete il vostro pretesto, potrete iniziare a pianificare il tipo di domande che usereste naturalmente. Ricordate, lo scopo è quello di far sì che l'obiettivo parli apertamente di dettagli rilevanti, che possono essere utili per completare la missione di ingegneria sociale.

SUGGERIMENTO

Il motto "Falli parlare" non è molto rilevante nell'ingegneria sociale. Non vogliamo che il nostro obiettivo, semplicemente, parli; vogliamo che ci ceda informazioni rilevanti per le nostre esigenze.

Nell'Operazione OfficeSpace ho utilizzato le domande a risposta aperta più volte, ma una che vale la pena di ricordare è quando chiesi ad Alicia il tipo di sicurezza attivo sugli ascensori. Non ha solo risposto alla domanda, ma mi ha parlato del nuovo sistema di sicurezza installato negli ascensori. L'utilizzo di una domanda a risposta aperta

in questa situazione mi ha permesso di ottenere un badge e anche informazioni importanti sui loro sistemi di sicurezza.

Domande a risposta chiusa

Le domande a risposta chiusa suscitano risposte brevi e limitate. Di solito è possibile rispondere con una o due parole. Gli esperti di interrogatori usano spesso le domande a risposta chiusa per verificare i fatti già noti. Inoltre, le domande a risposta chiusa sono eccellenti per leggere i messaggi non verbali. Quando ci viene posta una domanda a risposta chiusa, il nostro corpo risponde prima ancora della nostra voce. Il più delle volte, il nostro linguaggio del corpo dà una risposta onesta anche quando affermiamo una bugia. Potremmo scrollare le spalle o scuotere la testa, ma poi rispondere: “Sì”.

Uso domande a risposta chiusa molto spesso con i miei figli. Per esempio, potrei dire a uno di loro: “Ti ho detto di andare a letto alle 11. Hai spento il computer e sei andato a letto alle 11?”. La testa dice *no*, ma il bambino risponde: “Credo di sì. Non ho guardato l’orologio”.

Un vantaggio delle domande a risposta chiusa è che garantiscono all’ingegnere sociale la possibilità di ottenere dettagli precisi e di confermare determinate informazioni. Quando si utilizzano domande a risposta chiusa, è una buona idea iniziare con qualcosa di semplice, prima di puntare a qualcosa di più approfondito. Le basi del “chi, cosa, dove e perché” sono perfette per iniziare.

In Operazione OfficeSpace, ho usato delle domande a risposta chiusa con Beth l’addetta alla reception quando le ho chiesto se avesse ricevuto il memo. Fece un cenno affermativo, ma rispose anche verbalmente: “Sì”. Al contrario, quando ho usato lo stesso tipo di domanda con Alicia, domandandole se fosse a conoscenza dei problemi della ABC Corporation, lei strinse le spalle e rispose: “Sì”. Questa incongruenza mi dice che non era davvero sicura di saperlo.

Grazie a questa mia percezione della sua confusione, ho potuto aggiungere alcuni fatti che non erano necessariamente del tutto veritieri.

Domande fuorvianti

Mi è stato inviato un link a una pagina web che conteneva un video. La pagina iniziava con qualcosa del genere: “In questo studio, solo le persone veramente osservatrici e intelligenti possono contare il numero di volte in cui le persone con la maglia bianca si passano la palla”.

Mi sedetti a pensare: “Sono un ingegnere sociale, uno degli esseri umani più attenti ai dettagli del pianeta. Ce la posso fare!”. E feci clic su Play.

Non chiusi mai gli occhi e contai ogni passaggio. Avevo fissato continuamente lo schermo. Quando il video terminò, avevo alcune opzioni per il conteggio dei passaggi. Quando venne svelato il numero corretto, esclamai allo schermo: “Eccolo, eccolo!”. Ero pieno di orgoglio.

Ma il video proseguiva: “Ma quanti di voi hanno visto l’uomo in costume da gorilla e tutù ballare, attraversare il campo da gioco e uscire dalla parte opposta?”.

Assolutamente incredulo, esclamai: “Non c’era nessun gorilla!”. Dopo tutto sono un ingegnere sociale, uno degli esseri umani più attenti ai dettagli del pianeta, giusto? Non poteva assolutamente sfuggirmi una cosa così evidente.

Riprodussi il video dall’inizio e, con mio grande stupore, un uomo alto all’incirca un metro e ottanta, in costume da gorilla e tutù aveva attraversato il campo da gioco, aveva fatto una giravolta ed era uscito dall’altra parte.

Come potevo non averlo visto?

La risposta è semplice: la richiesta era fuorviante. Sono stato indotto a concentrarmi su una cosa – il conteggio del numero di passaggi fra le persone in maglia bianca – e il mio cervello ha bloccato tutto il resto.

Quindi, come può un ingegnere sociale utilizzare questa tecnica in una domanda? In uno scenario precedente, ho indotto l'obiettivo a pensare alle possibili ripercussioni di un mancato adempimento della mia richiesta di entrare nell'ufficio dell'amministratore delegato. Per farlo ho formulato una combinazione di una dichiarazione e di una domanda fuorviante. In sintesi, fu: "Capisco che la mia visita non era in programma, Jane. Firmi qui e me ne vado. Poi però lo spiega lei al suo capo che non ho potuto risolvere il problema del suo computer mentre era in vacanza?".

Oltre alle domande fuorvianti, utilizzo anche delle distrazioni quando accedo a un edificio. Ho una cartelletta con una fotocamera incorporata nella parte anteriore. C'è un foro (6 millimetri) con una lente che sporge e più in alto un altro più piccolo per il microfono. Temo sempre che un obiettivo lo veda. Così posiziono un ordine di lavoro o un altro foglio sulla parte anteriore della cartelletta e, con una bella penna di metallo, picchietto il foglio mentre dico qualcosa come: "Vede qui? Devo controllare il numero di serie del motore per vedere se è da richiamare". Finora nessuno ha mai visto la macchina fotografica, perché li distraggo e distolgo il loro sguardo.

Come professionisti dell'ingegneria sociale, dovrete pianificare in anticipo le domande fuorvianti. Costruitele insieme al vostro pretesto. Pensate a quello che potete fare per evitare che l'obiettivo veda le cose che non deve vedere.

In Operazione OfficeSpace, non volevo che Beth dedicasse troppo tempo al mio badge. Se non fosse stato del tutto credibile, lo avrebbe notato. Così glielo mostrai solo rapidamente e usai un rapido colpo di penna e un ordine di lavoro per indurla a guardare esattamente dove

volevo che si concentrasse. L’operazione fu efficace e mi permise non solo di distrarla, ma anche di aggiungere credibilità alle mie affermazioni.

Domande presuntive

Un altro modo in cui un ingegnere sociale può raccogliere informazioni durante la fase di sollecitazione consiste nell’usare affermazioni e domande presuntive. Potete usare questo tipo di domanda quando sapete una certa cosa e fate una supposizione per confermare quella conoscenza con una domanda o un’affermazione.

Questa è un’altra tecnica che uso coi miei figli, per scoprire dettagli non del tutto chiari. Per esempio:

Io: Allora, quando eri alla festa, Tammy si è fatto vivo?

Mio figlio: Solo molto tardi; non ti preoccupare, papà.

Con quel breve scambio ebbi la conferma che mio figlio era alla festa, così da poter continuare a sondare in quella direzione, con lo scopo di ottenere maggiori informazioni.

In qualità di professionista dell’ingegneria sociale, le domande presuntive possono essere utilizzate nell’approccio iniziale, per aggirare certi blocchi della conversazione. Un blocco è una dichiarazione o un’affermazione fatte con l’intento di impedire a qualcuno di proseguire in una certa direzione.

In Operazione OfficeSpace, usai questa tecnica con Alicia e Beth al primo approccio. La mia presunzione era di avere ogni diritto di stare lì e che loro avrebbero dovuto sapere perché ero lì e che mi avrebbero dovuto permettere di agire. Non sono ricorso all’arroganza o alla rabbia, ma ho solo adottato un’aria di appartenenza, come se sapessi esattamente dove dovevo andare e il motivo per cui ero lì.

Riepilogo

Una conversazione è come una cipolla: ha molti strati. Sollevate uno strato e potrete raggiungere il cuore, sempre più in profondità.

Ogni tecnica di sollecitazione è un elemento importante di una conversazione. Imparare a usarle può aiutarvi a diventare veri maestri di conversazione ed eccezionali ingegneri sociali. L'obiettivo della sollecitazione è quello di trarre informazioni conducendo una conversazione dall'aspetto del tutto normale. Facendo pratica con queste abilità, questo è esattamente quello che sarete in grado di fare. La cosa affascinante è che questo non si limita alle conversazioni verbali: queste stesse abilità funzionano anche nelle conversazioni via e-mail, in chat, messaggi, telefonate e qualsiasi altro mezzo.

Proprio come uno chef decide quali attrezzi e ingredienti usare per preparare un piatto, così voi potete aggiungere alcune domande alla conversazione, aggiungere un pizzico di dichiarazioni deliberatamente false e mescolare una sana dose di interesse reciproco per ottenere tutte le informazioni di cui avete bisogno.

Quando inizierete a padroneggiare queste abilità, servirete piatti dal "gusto" perfetto di sollecitazione e conversazione. Con quella freccia nella vostra faretra, l'ultima cosa di cui avete bisogno è quella che descriverò nel prossimo capitolo: imparare a leggere la comunicazione non verbale e il linguaggio del corpo.

Vedo anche quello che non mi hai detto

> È nostra responsabilità imparare a diventare emotivamente intelligenti. Si tratta di competenze non facili, la natura non ce le dà, dobbiamo apprenderle.
> - *Paul Ekman*

Quando scrissi il mio primo libro, *Social Engineering: The Art of Human Hacking* (Wiley, 2010), ero relativamente nuovo nel mondo della comunicazione non verbale. Ma avevo iniziato una relazione di lavoro con Paul Ekman che è stato mio mentore. Paul Ekman iniziò il suo viaggio per capire la comunicazione non verbale alla fine degli anni Cinquanta e negli ultimi sessant'anni ha guidato il campo di ricerca sulle comunicazioni non verbali.

Paul Ekman mi ha aiutato a perfezionare non solo il mio lavoro, ma anche il mio modo di comunicare. Ciò mi ha portato a scrivere il mio secondo libro, *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014), che approfondisce le espressioni facciali, il linguaggio del corpo, i gesti delle mani e ogni aspetto della comunicazione non verbale. Ho anche trattato una parte meno visibile della comunicazione non verbale: la distrazione dell'amigdala.

Se avete letto qualcuna delle missioni che ho descritto, probabilmente non vi sarà troppo difficile capire perché quando sono vicino a Paul Ekman, reagisco praticamente come potete vedere nella Figura 8.1.



Figura 8.1 Quello che la maggior parte delle persone immagina io faccia quando vedo Paul Ekman (il che non è lontano dalla verità). Fonte fotografica: https://commons.wikimedia.org/wiki/File:Elvis_Presley_-_TV_Radio_Mirror,_March_1957_01.jpg.

Ho in mente alcuni obiettivi, con questo capitolo. In primo luogo, voglio essere sicuro di mantenere gli standard elevati di Paul Ekman, nel garantirvi che tutto quello che vi dirò ha solide basi scientifiche. In secondo luogo, non voglio ripetere quanto ho già detto nei miei altri libri. In questo libro, presento la comunicazione non verbale in un'area chiave, che può letteralmente cambiare la vostra carriera di ingegneri sociali: la comprensione dei cambiamenti di base tra comfort e disagio.

In questo capitolo, vi avviso che distruggerò molti falsi preconcetti che potete aver sentito sul linguaggio del corpo e vi mostrerò che cosa cercare esattamente come professionisti dell'ingegneria sociale.

La comunicazione non verbale è essenziale

Prima di entrare nel cuore di questo capitolo, lasciate che vi aiuti a vedere il motivo per cui è importante imparare a leggere la comunicazione non verbale. Penso che il modo migliore per farlo sia raccontare una storia.

Stavo lavorando con Paul Ekman su *Unmasking the Social Engineer*, e il suo compito era quello di assicurarsi che quello che stavo scrivendo fosse scientificamente accurato, logico e approvato in base alle sue ricerche decennali.

Avevo scritto un capitolo su uno studio che era stato fatto sui neuroni specchio. Lo studio, sostanzialmente, affermava che i ricercatori credevano che nel cervello vi fosse un gruppo di neuroni che aveva il compito di rispecchiare la comunicazione non verbale delle altre persone.

Sulla base di una ricerca di Paul Ekman, sappiamo che quando proviamo un'emozione, abbiamo una reazione involontaria e che tale reazione emerge sotto forma di micro-espressioni. Inoltre, quando produciamo delle espressioni facciali, creiamo l'emozione associata a quell'espressione.

Feci una connessione: se i neuroni specchio ci fanno riflettere le espressioni altrui, che sono accompagnate dalle relative emozioni, possiamo controllare il contenuto emotivo del nostro obiettivo.

Mentre scrivevo *Unmasking the Social Engineer*, era in corso un dibattito scientifico sui neuroni specchio e la ricerca correlata. Di conseguenza, Paul Ekman mi scrisse un'e-mail molto simpatica, nella quale, sostanzialmente. diceva: "Vuoi che il tuo libro si basi su una ricerca antiquata o confutata, nel caso in cui la ricerca venga annullata?".

Risposi: "Ma, ma, ma… Ho già scritto una quarantina di pagine. E devo consegnare il capitolo tra cinque giorni". Speravo che Ekman rispondesse, sostanzialmente: "Ok, va bene così".

Invece scrisse: “Bene, allora immagino che tu abbia cinque giorni per leggere questa ricerca sull’amigdala e scrivere un nuovo capitolo”. E con quello, avevo una sessantina di pagine di informazioni su un argomento che potevo a malapena pronunciare, e dovevo leggerlo, capirlo, ragionarci e scrivere.

Certo, Paul Ekman mi aiutò molto, ma questo mi ha insegnato tre cose.

- È importante capire come funzionano le cose, se ho intenzione di aiutare veramente i miei clienti.
- È importante adattarsi e crescere, in base alle nuove ricerche.
- Il potere del sonno è davvero molto sottovalutato.

Durante la scrittura del capitolo sulla manipolazione dell’amigdala vidi, di nuovo, un collegamento nella ricerca tra l’impianto di un contenuto emotivo e il controllo della risposta del destinatario. Se l’amigdala elabora gli stimoli emotivi prima che il cervello abbia la possibilità di “accendersi” e posso far sì che l’obiettivo provi una certa tristezza o paura, posso approfittare della sua reazione empatica.

In altre parole, padroneggiare l’uso dei pretesti può aiutarmi a suscitare nei soggetti le emozioni che desidero; posso far loro sentire quello che voglio che sentano. Stiamo finalmente arrivando al punto: capire perché la comunicazione non verbale è così importante.

Quando una missione prevede un’attività di penetrazione in un luogo o quando devo svolgere un’attività di *vishing*, provo una certa paura, piuttosto intensa: la paura di fallire, la paura di essere scoperto, la paura di incespicare. Esaminiamo l’emozione che provo.

In quale modo la paura mi influenza, fisiologicamente?

- I miei occhi si dilatano e le mie palpebre si tendono.
- La mia bocca si piega verso l’alto in un ghigno e prendo un profondo respiro.

- I miei muscoli si tendono e spesso si irrigidiscono mentre mi preparo al “combatti-o-fuggi”.
- Il mio battito cardiaco aumenta.
- La mia produzione di sudore aumenta.

Ora, proviamo a pensare a quale dovrebbe essere il mio stato fisiologico per suscitare la risposta emotiva desiderata nel mio obiettivo, che dovrebbe essere un leggero turbamento, per suscitare empatia.

- Occhi sinceri e non tesi.
- Labbra abbassate agli angoli.
- Testa piegata di lato.
- Muscoli distesi.
- Un respiro tranquillo.

Vedete la differenza? Se il mio pretesto sta usando l’emozione della tristezza, ma il mio linguaggio del corpo mostra paura, che cosa succede all’obiettivo? Immagino che la maggior parte delle persone non penserà mai: “Ok, questa persona sta usando una storia basata sulla tristezza, ma mostra paura. Questo è un contenuto emotivo incongruente, che mi mette a disagio”. Tuttavia, abbiamo tutti un radar interno che ci dice quando dovremmo alzare gli scudi e metterci sulla difensiva. Se mostro paura, ma cerco di suscitare tristezza ed empatia, il radar del mio obiettivo dovrebbe assolutamente alzare quello scudo.

Uno studio davvero fenomenale intitolato *Chemosensory Cues to Conspecific Emotional Stress Activate Amygdala in Humans* (www.ncbi.nlm.nih.gov/pmc/articles/PMC2713432) lo dimostra in un modo… ehm… interessante.

I ricercatori hanno raccolto tamponi di sudore di persone che facevano esercizio fisico. Poi tamponi di sudore da un gruppo di persone che si era gettato da un aereo in volo a 13.000 piedi per uno

skydive in tandem. Infine, i ricercatori hanno sottoposto a test un gruppo di soggetti, collegando la fMRI alla loro testa e facendo loro annusare ciascuno dei tamponi di sudore (raccapricciante, ma vero).

Quando i soggetti di questo gruppo di test hanno annusato il sudore di coloro che si erano lanciati da un aereo, si è attivato il loro centro di gestione della paura, cioè l'amigdala. Quando i soggetti hanno annusato i tamponi dal gruppo di "sportivi", non si è attivata alcuna paura. Quindi, quando si parla dell'"odore della paura" la cosa ha davvero un fondo di verità.

Una riflessione

Al DEF CON 25, avevamo ospite Tim Larkin nel nostro episodio live di *The Social-Engineer Podcast*. Tim raccontò la storia di una donna musulmana che stava camminando verso un gruppo di giovani uomini. Gli uomini non dissero nulla alla donna, ma qualcosa del loro atteggiamento la fece sentire a disagio. Quindi, fece una cosa intelligente: si voltò e iniziò a camminare nella direzione opposta.

Tuttavia, tenne all'orecchio le cuffie, vanificando quindi un suo vantaggio. Uno dei giovani le corse dietro e le diede una spinta alla schiena, facendola cadere.

Questa è una storia triste e grottesca, ma spiega come i nostri radar interni funzionino anche se cerchiamo di zittire i loro segnali di allarme. Io dico sempre *non ignorare* quei radar. Ascoltarli può salvarvi la vita.

Ora che sappiamo che le altre persone possono percepire la nostra paura, pensiamo a quello che dobbiamo fare per prepararci ad approcciare un obiettivo. Ho due scelte:

- imparare a controllare le nostre paure, in modo da manifestare la giusta emozione;
- se ciò non fosse possibile, costruire un pretesto che comprenda in sé la mia naturale emozione.

Capire questo può aiutarvi ad avere un maggiore controllo sulle vostre emozioni, a sapere che cosa mostrare, e a imparare a utilizzare, leggere e poi anche reagire adeguatamente alle emozioni e ai sottoprodotti non verbali di quelle emozioni.

Prima di entrare nei dettagli delle comunicazioni non verbali, dovete imparare a interpretare gli elementi basi delle reazioni emotive.

I nostri specifici elementi di base

Essere in grado di leggere i contenuti emotivi di qualcuno può veramente migliorare la vostra capacità di comunicazione. Voglio concentrarmi sul modo in cui l'osservazione dei cambiamenti negli elementi di base ci possa aiutare come professionisti dell'ingegneria sociale.

Lasciatemi però prima definire gli elementi di base. In poche parole, si tratta dei contenuti emotivi che rilevate nel momento in cui iniziate a osservare. Non state cercando di capire la loro linea di condotta nell'arco di tutta una vita. Quindi, non preoccupatevi: non vi sto chiedendo di pedinare il vostro obiettivo per mesi o anni prima di ogni missione.

Osservate la Figura 8.2. Amaya ha combinato qualcosa e la mamma gliene sta parlando.



Figura 8.2 Quali elementi di base vedete?

Che cosa osservate? Nella Figura 8.2, qual è il contenuto emotivo di mia moglie, Areesa? Vedete la mascella rigida? Il dito puntato e le labbra tese? Tutti segnali di rabbia.

E che cosa dite di Amaya? Le sue braccia sono conserte, il suo mento è alzato in aria e il suo viso esprime irritazione. È chiusa e non esattamente in uno stato d'animo di ascolto.

Ora osservate la Figura 8.3 per vedere l'aspetto di Amaya dopo la fine della "discussione", quando non è più con la mamma.



Figura 8.3 Quali cambiamenti notate?

Amaya sembra un po’ rattristata e sconfortata. Forse sta riflettendo sull’accaduto.

Ora osservate la Figura 8.4. Amaya e Areesa stanno sorseggiando una bella tazza di tè e si raccontano della loro giornata di shopping.

Quali elementi di base notate? Entrambe sembrano felici. Sono rivolte l’una verso l’altra e stanno avendo un’amabile conversazione.

Le tre foto mostrano le stesse persone in circostanze differenti e mostrano diversi elementi di base. Qui si cela una lezione preziosa. Un elemento di base non definisce la personalità di una persona. Non è un profilo psicologico. E non si estende a lungo termine. L’elemento di base è semplicemente il contenuto emotivo manifestato in un momento ben preciso.

Essere in grado di leggere lo stato emotivo di una persona nel momento in cui ci si avvicina a essa è di vitale importanza per un ingegnere sociale. Il vostro approccio all'obiettivo Areesa dovrebbe variare molto dalla Figura 8.2 alla Figura 8.4 se volete avere successo.

Molto spesso, sento dire da qualcuno che sa capire in una manciata di secondi se una persona mente o dice la verità.



Figura 8.4 Quali elementi di base notate?

David Matsumoto, Hyi Sung Hwang, Lisa Skinner e Mark Frank hanno scritto un articolo intitolato *Evaluating Truthfulness and Detecting Deception* (https://leb.fbi.gov/articles/featured-articles/evaluating-truthfulness-and-detecting-deception) in cui affermano un punto molto importante: "Non è la semplice presenza o assenza di comportamenti, come l'evitare lo sguardo o l'irrequietezza, a indicare la menzogna. Piuttosto, è il modo in cui questi segnali non verbali

cambiano nel corso del tempo rispetto agli elementi di base di una persona e il modo in cui tali segnali si combinano con le parole pronunciate. E quando vengono considerati solo i segnali comportamentali di queste fonti, essi permettono di distinguere accuratamente tra menzogna e verità".

È chiara questa loro affermazione? Non esiste un segno evidente che indica sempre la menzogna o la verità. È il modo in cui cambiano nel tempo i segnali di una persona a indicarci i contenuti emotivi e il modo in cui dovremmo decifrarli.

Fate attenzione ai fraintendimenti

Le persone spesso hanno dei preconcetti sul significato di determinati segni non verbali, dei quali dovreste liberarvi prima di avventurarvi in questa professione. Non facendolo correte il rischio di interpretare male determinati comportamenti.

Analizziamo alcuni esempi insieme. Osservate la Figura 8.5. Che cosa vedete?



Figura 8.5 Amaya è arrabbiata o no?

Per anni, ci è stato detto che le braccia incrociate sono un chiaro indicatore di chiusura. Questo non è necessariamente vero. Se qualcuno cambia postura da un atteggiamento aperto a uno di chiusura mentre mi avvicino, questo potrebbe essere vero, ma alcune persone sono solite stare sedute o con le braccia incrociate solo perché è comodo e non perché siano chiuse. In entrambe le fotografie della Figura 8.5, le braccia di Amaya sono incrociate, ma la sua espressione facciale e la posizione della testa indicano quale emozione esprime.

Ora osservate la Figura 8.6.

In questa fotografia non potete vederlo, ma la gamba di Amaya si agitava freneticamente. È forse un segno che sta per ingannarmi? O

forse vuol solo dire che non è a suo agio? È difficile da dire. Alcune persone hanno sempre le gambe in movimento o si muovono molto. Di nuovo, notate quando inizia un movimento come questo e osservate con quale frequenza inizia e si arresta, per capire qual è il suo significato. Osservate l'intera immagine rappresentata nella Figura 8.6: la posizione del corpo, la sua gamba che rimbalza, la mano sulla nuca. Considerando tutti questi elementi, potreste giungere alla conclusione che Amaya si sentiva a disagio.



Figura 8.6 Sarà irritata, in procinto di mentire, fredda o a suo agio?

Le gambe di mio figlio Colin sono come un moto perpetuo. Ho sempre pensato che se avessimo potuto attaccarlo a un generatore, potevamo usarle per produrre energia elettrica per la nostra casa. Ma lui non è un tipo ingannevole; semplicemente si muove molto. Ecco un esempio di come ho usato questa conoscenza sulle caratteristiche di Colin:

Gli dissi: “Ehi, Colin, come è andata la festa, l’altra sera? Ti sei divertito?”.

Colin, mentre la gamba sembra voler scavare un foro nel terreno, risponde: “Sì, è andata bene. Tutto a posto”.

Ora, in quel caso, sapevo che si era accapigliato con Stewart e volevo dei dettagli. Dissi: “Oh, bene. Chi c’era?”.

Colin elencò tutti gli amici, senza parlare di Stewart. Mm… Risposi: “Oh, allora Stewart non c’era? Pensavo venisse”.

La gamba di Colin si fermò di colpo: “Sì, c’era anche lui”, disse, mentre la gamba ricominciava ad agitarsi.

“Ah… E… tutto ok con Stewart?”, chiesi.

Con la gamba ben piantata a terra, Colin rispose: “Sì, tutto bene”. Questa volta ci fu una pausa prima che Colin riprendesse a muovere la gamba.

L’indicatore che ci fosse un problema non era la gamba in movimento di Colin, ma il suo arrestarsi. Da lì a pochi secondi mi ha raccontato l’accaduto.

SUGGERIMENTO

Non parlate dei vostri metodi per far parlare i vostri figli fino a quando non saranno abbastanza grandi da poter capire o solo dopo aver smesso di utilizzare tali tattiche. In casa nostra è costantemente in corso una battaglia di astuzie, per vedere chi vincerà. Finora, sono molto avanti. Volendo segnare un punteggio, sarebbe GENITORI 5.981.387 – FIGLI: 5.

P.S.: Mia figlia non è d’accordo: dice che ho invertito i numeri.

Ora date un’occhiata alla Figura 8.7 e pensate a quello che vedete.



Figura 8.7 Questo è comfort o disagio?

Sfregarsi il viso, grattarsi o altri tipi di gesti della mano possono essere indicatori di disagio, ma a volte le persone hanno solo un prurito. Prendete nota di quando iniziano e perché.

Posso prendere ancora a esempio mio figlio Colin. Ha avuto l’asma e alcune allergie. Spesso aveva prurito dappertutto. All’arrivo dei pollini, Colin si toccava e grattava la faccia in continuazione. Nel suo

caso, la continua agitazione non era perché stesse mentendo, ma a causa delle sue allergie.

Se ci basiamo su idee sbagliate, possiamo cadere in una trappola, e attribuire contenuti emotivi, là dove non esistono. Il che può essere pericoloso, perché poi si inizia a reagire a emozioni che in realtà non ci sono. È non è il caso di trattare qualcuno come se fosse un tipo chiuso quando invece è solo freddo, o presumere che qualcuno stia mentendo solo perché… ha una fastidiosa allergia.

Il modo migliore per combattere questo errore consiste nell'affrontare ogni situazione senza giudizi preconcetti, anche quando dovete affrontare un obiettivo con il quale avete già interagito. Rimandate i vostri giudizi a dopo i primi 15-20 secondi di interazione.

Parlando del linguaggio del corpo, io cerco di concentrarmi sui cambiamenti che scorgo negli elementi di base e quindi cerco quei cambiamenti che indichino segni di comfort o di disagio. In queste pagine voglio darvi solo le basi per comprendere la differenza tra comfort e disagio. Una volta che avrete ben chiaro il significato di questi indicatori, avrete una mappa che vi dirà che cosa cercare e come decifrare quello che vedete.

Conoscere le regole di base

Questa parte del capitolo tratta quattro regole da tenere bene a mente quando cercate di interpretare il linguaggio del corpo. Applicandole, noterete una grande differenza nel modo di leggerlo e interpretarlo.

Non consideratele regole "matematiche": non c'è nessuna formula infallibile o magica, ma come un modo per imparare a padroneggiare la lettura della comunicazione non verbale.

Regola 1: concentrarsi sul cosa, non sul perché

Questa regola è semplice: non affrettate le connessioni tra il cosa e il perché in carenza di informazioni.

Spesso inizio la mia giornata di lezione sulla comunicazione non verbale ricordando agli allievi una cosa: “Solo perché possiate vedere una cosa, questo non significa che sappiate anche il perché”.

Pensateci: mentre spiego in classe, dico qualcosa e stabilisco un contatto visivo con uno di voi. Noto che ha le braccia incrociate, le sopracciglia inarcate, gli occhi spalancati e la mascella serrata. Vedo tensione nelle braccia e nelle mani. Tutti segni di rabbia o disagio.

Posso supporre che vi siate arrabbiati con me per qualcosa che ho detto o che magari vi abbia turbato. Ma magari state solo reagendo a un dolore che avete appena sentito a causa di un intervento chirurgico che avete avuto l’anno scorso. O magari avete solo un crampo allo stomaco. O magari non stavate proprio ascoltando e stavate pensando a qualche brutta faccenda.

Indipendentemente dal motivo per cui il vostro linguaggio del corpo è stato quello descritto, come potrei io collegare il cosa al perché? Come ho detto nel Capitolo 7, è tutta una questione di domande. Durante la lezione, non è appropriato che io smetta di spiegare per indagare sul perché mi guardavate arrabbiati.

Regola 2: esaminare le comunicazioni non verbali a “blocchi”

Quando iniziate a fare pratica effettiva con un obiettivo, è facile osservare un particolare movimento del corpo o espressione facciale e pensare di poter comprendere ciò che intende comunicare. Tuttavia, concentrarsi su un solo segnale è pericoloso. Avete bisogno di un contesto e di altri segnali per completare il messaggio che l’obiettivo sta trasmettendo. Cercate altri segnali non verbali corrispondenti, che chiariscano quale emozione viene manifestata.

Considerate questo scenario: state parlando al vostro coniuge e le/gli state dicendo che non concordate con una decisione. Mentre esponete il vostro parere, la/il coniuge incrocia le braccia. Questo significa automaticamente che non vi ascolta, è arrabbiato o che non concorda con quello che state dicendo?

Allargate un po' lo sguardo. Vedete della rabbia sul volto del coniuge? Notate un cambiamento di posizione dei fianchi e dei piedi? Puntano lontano da voi? Quali altri "blocchi di emozioni" possono aiutarvi a individuare se le braccia incrociate sono un gesto isolato o fanno parte di un più ampio messaggio emotivo.

Regola 3: cercare la coerenza

Cercate la coerenza tra la comunicazione verbale e non verbale. Se qualcuno scuote la testa, ma nel frattempo dice "Sì", questi due indicatori sono incoerenti.

Quando identificate una mancanza di coerenza nelle informazioni comunicate da qualcuno, fate affidamento sul messaggio non verbale per capire la vera risposta. Esaminando i blocchi di comunicazioni non verbali e cercando una mancanza di coerenza tra comunicazione non verbale e comunicazione verbale potrete avvicinarvi molto alla lettura accurata di quello che l'obiettivo vi sta davvero dicendo.

Regola 4: prestare attenzione al contesto

Immaginate che io guardi fuori dalla finestra del mio ufficio e che veda mia figlia seduta. Si è fatta piccola, quasi appallottolata. Ha le braccia incrociate sul suo petto e il mento abbassato. La testa è nascosta tra le braccia incrociate. Tutti questi sono segni di tristezza e di disagio.

Quello che non vi ho detto è che fuori ci sono solo 2 °C e lei è senza giubbotto.

Grazie al contesto, sapete che Amaya ha semplicemente freddo. Senza i dettagli contestuali della temperatura, sembra invece triste e a disagio. Per evitare di fraintendere la comunicazione non verbale, dovete comprendere il contesto della situazione in cui si trova il vostro obiettivo.

Oltre a queste quattro regole, ci sono alcuni concetti di base sul linguaggio del corpo, che dovete conoscere prima di entrare nei dettagli di ciascuna emozione.

Comprendere le basi della comunicazione non verbale

Ci sono alcuni elementi di base da acquisire all'inizio di un percorso di apprendimento della comunicazione non verbale. Queste basi sono applicabili a tutti gli esseri umani e non sono legate a una specifica cultura, genere, razza o religione. Comprendere queste basi vi aiuterà a capire come il nostro corpo comunichi esattamente quello che proviamo, indipendentemente da quello che stiamo cercando di mostrare.

Gli stimoli esterni arrivano al nostro cervello attraverso (se possibile) cinque modalità: vista, olfatto, gusto, tatto e udito. Questi stimoli vengono elaborati dal nostro cervello e possono scatenare una delle sette emozioni di base: rabbia, paura, sorpresa, disgusto, disprezzo, tristezza o felicità. L'emozione innescata genera risposte fisiologiche che emergono sul nostro volto e sul nostro corpo.

Per esempio, quando una persona è sicura, tende a farsi "più grande", il che aumenta il testosterone e riduce il cortisolo nel sangue, secondo uno studio intitolato *Postural Influences on the Hormone Level in Healthy Subjects* dei ricercatori R.S. Minvaleev, A.D. Nozdrachev, V.V. Kir'yanova e A.I. Ivanov

(https://link.springer.com/article/10.1023/B:HUMP.0000036341.80214.28). I ricercatori volevano controllare se alcuni movimenti yoga influenzassero le secrezioni di cortisolo, testosterone, deidroepiandrosterone (DHEA) e aldosterone. Per i nostro scopi, concentriamoci su cortisolo e testosterone.

I ricercatori scoprirono che, proprio assumendo certe pose associate a comportamenti di sicurezza di sé, il testosterone del soggetto saliva a oltre il 16% e il cortisolo scendeva all'11%. A proposito, il testosterone rafforza i comportamenti associati a una persona sicura di sé. Quindi, quasi come una profezia autoavverantesi, sembra che il fatto di mantenere una postura di forza rilasci sostanze chimiche che aiutano a sentirsi e ad agire in modo più sicuro di sé.

NOTA

Il cortisolo è un ormone che regola un'ampia varietà di processi organici, compreso il metabolismo e le reazioni immunitarie. Il cortisolo viene spesso chiamato "ormone dello stress", perché viene prodotto quando l'organismo è sotto stress. I ricercatori scoprirono che elevati livelli di cortisolo sono legati all'ansia e alla depressione.

In sostanza, quello che mi preme farvi capire è questo: sembra che la comunicazione non verbale di comfort stimoli la secrezione di ormoni e le reazioni di felicità, sicurezza di sé e forza, mentre la comunicazione non verbale di disagio possa generare reazioni di stress, ansia ed emozioni negative.

È importante comprendere come una certa comunicazione non verbale possa influenzare sia voi sia il vostro obiettivo. Come professionisti dell'ingegneria sociale, state influenzando o manipolando il contenuto emotivo del vostro obiettivo. Non prendete la cosa alla leggera.

Poiché l'effetto del vostro pretesto sull'obiettivo può essere a breve termine o di lunga durata, diventa importante pianificare attentamente i pretesti. Ricordate il motto: "Fai in modo che si sentano meglio, dopo

averti incontrato". Cercate il più possibile di usare un pretesto che inneschi un contenuto emotivo che non abbia un effetto dannoso duraturo sul vostro obiettivo.

Come potete determinare se il pretesto scelto possa avere effetti negativi duraturi? Cercate di determinare su quale emozione si basa il vostro pretesto. La paura, la rabbia, il disgusto e il disprezzo sono emozioni negative così forti che rischiate che l'obiettivo maledica di avervi incontrato.

Per esempio, c'è una certa differenza tra un *phishing* che dice "Grazie per il suo recente ordine di questo televisore da 55 pollici" e un altro che dice "Il vostro account è stato violato e il vostro conto bancario è stato azzerato".

Capire che la comunicazione non verbale e le emozioni possono influenzare profondamente l'obiettivo dovrebbe aiutarvi a determinare come utilizzare queste emozioni durante le vostre missioni di ingegneria sociale. A tal fine, una delle lezioni più profonde che ho imparato da Paul Ekman è che non solo un'emozione innesca una reazione non verbale, ma accade che quando forzate un messaggio non verbale su voi stessi, potete richiamare quella emozione. Questo concetto è stato supportato da numerosi ricercatori, incluso uno studio intitolato *Inhibiting and Facilitating Conditions of the Human Smile: A Nonobtrusive Test of the Facial Feedback Hypothesis* (www.ncbi.nlm.nih.gov/pubmed/3379579). I ricercatori Strack, Martin e Stepper hanno sottoposto a test le ipotesi di Paul Ekman degli anni Settanta e Ottanta e hanno dimostrato che creando l'espressione, è possibile scatenare un'emozione. Lo hanno fatto chiedendo ai soggetti di mettere una penna in bocca, per attivare i muscoli che simulavano un sorriso. Hanno dimostrato quanto affermato da Paul Ekman nella sua ricerca: che creare un'espressione facciale (anche forzata) genera la relativa emozione.

Il punto chiave da ricordare è che se create un’emozione, o se fate in modo che l’obiettivo esprima quell’emozione, lasciate all’obiettivo la sensazione di quell’emozione. Fate attenzione a usare con cautela questo “superpotere”.

Comfort vs disagio

È importante imparare a comunicare in modo efficace, e parte di tale comunicazione si svolge su un piano non verbale. Alcuni ricercatori hanno sviluppato statistiche su quanto di quello che diciamo è non verbale. Ho letto che si tratta dell’80%, dell’85% e addirittura del 90%, ma una delle cose che ho imparato da Ekman è stata che, anche se siamo tutti d’accordo sul fatto che una grande percentuale della comunicazione è non verbale, il metodo di comunicazione (parlato, scritto, di persona) influisce sul modo in cui viene utilizzata la comunicazione non verbale.

Quello che il nostro corpo e il nostro volto rivelano durante le normali comunicazioni può essere travolgente per coloro che sono in grado di riconoscere l’emozione che viene manifestata. Durante la normale comunicazione, il corpo e il viso di una persona può manifestare una miriade di emozioni, e può essere davvero impegnativo cercare di interpretarle tutte. Per questo motivo, quando si inizia a lavorare come ingegneri sociali, è meglio concentrarsi sulle comunicazioni non verbali più facili da interpretare: il comfort e il disagio.

Voglio affrontare questo argomento dal punto di vista dell’emozione e poi discutere se voi, come ingegneri sociali, pensiate di innescare questa emozione nel vostro obiettivo. Spiego come cercare i segni che potrebbero manifestare un comfort o un disagio per quella emozione. Ho diviso questo paragrafo in base alle emozioni, descrivendo alcuni degli indicatori della specifica emozione, sul volto e sul corpo. Questo

non vuole essere un elenco esaustivo di ogni singolo gesto, ma fornisce una base sulla quale costruire con la pratica, per iniziare a padroneggiare questa abilità.

Oltre a studiare questo paragrafo per imparare a leggere il linguaggio del corpo altrui, dovreste usare queste informazioni per imparare come il vostro linguaggio del corpo può influenzare i vostri obiettivi. Mostrando le emozioni che descrivo in questo paragrafo, potrete attivare quelle stesse emozioni anche negli altri. Decidete quali emozioni volete innescare e poi fate pratica di comunicazione non verbale di quelle emozioni. Imparate anche a riconoscere le emozioni e le cause scatenanti che non volete suscitare negli altri.

Rabbia

La rabbia è un'emozione forte che è stata etichettata come un'emozione "cancello". Questo significa che, molto spesso, la rabbia apre la strada ad altre emozioni, sentimenti o azioni. Queste azioni possono andare dall'uso di imprecazioni o parole forti fino al manifestarsi di comportamenti violenti.

Fisiologicamente, la rabbia ci rende tesi, carichi e pronti a combattere o difendere. I muscoli si tendono, la mascella si serra e a volte perfino i pugni si stringono – il tutto in preparazione a un combattimento o a una difesa. Mentre la persona si accinge a un'azione violenta, potreste addirittura vederla abbassare il mento, per proteggere il collo.

Nonostante questa tensione, potreste notare che una persona che sta sperimentando la rabbia cerca di farsi più grande. Per esempio, una persona arrabbiata potrebbe gonfiare il petto, allargare le spalle e allungare la postura. Inoltre, anche il respiro si fa più intenso e aumenta la frequenza cardiaca.

Chi è arrabbiato ha le seguenti caratteristiche facciali.

- Le sopracciglia si inarcano, e gli occhi si spalancano.
- La mascella si serra.
- I denti si chiudono o, se la bocca si apre, spesso non è per dire cose piacevoli.

Potete vedere tutto questo rappresentato nella Figura 8.8.

La rabbia può anche manifestarsi nel resto del corpo. La Figura 8.9 mi mostra con una mascella serrata e i pugni chiusi. Inoltre, il mio petto è gonfio, per farmi sembrare più grande. Tutto ciò indica rabbia (P.S.: questa è la foto che mostrerò a qualsiasi ragazzo che mostri un qualche interesse per Amaya). Se notate qualcuno di questi segni mentre vi avvicinate a una persona, fareste meglio a evitare quell'individuo.

Un'altra versione della rabbia è quella rappresentata nella Figura 8.10, in cui Amaya mostra una rabbia più sottile. Il suo sguardo, la sua mascella serrata e la fronte leggermente corrugata sono tutti segni di rabbia.

Il più delle volte potete scoprire che la rabbia è un disagio non verbale. È una di quelle emozioni che non amo suscitare nel mio obiettivo. Di conseguenza, cerco i segni di questa emozione e cerco di non usarla nelle mie missioni.

Molto spesso, se sono troppo aggressivo nel mio approccio o se il mio pretesto è troppo negativo, posso cogliere dei segni di rabbia. È un ottimo segnale di avvertimento che mi suggerisce di attenuare e ammorbidire la voce o il linguaggio del corpo, per alleviare i sentimenti di rabbia nel mio obiettivo.



Figura 8.8 Un’espressione di rabbia.



Figura 8.9 Espressione di rabbia nel corpo.



Figura 8.10 Una rabbia più sottile.

Disgusto

Anche il disgusto è un’emozione molto forte. Il disgusto può riguardare una persona, un luogo o una cosa. Spesso, qualcosa che ci fa provare una reazione di forte disgusto ci “rimane addosso” per molto tempo, dopo l’esposizione a tale emozione.

Quando ero un ragazzino, i miei genitori allevavano polli. Mi piaceva un sacco correre nel pollaio, prendere un paio di uova appena deposte e fare l'"uovo nel pane": una fetta di pane imburrata messa in una padella con un uovo nel mezzo.

Un giorno, afferrai il mio uovo e lo ruppi sul bordo della padella in ghisa rovente. Quello che uscì non fu un uovo fresco, ma un pulcino già mezzo formato. Quando colpì la pentola, iniziò a dimenarsi, mentre moriva. Quella scena e quell'odore mi fecero vomitare nel lavandino. Ero talmente disgustato, che dimenticai di spegnere il fornello, così che il povero pulcino si carbonizzò e l'odore di pollo in fiamme riempì la cucina.

L'emozione di disgusto che si è scatenata è stata così forte che anche dopo dieci anni l'odore di cottura di un uovo mi faceva ancora stare male. Alla fine, l'ho superato, ma il disgusto è un'emozione così forte che se la fate scattare nel vostro obiettivo, potreste non essere più in grado di recuperarlo.

Pensate alle cose che possono scatenare un'emozione di disgusto nel vostro obiettivo: odore corporeo, secrezioni, del cibo sul viso o fra i denti, un linguaggio volgare, la scelta delle parole e così via. È importante analizzare con attenzione il vostro approccio e voi stessi prima di avvicinarsi, in modo da non provocare disgusto nell'obiettivo.

Il disgusto si manifesta in vari modi. Sul viso è un'espressione bilaterale, nel senso che entrambi i lati del viso mostrano la stessa espressione, come rappresentato nella Figura 8.11.



Figure 8.11 Disgusto.

Mentre stavamo preparando la foto, il mio cane aveva prodotto qualcosa di spiacevole in salotto. Non potevo farmi sfuggire l’occasione e così ho catturato Areesa intenta a ripulire. Notate come sollevi i lati del naso, per bloccare sia il senso dell’olfatto sia la linea di visione. In sostanza, lei sta fisiologicamente “bloccando” quelle cose che stanno provocando il suo disgusto.

Nel corpo, una persona manifesta disgusto bloccando o allontanandosi da voi. Cercate i segni di mancanza di interesse o di repulsione.

Notate la posizione della gamba di Amaya nella Figura 8.12. Dov'è rivolto il suo interesse? Non sicuramente verso suo padre (che tristezza…). E anche se non mostra forti segnali di vero e proprio disgusto, il suo linguaggio del corpo mostra segni di disagio e disinteresse.

Poiché il disgusto è un'emozione così intensa e negativa, tendo a non usarla durante le mie missioni. Tuttavia, una volta mi è stato chiesto di usarla per creare una tribù di persone disgustate della stessa cosa. Sebbene questo meccanismo possa funzionare ed essere molto potente, può anche portare a risultati pericolosi, se non viene gestito correttamente.



Figura 8.12 Disinteresse.

Disprezzo

Il disprezzo è un'emozione particolare. L'*Oxford English Dictionary* definisce il disprezzo come "la sensazione che una persona sia senza valore". Paul Ekman offre una definizione più semplice, affermando che il disprezzo è un sentimento di superiorità morale.

Secondo la definizione di disprezzo di Ekman, il disprezzo si prova solo nei confronti di una persona, ed è l'unica espressione unilaterale, il che significa che appare su un solo lato del viso. All'inizio, il disprezzo può sembrare un ghigno o anche l'inizio di un sorriso, come potete vedere nella Figura 8.13.



Figura 8.13 Il ghigno di disprezzo può essere confuso con il sorriso.

Il disprezzo è caratterizzato dal fatto che un lato del viso si solleva: per esempio, l’angolo del labbro si solleva su un solo lato, come nella Figura 8.13. Non è raro vedere questo segno accompagnato da un movimento del mento, anche se è solo lieve.

Poiché il disprezzo è la sensazione di essere superiori a un’altra persona e spesso può condurre alla rabbia, potreste vedere i seguenti segni nel linguaggio del corpo, insieme al disprezzo.

- Sentirsi superiore a un’altra persona può far sentire fiduciosi. Quella sensazione di fiducia può essere manifestata in diversi modi, ma spesso la persona occupa più spazio, rendendosi più grande.
- Se il disprezzo porta alla rabbia, potreste notare nel linguaggio del corpo gli stessi segni che ho descritto nel paragrafo precedente. Tuttavia, prima che quella rabbia non verbale si manifesti appieno, si può notare un serrarsi della mascella e l’adozione di una postura più aggressiva.

A mio parere, il disprezzo non ha molto posto in una missione di ingegneria sociale. L’ho visto usare dagli stati e dalle organizzazioni terroristiche per reclutare e poi convertire alla loro causa, ma per la maggior parte degli incarichi di ingegneria sociale, non mi sembra possa portare a un risultato desiderabile.

NOTA

Le organizzazioni terroristiche spesso usano la rabbia che le persone provano nei confronti del loro governo o di certe ideologie e la convertono in disprezzo, alimentandola. Una volta che l’obiettivo prova disprezzo per, o si sente moralmente superiore a, l’oggetto della rabbia, l’organizzazione terroristica offre la “soluzione“, l’azione da intraprendere. È un’emozione incredibilmente divisiva, e funziona incredibilmente bene.

Paura

La paura ha molti scopi: ci avvisa del pericolo, ma può anche essere esilarante e divertente, se è ben controllata. Ad alcune persone piace essere spaventati o provare paura.

La paura della delusione, la paura del fallimento o la paura di prendere una decisione sbagliata possono essere utili per un professionista dell’ingegneria sociale, ma in genere evito di impiegare sfumature più forti della paura. I pretesti che, letteralmente,

minacciano o spaventano una persona, come quelli che fanno temere per il lavoro, la vita o la famiglia, scatenano un’emozione così intensa che quando scoprono di essere stati solo esaminati, possono andarsene con disgusto o disprezzo, e con rabbia.

La paura ha alcune chiare caratteristiche fisiche.

- Gli occhi sono spalancati, per poter osservare l’intera scena.
- Il corpo si tende e di solito la bocca emette un respiro udibile.
- La bocca è aperta, con le labbra tirate verso le orecchie.

Potete vedere queste caratteristiche nella Figura 8.14.

Nel corpo, la paura ha manifestazioni analoghe alle espressioni facciali. Il corpo tirato indietro, irrigidito, congelato si prepara alla lotta o alla fuga. Se spaventate l’obiettivo, potreste vederlo reagire come rappresentato nella Figura 8.15.



Figura 8.14 Classica espressione di paura.



Figura 8.15 Lo spavento nel linguaggio del corpo.

Notate come Amaya si sia tirata indietro, con tutto il corpo teso. La sua bocca è in posizione di spavento. Questo tipo di paura può essere intenso, perché non ha vie di fuga: ha le spalle al muro ed è "incastrata" in una poltrona.

La Figura 8.16 mostra un altro aspetto della paura manifestato dalle donne: coprirsi la gola.



Figura 8.16 La protezione delle vene della gola è un chiaro segno di paura.

Osservate i sottili indicatori del linguaggio del corpo che possono indurti a capire come si sente l’obiettivo. Se vedete segni di paura, potete decidere se tale paura è appropriata e fino a che punto siete disposti a usarla. Come ho detto, uso la paura in modo professionale, ma evito quel tipo di paura che può far temere all’obiettivo di essere minacciato o in pericolo.

Sorpresa

La sorpresa viene spesso confusa con la paura (lo spavento) perché sembra così simile. Con la sorpresa, gli occhi si spalancano, come fanno per la paura. Il corpo generalmente si blocca e anche la bocca si apre. Ma si apre con un'espressione, appunto, più di sorpresa: "Ohhhhh!". Potete vederla rappresentata nella Figura 8.17.

La sorpresa può essere utile per un ingegnere sociale, ma, come alcune altre emozioni cui ho accennato, tutto dipende da come la utilizzate. Non consiglio di nascondersi in un armadio e saltare fuori all'improvviso per sorprendere l'obiettivo, ma una verifica a sorpresa, una visita inattesa o una ricompensa può funzionare per suscitare la risposta desiderata.



Figura 8.17 La sorpresa, che spesso può essere confusa con la paura.

In una missione di *vishing* ho usato un premio a sorpresa ottenendo risultati sorprendenti. La chiamata andò in questo modo.

Obiettivo: Buongiorno, sono Beth. Come posso aiutarla?

Io: Beth, sono Paul dell'ufficio del personale. Ho ottime notizie per lei. Forse non l'ha sentito, ma nel suo reparto abbiamo organizzato un'estrazione, con in palio un iPhone nuovo di zecca e… sa che cosa? È uscito il suo nome!

Obiettivo: Ma dai! È uno scherzo! Non è possibile!

Io: Lo so. Adoro fare queste chiamate. I telefoni in palio sono dieci e fare queste chiamate è davvero divertente.

Obiettivo: Sì, ma io non ho mai vinto nulla. È incredibile!

Io: Come sa, in XYZ abbiamo alcune Beth, quindi devo verificare alcuni dettagli per assicurarmi che lei sia la Beth giusta. Mi fa lo spelling del suo nome completo?

Obiettivo: *E-l-i-z-a-b-e-t-h S-m-a-r-s-t-o-n*.

Io: Eccellente. E il codice dipendente?

Obiettivo: T238712P.

Io: Esatto, è proprio la Beth giusta. Ora deve solo accedere al sito, dove potrà accedere con le sue solite credenziali, e specificare dove vuole che le venga spedito il telefono. È `iphone.company-website.com`. [*Un sito web che abbiamo creato ma che non faceva nulla; non funzionava nessuno dei pulsanti.*]

Obiettivo: Ok, sono nel sito. C'è il nostro logo, ma quando faccio clic su Invio, non succede nulla. Che cosa devo fare?

Io: Hmm, ci sono. Quando fa clic su Invio, non passa alla schermata successiva? Qui da me funziona.

Obiettivo: No. Ora provo con un altro browser. [*E provò tutti i browser che aveva.*] Che figura: vinco qualcosa e non riesco neanche ad accedere.

Io: No, non c'è alcun problema. Lo faccio io per lei. Posso inserire i suoi dati?

Obiettivo: Davvero? Farebbe questo per me?

Io: Certo che lo farei. [*Sentendomi colpevole come un serpente.*] Chiede il nome e cognome… [*E pronuncio ogni lettera mentre fingo di scriverla.*] Ok, clic su Avanti. Chiede il codice dipendente, che ho scritto qui….

Obiettivo: Grazie mille. Sono così eccitata.

Io: Va bene. Adesso chiede il login nel dominio, presumo sia E.Smarston, giusto?

Obiettivo: No, in realtà è B.Smarston. Per Beth…

Io: Ok, fantastico. Ora chiede la password.

Obiettivo: [*Senza alcun tentennamento*] lo uso delle password davvero lunghe. È JustinandBeth99!

Io: Eccellente, ha funzionato. Dice che riceverà una e-mail entro 24 ore con ulteriori istruzioni per ricevere il telefono. Congratulazioni, Beth!

Obiettivo: Grazie davvero!

Con questo, abbiamo violato completamente la rete. Sì: a beneficio di tutti quelli fra voi che mi stanno preparando una mail carica di odio, sono stato manipolativo e ho usato un pretesto che ha fatto rimanere male l'obiettivo quando scoprì l'inganno. Ma notate: non l'ho minacciata; non l'ho messa in imbarazzo; non le ho fatto alcun male. Ho solo sfruttato la sorpresa per innescare un'emozione basata sulla felicità e questo l'ha indotta a cedermi ogni informazione, senza riflettere minimamente.

Dal punto di vista del linguaggio del corpo, ci sono alcune cose che potreste notare che indicano sorpresa. Le potete notare nelle Figure 8.18 e 8.19.



Figura 8.18 La sorpresa può far arretrare, con espressioni facciali sollevate.



Figura 8.19 Una forma di sorpresa può portare a coprire la bocca.

Secondo me, la sorpresa è una bella emozione per un professionista dell'ingegneria sociale. Con una corretta pianificazione ed esecuzione, può portare a grandi vittorie.

Tristezza

La tristezza è un’emozione molto complessa. Ha anche una vasta gamma di sfumature, dal momento che può variare dal sentirsi un po’ giù alla disperazione più totale. Come ingegneri sociali, ci sono alcuni modi per sfruttare la tristezza.

- Notare la tristezza dell’obiettivo e poi sfruttare quell’emozione per suscitare una reazione.
- Creare una situazione che dovrebbe indurre una certa tristezza nell’obiettivo, spingendolo a reagire nel modo desiderato.
- Manifestare tristezza con la comunicazione non verbale, per ottenere una reazione basata sull’empatia.

Alcuni di questi metodi impiegano un approccio più manipolativo rispetto ad altri. Tutto dipende da come impiegate queste emozioni e da qual è lo stato emotivo risultante della persona.

La tristezza ha alcuni indicatori facciali, rappresentati nella Figura 8.20.



Figura 8.20 Elementi facciali della tristezza

Sul viso, la tristezza si manifestata nel seguente modo.

- Gli angoli della bocca si abbassano.
- Le palpebre calano sugli occhi.
- Gli angoli delle sopracciglia si uniscono e salgono.

In alcuni casi di tristezza estrema, l’emozione si manifesta da una sola parte del viso.

La tristezza può anche essere trasmessa dal corpo. La tristezza ci fa desiderare di proteggerci, di trovare conforto e di diventare più piccoli: esattamente l’opposto della sicurezza di sé.

Le Figure 8.21, 8.22 e 8.23 mostrano alcuni esempi di segni non verbali di tentativi di trovare conforto.

Questo è solo un breve elenco, ma dovrebbe rendere l’idea. Questi segni non verbali possono aiutarvi a capire che la persona è a disagio.

La tristezza, in tutta la sua complessità, può essere molto utile per un ingegnere sociale: dovrete imparare a leggerla e a manifestarla. Tuttavia, vi avverto di non esagerare con tale emozione e con il livello di tristezza che instillate nei vostri pretesti.



Figura 8.21 Un abbraccio.



Figure 8.22 La chiusura dello sguardo.



Figura 8.23 Una sorta di rannicchiarsi.

Non voglio mai lasciare il mio obiettivo in preda a una travolgente sensazione di tristezza o dolore, ma solo usare il giusto livello di tristezza per suscitare una forte reazione empatica. In uno studio condotto da Jorge A. Barraza e Paul J. Zak intitolato *Empathy towards Strangers Triggers Oxytocin Release and Subsequent Generosity* (https://nyaspubs.onlinelibrary.wiley.com/action/doSearch?

AllField=10.1111%2Fj.1749-6632.2009.04504.x), i ricercatori hanno rilevato un aumento del 47% nel rilascio di ossitocina quando si attiva l'empatia, anche se il sentimento di empatia riguardava perfetti sconosciuti, mentre la tristezza può creare un calo di serotonina, dopamina e ossitocina nel cervello. Come professionista, cerco di attenermi al lato empatico della tristezza, invece di suscitare timore, dolore o depressione.

Basti pensare a quante volte questa tattica viene utilizzata nelle attività di marketing e beneficenza. Dai bambini senzatetto agli animali maltrattati, lo scopo è quello di scatenare in noi una reazione empatica per incoraggiarci a decidere più facilmente di cedere del denaro. Questo non significa che tali organizzazioni stiano conducendo attività disoneste o manipolatorie, ma solo che sanno come funziona il nostro cervello e come questo possa essere sfruttato per raggiungere il loro obiettivo.

Felicità

La felicità è un'emozione che tutti possiamo condividere e che è molto utile in tutte le interazioni umane. Quando ci sentiamo felici, contenti, in pace o rilassati, siamo maggiormente inclini a prendere decisioni più altruistiche. Tendiamo ad amare di più gli altri, i luoghi e le cose che ci fanno provare questa emozione.

Per questo motivo, è facile immaginare che, per un ingegnere sociale, la felicità è un'emozione che è bene padroneggiare, leggendola e suscitandola. La prima cosa che può davvero aiutarvi a capire se state facendo un buon lavoro nel creare felicità è imparare a identificare la differenza tra un sorriso vero e uno falso. L'unica cosa che distingue un sorriso vero da uno falso è l'attivazione del muscolo *orbicularis oculi*. Quando si attiva, questo muscolo solleva le guance e genera delle piccole rughe intorno agli occhi.

A metà dell’Ottocento, un ricercatore francese di nome Guillaume Duchenne postulò che un sorriso vero potesse essere simulato. Stava studiando neuroscienze impiegando una forma molto invasiva di elettroshock. Somministrava una scossa elettrica per stimolare il movimento muscolare (www.thevintagenews.com/2016/05/07/44782-2).

A causa del dolore indotto, Duchenne non si spinse troppo avanti, ma la sua ricerca sul modo in cui le emozioni si manifestano attraverso le espressioni facciali ha dimostrato che il volto è una vera e propria mappa delle emozioni. Intorno al 1855, sviluppò un metodo per usare la stimolazione con elettroshock per innescare una reazione muscolare e scrisse delle sue scoperte nel libro *Mécanisme de la physionomie humaine*. Il risultato è quello che vedete nella Figura 8.24.

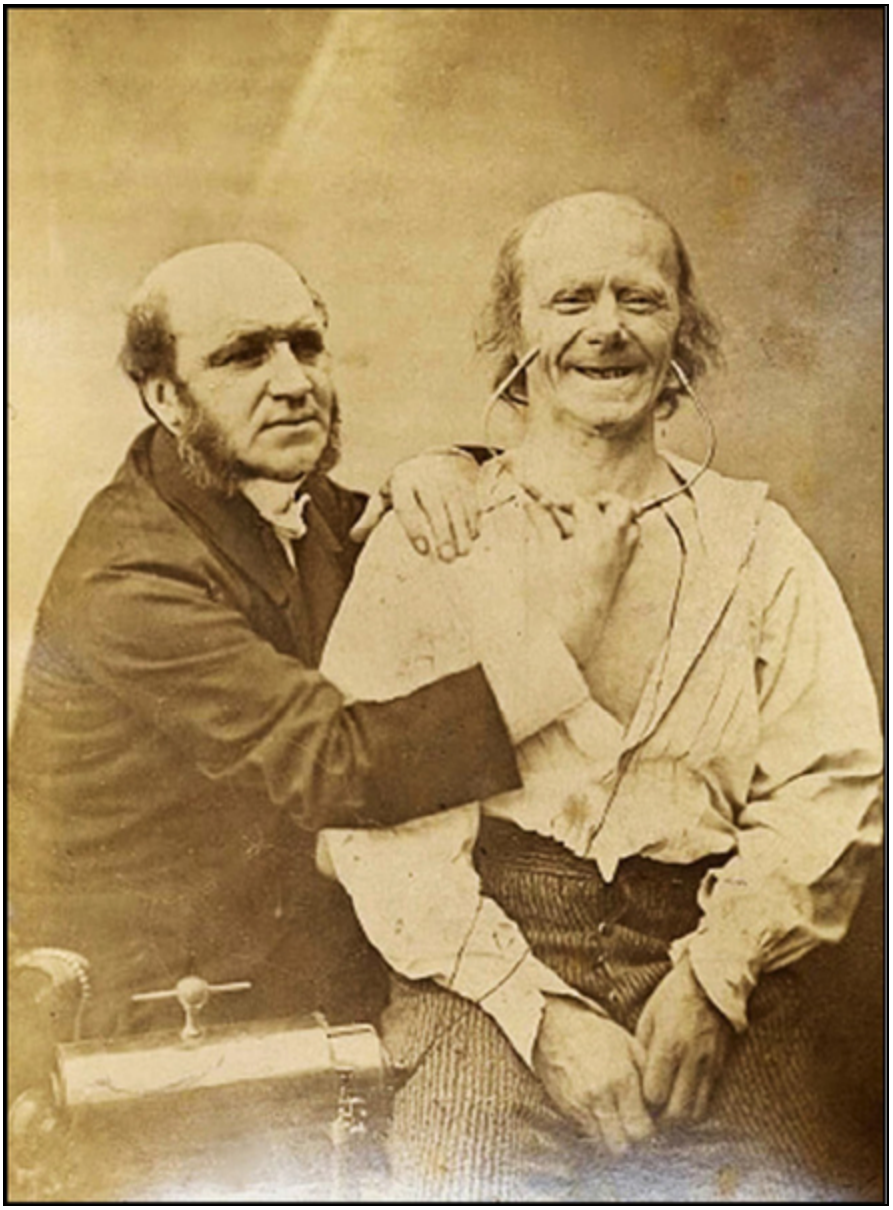


Figura 8.24 Un “vero sorriso” indotto. Fonte fotografica https://publicdomainreview.org/collections/the-mechanism-of-human-physiognomy. Tratto da Mécanisme de la physionomie humaine.

Leggere questa ricerca può aiutarvi a capire perché la felicità produce l’espressione facciale del sorriso. Ma come professionisti dell’ingegneria sociale, dovete imparare a riconoscere altri indicatori di felicità nel linguaggio del corpo.

Che aspetto ha l’emozione della felicità manifestata dal linguaggio del corpo di una persona? Se la felicità rilascia forti sostanze neurochimiche e crea un ambiente sicuro, possiamo aspettarci di vedere anche determinati segni nel corpo. Cercate le posizioni del corpo come quelle mostrate nelle Figure 8.25, 8.26 e 8.27.



Figura 8.25 Notate la posizione delle braccia, aperte e tranquille.



Figura 8.26 Una posizione ventrale può indicare fiducia e felicità.



Figura 8.27 La posizione ventrale è spesso associata a saluti cordiali e sinceri.

NOTA

Il ventre è la parte inferiore di un animale, il lato vulnerabile. Nell'uomo, questo significa esibire i polsi, la giugulare e quelle aree del corpo che proteggeremmo in caso di pericolo.

Sul viso, notiamo che gli occhi sono impegnati in un sorriso, oltre alla bocca, che, aperta o chiusa, forma un sorriso (vedi la Figura 8.28).

Molto spesso chi si sente felice tende a protendersi verso l’oggetto della sua felicità.



Figura 8.28 La felicità sul viso si manifesta con un sorriso sincero e l’inclinazione del capo.

Altri segni di felicità possono comprendere il fatto di sollevare le dita dei piedi o fare saltelli. Quando le persone si sentono tranquille, quando si sentono bene, tendono a farsi più grandi e a “gongolare”.

La felicità è una delle emozioni che cerco di usare più spesso come professionista dell’ingegneria sociale. Fare appello all’ego di una

persona è un ottimo modo per creare una felicità che può portare a una decisione emotiva. Affinché funzioni, tuttavia, l'appello all'ego deve essere realistico, credibile e appropriato al livello del legame che avete costruito in quel momento.

Trovo che, se ciò si adatta al pretesto che ho scelto, avvicinarmi a un obiettivo con una posizione ventrale e un sorriso caloroso con un'adeguata inclinazione della testa può fare molto nel far sentire a suo agio l'obiettivo.

Cercate dei modi per creare un ambiente felice nella scelta del vostro pretesto di ingegneria sociale e otterrete grandi risultati.

Riepilogo

La comunicazione non verbale è un argomento complesso ed esteso, che, mi rendo conto, non può essere trattato nelle poche pagine di un capitolo. La mia speranza è che, grazie a questa panoramica, sentiate di avere nuovi strumenti nel vostro arsenale. Capire come funziona un'emozione faciliterà il funzionamento di molti pretesti. Più comprenderete quello che l'altro vi sta dicendo senza usare parole, meglio imparerete a leggere le sue comunicazioni. Ecco alcune idee che spero di avervi trasmesso con questo capitolo.

- *Strumenti di base* – Come punto di partenza, il capitolo può aiutarvi a capire quali sono le sottigliezze da cercare nel viso e nel corpo, per leggervi ogni emozione.
- *Migliore comprensione* – Spero che abbiate un'idea più chiara di quali emozioni potranno funzionare meglio per voi e che riusciate non solo a vedere tali emozioni negli altri, ma a manifestarle con chiarezza.
- *Difesa* – Capire come vengono trasmesse le emozioni attraverso le espressioni facciali e il linguaggio del corpo può anche essere

molto utile come meccanismo di difesa. Comprendere come queste emozioni vengono utilizzate vi renderà più consapevoli quando le vedrete applicate contro di voi.

- *Addestramento* – In qualità di professionisti dell'ingegneria sociale, è essenziale che impariate a migliorare sempre le vostre competenze.

Voglio raccontarvi un'altra storia sull'ingegneria sociale che potrebbe aiutarvi a memorizzare gli spunti presenti in questo capitolo. Durante un DEF CON, ebbi un'interazione con un dipendente che mi aiutò a capire quanto fosse importante fare sempre attenzione alla comunicazione non verbale.

La conferenza è sempre un momento impegnativo per me e per il mio team. Praticamente non mi prendo mai una pausa, anche solo di pochi minuti, per cinque lunghi giorni. Accendo il mio interruttore e lo lascio acceso mentre mi nutro dell'energia e delle vibrazioni positive della folla.

Questa è un'esperienza potente per me, ma può anche aiutarmi a conoscere meglio i sentimenti altrui. Rimbalzo, urlando ordini e assicurandomi che tutto venga fatto a dovere. A questa conferenza, avevo dato degli ordini ad alcuni miei dipendenti su cosa portare. Era il nostro ultimo giorno e cercavamo di organizzare tutto in modo che potessimo uscire a cena nel nostro locale di sushi preferito.

Le cose stavano andando bene; tutto funzionava perfettamente, al 100%. Mancava solo la cerimonia di chiusura e poi potevamo finalmente rilassarci. Stavo cercando di essere ancora più consapevole delle emozioni degli altri e notai che il viso di una persona non manifestava solo fatica, ma un vero e proprio esaurimento. Un'altra persona stava esprimendo un intenso disagio.

Alla prima persona dissi: "Ehi, sembri veramente stanco. Se vuoi puoi chiedere di farti da parte e saltare la cerimonia di chiusura".

“Che cosa? Davvero ? Posso non venire?”, chiese con grande sorpresa.

“Ma certo! Pensavo che fosse ovvio. Scusami se non te l’ho detto prima”.

“Non avevo idea che fosse possibile. Pensavo fosse obbligatorio”, disse.

“Be’, è obbligatorio solo per Michele. Per il resto: tu puoi non venire”.

E il mio dipendente tirò un enorme sospiro di sollievo.

Con l’altra persona dovevo essere delicato. Non potevo permetterle di non venire senza creare problemi di fronte agli altri. L’emozione che leggevo sul suo volto era un misto di tristezza, rabbia e paura.

Mi avvicinai in privato, allontanandola dal gruppo e le chiesi se stesse bene. Non vi descriverò in dettaglio l’interazione, ma ci furono molte lacrime. Era stressata, perché sentiva di trascurare e ignorare troppe cose. E lei si sentiva molto stressata a causa della completa assenza di un po’ di respiro.

Appresi una nuova lezione. Durante l’ultimo giorno della conferenza, ero stato particolarmente attento alle emozioni del mio team. Tuttavia, mi resi conto che avrei dovuto usare questa abilità durante tutti i cinque giorni della conferenza, per rilevare i problemi prima che giungessero a quel livello di stress.

Lasciate che applichi questa storia all’ingegneria sociale: siate osservatori, ma non soltanto durante la missione. Cercate i segnali, ma state attenti anche durante tutte le comunicazioni. Notate i cambiamenti negli elementi di base e ai cali emotivi, che possono aiutarvi a scoprire quello che il vostro obiettivo prova prima, durante e anche dopo la vostra interazione.

Essere in grado di leggere la comunicazione non verbale è un’abilità potente. Aggiungendo a questa abilità anche la capacità di usare la

comunicazione non verbale per suscitare emozioni nel vostro obiettivo, avrete quasi raggiunto il livello “supereroe”.

Questo conclude il gruppo di capitoli in cui descrivo le abilità che impiego come professionista dell’ingegneria sociale. Nel prossimo capitolo, imparerete ad applicare queste capacità al test di penetrazione tipici dell’ingegneria sociale. A quali vettori potete applicare queste abilità? Questo è l’argomento del prossimo capitolo.

Hacking degli esseri umani

> Se leghi le tue aspettative di indipendenza al denaro, non l'avrai mai. L'unica vera sicurezza che un uomo può avere in questo mondo è una sana dose di conoscenza, esperienza e abilità.
> - *Henry Ford*

Per ricapitolare, ho riassunto qui quello che è cambiato nell'ingegneria sociale negli ultimi sette anni: l'OSINT e come utilizzarla, la modellazione della comunicazione, l'elaborazione del pretesto, la costruzione del legame, l'influenzamento, la manipolazione, la sollecitazione e la comunicazione non verbale. In termini di pura comunicazione, si tratta di una grande mole di conoscenze, ma poiché sono un professionista dell'ingegneria sociale, devo raccontarvi come applicare queste informazioni e utilizzarle nel contesto dell'ingegneria sociale.

In termini di elaborazione dell'attacco, esistono quattro vettori principali: il *phishing*, il *vishing*, lo *SMiShing* e l'impersonazione. Esistono anche combinazioni di questi tipi di attacchi per aver ragione dell'obiettivo.

In questo capitolo, spiego come potete usare in ciascuno di questi vettori le abilità che ho trattato nelle pagine precedenti. Poi affronto (brevemente, lo prometto) l'argomento sempre divertente della stesura del rapporto. Infine, parlerò di come entrare in attività e come chiudere con certi clienti.

Prima di tutto, tuttavia, devo parlare dei principi del *pen-test*. Questo getterà le basi per affrontare i *pen-test* nell'ambito dell'ingegneria

sociale.

NOTA

Una delle cose che non tratterò in questo capitolo è come sfruttare queste abilità dal "lato oscuro". L'intero libro è incentrato su come diventare professionisti dell'ingegneria sociale con l'obiettivo di "far sì che siano felici di averti incontrato". Gli usi dannosi delle competenze di cui ho parlato *non lasciano* nessuno felice di avervi incontrato.

Un aggressore con "pari opportunità"

Un'altra cosa che voglio chiarire fin dall'inizio è che i vettori dell'ingegneria sociale non sono tecniche efficaci solo sugli "stupidi". Funzionano su tutti gli esseri umani. Con il giusto innesco emotivo, nella giusta situazione, con il giusto pretesto è possibile aver ragione di chiunque.

Spesso mi viene chiesto se io sia mai stato attaccato con successo da un ingegnere sociale. Sfortunatamente, la risposta è affermativa. La motivazione giusta al momento giusto mi fece cadere su una e-mail di *phishing*. Fortunatamente, oltre a un po' di imbarazzo, non ebbi grosse perdite, perché sapevo come reagire rapidamente e che cosa fare per risolvere il problema; avevo un MAPP (che è l'argomento del Capitolo 10).

Non amo slogan come: "Non c'è rimedio contro la stupidità umana". Sì, riconosco che molti problemi di sicurezza sono il risultato della pigrizia o addirittura della stupidità, ma questo non significa che solo uno stupido possa cadere sotto uno di questi attacchi.

Ci fu un caso in cui un professore universitario subì una truffa 419 (chiamata anche truffa del principe nigeriano). Il professore vi cascò al 100%. Ci cascò così "bene" da rubare dei soldi dalla cassa dell'università dopo aver esaurito tutti i suoi risparmi di una vita.

Anche dopo essere stato catturato dall'FBI, accusò gli agenti di averlo indagato col solo scopo di mettere le mani sui milioni che stavano per arrivare sui suoi conti bancari.

NOTA

La truffa 419, nota anche come truffa nigeriana, trae il nome da un articolo del codice penale nigeriano (l'articolo 419, appunto) che si occupa di frodi. Le truffe nigeriane iniziano generalmente con "Sono un principe e ho milioni di dollari…". Ultimamente preferiscono parlare di una vedova che ha bisogno di aiuto. A ogni modo, queste truffe sembrano continuare a funzionare su persone che sperano che un piccolo investimento possa portare a enormi guadagni.

Sembra stupido, vero? Bene, questa è una risposta facile. Io invece valuto la situazione e considero che cosa ha spinto quest'uomo a cadere così bene nel tranello. Ecco alcuni pensieri da considerare.

- Aveva seri problemi finanziari, e la truffa gli dava una speranza di uscirne.
- Il suo sentimento di *avidità* è stato scatenato dalla somma enorme che pensava di vedersi arrivare sul suo conto bancario.
- Una volta *presa la decisione*, ha voluto rimanere *coerente* con la sua decisione.
- Sentiva di aver *aiutato* una persona in un paese del terzo mondo ad avere accesso a una vita migliore e, allo stesso tempo, di aver aiutato se stesso.

Esaminando la situazione da questo punto di vista, è più facile capire come il professore possa essere caduto così bene in questa truffa da rovinarsi la vita, commettere furti e frodi e ingannare la moglie, il tutto per una speranza, per avidità e per il desiderio di rimanere coerente con la decisione di aiutare se stesso e un'altra persona.

Non so dirvi quante volte un amministratore delegato o un'altra persona di alto livello mi ha detto che lui non sarebbe mai caduto nelle mie truffe, solo scoprire con rabbia di essere proprio lui la fonte dell'accesso remoto per un *pen-test*. Chiunque può essere vittima di un

attacco, indipendentemente dalla posizione che ricopre in un'organizzazione.

I principi del pen-test

In un *pen-test* (test di penetrazione) un'azienda assume un professionista perché tenti di violare la sua rete. L'obiettivo finale è quello di evidenziare e poi correggere eventuali problemi prima che possano essere sfruttati da un malvivente.

Nel corso degli anni, il *pen-test* è diventato uno strumento di sicurezza standard e molte regole di conformità richiedono alle aziende di condurre *pen-test* almeno una volta l'anno. Al momento non ci sono molte leggi che obblighino le aziende a includere l'ingegneria sociale in questi test.

Del resto, un'azienda che voglia solo spuntare una casella per poter dire di aver svolto i test in modo da soddisfare i requisiti di conformità, di solito non è un buon cliente. Lo fanno perché sono costretti a farlo, non per convinzione. Pensatela in questo modo: quando i figli puliscono la cucina perché vogliono sorprendervi, fanno un lavoro migliore rispetto a quando li avete costretti a farlo.

Esistono alcuni standard scritti relativi al *pen-testing*, e anche regolamenti che possono aiutare i *pen-tester* ad apprendere alcune *best practice* per l'esecuzione dei test. Nel 2009, iniziai a scrivere una "intelaiatura" per l'ingegneria sociale, che ora è il fulcro di `www.social-engineer.org`. Si chiama *The SE Framework* e molte organizzazioni in tutto il mondo l'hanno adottata come standard per pianificare le loro attività annuali di ingegneria sociale. Tuttavia, non esiste ancora un chiaro insieme di standard per il *pen-testing* di ingegneria sociale. Penso che il motivo sia soprattutto legato al fatto che l'ingegneria

sociale è così dinamica, ed è quasi impossibile pianificare ogni sua fase.

Ci sono alcuni passaggi o fasi che delineano il classico percorso di un vettore di attacco di ingegneria sociale, rappresentati nella Figura 9.1.

L'informazione è la linfa vitale di un attacco di ingegneria sociale. Quindi, ha senso che l'OSINT, la raccolta di informazioni, venga sempre per prima. Non potete pianificare un attacco senza aver condotto un'approfondita ricerca.

Dopo aver raccolto le vostre informazioni di OSINT, potrete facilmente determinare quali pretesti potrebbero funzionare. Sapere come un'azienda utilizza i *social media*, come comunica, dove è geograficamente localizzata e altri dettagli sul suo funzionamento interno consente di sviluppare alcune buone idee sul pretesto.

Dopo aver sviluppato queste idee, potete iniziare a pianificare i vettori di attacco. Invierete un'e-mail di *phishing*? Oppure impiegherete il *vishing* per ottenere maggiori informazioni o le credenziali? Utilizzerete un attacco basato su un apparecchio mobile? Andrete di persona nella loro sede? Impiegherete una combinazione di questi vettori? Potrete rispondere a tutte queste domande non appena inizierete a pianificare gli attacchi.

Da qui in poi si lanciano gli attacchi, raccogliendo i risultati da tutti i passaggi e segnalando al cliente tutto quello che è avvenuto. Tuttavia, un *pen-test* non segue sempre passaggi rigorosamente lineari. Potreste fare un po' di OSINT, trovare un ottimo vettore di attacco e poi voler approfondire l'OSINT per vedere se è possibile trovare altri dati utili.



Figura 9.1 Le fasi dell'ingegneria sociale.

Indipendentemente dall'approccio, i principi del *pen-test* di ingegneria sociale dovrebbero includere i seguenti punti.

- Volete registrare le telefonate? In molti Stati questo è illegale senza avere il consenso. E non date per scontato che il cliente vi dia il suo "consenso" di fare quello che volete. Volete registrare il video del vostro accesso? Assicuratevi che tale registrazione sia approvata.
- Non date per scontato che il cliente conosca esattamente ogni fase di un *pen-test* di ingegneria sociale. Spiegate i servizi che intendete offrire, in modo che siano ben chiari. Ciò offrirà anche al cliente la possibilità di chiedervi informazioni su ogni fase del *pen-test* prima che procediate e che creiate potenziali problemi.
- Assicuratevi di ottenere il permesso scritto per registrare le chiamate che effettuerete.In molti stati il consenso deve essere

formale e di entrambe le parti, quindi procuratevi il consenso dell'azienda, in modo da non incorrere in problemi legali.

- Trascrivete esattamente la stringa o lo strumento di ricerca Google che avete utilizzato, in modo che il cliente possa replicare i passaggi, se necessario.
  Ho sentito alcuni *pen-tester* dire di temere che in questo modo il cliente possa svolgere il *pen-test* da solo. Ma in tutti questi anni di attività, neppure un cliente ha smesso di usare i miei servizi solo perché "avevo detto troppo".
- La storia è importante quanto i risultati.
  Per esempio, potreste dire al cliente che c'è stato un rapporto di clic del 90% e che il 47% delle persone che avete chiamato vi ha fornito le credenziali di accesso al dominio, cifre sicuramente spaventose. Ma dovete anche spiegare ogni fase del processo: il modo in cui avete sviluppato quel vettore di attacco, chi vi ha resistito e perché. Tutti questi dettagli sono elementi importanti della storia da comunicare al cliente.
- Non parlate su Twitter o sui *social* dei vostri exploit di successo contro i vostri clienti (*sul serio, quando leggo queste cose rabbrividisco*).
  Immaginate di andare dal vostro medico per un esame invasivo. Il medico infila sonde in luoghi del vostro corpo che preferireste non venissero sondati. È fastidioso, forse anche un po' doloroso e sicuramente imbarazzante. Termina l'esame, domanda scusa un attimo, estrae il telefono per controllare alcune app e vedete che scrive un tweet in cui dice: "Dovreste vedere che razza di tumore ho trovato su quest'ammasso di lardo che ho esaminato oggi. LOL". Non ha menzionato il vostro nome e non ha messo alcuna fotografia, ma come *vi fa sentire* la cosa? Vi piacerebbe un medico così? Lo sentite "dalla vostra parte"? Se fossi il paziente,

questa sarebbe l’ultima volta che avrei a che fare con quel medico.

Pensate a che cosa significhi un tweet sulla facilità con la quale avete avuto accesso alla sede di un cliente o sul livello della sua sicurezza. È imbarazzante e non professionale.

Questi cinque principi sono buoni orientamenti generali da applicare ai vostri incarichi. Prima di entrare nelle regole che possono aiutarvi per ogni vettore di attacco che potreste utilizzare, ho altre due linee guida: documentate *tutto* e siate giudiziosi nella scelta dei pretesti.

Documentate tutto

Il cliente vi sta pagando per scavare in profondità e anche se non utilizzate l’OSINT che avete scoperto con i vostri attacchi, il cliente ha comunque bisogno di sapere che cosa avete scoperto. Inevitabilmente, ci saranno momenti nel vostro lavoro in cui troverete materiale davvero sensibile. La domanda è, come gestire la situazione?

In un test, siamo stati incaricati di condurre un *pen-test* contro una dirigente di alto livello di un istituto finanziario. Durante le ricerche, trovammo le foto che aveva pubblicato quando era ragazza, che ormai erano finite sul sito web di un fotografo come materiale promozionale. Purtroppo, alcune di quelle foto erano state rubate dai pornografi e venivano utilizzate per promuovere i loro siti. Come gestire questa situazione in modo professionale?

Abbiamo valutato che questa informazione era troppo dannosa per la persona e troppo imbarazzante per poterla impiegare in un attacco di *spear-phishing*. Quindi abbiamo scartato questa via, abbiamo eseguito il nostro *pen-test* e poi abbiamo richiesto un incontro speciale con la dirigente in questione. Ci siamo offerti di aiutarla a eliminare queste foto dai siti web in cui si trovavano, e di non segnalarle alla sua

azienda. Lei ha davvero apprezzato la delicatezza ed è ancora oggi un'amica.

Siate giudiziosi con i pretesti

Sono state innumerevoli le volte in cui abbiamo trovato qualcosa di davvero imbarazzante su un cliente. Personalmente ho scelto di non usare mai questa via per costruire il pretesto. Alcuni di voi probabilmente penseranno che abbia solo sprecato buone opportunità. Tuttavia, ricordate che il mio obiettivo è quello di "lasciarli felici per avermi incontrato". Inoltre, il mio scopo è quello di educare, il che è difficile se umilio il soggetto. Di conseguenza, sono giudizioso e sensibile nella scelta di un pretesto. Detto questo, ricordo di avervi precedentemente raccomandato di segnalare sempre quello avete trovato: così anche quando non utilizzate informazioni imbarazzanti, dovreste dire al cliente che cosa avete trovato.

Un mio cliente chiese alla mia società di fare attività di *spear-phishing*. Uno dei suoi dipendenti aveva impiegato il suo indirizzo e-mail aziendale per accedere a un sito di "appuntamenti" e postare commenti su alcune ragazze molto carine e molto poco vestite, dicendo loro che stava arrivando in città per un viaggio di lavoro e voleva incontrarle. Mettete da parte tutto quello che potete pensare sul fatto che avrebbe tradito la moglie e sui problemi di sicurezza legati all'uso pubblico del suo indirizzo e-mail aziendale su un sito come questo. Un *phishing* basato su una di queste donne avrebbe funzionato? Posso esserne certo quasi al 100%, ma decidemmo di non usarlo. Anche in questo caso, lo scopo professionale di un ingegnere sociale è quello di educare e assistere, piuttosto che umiliare per avere successo.

Il phishing

Il *phishing* è definito come l'atto di inviare e-mail maligne che fingono di provenire da fonti attendibili. Gli obiettivi del *phishing* possono essere suddivisi come segue.

- Fornire *payload* dannosi per ottenere l'accesso da parte degli autori dell'attacco.
- Acquisire credenziali.
- Raccogliere altri frammenti di informazioni, per condurre ulteriori attacchi.

Lo scopo dell'e-mail di *phishing* determina il contenuto, il pretesto e il metodo di consegna. Come professionisti dell'ingegneria sociale, vi potrebbe essere chiesto di impiegare diversi tipi di metodi di *phishing*.

Phishing educativo

A volte, il cliente non vuole sottoporre a test le risorse di rete dell'azienda, ma solo il lato umano. Un modo efficace per farlo è quello di inviare un'e-mail di *phishing* solo educativo, il che significa che quando l'obiettivo interagisce con il messaggio, non riceve alcun codice dannoso e non viene ottenuto un accesso remoto. Ci si limita a registrare il suo *ping* su un sito, per segnalare che è stato fatto clic sul messaggio di *phishing*. Le statistiche vengono poi utilizzate per aiutare il cliente a capire quanto sono suscettibili le persone al vettore di attacco del *phishing* e dove potrebbe essere necessario prevedere maggiore informazione.

Con questo tipo di *phishing*, lo scopo è quello di usare la curiosità, l'avidità, la felicità o una sana paura per convincere qualcuno a fare clic. Per farlo, potete basare il pretesto sull'OSINT rivolta verso un obiettivo specifico o verso l'intera azienda. Al mio team è capitato di

inviare questo tipo di e-mail di *phishing* a una sola persona o anche a centinaia di migliaia di persone contemporaneamente.

Ecco un esempio che illustra il motivo per cui è importante seguire i principi esposti nel paragrafo precedente: avevo scritto un messaggio di *phishing* per un cliente che sembrava un legittimo invito di LinkedIn. Lo inviai ai 7.000 utenti del cliente. Ottenni un rapporto di clic molto alto, circa il 73%. Ero piuttosto soddisfatto e tutti, me incluso, sono rimasti impressionati dal successo di questo tentativo di *phishing*.

Stava arrivando un altro impegno importante e riuscii a riutilizzare il mio *phishing* di Invito a LinkedIn. La settimana successiva lo inviai a 10.000 utenti, ma i clic non arrivarono. Al termine della campagna, il rapporto di clic era solo del 4%, circa. Non potevo crederci. Dopotutto, era un ottimo messaggio di *phishing*, giusto? Chiesi al cliente di provare e scoprire dai propri utenti perché questo tentativo di *phishing* era fallito così miseramente.

Si scoprì che era mia la colpa del fallimento. L'azienda 1 era di produzione, con dipendenti in una fascia d'età compresa tra i 35 e i 55 anni. L'azienda 2 era di commercio e l'età media dei dipendenti era fra i 19 e i 29 anni. Quando l'azienda 2 chiese ai suoi collaboratori se avessero visto l'e-mail e perché non avevano fatto clic, hanno risposto con commenti del tipo: "Sì, l'ho visto, ma solo i vecchi usano LinkedIn. Io uso Facebook".

Ero sbigottito. Dato il successo con l'azienda 1, pensavo che quel messaggio potesse funzionare in qualsiasi situazione. Per ogni azienda occorre predisporre un messaggio di *phishing* personalizzato. Questa esperienza mi ha anche convinto a non utilizzare soluzioni di *phishing* del tipo Software as a Service (SaaS) che si basano esclusivamente su modelli.

Anche quando lo scopo del vostro tentativo di *phishing* è educativo, richiede comunque i passaggi nella piramide rappresentata nella Figura 9.1. A partire dall'OSINT, si prepara un messaggio di *phishing* che si rivolge al pubblico di destinazione e raggiunge l'obiettivo desiderato.

Phishing per un pen-test

Il *phishing* per un *pen-test* non si discosta sostanzialmente dal *phishing*, tranne per una grande differenza: l'obiettivo finale. Invece di essere orientato all'educazione, il *phishing* è volto a ottenere l'accesso remoto, le credenziali o qualche altro tipo di violazione.

Il *phishing* per un *pen-test* usa generalmente pretesti che coinvolgono i sentimenti di paura, avidità, sorpresa e perfino tristezza. Uso queste emozioni perché in un *phishing* per un *pen-test* ho bisogno di qualcosa di più del semplice clic. Spesso ho bisogno che l'obiettivo apra un documento e svolga passaggi e/o immetta le credenziali. Poiché questi passaggi prendono più tempo, ho bisogno di mantenere l'obiettivo in *alpha mode* più a lungo, e quindi la molla emotiva dev'essere più forte.

Un esempio di questo riguarda un'azienda sulla quale ho condotto un *pen-test* e che era pervasa da una grande passione per tutti i prodotti Apple. Quasi tutti i dipendenti di questa società utilizzavano un MacBook e avevano un iPhone nuovo di zecca. Il *pen-test* è caduto proprio nel periodo in cui veniva lanciata una nuova versione di iPhone. L'e-mail di *phishing* che inviai ai dipendenti dell'azienda aveva una bella foto del nuovo iPhone e un messaggio che sembrava provenire dalle risorse umane.

[Nome azienda] *premierà 10 fortunati dipendenti con il nuovo iPhone e un intero anno di traffico vocale e Internet. Il sorteggio si svolgerà venerdì prossimo alle ore 15:00.*

Per partecipare, tutto quello che dovete fare è andare su questa pagina della intranet interna e fare accesso con nome-utente e password. Parteciperete automaticamente: `https://iphone.updates-company.com`

In bocca al lupo!

Acquistammo il dominio `updates-company.com` e creammo una pagina intranet fittizia con due caselle di testo e un pulsante, oltre al logo aziendale. Inviai l'e-mail di *phishing* a 1.000 persone e ricevetti 750 credenziali di accesso aziendale.

Il giusto stimolo emotivo al momento giusto rivolto alle persone giuste porta a un successo enorme.

Spear-phishing

Lo *spear-phishing* e tutte le sue varianti sono una forma di *phishing* molto personalizzata. Dopo aver approfondito l'attività di OSINT sia sull'obiettivo sia su ogni membro della famiglia, in genere seleziono qualcosa di molto personale, da usare come pretesto. Molto spesso, l'OSINT che trovo e utilizzo proviene da un post che un membro della famiglia ha pubblicato sui *social media*.

In un caso, scoprii che un obiettivo e un gruppo di suoi amici erano andati a Las Vegas per un weekend fra uomini. Il gran numero di foto che i suoi amici hanno pubblicato delle loro scappatelle di quel fine settimana mi ha portato a scegliere questo pretesto.

La mia e-mail di *phishing* proveniva dall'albergo in cui aveva soggiornato. Ecco il suo contenuto.

Sig. [nome dell'obiettivo],

I giorni 3-8 luglio è stato ospite del nostro hotel. Dopo la sua partenza, il personale di pulizia della stanza ha trovato un oggetto che

potrebbe essere suo. Può per favore controllare l'immagine allegata e dirci se l'oggetto è di sua proprietà?

Se l'oggetto è suo, questo link rimanda al modulo per la richiesta di spedizione da parte nostra.

Cordiali saluti,

Lo staff dell'albergo

Ora perché scelsi di inserire il link anche se sapevo che l'allegato carico di *malware* non avrebbe mostrato alcuna immagine? Perché c'era la possibilità che la persona che riceveva l'e-mail rivendicasse l'oggetto a prescindere. Il modulo richiedeva le seguenti informazioni:

- nome e cognome;
- indirizzo di posta;
- numero di telefono;
- indirizzo e-mail;
- data di nascita (doveva essere maggiorenne);
- le ultime quattro cifre della carta di credito utilizzata dal destinatario per prenotare la stanza.

Questo pretesto ebbe molto successo e non solo ha portato a una violazione completa del sistema, ma a un sacco di OSINT aggiuntiva, che impiegai poi per condurre ulteriori attacchi.

Anche quando uso delle informazioni personali per un pretesto di *spear-phishing*, non utilizzo informazioni che possano essere dannose per la persona. Per esempio, in questo stesso *pen-test* di *phishing*, non avrei mai usato un pretesto come questo: "Abbiamo trovato alcune sue foto in compagnia di una prostituta mentre era in visita a Las Vegas. Fai clic per pagare il riscatto" e neanche qualcosa di anche lontanamente simile, anche se avessimo trovato informazioni in merito. Se avessi scoperto quel tipo di dati durante l'OSINT, l'avrei segnalato direttamente all'obiettivo, chiedendo come voleva che ci occupassimo della questione.

Riepilogo sul phishing

Non so voi, ma io ricevo in media più di 200/250 e-mail al giorno, da tutti i miei account. L'ultima volta che ho controllato, il mio scopo non era solo di controllare la posta elettronica.

Curiosità

Secondo un rapporto di The Radicati Group (www.radicati.com/wp/wp-contenuto/upload/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf), nel 2017 sono state inviate in media 269 miliardi di e-mail al giorno. Si tratta di 3,1 milioni di e-mail ogni singolo secondo di ogni giorno. Un altro dato divertente: penso che la metà di queste e-mail giunga nella mia casella di posta (ok, ho esagerato un pochino…).

Poiché usiamo la posta elettronica per condurre le nostre attività, per comunicare con tutto il mondo, per tenerci in contatto, per inviare lettere e anche per fare acquisti, questo è anche il vettore più utilizzato per gli attacchi di ingegneria sociale. Come professionisti dell'ingegneria sociale dovete imparare a confezionare e-mail dall'aspetto professionale e basate su una solida attività di OSINT, per dimostrare veramente la sensibilità del vostro cliente a questo vettore.

Il vishing

Nel 2015, il termine *vishing* è stato inserito nell'*Oxford English Dictionary*. Ho anche provato a rivendicare la paternità del termine, ma nessuno mi ha creduto (sto un po' scherzando, ma solo un po'…).

Vishing è la contrazione di *vocal-phishing*, ovvero è un *phishing* svolto per telefono. Questo vettore è molto più comune di quanto non fosse anche solo un paio di anni fa e secondo me il motivo della sua popolarità è la sua efficacia.

Ecco alcuni degli scopi per cui sceglierei di usare il *vishing* per un *pen-test*:

- Raccolta di credenziali;
- OSINT;
- Violazione completa.

Tratterò ciascuno di questi tipi di attacchi, in modo da fornirvene un quadro completo.

Vishing per la raccolta di credenziali

Molto spesso in un *pen-test*, io e il mio team abbiamo dei piani tecnici per compromettere la sicurezza, ma proviamo a condurre un attacco *vishing* o *phishing* per vedere se riusciamo a ottenere le credenziali, che ci daranno un modo più semplice per accedere alla rete.

In un caso, dopo aver condotto un'OSINT online, avevo 10 o 15 numeri che volevo provare a utilizzare per raccogliere le credenziali. Sviluppai il mio pretesto basato su un'altra attività di OSINT. Scoprii che l'azienda che era il nostro obiettivo utilizzava una società IT esterna in *outsourcing* per gestire il passaggio da un sistema operativo a un altro. Si trattava di un enorme aggiornamento, che coinvolse non solo il sistema operativo, ma anche molti altri software, che avrebbero dovuto essere aggiornati.

Il mio pretesto si chiamava Paul, della Secure IT (un nome del tutto inventato per questo libro): dovevo controllare lo stato di aggiornamento dei dipendenti, perché avevamo notato alcuni problemi con il traffico in arrivo dalla loro macchina. Andò così.

Obiettivo: Buongiorno. Sono Steve. Come posso aiutarla?

Io: Salve, Steve. Sono Paul di Secure IT. Volevo …

Obiettivo: [*interrompendo*] Ah, sì, proprio voi! Ma non sapete quanto lavoro devo fare? E il vostro ultimo aggiornamento mi sta bloccando!

Io: Capisco, Steve. È per questo che l'ho chiamata. Abbiamo notato la presenza di una grande quantità di pacchetti malformati provenienti dal suo indirizzo IP e pensiamo che potrebbe trattarsi di un problema di *DNS poisoning* causato da uno *stack overflow*. [*La mia voce si spense, alla fine, mentre pregavo che non fosse un tecnico.*]

Obiettivo: *Poisoning*? Mi hanno avvelenato il computer? Di che diavolo sta parlando, Paul?

Io: Scusi, a volte mi esce il gergo tecnico. Sono davvero dispiaciuto. Significa che durante l'installazione potrebbe essersi verificato un problema che rallenta il suo computer. Posso guidarla in alcuni passaggi per vedere se possiamo aggiustarlo subito? Ha voglia di farlo?

Obiettivo: Ascolta, Paul. Avrei preferito che inviaste un incaricato qui per risolvere il problema. Non capisco una parola di quello che ha detto.

Io: Ho capito Steve. Non posso inviarle un incaricato per i prossimi quattro o cinque giorni. Ma posso aiutarla a distanza. Se desidera posso accedere al computer e correggerlo da remoto.

Obiettivo: Certo, se riesce a far funzionare di nuovo la mia macchina, per me va bene. Di che cosa ha bisogno?

Io: Io sono pronto per eseguire il login ed effettuare le regolazioni. Nome-utente e password di accesso?

Obiettivo: [*senza esitazioni*] SMaker, con la "S" e la "M" maiuscole. E la password è buona, inviolabile: Krikie99.

E con quello avevo le chiavi del regno.

Quando si tratta di raccogliere le credenziali, trovo che il lavoro è più facile se riesco a trovare qualche informazione di OSINT che mi aiuti a costruire un pretesto credibile, usando dettagli tratti da qualcosa di rilevante e reale per l'obiettivo. Inoltre, oltre al *vishing* per delle credenziali di accesso al dominio, ho richiesto credenziali per VPN, e-

mail, archiviazione protetta, database e perfino codici di accesso alle porte.

Vishing per l’OSINT

A volte, nel caso di un *pen-test*, non ho abbastanza dettagli per completare un attacco o voglio verificare alcuni dettagli prima di entrare in azione. In un caso, avevo pianificato un attacco di *spear-phishing* e *vishing* per un obiettivo, ma avevamo individuato più numeri di telefono e indirizzi e-mail che potevano essere suoi.

Sviluppammo un rapido pretesto, per determinare il numero corretto. Scoprimmo che l’obiettivo viaggiava frequentemente tra il Canada e Londra. Individuammo il numero di un Hotel Hilton a Londra, lo falsificammo e poi iniziammo a chiamare i numeri che avevamo per l’obiettivo, uno per uno.

Obiettivo: Sì?

Io: Salve, parlo con Alfred Gaines?

Obiettivo: Ehm, sì. Chi parla?

Io: Mi dispiace. Sono Paul dall’Hilton di Londra. Volevo chiederle un minuto per ringraziarla per il suo recente soggiorno presso di noi. Abbiamo da sottoporle un breve sondaggio sul suo soggiorno, se ha qualche secondo…

Obiettivo: Il mio soggiorno? Ma di cosa sta parlando? Sono mesi che non alloggio a un Hilton di Londra. Come ha avuto il mio numero?

Io: Signore, sono molto dispiaciuto per l’errore. Questo è il numero di telefono di Alfred Gaines, 846-555-1212, giusto?

Obiettivo: Sì, sono io, ma ci dev’essere un errore sui miei recenti soggiorni lì da voi.

Io: Ok, posso inviarle la fattura via e-mail, così mi dice se si tratta di lei?

Obiettivo: Certo che può.

Io: Eccellente. Posso inviarla ad `a.gaines@hmail.com`?

Obiettivo: Beh, preferirei usare l'altro indirizzo e-mail. Quello non lo controllo spesso. Lo invii a `gainesat@gmail.com`.

Io: Ok, non si preoccupi, signore. Gliela mando subito.

In questo modo abbiamo avuto conferma del numero di telefono, dell'indirizzo e-mail e un chiaro vettore con il quale attaccare l'obiettivo e tutto grazie a questa chiamata di *vishing*.

Io e il mio team abbiamo usato questa tecnica molto spesso per verificare i dati che trovavamo e per scoprire nuove informazioni. Trovo questa forma di *vishing* molto efficace, perché all'obiettivo non viene dato molto tempo per decidere se aiutarci. Inoltre, la maggior parte delle aziende non educa adeguatamente i propri dipendenti in questo senso. La combinazione di questi due fattori crea un grande rischio per le aziende.

Vishing per la violazione completa

È possibile eseguire una violazione completa utilizzando solo il *vishing*. I principi rimangono gli stessi e, con il giusto pretesto e sufficienti prove a supporto, un professionista dell'ingegneria sociale può facilmente ottenere anche i dettagli più delicati.

In un caso, io e il mio team abbiamo avuto il compito di sottoporre a test un grande istituto finanziario usando come vettore il *vishing*. L'obiettivo era quello di contattare i dipendenti di livello C per vedere se concedevano il loro nome-utente e la loro password o qualsiasi altra informazione sui loro sistemi o dati.

Il nostro pretesto sarebbe stata una dirigente, in viaggio alle Hawaii per la luna di miele e che, mentre era in aeroporto, era stata chiamata dal capo, che non riusciva a trovare un report essenziale per la riunione

di lunedì. Sapeva di averlo sul suo desktop, ma aveva dimenticato le credenziali per l'accesso remoto.

Caricammo una clip di YouTube, denominata "rumore di sottofondo in aeroporto" e avviammo la chiamata. Stavo ascoltando, muto, per comunicare pensieri o idee veloci alla mia complice. Andò così.

Obiettivo: Supporto. Come posso aiutarla?

Agente SE: [*respiro pesante e stress nella voce*] Mi sente? Mi scusi ma il rumore in aeroporto è così forte!

Obiettivo: Salve, sì, forte e chiaro. Con chi sto parlando?

Agente SE: Oh, Dio, mi scusi. [*Un sospiro*] Sono Jennifer Tilly, vicedirettore del Finanziario. Sto andando alle Hawaii per il mio viaggio di nozze e il direttore mi ha chiamato per dirmi che l'ultimo budget di bilancio non si trova nella directory. Ne ha bisogno per la riunione di lunedì e ho bisogno di accedere per inviarglielo, ma ho dimenticato il login remoto.

Obiettivo: Va bene. Vediamo se posso aiutarla. Innanzitutto, ho bisogno di verificare la sua identità. Ma prima di tutto congratulazioni per il matrimonio e spero che si divertirà molto alle Hawaii.

Agente SE: Grazie mille. Sono così eccitata. Questa è la mia prima volta alle Hawaii e posso andarci con il mio migliore amico, che ora è mio marito.

Obiettivo: Tanti auguri. Mi scalda il cuore sentire persone che parlano in questo modo. Signora Tilly, posso avere il suo codice interno, per favore?

Agente SE: Sa che cosa? Il capo mi aveva promesso niente lavoro per due settimane, e io non ho portato con me nulla: niente portatile e niente tesserino. A volte dimentico il mio compleanno, figurati il mio codice interno.

Obiettivo: [*cercando di essere utile*] Beh, proviamoci: inizia con 17. Si ricorda le altre cinque cifre. [*Altra informazione molto importante*.]

Agente SE: Spiacente, vago nel vuoto. Mi manca qualcosa come 98231?

Obiettivo: Beh, un nove e un otto ci sono nel codice, ma proviamo con qualcos'altro. Mi dica il nome del suo capo.

Agente SE: Certo è Mike Farely.

Obiettivo: Ok, fantastico. E la sua e-mail?

Agente SE: `j.tilly@nome-azienda.com`

Obiettivo: Perfetto. Ok, ecco che cosa posso fare, posso resettare la sua password e inviargliela al cellulare; così potrà accedere e copiare quel report. Mi lasci solo… [*rumore di battitura e clic*] Signora Tilly, mi dispiace, ma non vedo installato l'accesso remoto. Quindi, anche se resettassi la password, non potrebbe accedere.

Agente SE: Oh, no! È terribile. Ma ne devo andare per due settimane e il volo parte fra mezzora. Come posso fare? Mi aiuti per favore! [*Quasi in lacrime e con molta ansia nella voce.*]

Suggerii alla mia complice di chiedere se poteva installare l'accesso remoto per noi sulla sua macchina e poi darci un codice di accesso monouso.

Obiettivo: Bene, possiamo avviare una richiesta di installazione dell'accesso remoto, ma molto probabilmente impiegheranno ore, se non addirittura domani.

Agente SE: È stato così gentile. Mio marito mi sta guardando male: dovevamo starcene seduti insieme nella lounge a sorseggiare un calice di champagne e io sono ancora attaccata ai miei problemi di lavoro. Come possiamo accelerare le cose?

Obiettivo: Senta, Jennifer: sta andando in luna di miele e questo è fantastico; mi faccia vedere che cosa posso fare. Può restare in attesa un attimo?

Agente SE: Certo, ma non ho molto tempo. Tra un po' ci imbarchiamo.

Sentimmo l’obiettivo chiedere al collega: “Questa povera donna sta andando in luna di miele; dobbiamo aiutarla a partire tranquilla. Sono sicuro che possiamo farlo in fretta, giusto?”.

Non riuscimmo a sentire il commento dall’altra persona, ma ci sembrò che tutti fossero sinceramente intenzionati ad aiutare Jennifer. Qualche istante dopo, l’obiettivo mise il telefono in attesa per fare un’altra chiamata prima di tornare alla chiamata con la mia complice.

Obiettivo: Signora Tilly, beh, abbiamo un regalo di nozze per lei: un agente, ora, sta installando l’accesso remoto sulla sua macchina. Ci metterà 10 minuti, poi dovrebbe tornare ad accedere alla sua macchina.

Agente SE: Lei è la persona più straordinaria che abbia mai incontrato! Mio marito sarà così felice e questo è il miglior regalo possibile! Grazie!

Obiettivo: Quando riceverò l’OK dall’addetto, le invio un codice monouso per ottenere l’accesso.

Agente SE: Oh no… non posso farlo. Non ho il telefono di lavoro con me, non riceverò l’SMS.

Obiettivo: Oh, no, signora Tilly. Non possiamo superare questo passaggio. Non so che cosa fare.

Agente SE: Ma è terribile! Mi servirà di lezione, sono così stupida. Avrei dovuto portare comunque il telefono con me. Ora dovrò cancellare il volo e prendere qualcosa nei prossimi giorni. Che tristezza. Ma grazie, è stato davvero carino e utile. Grazie mille.

Obiettivo: No! Non le faremo saltare la luna di miele; non esiste… [*E, con un sussurro*] Ascolti, le manderò il codice sul telefono personale; poi, quando verrà emessa, le manderò anche la password, ok?

Agente SE: Davvero farebbe questo per me? Mi viene da piangere…

Obiettivo: Non è nulla. Dobbiamo assolutamente metterla su quel volo e senza pensieri di lavoro.

Con questo ottenemmo l'accesso remoto, una password e la possibilità di violare l'intera azienda.

SUGGERIMENTO

Noterete che tendo a impiegare pretesti emotivi che chiedono all'obiettivo di essere "salvati" o "aiutati". È assolutamente deliberato. Dare a qualcuno la capacità di fidarsi concedendo la propria fiducia crea un legame molto forte tra due persone. Avviene un rilascio di ossitocina e così quel legame fa sì che l'obiettivo desideri essere coerente nel suo desiderio di aiutarvi, indipendentemente da quanto errata possa essere quella decisione.

L'utilizzo del *vishing* per la violazione completa può facilitare molto il lavoro del *pen-tester*. Molto spesso, è importante capire che un *vishing* per violazione può dover partire da un *vishing* per OSINT, prima di passare a pretesti sempre più dettagliati.

Riepilogo sul vishing

Il *vishing* è un vettore d'attacco potente, che può anche essere devastante nelle mani sbagliate. Dal momento che può essere utilizzato per quasi ogni aspetto dell'attacco, è un'arma potente.

Per un professionista dell'ingegneria sociale, è fondamentale non aver paura di parlare al telefono, per avere successo. Imparate a padroneggiare questo mezzo, anche se non è il vostro metodo di comunicazione preferito. La capacità di parlare al telefono e di stabilire legami, di acquisire la fiducia altrui e di ottenere informazioni senza poter osservare il vostro obiettivo vi renderà più efficaci.

Lo SMiShing

Questo è un breve paragrafo, perché lo *SMiShing* non è molto utilizzato dai malintenzionati e neanche dai professionisti

dell’ingegneria sociale. Nel 2017, Wells Fargo è stata violata e, dopo quella violazione, abbiamo notato un aumento di attacchi di *SMiShing*. Molti di loro somigliavano molto a quello che potete vedere nella Figura 9.2. La maggior parte dei messaggi di *SMiShing* ha un aspetto semplice. Ma si tratta di attacchi efficaci e generalmente volti a caricare un *malware* sul dispositivo mobile o a sottrarre le credenziali.

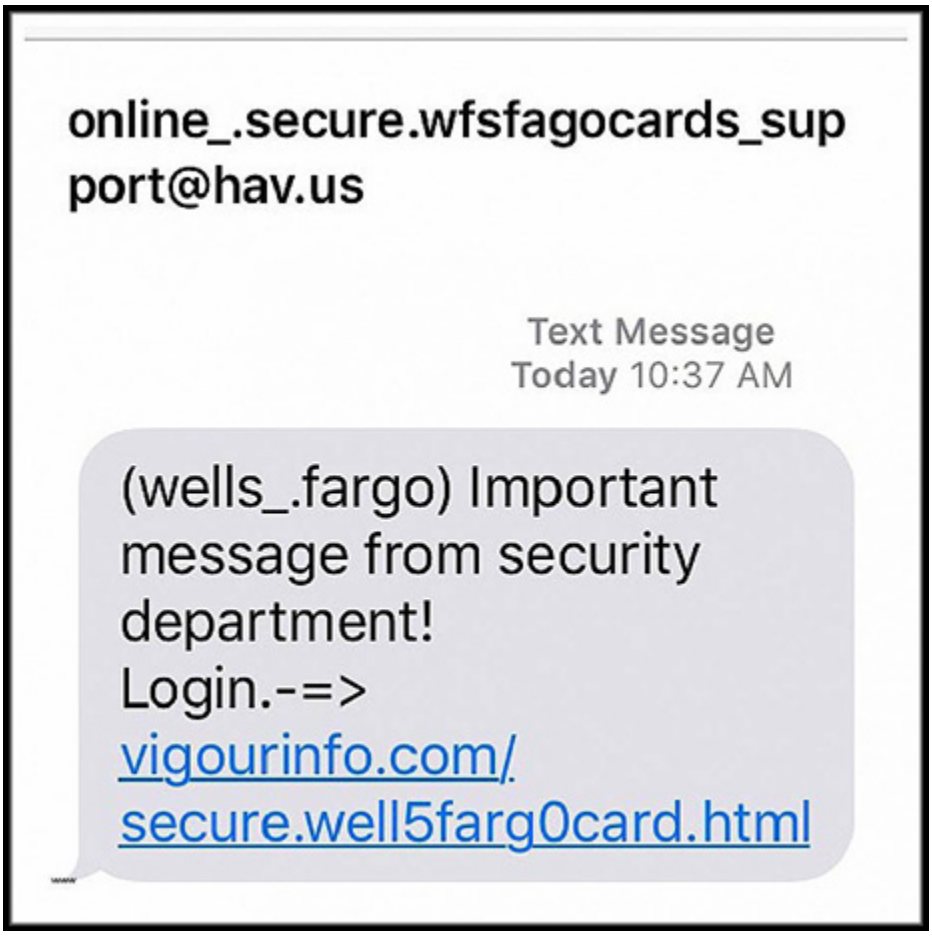


Figura 9.2 Un classico messaggio di SMiShing.

Negli ultimi due anni, i sistemi operativi mobili sono stati soggetti a *malware* e altri attacchi, nella speranza di ottenere l’accesso al dispositivo della vittima. Con la crescente adozione di politiche BYOD (Bring Your Own Device) da parte delle aziende, abbiamo notato un aumento di violazioni nei dispositivi mobili. Le violazioni possono

andare dalla lettura delle e-mail, all'attivazione da remoto della videocamera o del microfono, all'utilizzo del dispositivo mobile come una sorta di *access point* remoto.

Per questo motivo, è importante che anche un ingegnere sociale sappia utilizzare lo *SMiShing* nella sua attività. Ecco alcune regole che rendono lo *SMiShing* molto differente dal *phishing*.

- *Siate brevi*. Un messaggio di *SMiShing* deve essere breve e semplice: nessun preambolo, nessun testo di attacco e di chiusura, solo i fatti e un link.
- *Il link*. A mio parere, è sempre meglio avere un nome di dominio simile a quello da attaccare, ma se ciò non fosse possibile, gli URL abbreviati sono molto più accettati negli SMS rispetto a quanto accade per i messaggi e-mail. Cercare di controllare un link è quasi impossibile su un dispositivo mobile, pertanto l'utente deve disporre di una formazione avanzata per visualizzare i link errati.
- *Non lesinate sui dettagli*. Se state tentando di raccogliere le credenziali, non pensate di non aver bisogno di elementi di branding o che la pagina web sembri credibile solo perché il vostro obiettivo sta utilizzando un dispositivo mobile. Per assicurarvi di sottoporre a test l'obiettivo, assicuratevi di dedicare del tempo a rendere il tutto reale.
- *Non prevedete troppi passaggi*. L'obiettivo ha un dispositivo mobile, quindi se dovrà compiere più di tre passaggi, potrebbe non sentirsi motivato a continuare.

Mentre vediamo aumentare le politiche BYOD e il lavoro da casa, diventerà ancora più importante per il professionista dell'ingegneria sociale capire come impiegare questo vettore e usarlo per sottoporre a test una popolazione.

I telefoni cellulari resteranno con noi ancora a lungo e sono sempre più integrati nella nostra vita lavorativa. Ciò renderà ancora più difficile per i nostri clienti rilevare gli attacchi.

L’impersonificazione

Si tratta di uno dei vettori più pericolosi, ma è anche uno dei più rischiosi da impiegare per chi si occupa di ingegneria sociale. Pertanto, è il vettore meno utilizzato dei quattro. L’impersonificazione prevede l’impersonificazione fisica di un dipendente dell’azienda obiettivo o di qualcuno che ha un’autorità tale da poter essere considerato affidabile (rappresentanti delle forze dell’ordine, manutentori e così via).

Per quanto riguarda me e il mio team, l’impersonificazione è il vettore più divertente per aiutare i clienti, ma il rischio per noi è piuttosto basso. Con un vero attacco, il rischio è molto maggiore e questo significa che l’operazione richiede una grande attività di pianificazione. Nei nostri *pen-test*, abbiamo una carta “Uscite gratis di prigione”, il che significa che non possiamo davvero metterci nei guai con le nostre imprese. Al contrario, i veri cattivi, se vengono catturati, dovranno trascorrere un sacco di tempo in prigione.

Impersonificazione vs Red Team

Un Red Team in genere (ma non necessariamente) agisce di notte e si concentra sul tentativo di violare la sicurezza fisica: ascensori, serrature, telecamere di sicurezza e così via. L’impersonificazione si concentra invece sui fattori umani della sicurezza fisica. Quindi, invece di forzare una serratura, intendiamo convincere la persona di guardia a lasciarci entrare. Invece di sfondare quella porta, stiamo facendo in modo che qualcuno con il distintivo ci lasci passare. Un Red Team si concentra sui dispositivi di sicurezza, mentre l’impersonificazione si concentra sulle persone.

Pianificazione di un pen-test con impersonificazione

Un *pen-tester* deve tenere presente che *tutti* i sensi dell'obiettivo sono interessati quando si tratta di svolgere un'impersonificazione. Considerando che il *phishing* impegna solo nella vista e il *vishing* impegna solo l'ascolto, l'impersonificazione deve rivolgersi a quasi tutti i sensi (anche se in genere non coinvolge troppo il gusto).

Per questo motivo, è importante pianificare accuratamente i principi del *pen-test*, come descritto nei prossimi paragrafi.

Raccolta di informazioni

La raccolta di informazioni è una parte importante di una valutazione per un'impersonificazione fisica. Spesso chiedo agli allievi di ideare un pretesto che garantisca l'ingresso. Pensateci per un attimo. Avete un'idea?

Gli allievi spesso suggeriscono qualcosa come il fattorino UPS. Le mie successive domande li aiutano ad andare oltre la loro affermazione iniziale: "Ok, fantastico. E poi? Quanti di voi hanno visto un fattorino UPS in giro per l'ufficio? Di solito consegnano alla reception o all'ufficio di gestione della corrispondenza".

Un'OSINT è essenziale per sviluppare un pretesto plausibile per l'impersonificazione. In una delle mie missioni, scoprii che un cantiere aperto in zona fece in modo che dei ragni che normalmente proliferavano in primavera venissero fuori un po' prima dalla loro tana. Era un fatto così disgustoso da riempire i notiziari locali. Il mio pretesto fu quindi un disinfestatore e funzionò benissimo.

Sviluppo del pretesto

Ho parlato dell'ideazione del pretesto quando ho parlato di raccolta delle informazioni, ma non commettete l'errore di tentare di pianificare il pretesto, prima dell'attività di OSINT. Inoltre, dopo aver scelto il vostro pretesto, dovrete considerare alcuni altri aspetti: gli abiti, gli attrezzi, l'aspetto e così via. Inoltre, considerate se l'attrezzatura dovrà apparire nuova o usata. Dovete pensare a tutti i dettagli che possono rendere più credibile il pretesto.

Recentemente, ho dovuto violare un paio di banche insieme a uno dei miei dipendenti e ho scoperto con l'OSINT che la banca aveva appena completato un test di conformità PCI [relativa ai pagamenti con carta di credito, NdT]. Trovammo il nome dell'azienda che aveva compiuto il test, quindi siamo arrivati completamente equipaggiati, dotati di badge e di carte. Questo ci portò direttamente nel centro di controllo degli sportelli automatici, ATM, senza alcun problema. Da lì, potemmo accedere a due diversi computer, ottenendo perfino le credenziali degli altri impiegati che lavoravano in quell'ufficio.

Quando un manager mi si avvicinò, chiedendomi quale fosse il nostro contatto interno, non avevo un nome. Questa è stata una mia svista: la missione fu un fallimento e venimmo scoperti. Tuttavia, in una mezzora di lavoro, avevamo violato la rete e avevamo avuto accesso al centro di test degli ATM, con accesso a più computer. Tuttavia, quella informazione ci avrebbe evitato la cattura e ci avrebbe dato più tempo.

Pianificazione ed esecuzione degli attacchi

Una volta che avete il pretesto, dovete capire bene quali sono gli obiettivi quando entrate nell'edificio. In altre parole, dovete sapere *che cosa non potete fare*. Potete lanciare una shell remota? Siete autorizzati a violare un server? Siete autorizzati a sottrarre un dispositivo? Non date per scontato che per il solo fatto che siete stati

assunti per “giocare ai cattivi”, abbiate piena libertà d’azione. Sarebbe una supposizione potenzialmente pericolosa.

Pianificate la conduzione dell’attacco dall’inizio alla fine, quindi assicuratevi di avere a disposizione gli strumenti necessari per sottoporre a test e raggiungere questi scopi.

Una volta che il piano sarà terminato, assicuratevi che la carta “Uscite gratis di prigione” copra tutto quello che intendete fare, e se non copre tutto, fatelo includere.

Le pratiche perfette rendono perfetti.

Redazione dei report

Ricordate: la parte più importante di una missione consiste nel dire al cliente che cosa avete fatto, come e che cosa occorre fare. Prima ancora di iniziare, assicuratevi di avere il permesso di eseguire registrazioni audio e video. Oppure, se non avete questa autorizzazione, cercate il modo di catturare la storia per il report.

Per me, è importante raccontare una storia, con questo tipo di attacco. Voglio che il cliente si senta come se potesse vedere, sentire e percepire l’attacco e che abbia modo di capire che cosa ha funzionato e che cosa no. Trovo molto utile essere traboccante di elogi per i loro successi e, ovviamente, anche per i miei.

Il mio scopo nel produrre il report è che la sua lettura faccia sentire meglio il cliente. Per ottenerlo, non posso essere imbarazzante o eccessivo o dispregiativo.

I principi enunciati finora vi aiuteranno con le vostre missioni con presenza *in loco*. Trovo che questa parte del lavoro richieda molta pianificazione. Tuttavia, potrebbero esserci altre domande sulle informazioni da includere nel report. Ecco alcune considerazioni sulla gestione di alcuni dati sensibili.

La legalità delle registrazioni

Non sono un avvocato e nulla di quello che dico dovrebbe essere interpretato come un consiglio di natura legale. Dovreste assolutamente dotarvi di un avvocato per gestire questo genere di cose.

Per le missioni della mia azienda, ci comportiamo così.

- Prima di eseguire il lavoro, ricerchiamo le leggi statali e/o locali in termini di registrazione audio e video.
- Otteniamo il permesso scritto del cliente per l'una e per l'altra registrazione.
- Mai, mai, mai, ma proprio mai (ho già detto *mai*?) usiamo queste registrazioni in pubblico o per scopi di formazione senza il relativo permesso.
  E anche se abbiamo il permesso, ci premuriamo di epurare le registrazioni, in modo che nessuno sia riconoscibile. Occorre togliere tutti i nomi, i luoghi di lavoro e tutte le parole identificative.
- Ci assicuriamo che tutte le registrazioni vadano al cliente, per scopi educativi.
- Garantiamo la conservazione, il trasporto e l'utilizzo sicuro delle registrazioni.

È importante che comprendiate i rischi di quello che state facendo e sappiate anche come prevedete di utilizzare quello che avete raccolto. In una missione chiesi a una donna di inserire il suo nome-utente e la sua password in un computer lì vicino. Mentre stava obbedendo alla mia richiesta, non solo registrai il suo viso, ma catturai anche le credenziali sulla fotocamera. Per evitarle l'imbarazzo, sfocai il suo viso. Naturalmente, il cliente avrebbe potuto chiedermi di vedere il video originale: la scelta è la sua e ha il diritto di farlo. Ma prima ho presentato il video sfocato, e il cliente non ha avuto obiezioni. Se il

video dovesse essere utilizzato a scopo didattico, non voglio che la donna debba continuamente sentirsi in imbarazzo.

Considerazioni sulla “bonifica” delle registrazioni

In una missione stavo registrando tutto usando una fotocamera microscopica nascosta in una cartelletta. Incappai in un rack per server mentre stavo cercando di eludere la sicurezza, lo aprii e vi trovai due persone impegnate in attività che… ehm… non avevano molto a che fare con il lavoro. Per un attimo dimenticai la mia missione di ingegneria sociale. La coppia nascosta nell’armadio si arrabbiò molto e mi urlò di andarmene e così feci. Più tardi, mi resi conto di aver registrato quasi un minuto delle loro attività. Questo, ovviamente non era un qualcosa che potessi mostrare al cliente e pensai a un modo per giustificare quel “buco” di registrazione.

Alla fine, decisi che l’azienda mi aveva pagato per aiutarla a proteggere se stessa, la sua rete e anche il suo personale. Quella a cui avevo assistito era una violazione della politica aziendale e, per quanto ne sapevo, avrebbe anche potuto essere un *honeypot*. Quanto sarei stato ritenuto responsabile se non avessi segnalato il comportamento e poi avessi sentito che l’azienda era stata violata mentre ero presente e avrei potuto impedirlo?

SUGGERIMENTO

Nel mondo dello spionaggio, un *honeypot* è una persona che va sotto copertura per sedurre un’altra persona con lo scopo di sottrarle informazioni riservate. Il termine viene anche usato per descrivere un sistema (un computer) configurato per raccogliere dettagli da utenti ignari.

Decisi che era mio dovere denunciare questo incidente. E sì, il risultato fu che il responsabile del gesto fu licenziato. Perché la donna, invece, no? Beh, lei non lavorava per l’azienda: l’uomo l’aveva fatta

entrare per svolgere in un armadio per server attività che avrebbero potuto essere condotte più comodamente fra le pareti domestiche, in una stanza d'albergo o dove volevano, ma non certo sul luogo di lavoro.

Dovete decidere quali parti della registrazione disinfettare. Io intervengo quando qualcuno ha intrapreso un'azione che non è illegale. Se è caduto sotto l'attacco di ingegneria sociale, ma non ha infranto le regole aziendali. Il mio scopo è sempre quello di cercare di garantire che il fine sia l'istruzione e non il licenziamento.

Tuttavia, se trovo qualcuno intento a scaricare immagini pornografiche, impegnato in attività sessuali, intento a sottrarre all'azienda qualcosa, mentre accede a dati riservati o, Dio non voglia, coinvolto in attività di pedofilia, penso che tali soggetti non meritino alcuna gentilezza da parte di un professionista dell'ingegneria sociale incaricato di proteggere i suoi clienti.

Procurarsi le attrezzature

Ci sono molti posti dove potete trovare attrezzature "da spie". Da Amazon ai negozi specializzati, ci sono molte possibilità. Tenete presente che le attrezzature di buona qualità costano. La pencam da 25 dollari vi darà immagini di scarsa qualità e tremolanti, mentre la webcam da 600 dollari con funzionalità di registrazione DVR sarà molto probabilmente ben più efficace.

Fate qualche ricerca prima di concludere un acquisto. Faccio sempre quanto segue prima di effettuare un ordine:

- posso controllare la politica di reso ed evito di trovarmi costretto a spedire l'oggetto in un paese straniero, in caso di malfunzionamenti.

- leggo le recensioni sia del prodotto sia della casa produttrice, per assicurarmi di ottenere il miglior risultato possibile.

NOTA

Potreste impiegare un po’ di tempo per abituarvi a filmare da una buona inquadratura, e nel contempo mantenere un comportamento professionale. Per questo motivo, provo a impiegare contemporaneamente un paio di fotocamere, in modo da ottenere almeno una buona inquadratura.

Riepilogo sull’impersonificazione

Con la giusta pianificazione, l’esecuzione di questo complesso vettore d’attacco può diventare molto più semplice. Ricordate che impersonificare e fare da Red Team non sono la stessa cosa e dovrete condurre un’attenta pianificazione per assicurarvi di sottoporre accuratamente a test i protocolli di sicurezza fisica.

È importante che, come *pen-tester*, comprendiate la portata di quello che state facendo, in modo da poter attaccare tutti gli obiettivi richiesti dal cliente. Questo soprattutto perché lo scopo finale è quello di produrre un report che mostri come risolvere i problemi rilevati. Questo paragrafo sarà più utile se oltre a capire che cosa avete fatto, scoprirete il perché l’attacco ha funzionato.

Stiamo assistendo a un numero sempre maggiore di violazioni che riguardano il lato fisico della sicurezza: chiavette USB perdute, furto fisico di dispositivi e, peggio ancora, violenze sul luogo di lavoro. Per questi motivi, è essenziale per un *pen-tester* professionista avere la completa padronanza del vettore di impersonificazione.

I report

All’inizio della mia carriera, sono stato assunto per accedere a sette magazzini per lo stoccaggio di merci. Ebbi un rapporto di successo del

100%. Riuscii perfino ad accedere a un magazzino due volte nello stesso giorno, impiegando due diversi pretesti.

Fu una bella sensazione e avevo registrato e preparato tutto per il cliente. Il responsabile del progetto mi disse di iniziare a scrivere il report e mi inviò un documento modello, vuoto a eccezione di alcune intestazioni.

Penso di averlo fissato per ore, iniziando e poi fermandomi, poi cancellandolo e ricominciandolo. Dopo decine di ore, avevo completato quello che pensavo essere un capolavoro nella storia dei report.

Immaginavo già il team riceverlo, leggerlo e prostrarsi davanti a me mentre rientravo. Lo inviai e attesi la pioggia di elogi.

Il giorno dopo squillò il telefono e la chiamata andò più o meno così (ho cercato di edulcorarlo un po'):

"Ehi Chris, che cos'è quel mucchio di spazzatura che hai inviato alla mia casella di posta? È uno scherzo? Ti stai prendendo gioco di me? Pensi che questa roba possa essere chiamata un report? Te lo rendo con… qualche piccola correzione. Sistemalo! *Subito!*".

Quando ricevetti il rapporto, non era più nero su bianco: era soprattutto rosso, verde e bianco. Sembrava che nemmeno una frase fosse stata risparmiata.

Mi ci vollero due settimane per correggere il documento, e quella fu la peggiore esperienza nella mia carriera di redazione di report. Tuttavia, allo stesso tempo, fu anche l'esperienza migliore che abbia mai avuto. Mi insegnò che aspetto deve avere un buon report. Il mio report iniziale conteneva una trama che mi faceva sembrare incredibilmente abile, meglio di James Bond. Tuttavia, gli mancavano troppi elementi chiave utili per il cliente.

Questa parte del capitolo non intende essere un seminario sulla scrittura di report, tuttavia ho alcuni principi da condividere con voi.

Professionalità

Pensate di andare dal medico, una persona che speri sia professionale. Come vi sentireste se, dopo essere salito sulla bilancia, vi dicesse: "*Wow Nelly!* Sei un pesce o una balena?". Per poi darti una pacca sulla spalla e dirti: "Sto scherzando!".

Forse non sarebbe una condotta molto professionale. Allo stesso modo, i nostri clienti non vogliono sentire cose come: "Vi abbiamo davvero massacrati!" o "Wow, davvero quel tipo ha messo questa cosa sul Web?" o " Sono il re del vostro magazzino".

Ricordate che questo report verrà letto da molte persone e che per favorire i cambiamenti è bene che le persone si sentano felici e non imbarazzate o umiliate. Il vostro linguaggio, il modo di descrivere le operazioni e il modo in cui comunicate i fatti devono esprimere professionalità.

Grammatica e ortografia

La grammatica e l'ortografia possono essere particolarmente infide. Dedicate sempre del tempo a eseguire un controllo ortografico sul vostro report e poi chiedete a una persona fidata di rileggerlo e correggerlo.

Anche con questi controlli, potreste comunque lasciare alcuni errori. È inevitabile. Nessuno si aspetta la perfezione, ma inviando un report zeppo di errori, il cliente dubiterà anche del lavoro svolto.

Tutti i dettagli

Ho sentito *pen-tester*, in passato, dire di escludere alcuni dettagli, per esempio come hanno condotto l'OSINT, l'esatta stringa di ricerca di Google impiegata o qualche altro elemento, perché temono che se

daranno al cliente troppe informazioni, non avrà più bisogno della sua attività di ingegneria sociale.

Per me, questa affermazione è semplicemente sciocca. Ho sentito questa stessa argomentazione quando ho scritto il mio libro *Phishing Dark Waters*, nel quale delineavo l'esatta metodologia e le operazioni per creare uno schema di *phishing*. Si è verificato l'esatto contrario: molte aziende usano quel libro per creare ottimi programmi di sensibilizzazione sul *phishing*, così come molti che lo hanno letto hanno poi voluto il mio aiuto.

Non preoccupatevi di informare troppo i vostri clienti. Molti di loro apprezzeranno la vostra competenza e saranno impressionati dalle vostre scoperte. E vorranno che l'attacco sia svolto da qualcuno abbastanza sicuro di sé da fornire loro tutti quei dettagli.

Detto questo, se trovate elementi sensibili, assicuratevi di comunicarli al vostro contatto, per chiarire che cosa dovrebbe o non dovrebbe essere incluso nel report.

Mitigazione

La mitigazione è forse la parte più importante di un report, ma è anche la più trascurata. Volete che il vostro medico vi dica che avete una malattia incurabile e che vi saluti con un "Buona fortuna…" o con un: "Ci vediamo alla prossima visita… speriamo"? Ovviamente no. Non dovreste fare la stessa cosa ai vostri clienti. Dare loro qualche mitigazione che sia accettabile.

Se quello che avete in mente per "mitigazione" sono solo quelle che io chiamo banalità e sciocchezze, che significato avrà per i vostri clienti? Per esempio, supponiamo che abbiate compiuto un test di *vishing* per un cliente e abbiate raggiunto un tasso di successo dell'80% nel corso del mese. Quale delle seguenti opzioni di mitigazione pensate aiuterà di più il cliente?

- *Opzione 1* – L’ingegnere sociale consiglia di continuare a sottoporre a test la popolazione e di utilizzare incentivi positivi per sollecitare risposte adeguate agli attacchi di *vishing*.
- *Opzione 2* – L’ingegnere sociale ha analizzato i dati della campagna di *vishing* di questo mese e rileva i due punti seguenti che potrebbero essere utilizzati per migliorare la situazione.
  - I chiamanti di sesso femminile hanno ottenuto risultati migliori rispetto ai chiamanti di sesso maschile. Ciò potrebbe indicare che è necessario istruire meglio il personale sui modi in cui riconoscere una sollecitazione.
  - Quando viene specificato un falso nome, solo il 12% dei rispondenti ha verificato il nome. E alcuni hanno addirittura continuato a fornire informazioni anche dopo non aver trovato il nome. Ciò dimostra la necessità di sollecitare il personale a verificare sempre il chiamante.

  L’ingegnere sociale vorrebbe programmare una chiamata per discutere l’implementazione di un programma educativo mentre la popolazione continua a essere sottoposta a test.

Ovviamente la seconda opzione è la migliore, ma troppe volte (e ammetto il mio team se ne è reso colpevole fin troppe volte), i rapporti includono affermazioni non utili, che non aiutano il cliente e servono solo come riempitivo.

Anche dopo aver svolto questo lavoro per anni, si tratta di una battaglia costante per assicurarsi che non prevalga la compiacenza, e dedico il 100% del mio impegno, per i miei clienti.

Passi da intraprendere

Oltre alla mitigazione (risolvendo però il problema) i clienti spesso vogliono sapere: “E adesso?”. I passi da intraprendere sono un

elemento essenziale in un report. Permette al cliente di sapere che cosa dovrebbe fare per migliorare.

Non significa che dovreste semplicemente stabilire: “Ci vediamo al prossimo *pen-test*”. Dovete seguire le stesse regole di mitigazione di cui ho appena parlato. Date ai vostri clienti sufficienti dettagli per consentire loro di intraprendere un percorso di miglioramento.

Molti dei miei clienti richiedono un servizio mensile, e così il percorso da seguire è già noto, ma questo non significa che io possa accontentarmi di questo. Il cliente vorrà comunque sapere se è il caso di modificare le cose o di adattare il programma.

Mettendo insieme tutti questi passaggi, otterrete ottimi report, che aiuteranno veramente i vostri clienti e faranno sentire meglio sia loro, sia voi.

Le grandi domande per il pen-tester dell’ingegneria sociale

In conclusione di questo capitolo, voglio trattare alcune delle domande più frequenti che ricevo come *pen-tester*. Sono sicuro che ci sono moltissime altre domande, ma queste sono le più comuni. Spero che vi aiuteranno se vi occupate di ingegneria sociale o se pensate di farne una professione.

Come posso trovare lavoro come ingegnere sociale?

Questa credo sia la domanda che più mi è stata posta in tutta la mia carriera. Dopo aver deciso di intraprendere questa attività, che cosa fare? Bene, dovete iniziare da qualche parte, ed è per questo che la risposta è così difficile. Probabilmente avete lavorato in questi ultimi

dieci anni. Probabilmente avete acquisito esperienza e abilità, e in base a quelle siete stati ripagati. Iniziare una nuova carriera come ingegneri sociali significa ricominciare non solo in termini di competenze e abilità, ma anche in termini di paga. Il mio consiglio è esortarvi a:

- uscire dalla vostra zona di comfort;
- ricominciare;
- imparare nuove abilità;
- accettare un drastico calo di stipendio, se necessario.

Se riuscite ad accettare queste cose, potete aspettarvi una bella carriera nell'ingegneria sociale. *Ma* (dannazione, c'è sempre un *ma*) non aspettate che le aziende di ingegneria sociale vi chiamino per offrirvi un lavoro. C'è solo una manciata di veri ingegneri sociali, sul mercato, ma voi dovete ancora dimostrare di essere differenti da tutti gli altri. Queste cose richiedono un po' di impegno.

NOTA

Essere professionisti dell'ingegneria sociale non significa solo entrare nelle banche e violarle con il *phishing*. C'è anche un sacco di lavoro d'ufficio e report da scrivere. Essere ingegneri sociali professionisti non significa solo essere in grado di comunicare con gli altri o di pensare rapidamente e razionalmente sotto pressione: il "pacchetto" comprende molto altro.
Dove sono i vostri punti deboli?
- Sollecitazione.
- Fluidità di parola.
- Prontezza di pensiero.
- Capacità di redazione di report.
- Capacità di discorrere in modo professionale.

Cercate di identificarli, così da poterli risolvere.
Su `https://youtu.be/RGnzf66-a4A` trovate un discorso che tenni al DerbyCon7 su questo argomento. (Avvertenza: il video inizia con uno scherzo del mio amico Dave Kennedy, ma poi prosegue perfettamente centrato sul tema.)

Come posso convincere i miei clienti a svolgere attività di ingegneria sociale?

Supponiamo che siate già *pen-tester* e che stiate svolgendo alcuni lavori di ingegneria sociale, questo paragrafo fornisce alcune idee su come convincere i vostri clienti ad assumervi per ulteriori missioni di ingegneria sociale.

Non offrite loro un servizio gratuito

Alcuni sono convinti che, offrendo ai clienti dei servizi gratuiti, questi saranno invogliati a reclutarvi per un lavoro a pagamento. Ho un aneddoto che spiega perché questa tattica non funziona nel modo che potreste aspettarvi.

Quando iniziai a lavorare nel settore tecnologico e assemblavo computer, provai a lanciare un seminario gratuito sulla sicurezza per le piccole imprese. In questo seminario, fornivo oltre un’ora di suggerimenti su antivirus, reti, condivisione di file e molto altro ancora. Alla fine, ho previsto cinque minuti in cui spiegavo perché le aziende avrebbero dovuto assumermi come loro fornitore.

Collaborai con una Camera di commercio locale e offrii la lezione gratuitamente. Organizzammo tre di questi seminari e il numero di persone che li frequentarono fu enorme. Avevo 20, 30 o più persone iscritte a ogni seminario. Già vedevo concretizzarsi le mie ambizioni.

Il giorno del mio primo seminario girai per la sala, sistemai il proiettore e preparai le dispense e tutto il materiale omaggio che avevo pagato di tasca mia. Cinque minuti prima dell’orario di inizio, c’era una sola persona nella sala. Due minuti prima dell’orario di inizio, c’era ancora una sola persona nella sala. Arrivò l’ora del seminario e non si presentò nessuno. Fu piuttosto imbarazzante. Iniziai a parlare

per una sola persona. Dopo cinque minuti, mi disse: “Ehi, tutto questo è davvero strano. Vogliamo andare a pranzare e a parlare?”.

Davvero non capivo che cosa fosse successo. Dopo aver assistito alla stessa situazione nel secondo seminario, cancellai il terzo. Qualcuno mi suggerì: “Ehi, per il prossimo seminario fa’ pagare 50 dollari a persona per iscriversi. Dì loro che riceveranno più di 50 dollari di materiale gratuito, ma falli pagare”.

Ero riluttante perfino a provare. Pensai che se non erano venuti gratis, di certo non sarebbero venuti a pagamento. Tuttavia, seguii il consiglio, e al seminario avevo dieci persone, ognuna delle quali aveva pagato 50 dollari.

CHE COSA??? E non importa che il numero dei presenti fosse più piccolo degli iscritti iniziali. Quello che importava era che i dieci partecipanti avevano pagato per il privilegio di venire ad ascoltare.

Più tardi, parlai con l’amico che mi aveva suggerito di prevedere una somma per la partecipazione al seminario, e mi spiegò che quando la gente paga, anche una somma modica, quello che si offre assume un valore. Se qualcuno si iscrive e paga, ma poi non partecipa, perde 50 dollari. Questo si trasforma in un potente incentivo a partecipare.

Quando ero agli inizi della mia carriera di ingegnere sociale, non sapevo nulla di cosa significasse, davvero, offrire qualcosa gratuitamente. Ricevevo offerte per tenere discorsi in tutto il mondo, ma non chiedevo nulla in cambio. Scoprii mio malgrado che molto spesso le persone si cancellano o non si presentano.

Una mia amica, Ping Look, mi disse di smettere con questa politica e di iniziare ad addebitare un importo fisso. Ero molto riluttante ad ascoltarla, ma, riflettendo sulla mia precedente esperienza, decisi di provare.

Sorprendentemente, le persone erano più che disposte a pagare un importo elevato. Sembravano anche apprezzarmi di più. Questo

cambiò il modo in cui condussi i miei affari, e da quel momento in poi non feci più nulla gratis.

La morale di questa lunga storia? Non pensate che qualcuno apprezzi il fatto che regaliate il vostro talento. Non funziona così. Potete trovare il giusto equilibrio: offrire un servizio di alto livello con uno sconto o offrire un contratto di tre mesi abbuonando un mese. Cercate di essere creativi in termini di importi, ma sappiate che lavorare gratis non fa altro che svalutare il vostro talento.

Siate rapidi nei fallimenti e pronti a passare ad altro

Se incontro un potenziale cliente che è riluttante ad assumermi, gli propongo di iniziare con uno *spear-phishing* su una persona di alto livello presente in azienda, per dimostrargli quanto possa essere efficace il mio lavoro. Di solito quando il rappresentante dell'azienda vede il pericolo e il beneficio, diventa pronto a investire un budget per questi tipi di servizi. Un piccolo incarico spesso è sufficiente per spuntare ulteriori contratti con un'azienda. Ma a volte questo non è sufficiente, e un'azienda non ha intenzione di impegnarsi in ulteriori servizi di ingegneria sociale.

Se pensate di non poter fare nulla per convincere un'azienda che potete aiutare, che cosa dovreste fare? Andarvene. È molto meglio essere rapidi nei fallimenti e pronti a passare ad altro che provare a far entrare un piolo quadrato in un buco rotondo.

Se un'azienda non vede la necessità di considerare l'ingegneria sociale nell'ambito della sua politica di sicurezza, probabilmente non vorrà i vostri servigi. Sentiranno che è inutile lavorare con voi.

Ho avuto un cliente con il quale ho lavorato per quattro anni. Quando iniziai con questa società, era quasi il cliente perfetto. Avevo uno straordinario contatto, una persona rara. Il programma ebbe un tale successo che il cliente vide enormi cambiamenti. Un giorno al nostro

contatto interno, una donna, che gestiva il programma, venne offerto un lavoro presso un'azienda molto più grande, che voleva che gestisse il suo programma di sicurezza. Colse al volo l'occasione e poi capii il perché. Al suo posto venne assunta un'altra donna.

Dal primo giorno di lavoro, le cose non funzionarono. Si offendeva facilmente, prendeva le cose in modo troppo personale, non era disposta a correre rischi e non voleva che il programma fosse approfondito come prima. Di conseguenza, il programma fallì. Le persone tornarono ai loro vecchi modi e, sebbene le statistiche sul *phishing* sembrassero ancora fantastiche sulla carta, il programma era stagnante.

Sei mesi prima di lasciarli, avevo detto al mio team che li avremmo persi come clienti: ero sicuro che sarebbe accaduto. Era solo il secondo cliente che perdevo in questo modo, ma penso che sia stato meglio così. Non volevano indirizzare il programma là dove aveva bisogno di andare, e la cosa era frustrante, sia per loro sia per noi.

Avendo solo un certo numero di ore in un giorno e di clienti gestibili, preferisco dedicarmi a clienti che vogliono vedere un cambiamento. Non abbiate paura di rinunciare a un'offerta se è palesemente inappropriata.

Quanto dovrei farmi pagare?

Sento spesso questa domanda, ma è qualcosa che non mi sembra il caso di mettere in un libro, perché la risposta non è facile, né univoca. Tuttavia, dal momento che è una domanda molto popolare, cercherò di trattare questo argomento come meglio posso.

In primo luogo, dovete capire quale tariffa oraria è possibile addebitare come consulenti. Eseguite una piccola ricerca e trovate siti che forniscono suggerimenti sugli importi addebitabili nel campo della sicurezza.

La tariffa dipende da diversi fattori: anni di esperienza, competenza nel settore, notorietà dell'azienda e servizi offerti.

Per semplificare le cose, diciamo che la tariffa dovrebbe essere di 100 dollari all'ora. Esamino le mie tariffe decidendo (in base all'esperienza) che il *phishing* di 1000 e-mail al mese mi richiederà 20 ore al mese. Ogni settimana dedico 3 ore all'OSINT e 7 ore ai report, il che significa che investirò un totale di 30 ore al mese. Il mio calcolo della tariffa sarà simile a:

30 ore al mese × 100 $ all'ora × 12 mesi = 36.000 $ per un contratto annuale

Questa non è una regola rigida. È solo il metodo che uso io per valutare il prezzo del mio lavoro. Posso cambiare la tariffa in base a cose come:

- le dimensioni dell'azienda;
- la sottoscrizione di contratti pluriennali;
- quanto mi piace il cliente (molto soggettivo).

Il punto è che il calcolo precedente può aiutarvi a capire la vostra tariffa, ma potrebbe non essere esatto. Ma almeno vi fornirà indicazioni iniziali.

NOTA

Queste sono solo alcune delle domande che mi vengono poste più spesso. Ce ne sono molte altre: troppe per poterle inserire in un libro. Prometto che se mi scriverete su `www.social-engineer.com/contact-us/`, farò del mio meglio per rispondervi o per aiutarvi a trovare una risposta.

Riepilogo

Ho letto un report in cui si diceva che solo una minoranza delle aziende fornisce una vera formazione sulla consapevolezza del *phishing* attraverso campagne mensili.

Se solo una piccola percentuale di aziende (negli Stati Uniti) sta fornendo formazione e la mia azienda è cresciuta del 300% negli ultimi tre anni, che cosa succederà quando il 20%, il 30% o il 50% delle aziende statunitensi inizieranno attivamente la formazione?

Il fatto è che c'è un enorme bisogno di professionisti di qualità nel campo del *pen-testing* e dell'ingegneria sociale. Non posso fare tutto il lavoro da solo, quindi vorrei aiutare quante più persone possibili per consentire loro di fornire i migliori servizi dei quali tutte le aziende hanno bisogno.

Non credo che esisterà un tempo in cui gli esseri umani non lavoreranno più. Di conseguenza, la vulnerabilità umana esisterà sempre. Inoltre, tutti dobbiamo fare i conti con una serie infinita di attacchi ai nostri centri dell'empatia, della paura e del ragionamento. Questi attacchi possono logorarci e farci prendere decisioni sbagliate.

Avremo sempre bisogno di professionisti nel campo dell'ingegneria sociale per aiutare le aziende a proteggersi da questi attacchi. Penso che ci sarà un enorme spazio per l'intelligenza artificiale e per le tecnologie volte a respingere questi attacchi, ma non ci sarà mai un momento in cui non avremo più bisogno di esseri umani per aiutare altri esseri umani.

Forse state leggendo questo libro perché volete entrare nel business dell'ingegneria sociale. O forse lo state leggendo, da professionisti, per trovare nuovi trucchi e suggerimenti. E ci possono essere molti altri motivi per cui potreste aver scelto questo libro. Per uno di questi motivi, dovreste considerare il prossimo capitolo, che vi aiuterà a preparare un MAPP.

Avete un MAPP?

> Credo molto nel concentrarsi sul possibile, lasciar perdere l'impossibile e non sprecare energie su quel che non merita.
> - *Josh Citron*

Sento che un libro incentrato sulla formazione di un professionista dell'ingegneria sociale non sarebbe completo senza questo capitolo. Potete combinare tutti gli attacchi, gli aspetti psicologici, fisiologici e anche la redazione di report, ma senza un *MAPP*, al vostro puzzle mancherà un pezzo gigantesco. Che cos'è un MAPP? MAPP sta per *Mitigation and Prevention Plan*.

Perché avete bisogno di un piano di mitigazione e prevenzione? Come potete aiutare la vostra azienda o i vostri clienti a svilupparne uno? Che cosa potete mitigare e pianificare negli attacchi di ingegneria sociale? Questo capitolo risponde proprio a queste domande.

Quando iniziai a guadagnare slancio con i miei clienti, mi resi conto di qualcosa di importante. Il mio scopo era veramente strano: essere così bravo da diventare disoccupato; dovevo aiutare i miei clienti a imparare a difendersi dagli attacchi di ingegneria sociale al punto che alla fine non avrebbero più avuto bisogno di me.

Conoscete quelle società di *pen-testing* che pubblicizzano un tasso di successi del 100%? Beh, quanto è demoralizzante per un cliente staccarvi l'assegno sapendo che non migliorerà mai. O che, per quanto possano migliorare, l'ingegnere sociale vincerà sempre? Il messaggio che si dà è che non ha alcuna speranza. Niente di quello che potrà fare

riuscirà mai a coprire tutte le falle dei loro sistemi di sicurezza. Alla fine, è davvero logico che i clienti dicano: “Perché, allora, dovremmo cercare di proteggerci?”.

Come in una sorta di illuminazione, decisi che dovevo aiutare i miei clienti a pianificare una mitigazione degli attacchi e a diventare così bravi a sventare questi miei attacchi che alla fine tutto ciò di cui avrebbero avuto bisogno era pura manutenzione. Se, come me, siete professionisti dell’ingegneria sociale, avete proprio la necessità di leggere questo capitolo, per avere successo. Se siete un’azienda, questo capitolo vi aiuterà a pianificare il vostro MAPP.

La cosa avvenne quando capii che dovevo occuparmi della mia salute. Avevo provato un sacco di soluzioni, da solo, ma tutte fallirono miseramente. Nella comunità degli hacker *white hat* (i “buoni”), qualcuno aveva apportato drastici cambiamenti. Ne parlai con uno di loro e chiesi come aveva fatto e mi mise in contatto con un personaggio di nome Josh Citron.

Josh volle fare una videochat per la nostra prima conversazione. Io davvero non volevo: lo immaginavo in forma smagliante e l’ultima cosa che volevo fare era una videochat di me, grande e grosso, con lui. A peggiorare le cose, cercai su Internet, e non fu troppo difficile trovare qualche sua foto. È una specie di culturista, in grado di sollevare piccoli veicoli e correre per chilometri.

Ora, immaginate se, nel nostro primo incontro, le sue prime parole fossero state: “Ok, Chris. Ecco il discorso. Se fai tutto quello che ti dico, ascolti ogni consiglio senza imbrogliare e continui a pagarmi… be’, non ce la farai mai, comunque. Rimarrai grasso e probabilmente non diventerai più forte, mai. E ora, iniziamo!”. Probabilmente avrei guardato Josh come un *pazzo*! E se mi avesse guardato con sdegno in quella videochat e mi avesse trattato male perché tutto quello che

vedeva era una “palla di lardo”, probabilmente non avrei più voluto sentirne parlare.

Al contrario, Josh mi disse che se avessi fatto quello che mi diceva, avrei notato dei cambiamenti graduali e, quando avessi raggiunto i miei obiettivi, saremmo passati a un programma di mantenimento. Poiché mi trattava con dignità e rispetto, mi sentii pronto a impegnarmi.

Josh mi aiutò a creare un MAPP che avrebbe mitigato il rischio delle cattive abitudini e avrebbe costruito abitudini migliori e più salutari. E non ci fu niente di terribile, come una dieta radicale che eliminasse ogni cosa che avesse un sapore in cambio di insalate e tristezza. Ho apportato alcune modifiche alle abitudini, migliorato i miei processi decisionali e acquisito nuove conoscenze per poter prendere la miglior decisione possibile in tutte le situazioni.

Questo processo può essere applicato direttamente anche allo sviluppo di un MAPP nel campo dell’ingegneria sociale e della sicurezza. Ho sviluppato quattro passaggi che, se seguiti, daranno come risultato questo MAPP, con tutti i vantaggi che ne derivano.

- Passaggio 1 – Imparate a identificare gli attacchi di ingegneria sociale.
- Passaggio 2 – Sviluppate politiche attuabili e realistiche.
- Passaggio 3 – Svolgete regolari controlli in tempo reale.
- Passaggio 4 – Implementate efficaci programmi di sensibilizzazione sulla sicurezza.

Ecco che cosa vi prometto: seguendo questa procedura, *noterete* nella vostra popolazione i cambiamenti che desiderate. Non accadrà tutto in una volta. In realtà, a seconda di elementi come il *turnover*, la cultura aziendale e così via, la cosa potrebbe richiedere un paio di anni o più, ma funziona.

Siete pronti per iniziare?

Passaggio 1 – Imparate a identificare gli attacchi di ingegneria sociale

Quando ero giovane, volevo imparare a combattere, così mi iscrissi a un corso di arti marziali. Ricordo il giorno che incontrai il mio allenatore. Come test, mi chiese di bloccare i pugni che mi tirava. Mi sembrò che, dal nulla, materializzasse dei pugni indirizzati a ogni parte della mia testa e del mio corpo. Non riuscii a bloccare un singolo colpo.

Per fortuna, in realtà non mi colpì – mi toccò appena, ma sentii ogni singolo colpo. Dopo un anno, ero in grado di bloccare la maggior parte dei colpi che mi arrivavano. Quello che era cambiato era che avevo imparato a identificare l'aspetto di un attacco, e quindi avevo imparato a reagirgli.

Il passaggio 1 sembra auto-esplicativo, ma non lo è. Quante persone nella vostra azienda pensate siano in grado di definire gli attacchi di *phishing*, *vishing*, *SMiShing* e impersonazione? Quante persone pensate si rendano conto di quanto pericoloso possa essere il nome del vostro smaltitore di rifiuti nelle mani di un aggressore? Quante persone nella popolazione dei dipendenti pensate sappiano che cosa sono il *malware*, il *ransomware* o un *trojan*?

Non fraintendetemi: non voglio dire che ogni dipendente debba essere un Bruce Lee dell'ingegneria sociale, ma che ogni persona deve almeno capire contro che cosa si trova a combattere. Questo primo passo per comprendere quali sono gli attacchi, quale aspetto potrebbero avere e dove possono mirare è vitale.

Potreste chiedervi: "Ma come facciamo?". È una gran bella domanda. Immaginate se fossi entrato in quel *dojo* e l'allenatore mi avesse detto: "Ok, vuoi imparare a combattere? Sali sulle stuoie con

questo esperto di quinto grado che combatte da vent'anni e cavatela". Sarei fuggito dal *dojo*. E se mi avesse messo davanti a un computer per venti minuti e mi avesse mostrato un video di addestramento sulle arti marziali e poi mi avesse messo sul ring, avrei avuto una reazione simile. Non vi allarmate. Non sto dicendo che la formazione al computer sia del tutto inutile, ma impiegarla come elemento principale di un programma di allenamento è un errore. I video hanno un ruolo specifico, di cui parlo più avanti in questo capitolo.

Quello che ricevetti dal mio allenatore – e quello che dovreste aspettarvi da un esperto di ingegneria sociale – fu imparare a riconoscere e parare un "colpo" di ingegneria sociale. Mi diede un allenamento adeguato in termini di postura e posizione del corpo e poi mi insegnò a sferrare colpi pesanti e colpi leggeri. Quando l'allenatore sentì che ero pronto, mi scontrai con una persona che non voleva uccidermi, ma solo aiutarmi a imparare.

Questo primo passo per imparare a identificare e conoscere questi attacchi metterà la vostra squadra in grande vantaggio rispetto a una persona media. Aiuterà la popolazione dei dipendenti a comprendere il valore delle informazioni in loro possesso – che una semplice e-mail può essere utilizzata per violare un'intera azienda; che una telefonata apparentemente casuale può essere utilizzata per ottenere password e altri dettagli riservati; che se il loro telefono viene violato, può essere utilizzato per condurre un attacco alla rete domestica e di lavoro; e che solo perché una persona è sorridente e cordiale, questo non significa che si debba ignorare la politica dei badge.

Aiutare la popolazione dei dipendenti a comprendere i possibili attacchi può informarli quanto basta per renderli più consapevoli. Poiché questo è il mio lavoro quotidiano, a volte dimentico che non tutti sanno dell'esistenza di questo genere di attacchi.

Ero con un amico che mi raccontava di come sua nonna avesse donato una grossa somma di denaro tramite MoneyGram solo perché qualcuno aveva finto di essere suo nipote e di aver bisogno di soldi per la cauzione. Dissi: “Oh, no. La *truffa della nonna*!”.

Chiese: “La che cosa?”.

Gli spiegai come questo tipo di attacco è fin troppo comune. La sua reazione fu di rabbia e mi disse: “Ma se tu sai che esistono queste cose, perché non avverti gli amici?”.

Aveva ragione. Presumevo che tutti sapessero di queste cose, ma non è così. Un mio avvertimento li avrebbe salvati? Forse no, ma la lezione era comunque valida.

Ripensate alla mia esperienza con l’allenatore nutrizionale e di attività fisica Josh. Dopo quella video-chat iniziale, dovetti spedirgli ogni settimana il mio diario giornaliero degli impegni, anche nei giorni di cedimento. Sapete che cosa non fece mai? Rimproverarmi come un bambino, incolparmi, abbandonarmi. Invece mi disse: “Va bene, faremo meglio questa settimana”.

Applicate questo atteggiamento e imparate a usarlo. Non supponete che la conoscenza di questi attacchi sia così ovvia. Se qualcuno non ne è a conoscenza, questo non significa sia stupido, ingenuo e che meriti di essere colpito. Al contrario, esercitate l’empatia e pensate: “Va bene, possiamo fare meglio la prossima volta. Come possiamo farlo?”. Questo vi aiuterà davvero a compiere il passo successivo con maggior successo.

Passaggio 2 – Adottate politiche attuabili e realistiche

Una delle cose in cui Josh mi aiutò fu capire quale fosse il vero concetto di una porzione di cibo. Mi diceva quante proteine,

carboidrati e grassi avrei dovuto assumere in un giorno e lasciava a me il compito di prendere le decisioni. Quindi, potevo anche assumerle tutte in un unico pasto, ma mi sarei sentito parecchio affamato più tardi.

Josh mi insegnò anche a non fare affidamento sugli occhi. Una volta mi disse di mettere su un piatto quelle che pensavo fossero le giuste quantità di diversi cibi. Poi dovevo pesarlo e… wow, sbagliavo sempre, in eccesso. Questa regola, o "politica", mi aiutò a imparare una lezione importante sul modo in cui cambiare le mie abitudini decisionali.

Nel mondo della sicurezza, *politica* può sembrare una parolaccia. La maggior parte della gente detesta creare politiche, farle rispettare e/o doverle seguire. Scoprii che le politiche spesso hanno una cattiva reputazione perché non hanno senso o non sono state chiarite in termini di intenti. Altre volte sono così restrittive che sembrano volte a creare un rapporto conflittuale con la popolazione.

Trovare un equilibrio non è cosa facile, ma è essenziale riuscire a creare un ambiente sicuro e dotato di una cultura di consapevolezza della sicurezza.

Che cosa rende "buona" una politica? Che cosa non la rende troppo restrittiva e tuttavia attuabile e realistica? Ci sono alcuni aspetti di una buona politica che vi aiuteranno a costruire solide regole per migliorare la situazione.

Tenete i ragionamenti fuori dalle politiche

Troppe volte le politiche sono così vaghe e generali che possono obbligare a troppi ragionamenti o costringono a prendere decisioni non avendo istruito le persone sul genere di attacchi che potrebbero dover affrontare. Ora, non sto dicendo che dovreste considerare i dipendenti

come perfetti sprovveduti. Considerate solo che meno tempo occorre spendere a ragionare su qualcosa, e meglio è. “Semplice è meglio”.

Un esempio: la mia azienda ha compiuto un certo lavoro di *vishing* per una grande istituzione finanziaria e oltre l’80% delle volte siamo riusciti a ottenere dettagli molto personali sugli obiettivi. Abbiamo giocato sulla loro empatia e fiducia.

A onor del vero, in questa azienda di credito c’erano davvero belle persone e non volevamo che cambiassero. Che pessimo consiglio sarebbe dire: “Rendete i vostri dipendenti più paranoici e infidi”? Quello che fece questa azienda fu sbalorditivo. Crearono una politica reale e attuabile: “Non siete autorizzati a fornire alcuna informazione agli utenti non autenticati”.

E non si fermarono qui. Definirono sia le informazioni riservate sia il modo in cui autenticare correttamente gli utenti. Poi fecero un’altra cosa che fece un’enorme differenza: disabilitarono la capacità dei dipendenti di superare questa prima fase se le loro domande non avessero ricevuto una risposta adeguata. Un esempio…

Attaccante: Buongiorno. Sono Joe Smith. Ho bisogno di alcune informazioni sul mio account. Ho il mio numero di conto, ma ho dimenticato la mia password. Mi potete aiutare per favore?

Incaricato: Certamente. Ma prima, Joe, ho bisogno che lei verifichi la sua identità. Può per favore…”.

L’agente era incaricato di porre una serie di domande, poi doveva inserire le risposte nelle caselle di testo e solo se le risposte erano corrette poteva procedere.

Oltre a questa politica, istruii il personale e riprovammo. Quando il personale era armato di questa ottima politica e di solide basi di conoscenza, era invalicabile. Erano ancora persone gentili (almeno una decina di volte l’incaricato era veramente dispiaciuto di non poterci “aiutare” e ha cercato in tutti i modi di farlo, ma senza successo).

Un’attenta politica e un’adeguata educazione hanno permesso agli incaricati di proteggere l’azienda senza dover prendere decisioni.

Rimuovete la possibilità di sfruttare l’empatia

Questa linea guida non significa “togliere l’empatia”. Non lo suggerirei mai. Tuttavia, dovete evitare che l’empatia offra a un estraneo la possibilità di aggirare le regole.

Ho una cara amica nel Regno Unito: Sharon Conheady. Mentre era al termine della gravidanza, compì un lavoro di ingegneria sociale. Sfruttò la sua gravidanza per suscitare empatia.

Sharon riempì una grande scatola con oggetti dall’aspetto pesante. Mentre si dirigeva verso la porta, faticando a portare la scatola, vari uomini corsero in suo aiuto. Non solo portarono la scatola nella sala server per lei, ma dimenticarono completamente di controllare il suo badge. Dopo tutto, una donna incinta non può certo essere una criminale, giusto? Sbagliato.

Questi uomini hanno fatto la cosa giusta nell’aiutare una donna incinta. Non vorremmo mai impedire alle persone di mostrare questo tipo di sensibilità. L’azienda istituì quindi una politica per istruire lo staff anche sull’aiuto ai bisognosi: prima controllare il badge e solo dopo scortare la persona nel punto interno richiesto.

Dire semplicemente “Controllate tutti i badge” non è sufficiente, perché quando entra in gioco l’empatia, la buona vecchia amigdala spegne i centri di ragionamento e le persone iniziano a prendere decisioni basate unicamente sull’emotività. Un’adeguata educazione, e l’impiego di promemoria e istruzioni chiare aiuteranno a evitare la sospensione di ragionamento prodotta dall’empatia e garantiranno che le operazioni vengano sempre svolte in sicurezza.

Rendete le politiche realistiche e attuabili

Ho letto con i miei occhi politiche che dicevano: “Non fate clic su link pericolosi”. Come vi sembra? Se state dicendo: “Sì, è ottima, penso di usarla”, vi chiedo di mettere giù questo libro e di usarlo per prendervi a schiaffi.

Ora che avete fatto, continuate a leggere.

Questo tipo di politica è dannosa, perché non è abbastanza dettagliata. Come fa un dipendente a sapere che un certo link è pericoloso? Perché mai un link `supporto-microsoft.com` non dovrebbe appartenere a Microsoft?

La politica non include una clausola “Se”. Se fate clic sul link, che cosa succede? Questa politica richiede un’ulteriore parte che indichi qualcosa come: “Se un messaggio di posta elettronica, una telefonata o una persona dal vivo interagiscono con voi e ritenete che qualcosa non sia corretto, segnalate l’accaduto a `xxxxxxx@company.com`”.

Ma c’è di più! Ora dovete dire ai vostri dipendenti *come* segnalarlo correttamente, inoltrando l’e-mail, inviando informazioni sul telefono del chiamante e così via. Quali dettagli devono essere segnalati? Quali sono le conseguenze per la segnalazione?

Una politica realistica aiuta il dipendente a considerare la situazione da tutte le angolazioni, senza ambiguità. Lavorando con un’azienda, ho contribuito a sviluppare un progetto educativo basato su una nuova politica anti-*phishing*. Andò più o meno così:

Il phishing è una minaccia per la nostra azienda e anche per ognuno di voi. I malintenzionati cercheranno di estorcervi informazioni attraverso attacchi basati su e-mail. Possono utilizzare documenti dannosi, con le estensioni EXE, PDF, XLS o DOC. Oppure possono inviarvi link a siti web che non sono quelli che sembrano e contengono malware o altri programmi pericolosi.

Se ricevete un’e-mail da qualsiasi fonte di cui non siete sicuri, prima di eseguire una qualsiasi altra azione, segnalatela a `abuse@company.com` *facendo clic su Inoltra nella schermata e indicando come destinatario (campo A:) tale indirizzo.*

Un incaricato vi risponderà entro 24 ore per dirvi se quell’e-mail è sicura.

Se avete fatto clic su un link o avete aperto un allegato che temete sia dannoso, non è troppo tardi. Segnalate l’e-mail al dipartimento abusi.

Naturalmente, c’erano molte più informazioni nella politica e anche dei link alla formazione interna e ad altre risorse. Ma avete afferrato il concetto. Una buona politica è realistica e fornisce indicazioni chiare sulle azioni da intraprendere e da non intraprendere.

Tornando alla mia storia sulle arti marziali, è come se l’allenatore che mi mostra quale postura tenere, come tenere le braccia e le mani e che cosa guardare mi spiegasse anche *perché* ognuna di queste cose è importante. Una buona politica aiuta una persona a sapere non solo il *cosa*, ma anche il *perché*. Se ben realizzata, alla fine la popolazione dei dipendenti reagirà alle situazioni con una memoria muscolare.

E a questo punto, sarete pronti a passare all’applicazione del terzo passo.

Passaggio 3 – Svolgete regolari controlli in tempo reale

Ogni settimana, mando un foglio a Josh che descrive apporti calorici, esercizio fisico, sonno, peso e un sacco di altri dettagli. Ogni giorno, registro questi dati, sapendo che li leggerà subito. Questo controllo in tempo reale mi tiene sulla rotta giusta. Mi aiuta anche a

tenere a mente l’obiettivo e avvisa subito Josh di eventuali incongruenze o problemi.

Una volta, in un periodo in cui viaggiavo molto, smisi di segnare i dati e cercai di inventarli. Quando Josh vide che i dati e le cifre non coincidevano, mi pose una serie di domande; arrivammo al fondo del problema e lavorammo per correggerlo e andare avanti. Questo controllo di “realtà vera” fece la differenza tra un programma efficace e un programma destinato al fallimento.

Questo è esattamente il significato del Passaggio 3 nel vostro programma di sicurezza. Avete istruito il personale sugli attacchi che devono aspettarsi. L’avete addestrato su che cosa fare quando si verificano questi attacchi. Avete impostato i criteri per aiutarlo a prendere la migliore decisione possibile quando si imbatte in un attacco. Ora, quanto ha recepito tutte queste informazioni? La memoria muscolare si attiva quando i dipendenti vengono messi alla prova? L’unico modo per scoprirlo è scegliere il giusto consulente per la sicurezza e andare sul ring insieme.

La scelta del consulente è importante. Se siete ingegneri sociali e sperate di diventare clienti di un’azienda, è importante per voi sapere di che cosa ha davvero bisogno un’azienda davvero intelligente. Ricordate, lo scopo non è solo quello di essere sempre al 100% o di aver impiegato le tecniche d’attacco più sorprendenti. Dovete usare le vostre conoscenze e applicarle per aiutare l’azienda a migliorare.

Come si può sapere se il partner che state considerando è all’altezza? Ecco alcuni suggerimenti.

- *Ponete buone domande* – Non abbiate paura di chiedere conto dei posti di lavoro precedenti o come l’azienda desidera che venga gestita una certa situazione. La risposta che ottenete è in linea con i vostri valori?

  Per esempio, stavo facendo una consulenza per un’azienda e mi

chiesero come suggerivo di trattare quei dipendenti che fallivano nei nostri test. La mia risposta fu onesta e semplice: dissi loro che era essenziale educare le persone su quello che avevano fatto di sbagliato, rimetterle alla prova dopo tale educazione e poi determinare se esse rappresentassero una minaccia per l'azienda. Licenziare sistematicamente coloro che falliscono i test era una pessima idea. Quella mia risposta era in linea con la loro cultura aziendale: andammo d'accordo. Durante gli incontri preliminare con le aziende che mi assumono per lavori di ingegneria sociale, spesso mi viene chiesto di specificare gli scenari d'attacco che avevo in mente di utilizzare. Di solito dico loro che ho bisogno di fare delle attività di OSINT prima di poter sviluppare qualsiasi ipotesi, ma poi suggerisco loro qualcosa che ho svolto in un'azienda simile, a titolo di esempio.

Se siete un'azienda alla ricerca di un partner, andate alla riunione con buone domande in mente; e se siete il potenziale partner, munitevi di buone risposte.

- *Abbiate referenze qualificate* – Ottenere dalle aziende il permesso di utilizzare il loro nome come referenza può essere difficile, perché molti clienti non vogliono svelare i servizi di ingegneria sociale che hanno richiesto. Molte grandi organizzazioni sono state violate proprio dai loro fornitori. Nel mio caso, ho tre o quattro clienti che mi hanno dato il permesso di usarli come riferimenti per i potenziali clienti. Se potete ottenere referenze, penso che questa sia una parte molto importante del vostro puzzle. Aiuta il potenziale cliente a capire com'è lavorare con l'azienda che intendono incaricare.

  Tenete però presente che nessuno vi darà come referenza un cliente insoddisfatto. Lo scopo è solo quello di dare un'occhiata al

modo in cui l’azienda lavora con i suoi clienti e alla qualità che offre.

- *Definite chiaramente le regole* – Per un cliente, niente è peggio che pensare che un *pen-test* metterà alla prova un solo livello e poi scoprire che l’incaricato ha lavorato su cinque strati e spiegare al capo che cosa è successo. Il modo migliore per assicurarsi che non ci siano problemi è disporre di un insieme di regole che definiscano chiaramente il test, e poi non superare nessun limite. Questo insieme di regole ben definite equivale alle protezioni indossate dai pugili durante gli incontri.

Come clienti alla ricerca di un *pen-tester*, potreste avere in mente alcuni requisiti, che vi piacerebbe applicare alla scelta del fornitore, ma questi tre sono un buon punto di partenza per assicurarvi di scegliere il miglior partner con il quale confrontarvi.

Una volta che avrete scelto un partner, iniziate a svolgere i test e poi utilizzate i risultati per determinare quali servizi vi servono e con quale frequenza è il caso di ripetere i test. Un buon partner saprà aiutarvi a determinare quello che è necessario per voi e sarà anche onesto a proposito delle vostre esigenze (senza basare tutto solo sui guadagni).

Alcuni servizi danno il loro meglio se svolti mensilmente, come i test di *phishing*. Altri funzionano meglio se vengono svolti annualmente o semestralmente, come i test di penetrazione. Non esiste una soluzione *passepartout*: dipende in gran parte da quali sono le vostre esigenze e da come volete raggiungere gli obiettivi che desiderate.

Un altro fattore è l’efficacia con la quale si applica il Passaggio 4.

Passaggio 4 – Implementate efficaci programmi di

sensibilizzazione sulla sicurezza

Josh pubblica video di se stesso mentre esegue determinati esercizi, corre e svolge altre attività salutari. I video che pubblica sono piccole lezioni che aiutano a chiarire il suo programma a coloro che lo seguono. È un po' come svolgere dei programmi di consapevolezza della sicurezza.

Forse starete pensando: "Non hai appena parlato della consapevolezza della sicurezza? Perché si ripete?". Ebbene, no, non è così. Tutti i passaggi precedenti fanno parte del vostro programma di sensibilizzazione alla sicurezza, ma questo passaggio riguarda in particolare l'applicazione dei tre passaggi precedenti per creare programmi di sensibilizzazione realistici e applicabili.

Lasciate che vi racconti un'altra storia a supporto di questo punto. Ho avuto un cliente per il quale conducemmo una vera raffica di test. Il mio team di ingegneria sociale dedicò molto tempo all'OSINT, poi eseguì attacchi di *vishing* e di *phishing*.

Scoprimmo che con gli attacchi di *vishing*, i dipendenti avevano una capacità quasi innaturale di fermarci. Rifiutavano di darci i nomi, non ci davano gli interni e non confermavano neppure la presenza o assenza di qualcuno in ufficio. Ma rispetto agli attacchi di *phishing* riscontrammo alcune gravi vulnerabilità.

Considerammo quello che stavano facendo e scoprimmo che avevano un solido piano di educazione contro il *vishing* e il *phishing*, ma che le nozioni sul *vishing* trattavano solo le basi. Insegnavano ai dipendenti gli attacchi, offrivano loro scenari realistici con politiche effettivamente attuabili e li mettevano alla prova regolarmente in un ambiente sicuro.

Al contrario, il loro programma contro il *phishing* consisteva solo di alcuni video all'anno. Avrei potuto vendere loro un programma di formazione sul *vishing* e sul *phishing* nuovo di zecca, ma non ce n'era

bisogno. Lavorai con loro su un programma di *phishing* e li incoraggiai a non cambiare *nulla* del loro programma sul *vishing*. In altre parole, li aiutai ad adattare il loro programma di sensibilizzazione alla loro specifica situazione, sulla base di quello che già avevano fatto nei precedenti tre passaggi.

Il prossimo cliente *non sarà* uguale, e sarà differente da quello dopo e da quello dopo ancora – ognuno sarà unico. Ecco perché per creare programmi applicabili occorre un lavoro serio, che non può essere demandato a modelli o approcci modulari alla sicurezza.

Adattando i programmi di sensibilizzazione alla sicurezza alle specifiche esigenze del vostro cliente, potete aiutare i loro dipendenti a imparare non solo che cosa non fare, ma anche che cosa dovrebbero fare quando e se succede qualcosa di brutto. Una consapevolezza della sicurezza veramente applicabile aiuta i dipendenti a comprendere e supportare le politiche e i programmi stabiliti.

Ecco un altro esempio che deriva dalla mia esperienza con gli allenamenti di Josh. Quando Josh mi dice di ridurre un certo tipo di alimento o di aumentare una certa attività, posso sostenere pienamente questi cambiamenti, anche se non li gradisco. Perché?

- Vedo l’effetto positivo di questi cambiamenti.
- Josh mi spiega bene che cosa sta facendo, e quindi il significato delle sue richieste mi è chiaro.
- Mi offre suggerimenti utili per avere successo quando devo affrontare delle sfide.
- Quando non ci riesco (capita), Josh non mi sgrida e non mi tratta da svogliato (che è quello che sento di meritarmi). Mi tratta come una persona che ha bisogno di un incentivo e cerca di trovare un piano più alla mia portata.

Questo programma mi ha aiutato a migliorare la mia salute e un piano di sicurezza applicabile può fare lo stesso per la vostra sicurezza.

Non supponete che, per il fatto che l'avete compreso, tutti in azienda l'abbiano compreso. Potrebbero aver bisogno di un po' più di tempo per riuscirci.

Per ricapitolare

Ripensate ai tempi bui, prima che lo smartphone avesse tutte le funzionalità conosciute dall'uomo, inclusa una mappa del mondo intero con localizzazione GPS. Ricordate quei tempi? Io sì.

Ricordo quando si usavano le mappe cartacee per le indicazioni stradali. Proprio come nel Passaggio 1 – sull'imparare a identificare gli attacchi – avevo un punto di partenza sulla mia mappa. Cercavo il percorso più veloce evitando le strade a pedaggio e le strade secondarie, il tutto mentre mi avvicinavo sempre più alla destinazione.

Poi, come nel Passaggio 2 – sull'adozione di politiche attuabili e realistiche – mi assicuravo di rimanere sulle vie di grande traffico, per massimizzare la velocità.

Quindi, come nel Passaggio 3 – sui regolari controlli della situazione reale – verificavo periodicamente la strada sulla quale mi trovavo e la confrontavo con la mappa per assicurarmi di non essermi sbagliato.

Infine, l'ultimo pezzo è il programma di sensibilizzazione (Passaggio 4), che è proprio come l'elemento finale dell'utilizzo di una mappa; arrivavo dal punto A al punto B in modo sicuro e nel tempo che avevo programmato.

Avere una mappa nella vita reale mi ha portato in giro per tutti gli Stati Uniti. Avere un MAPP nel vostro programma di sicurezza può fare lo stesso, aiutandovi a concepire nei dettagli il vostro piano di mitigazione e prevenzione.

Compiere un solo passo non sarà sufficiente, così come non basta avere in macchina una mappa cartacea per portarvi dal punto A al

punto B. Dovete avere un piano e poi agire per farlo funzionare.

Non posso promettervi che ognuno di voi si trasformerà nel "Josh della sicurezza", ma questi quattro passaggi vi aiuteranno a esercitare i muscoli di sicurezza in modo positivo. Il resto di questo capitolo descrive alcune altre cose che possono aiutarvi a creare il vostro MAPP.

Aggiornatevi continuamente

Supponiamo che abbiate applicato i quattro passaggi. Potete mettere un timbro fuori dalla porta con su scritto "Hacker-proof"?

Beh, certo che potete, ma solo se volete sentirvi derisi mentre verrete hackerati. In generale, seguendo questi passaggi farete in modo di non essere i "frutti più bassi della pianta" e farete sì che gli aspetti umani risultino più resistenti agli attacchi. È sempre una bella posizione, ma c'è sempre la possibilità che qualcuno in azienda cada vittima di un attacco di *phishing*, *vishing*, *SMiShing* o di un tentativo di impersonazione. Se ciò dovesse accadere, che cosa può aiutarvi a mettervi ancora più in sicurezza?

Assicuratevi di caricare tutti gli aggiornamenti sui vostri computer. Non so dirvi quante volte, durante gli audit di sicurezza di routine, ho trovato aziende che utilizzavano browser, reader per file PDF, client di posta elettronica, o anche (gasp!) sistemi operativi arretrati di tre o quattro versioni. Sono versioni contenenti un gran numero di punti vulnerabili. Mantenere aggiornati i sistemi può proteggervi da tante violazioni che possono certamente verificarsi se mantenete in rete software obsoleti.

Lo scrivo sapendo benissimo che è molto più facile a dirsi che a farsi. Mi rendo conto che potrebbero esistere sistemi "storici", *legacy*, il cui aggiornamento richiederebbe tempo, impegno e denaro. Tuttavia, ricordate che dal 2017 in media una violazione della sicurezza è

costata a ogni azienda 3,62 milioni di dollari. E questa è solo la media! Nel 2017 ci sono state alcune violazioni che hanno causato danni di 10 o anche 300 milioni di dollari.

Non sono così ingenuo da pensare che gli aggiornamenti avrebbero protetto queste aziende dalle violazioni che hanno subito, ma credo di essermi spiegato. Potete sostenere quel costo prima di una violazione (per proteggersi) oppure dopo (quando dovrete pagare per le conseguenze). Ma se la vostra idea di sicurezza somiglia a quella rappresentata nella Figura 10.1, forse è il caso di parlarne più seriamente.

Nascondere la testa *sperando* che così i predatori non ci vedano è poco serio. Decidete *quando* volete pagare: prima della violazione o dopo. Io penso sia meglio pagare prima, anche se la cosa potrebbe costare tempo, denaro e stress. Ma proteggerete i vostri clienti e la vostra reputazione e vi risparmierete l’imbarazzo.



Figura 10.1 Questa sarebbe sicurezza?

Imparate dagli errori dei vostri pari

Andate su Google, digitate le parole “violazioni della rete” (*network breaches*) e scegliete Notizie (*News*). A me ha dato il risultato che potete vedere nella Figura 10.2.

Ognuna di queste storie contiene dettagli su una violazione: come è avvenuta, che cosa l'ha causata e quale vulnerabilità è stata sfruttata (risorse umane, hardware, software o un mix queste). Comprendere gli attacchi che interessano altre società può aiutarvi a proteggere la vostra azienda.

Quando vedete che un attacco ha preso di mira un certo firewall, è tempo per verificare se avete tale firewall e se l'avete aggiornato. Quando vedete che le truffe di *phishing* basate su e-mail commerciali sono in aumento, è il momento di premunirsi, offrendo un'istruzione e politiche adeguate. Non importa quale sia la causa delle violazioni di cui avete letto, cominciate a interessarvi alle nuove minacce e confrontatele con l'infrastruttura, per scoprire se avete punti deboli.

Ci sono molte società che vendono servizi di modellazione delle minacce e potreste richiedere il loro aiuto. In caso contrario dovreste almeno iniziare a modellare da soli i rischi e determinare dove potete migliorare, solidificare e rafforzare i programmi e i protocolli, rimanendo vigili contro gli attacchi.

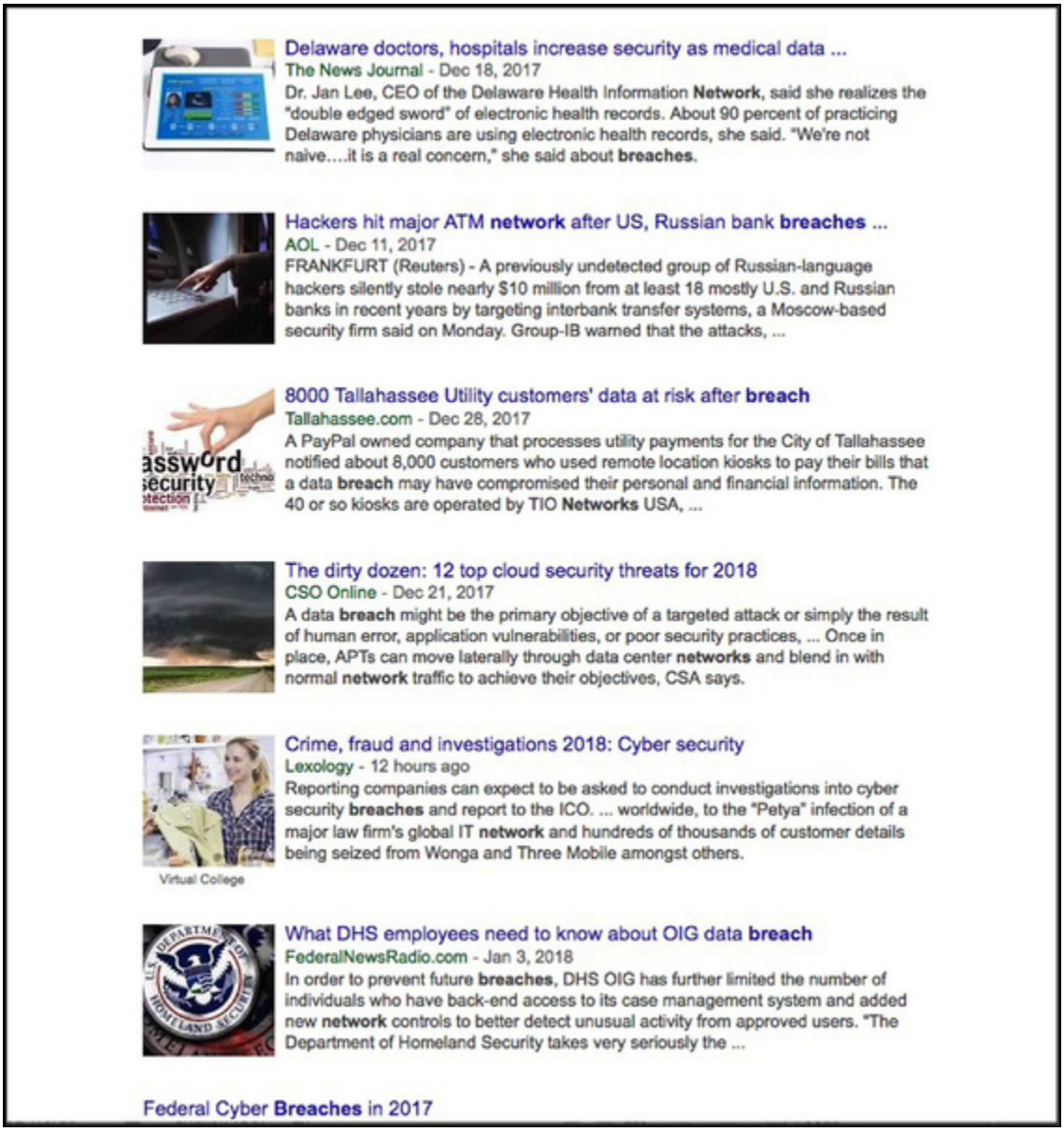


Figura 10.2 Un piccolo esempio di “cattive notizie”.

Create una cultura di consapevolezza della sicurezza

Userò di nuovo Josh e il suo piano di allenamento anche per illustrare questo punto. Dopo aver lavorato con Josh per un po’, è

diventato più facile identificare quei comportamenti e quelle situazioni che avrebbero messo a rischio i miei progressi. Per esempio, evitare di calcolare le calorie assunte durante il giorno o tentare di indovinare il peso di una porzione erano generalmente comportamenti non ottimali, che mi impedivano di conseguire i risultati sperati. D'altra parte, andare a una pizzeria all-you-can-eat e cercare di convincere me stesso a fermarmi dopo due fettine sarebbe stata una vera impresa.

Josh mi aiutò a capire che le decisioni che prendevo durante un giorno potevano aiutarmi ad adottare uno stile di vita salutare. Nessuno ha bisogno di una fiorentina da 7 etti. Meglio un filetto da 2 etti. Se voglio prendermi un dessert, devo prendere decisioni appropriate nelle altre parti della giornata, in modo da non far saltare il mio programma. E così via.

Che cosa ha a che fare tutto questo con la creazione di una cultura di consapevolezza della sicurezza nella vostra organizzazione? Tutto!

Con una formazione adeguata, promemoria e ricompense, potete creare una cultura in cui la popolazione dei dipendenti è consapevole che anche piccole decisioni possono avere effetti di lunga durata. E si renderà anche conto che le decisioni importanti possono essere devastanti, quando si compie la scelta sbagliata.

Nel mio lavoro con Josh, la ricompensa è la perdita di peso, il sentirsi meglio, avere un aspetto migliore e stare meglio. Quella ricompensa è una buona motivazione a spingermi a continuare il programma. Non tutti i dipendenti si sentiranno ricompensati per aver "colto il *phishing*" o "beccato il *vishing*". E questo non perché non si curino dell'azienda – è solo che alcune persone sono così impegnate da considerare i programmi di formazione come un male necessario ma anche uno spreco di tempo.

Saranno gli elementi più difficili da "convertire", ma la conversione è possibile. In un'azienda con la quale ho lavorato, un responsabile di

reparto mi ha confessato che odiava i test che stavamo conducendo. Di conseguenza, il suo dipartimento di 450 persone sembrava essere una delle più grandi minacce per l'azienda. Attacchi di *malware*, *phishing* e di altro tipo causavano grossi problemi in questo reparto.

Il responsabile si rese conto che il suo personale non si stava adeguando. Era frustrato e voleva adottare una politica di accuse e punizioni nei confronti dei peggiori trasgressori. Non ho mai visto questa metodologia funzionare in modo efficace: normalmente crea una relazione di reazione contro la dirigenza. In questi casi, la conformità, se si ottiene, è solo il risultato della paura, della rabbia o del risentimento. In un incontro con il cliente, chiesi di provare con un rapido gioco con il team del *call center*. Dissi che avrei mandato loro il peluche di un pesce e volevo che annunciassero che la prima persona a *non fare clic* e a *segnalare un attacco di phishing* avrebbe tenuto sulla scrivania quel pesce per tutto il mese. Quella persona sarebbe chiamata il "Re Phisher" del mese.

Ora, potreste pensare che si sia trattato di un'idea ridicola. È vero, lo è. Ma dopo due mesi, non potete immaginare quanto imperversasse la gara tra 450 adulti per avere quel peluche sulla loro scrivania. Era diventato un punto d'onore essere il "Re Phisher".

I risultati furono ben più di una accresciuta applicazione del programma. Poiché i dipendenti cercavano attivamente il *phishing*, in pochi mesi i tassi passarono da una media del 7% a oltre l'87%. I clic scesero da circa il 57% a meno del 10%. E il risultato più gratificante fu il calo del *malware* rilevato in rete: di oltre il 79%.

Questo semplice stratagemma ha creato una cultura della consapevolezza della sicurezza. I dipendenti iniziarono a prendere decisioni migliori, videro i miglioramenti e si sentirono più motivati a mantenerli.

Che cosa aiuterà a migliorare la situazione nella vostra organizzazione? Non posso dirvi esattamente quello che vi serve senza prima parlare con voi, ma vi offro alcune idee che ho visto all'opera nel corso degli anni.

- *Premi* – Ho visto di tutto, dal pesciolino di peluche alle lotterie per buoni sconto e altri premi per aver scelto sempre l'azione giusta per un tot numero di mesi. Naturalmente, i premi possono essere costosi se il gruppo è grande, e mancherebbe la motivazione se la ricompensa fosse qualcosa di inutile o insignificante. In un'organizzazione, cercarono di regalare una card da 5 dollari al trimestre a coloro che avevano manifestato un comportamento ideale per l'intero trimestre. Il regalo era troppo piccolo per essere un vero motivatore. Il premio deve motivare sul serio, ma non è necessario che sia un tv da 60 pollici o un anno di stipendio. Deve solo essere qualcosa che rappresenti un reale apprezzamento per le azioni e l'atteggiamento richiesto.
- *Rinforzo positivo* – Ho visto aziende creare nell'intranet classifiche di coloro che sono rimaste nel gruppo dei comportamenti ideale per tot mesi. Alcuni hanno chiamato "Star Employees" nelle pagine intranet coloro che hanno aiutato a catturare il *phishing* per tot mesi consecutivi. Il rinforzo positivo funziona molto meglio della vergogna e dell'imbarazzo e motiva positivamente i comportamenti desiderati.
- *Addestramento extra* – Ho visto molte aziende avere un grande successo con sessioni che chiamano "Lunch and Learn". Portano una pizza o qualche altra leccornia (se mi invitate, vi prego di farmi trovare un'insalata o qualcosa di sano, così Josh non se la prende con me) e tengono un breve discorso o un video o una presentazione su qualche argomento di sicurezza, a beneficio dei presenti. Certo, chi partecipa può farlo per la pizza, ma le sessioni

alle quali ho partecipato sono sempre finite con molte persone che sono riuscite a cogliere almeno un po' di informazioni utili. È anche una grande opportunità per rafforzare i concetti e le azioni che volete siano prese dai dipendenti.

- *Rinforzo top-down* – Questo sembra avere poteri quasi mistici, come una sorta di incantesimo sulla popolazione. Quando l'amministratore delegato fa sapere al gruppo che anche lui sta ricevendo del *phishing* come la popolazione dei dipendenti e di come è andata a finire, lancia un messaggio molto chiaro di "siamo tutti nella stessa barca, ma davvero!". In un'organizzazione con la quale ho lavorato, la reazione iniziale al programma di *phishing* è stata tutt'altro che ideale. In un caso estremo, una donna che aveva compiuto solo azioni sbagliate quando ha ricevuto il *phishing* era così arrabbiata, da chiedere il mio telefono e massacrarmi per 10 minuti. Mi disse che sono una persona orribile e che devo riconsiderare il modo in cui conduco la mia vita. Pochi mesi dopo, l'amministratore delegato di questa grande organizzazione tenne una grande riunione aziendale. In quell'incontro, l'amministratore delegato menzionò il programma di *phishing*; spiegò di essere stato oggetto di *phishing*, come tutti gli altri, e che stava imparando a essere più consapevole. Come se avesse sventolato un talismano mistico, la rabbia cessò, l'aggressività nei confronti del mio team di ingegneria sociale si ridusse drasticamente e trovammo un tasso molto più elevato di conformità. A volte qualcuno nella popolazione sente di essere stato scelto per fare la figura dello stupido. Ciò può creare un rapporto conflittuale e il fatto di ottenere un supporto dai massimi vertici dell'azienda può essere di grande aiuto.

Ecco altri due punti che dovreste tenere a mente.

- *Siate pazienti* – Non date per scontato che, per il solo fatto che avete svolto tutta la formazione in modo corretto, la vostra popolazione di dipendenti adotterà subito le politiche. Potrebbe essere necessario del tempo e uno sforzo continuo per convincere i dipendenti ad adottare il giusto punto di vista e ad avere la vostra stessa passione per questo problema.
- *Moderate le aspettative* – Suona familiare? Dovrebbe. Questo non solo aiuta a costruire un legame, ma può aiutarvi a creare una cultura della consapevolezza della sicurezza in azienda. Solo perché voi potete cogliere il *phishing* o identificare la chiamata di *vishing* o individuare la persona estranea, questo non significa che ogni dipendente sarà così veloce a fare la stessa cosa.

Essendo pazienti e gestendo le vostre aspettative, aiuterete i vostri dipendenti a essere in linea con la nuova formazione.

Riepilogo

Per quanto difficile possa essere, all'inizio, credere di potercela fare, potete creare una cultura della consapevolezza della sicurezza. Potete considerare il vostro attuale "stato di forma" e pensare che la cosa richiederà troppo impegno o tempo. Tuttavia, ne vale la pena. I vantaggi di avere una cultura della consapevolezza della sicurezza superano di gran lunga i rischi.

In una e-mail, Josh mi disse: "Questo è un viaggio che dura tutta una vita, non tre o dodici mesi. Cambiare le abitudini è difficile, ma siamo tutti *work in progress*".

Questo non significa continuare a fare la stessa cosa più e più volte e sperare di migliorare. È importante fallire velocemente e andare avanti. Provate qualcosa di quanto trovate in questo capitolo e se non

funziona, non insistete. Scoprite perché non ha funzionato e provate qualcos'altro.

Josh cambia costantemente il mio programma, a volte settimanalmente. È raro che il programma rimanga lo stesso per più di un mese. Non sto dicendo che dovete cambiare le cose così spesso, ma nel suo comportamento c'è una lezione. Perché il mio programma funzioni, devo sentire settimanalmente Josh, per dargli il quadro completo della mia settimana precedente. Lui prende in considerazione i miei viaggi, le mie scelte dietetiche, la quantità di esercizi e anche i miei problemi personali nella settimana. Tutte queste informazioni lo aiutano a vedere se occorre applicare cambiamenti per mantenere i progressi fatti. Sono sicuro che svolge un'analisi completa e che le decisioni che prende sono frutto di un profondo ragionamento.

Questo è direttamente correlato al modo in cui potete applicare questo capitolo al vostro programma di consapevolezza della sicurezza. Assicuratevi di avere un quadro completo della vostra organizzazione, dal lato fisico dei test alla psicologia della vostra popolazione di dipendenti. Cercate di capire a quali stress potrebbero essere sottoposti e in quale modo essi possono influenzare il loro processo decisionale. Una volta che avrete un quadro completo, sarà più facile pianificare il vostro programma di sicurezza. Sviluppate un percorso chiaro, avviate il programma e poi osservate come procede.

Non posso dirvi che questo vi renderà *hacker-proof*. Non posso neanche prevedere il tasso di successo che rileverete. Tuttavia, posso promettervi che noterete un cambiamento. Posso promettervi che inizierete a creare una cultura nella quale le persone non solo sapranno quali tipi di attacchi aspettarsi, ma sapranno anche difendersi da questi attacchi.

Come potete applicare tutti i concetti esposti in questo libro, come aspiranti *pen-tester* o come azienda che cerca di difendersi dagli

ingegneri sociali? L’ultimo capitolo aiuta a riepilogare tutto questo e vi prometto che non menzionerò Josh. (Scusa, Josh. I tuoi 15 minuti sono terminati.)

E ora?

È più facile limitarsi, ma così facendo non raggiungerete mai il vostro vero potenziale.
- *Chris Witty*

Quando ripenso agli ultimi otto o nove anni, non avrei potuto prevedere quello che stava arrivando. Non avrei mai immaginato che avrei costruito un business di successo facendo quello che amo fare, come anche un'associazione non-profit che si occupa di proteggere i bambini.

Questa avventura mi ha educato, mi ha plasmato e mi ha aiutato a diventare quello che sono oggi. Non tutto è stato perfetto e ho ancora molto spazio di crescita e proprio questo è il punto che voglio chiarire in questo capitolo.

Nell'ingegneria sociale non esiste un proiettile d'argento, né una bacchetta magica. Non potete leggere queste pagine e pensare che con un po' di legami, un pizzico di influenzamento e una spolverata di comunicazioni non verbali, il tutto decorato con un ciuffo di fiducia, possiate diventare veri ingegneri sociali. Ci vuole lavoro, autocritica e poi ancora lavoro.

Inevitabilmente, qualcuno mi chiede come entrare nel settore e trasformare l'ingegneria sociale in una professione. La risposta a questa domanda presenta molte sfaccettature, e in questo capitolo vi dico quello che cercherei io nei potenziali ingegneri sociali.

Soft skill di un ingegnere sociale

Ho incontrato tante persone dotate di incredibili abilità, ma che non erano in grado di gestire il lavoro. Persone che, letteralmente, non avrebbero potuto andare avanti in questo settore. E ho anche incontrato persone che non avevano una briciola di fiducia in se stessi, ma che si sono rivelate ingegneri sociali sorprendenti.

Ci sono quattro caratteristiche ben precise in questi due gruppi, che penso possano aiutarvi se volete intraprendere questo percorso professionale. Qualità che ritengo veramente essenziali per i vostri progressi.

Umiltà

In assoluto, la principale qualità di coloro che eccellono in questo campo è l'umiltà. Spesso, l'essere umili o mansueti è considerata una debolezza, ma fermatevi un attimo e pensate a una persona, nella vostra vita, che ritenete essere veramente umile. Avete in mente qualcuno? (PS: se avete detto voi stessi, non siete sulla buona strada.)

Ora rispondete a questa domanda, senza riflettere: "Come vi fa sentire quella persona?". Per me, è una combinazione di "felice, rispettato e importante". Non è qualcosa di più potente che essere considerato come qualcuno che sa tutto e non può essere corretto, in altre parole, qualcuno che *non sa* cos'è l'umiltà?

Quando ho avuto il privilegio di lavorare con Paul Ekman, ho avuto modo di sperimentarlo in prima persona. Poiché ha un intelletto di prim'ordine, mi aspettavo che lavorare con lui fosse duro e impegnativo. Tuttavia, lo trovai davvero umile, aperto ad altri pareri e disposto a lasciare spazio alla libertà creativa. Quando avevo bisogno di essere corretto era fermo, ma anche perspicace e motivante.

Ogni persona che ho visto eccellere nel campo dell'ingegneria sociale e con la quale mi è piaciuto lavorare aveva una sana dose di umiltà e di volontà di migliorare.

Motivazione

Considero il lavoro come un qualcosa che potete fare ogni giorno, svolgendo i vostri compiti e del quale potete poi dimenticarvi al termine della giornata. Se cercate questo genere di lavoro, forse l'ingegneria sociale non fa per voi. Essere professionisti dell'ingegneria sociale è più di una professione. Qualcosa che vi cambierà la vita mentre siete al lavoro e quando siete da tutt'altra parte. Tuttavia, le competenze non vengono dal nulla, quindi sarà necessaria la giusta motivazione per apprendere, crescere e continuare a migliorare.

Estroversione

No, no, aspettate! Prima di gettare il libro nel cassonetto della carta e urlare "Io sono un introverso!", lasciatemi dire che non vi sto chiedendo di cambiare. Vi sto solo suggerendo di cercare in voi un po' di estroversione e di imparare ad "accenderla" nel lavoro.

Forse ricordate, dal Capitolo 3, che io sono un comunicatore fortemente *D* (diretto). I tipi *D* sono generalmente noti per "dire" e non per invitare. Mi sento naturalmente incline al "fare", ma quando iniziai a tenere conferenze e a svolgere formazione, mi resi conto che la comunicazione diretta non era efficace per influenzare (*I*). Ho studiato alcuni dei modi in cui comunicano gli *I* e ho iniziato a usare quelle abilità durante le lezioni. Il risultato? Mi stancavo di meno e piacevo di più agli allievi.

Vi suggerisco di fare pratica delle abilità mancanti una alla volta, finché non diventerà uno strumento che potete estrarre spontaneamente dalla vostra "cassetta" quando ne avete bisogno. Per quanto doloroso possa essere per voi dire: "Oggi, ho intenzione di avviare una conversazione con due perfetti sconosciuti", vi suggerisco di fare proprio questo. Dopo un po', questo compito diventerà molto più facile e proverete il bisogno di intensificare la sfida.

Dopo un po' potrete passare a un altro aspetto della comunicazione, finché non sarete in grado di "accendere" e "spegnere" tali competenze a piacimento.

Informazioni extra

Secondo la ricerca di Meyers Briggs (www.myersbriggs.org/my-mbti-personality-type/mbti-basics/extraversion-or-introversion.htm?bhcp=1), un estroverso può sentirsi rigenerato dalle interazioni, mentre un introverso può sentirsi esaurito in quella stessa situazione. Continua affermando che un estroverso è espansivo, a suo agio nei gruppi, ha una vasta gamma di amicizie, si getta nell'azione fin troppo velocemente e può peccare in termini di attenzione ai dettagli.

Un introverso, al contrario, è riflessivo, sta bene da solo, preferisce conoscere solo poche persone, trascorre troppo tempo a pianificare e può essere lento nell'entrare in azione.

Disponibilità a provare

La paura di fallire è una delle più grandi cause per cui certe persone non sono efficaci in questo lavoro. Alcuni si sentiranno perfino immobilizzati. Coloro che eccellono come professionisti dell'ingegneria sociale sono coloro che sono stati in grado di uscire dalla propria zona di comfort, per rendersi conto che a volte un fallimento è il miglior insegnante. Coloro che manifestano la volontà di provare cose nuove sembrano essere in grado di adattarsi ai gruppi più disparati e alle situazioni più varie. Ho notato che coloro che

temono le nuove culture, cibi, persone ed esperienze spesso trovano questo lavoro troppo stressante ed estenuante.

Credetemi, funziona davvero!

Ho visto una persona convinta che non sarebbe mai diventata un vero ingegnere sociale applicare queste quattro qualità e diventare un ottimo ingegnere sociale. Ricordo quando lo incontrai per la prima volta. Entrò a lezione, si sedette in fondo alla classe, incrociò le mani in grembo e chinò la testa.

Mi resi conto, quando lo incontrai, che era un introverso estremo. Ero curioso di sapere perché fosse seduto proprio al *mio* corso di ingegneria sociale. Gliel'aveva ordinato il suo capo? L'azienda l'aveva incaricato e doveva essere presente? Iniziai, al solito, la mia lezione: inizio ogni giorno con una buona dose di Clutch (la migliore rock band del mondo). Quando attaccò il primo accordo della prima canzone, questo studente, Ryan, sollevò la testa e vidi un chiaro segno di conforto sul suo viso.

Mi dissi: "Ok, bene. È un fan dei Clutch". Mi presentai. In una breve conversazione, scoprii che non c'era nessun capo e nessun obbligo: voleva semplicemente sfidare se stesso, uscire dalla sua zona di comfort e provare qualcosa di nuovo. Sentivo ancora che si aspettava che la cosa fosse troppo difficile.

Nei quattro giorni successivi, vidi Ryan dimostrare una straordinaria disponibilità a provare tutto quello che gli chiesi di fare. Era motivato a non rinunciare a nessun compito. Diventò perfino sempre più estroverso con il passare della settimana. La cosa più importante che notai era che, di solito, veniva da me a chiedermi consigli, critiche e correzioni sui suoi compiti serali.

Alla fine del corso, Ryan ricevette il premio per lo studente del corso che più era cambiato. Dissi al mio team: "Ho intenzione di

assumere Ryan, entro un anno o due”.

Tuttavia, assumerlo si rivelò un compito non facile. Ryan era cambiato. La sua azienda notò questi cambiamenti e lo ricompensò. Passò dal condurre pen-test a dirigere tutti gli attacchi di ingegneria sociale. Ora svolgeva *vishing*, *phishing* e accessi non autorizzati. E, soprattutto, era bravo a farlo.

Mi ci vollero tre anni per assumerlo, ma ora Ryan controlla tutto il lavoro di ingegneria sociale della mia azienda. È ancora un introverso. Ama ancora progettare (troppo, secondo me), ma è motivato, è disposto a provare cose nuove, è in grado di accendere la sua estroversione e chiede sempre regolarmente consigli, aiuti e suggerimenti.

So che un giorno lavorerò per Ryan, ne sono sicuro. Se lui ha avuto successo nel campo dell’ingegneria sociale, potete farlo anche voi. Avete solo bisogno di applicare i quattro principi che ho appena descritto.

Competenze tecniche

Forse una delle domande che mi vengono poste più frequentemente riguarda quali tipo di corsi legati all’ingegneria sociale sia il caso di seguire. Non esiste una risposta semplice a questa domanda, ma permettetemi di indicarvi la giusta direzione.

Le competenze tecniche sono importanti in questo lavoro, perché vi troverete continuamente a interagire con le tecnologie. Capire come usare le tecnologie più semplici, come usare le chiavette USB, avviare macchine e connettersi a una VPN, può aiutarvi molto con i pretesti e dopo aver ottenuto l’accesso.

Detto questo, dovete per essere grandi programmatori di *exploit*? Niente affatto. Ecco la mia regola rapida per aiutarvi a determinare quali dovrebbero essere le vostre competenze tecniche. Lavorerete da

soli o in un team? Se lavorate da soli, allora potreste dover avere alcune solide competenze tecniche. Se non le avete, ciò limiterà gravemente le vostre offerte di servizi.

Se vi troverete a lavorare in un team, verificate che i vostri compagni di squadra abbiano le competenze necessarie, in modo da poter bilanciare e distribuire le abilità. Nel mio team, abbiamo un buon mix di tecnici e non tecnici che lavorano insieme.

Se avete stabilito di aver bisogno di determinate competenze tecniche, ecco alcune cose che ritengo importanti:

- conoscenza di base del funzionamento dei computer;
- conoscenza dei pacchetti di produttività per l'ufficio (Word, Excel…);
- conoscenza delle diverse parti di un computer e del loro funzionamento;
- capacità di usare i sistemi operativi OS X, Windows e Linux;
- comprensione del funzionamento di una rete;
- nozioni di configurazione di un server di posta;
- abilità nel fotoritocco.

Se dovrete svolgere *pen-test*, dovrete avere anche le seguenti competenze:

- conoscenza dei framework di *exploit*, come Metasploit ed Empire;
- capacità di leggere e comprendere il codice;
- competenze di programmazione.

Formazione scolastica

"Qual è il migliore percorso scolastico per diventare ingegneri sociali?". Ogni volta che sento questa domanda, il che accade molto

più spesso di quanto possiate immaginare, dico a quella persona di non essere qualificato per guidarli sotto questo aspetto. Dopotutto, la mia esperienza a scuola si è conclusa quando scrissi un *war-dialer* e il preside e la polizia mi suggerirono di lasciare la scuola.

Curiosità
All'inizio degli anni Novanta non c'erano leggi sui crimini informatici e la maggior parte degli "hacker" era costituita solo da persone curiose, per nulla intenzionate a distruggere quel che toccavano. Scrissi un programma, un *war-dialer*, che collegava insieme due modem da 4.800 baud; quindi componeva un numero, riproduceva dei codici per dire al numero di disattivarsi per cinque minuti minuti e poi riattaccava; e poi ripeteva tutto da capo. Usai la tecnica del *threading*, che permetteva al programma di chiamare anche molti numeri contemporaneamente. Questo script spense il 60% dei sistemi telefonici della mia contea per un giorno intero. In conseguenza di ciò mi venne chiesto di lasciare la scuola di informatica che frequentavo.

Nonostante il mio problematico background formativo, ho alcune opinioni su quale tipo di istruzione sia vantaggiosa. Non dovete diventare maestri in questi campi, ma vi suggerisco di acquisire almeno le basi.

- *Psicologia* – La chiave consiste nel ricordare che anche se non siete psicologi o terapeuti, è importante avere conoscenze di base del funzionamento degli esseri umani e di come prendono decisioni.
- *Lingua, grammatica e scrittura* – potete anche essere il miglior ingegnere sociale esistente sulla faccia della Terra, ma se non sapete scrivere un report efficace e chiaro, i vostri sforzi non verranno mai riconosciuti. Vi suggerisco un corso di alta qualità che possa aiutarvi a imparare bene la lingua e ad aumentare il vostro lessico professionale.
- *Psicologia sociale* – Scoprire come interagiscono gli esseri umani nei gruppi sociali, che cosa ci influenza e come questi gruppi

influiscono su di noi vi renderà sicuramente ingegneri sociali migliori.

Potreste chiedermi: “Questo è tutto?”. Beh, come ho detto, non sarò certo il vostro guru in termini di scelta della scuola. Vi sto solo offrendo suggerimenti basati sulla mia esperienza. Se poi non avete un’istruzione formale in questi campi, non pensate che non potrete mai avere successo. Potete sempre leggere libri, visitare siti web, ascoltare podcast e parlare con persone dotate delle conoscenze che cercate, in modo da cercare di ottenere una comprensione di base di molti di questi argomenti. Ricordate che l’obiettivo finale non è quello di diventare psicologi, terapeuti, linguisti o psicologi sociali. Dovete solo essere esperti quanto basta per capire quando è in gioco un certo principio.

Prospettive di lavoro

Se potessi aver creato, con questo libro, un modo infallibile per trovare lavoro, penso che avrei in mano un bestseller del “New York Times”. La triste verità è che non esiste un modo rapido e sicuro per garantirlo, ma posso indicarvi alcuni percorsi che, mi sembra, funzionino.

Avviate una vostra attività

Potete iniziare a offrire servizi di ingegneria sociale alle aziende della vostra zona. Oggi, avviare questo tipo di società non è così difficile come quando iniziai io. (A proposito, benvenuto!) Quando iniziai, mi offrii di regalare cinque (sì, solo cinque) e-mail di *phishing* solo per convincere il cliente a provare. Eppure, ancor oggi, i potenziali clienti a volte rifiutano l’offerta. Al giorno d’oggi, i clienti vogliono vedere l’ingegneria sociale usata per *pen-test* e servizi. I

media, le notizie e il mondo in generale hanno contribuito a far sì che le aziende siano consapevoli delle minacce rappresentate dall'ingegneria sociale, e questo facilita il vostro lavoro.

Ma pur con i cambiamenti avvenuti negli ultimi anni, ci sono ancora alcuni ostacoli su questo percorso. Pensate a quello che state chiedendo a un'azienda: "Per favore, dovrebbe darmi una lista dei vostri utenti e lasciarmeli tormentare con il *phishing* o il *vishing*. Ah, e poi entrerei in azienda a prendere 'cose', un po' qui e un po' là. Se volete, già che ci sono, posso ottenere un accesso remoto e attaccarvi dall'interno".

La maggior parte delle aziende vorrà sapere con chi lavorate, quali referenze avete, chi vi conosce e molti altri dettagli che rendono davvero difficile iniziare. Ma non arrendetevi – ci sono varie cose che potete fare per farvi conoscere.

Tenete una conferenza o scrivete post o articoli su blog e invitate le persone a leggerli e a commentarli. Farsi anche un piccolo nome pubblico in questo mondo può aiutare a rendere la vostra azienda un concorrente valido per la fornitura di questo genere di servizi. Ho visto persone avviare un'attività di successo generando solo un po' di entusiasmo nella comunità, anche se non avevano precedenti esperienze nel campo dell'ingegneria sociale. Sono venuti al DEF CON, hanno partecipato alla gara di Social Engineering, The Flag (SECTF). Dopo che si sono comportati bene e hanno vinto, hanno cominciato a creare aziende di successo che oggi forniscono servizi di ingegneria sociale. Costruirsi una certa credibilità li ha aiutati lungo il loro percorso.

Fatevi assumere da un'azienda che svolge attività di pen-test

La maggior parte delle aziende più prestigiose offre un qualche servizio di ingegneria sociale. Un percorso che ho visto funzionare per alcune persone è stato quello di farsi assumere in un'azienda che svolge *pen-test*. Per chi è appena diplomato e senza esperienza, sarà necessario partire dal fondo.

Ma una volta che sarete stati assunti, rendetevi disponibili a svolgere attività di *vishing*, ad aiutare con il pretesto e così via. Se svolgerete un buon lavoro, l'azienda vi darà altre opportunità. Se avrete successo, potreste scalare rapidamente la classifica delle preferenze.

Tuttavia, questo percorso può richiedere mesi o addirittura anni. Potete anche offrirvi, ma la vostra azienda potrebbe non usarvi per un po' . Dovreste avere un piano: per quanto tempo siete disposti a provare? Il mio suggerimento è quello di intraprendere questa strada con pazienza e con la volontà di apprendere nuove competenze, che potranno aiutarvi mentre rimanete in questa azienda.

Fatevi assumere da un'azienda di ingegneria sociale

Una rapida ricerca su Google basta per capire che ci sono poche aziende che si concentrano sull'ingegneria sociale e solo alcune di esse lo fanno come loro attività principale. La mia azienda è focalizzata esclusivamente sull'ingegneria sociale e riceviamo ogni mese molte richieste di persone che vogliono lavorare per noi. Mi piacerebbe assumerli tutti (se sono qualificati), ma assumiamo solo quando abbiamo bisogno di personale.

Tuttavia, nulla vi impedisce di chiedere. Potete contattare queste aziende e dire che state entrando in questo campo. Condividere quanto avete scritto, raccontato e/o fatto e lasciare che tali società vi facciano sapere se hanno posizioni da coprire. Entrare nella lista delle potenziali assunzioni potrebbe farvi avere un lavoro da sogno.

Qualunque percorso scegliate di intraprendere, questo settore avrà sempre bisogno di persone. L'ingegneria sociale non sta sparendo e quindi c'è sempre la necessità di trovare persone qualificate che vogliano fare la differenza.

Il futuro dell'ingegneria sociale

Voglio essere serio. Oltre ai rapporti che parlano di attacchi di hacker – come per esempio il rapporto Verizon DBIR, il rapporto CISCO e molti altri – l'ingegneria sociale è ormai in uso in alcuni luoghi molto, molto oscuri.

Ogni giorno ci sono nuovi rapporti su persone che lasciano la loro famiglia e la loro casa per unirsi a organizzazioni terroristiche. Che cosa sta succedendo?

Analizzando queste storie, potete trovare tutti gli elementi dell'ingegneria sociale che ho menzionato in questo libro. Le persone che si uniscono ai gruppi terroristici sono arrabbiate, emotive e in cerca di una loro "tribù". Poi arriva una tribù che dà loro risposte e motivazione per "risolvere" i loro problemi. Improvvisamente quelle persone si sentono necessarie, desiderate e accettate. La nuova tribù inizialmente chiede solo piccole cose, per costruire la fiducia e un solido legame. La cosa continua fino a quando la conversione non è completa.

Secondo un articolo intitolato *The Geography of Foreign ISIS Fighters* di Richard Florida ("CityLab", agosto 2016, www.citylab.com/equity/2016/08/foreign-fighters-isis/493622), più di 19.000 persone hanno lasciato la loro casa in Tunisia, Russia, Arabia Saudita, Turchia e Giordania per unirsi all'ISIS. Nei paesi occidentali come il Regno Unito, la Francia, la Germania e gli Stati Uniti, i numeri sono

più bassi (non più di 2.000 persone hanno aderito), ma vengono sempre impiegati gli stessi principi di reclutamento.

Un'altra tendenza molto preoccupante è il modo in cui questi principi vengono usati dai pedofili per attrarre nella rete i bambini. Usando una chat online, questi predatori iniziano a intessere una relazione con un bambino, inserendolo nella sua "tribù". Un predatore cercherà un bambino in difficoltà coi suoi genitori o che ha una difficile vita sociale e poi costruirà un legame, lo ascolterà attivamente, utilizzerà domande a risposta aperta e suggerirà idee e concetti che alla fine diventeranno le idee del bambino stesso.

Il centro statunitense NCMEC (*National Center for Missing and Exploited Children*) riferisce che nel 2017 nei soli Stati Uniti sono scomparsi 465.676 bambini (`www.missingkids.com/KeyFacts`). In quello stesso anno, su 25.000 casi di fughe trattati dall'FBI, un bambino su sette era stato vittima di un abuso sessuale. Molti di questi bambini sono stati attirati dai pedofili.

So che tutto questo è molto triste, ma sto cercando di convincervi dell'utilità dell'ingegneria sociale. Dagli attacchi alle aziende, agli attacchi personali contro vostra nonna, al reclutamento in gruppi terroristici alle reti di pedofili, l'ingegneria sociale è qui per restare ed è sempre più utilizzata.

Abbiamo bisogno che le persone stiano dalla parte giusta, per aiutare a difendere, proteggere, istruire e responsabilizzare gli altri nel comprendere queste abilità e imparare a difendersi da questi attacchi. Vi prometto che non sarà facile, ma molto gratificante.

Negli ultimi otto anni della mia carriera, ho avuto la possibilità di lavorare con decine di aziende in tutto il mondo che hanno visto drastiche riduzioni nella loro sensibilità agli attacchi di ingegneria sociale. Un'azienda mi ha riferito di aver rilevato una riduzione

dell’87% del *malware* nella sua rete interna e ha collegato questo risultato alla nostra educazione nel campo del *phishing*.

Un’altra azienda mi ha riferito che i suoi agenti erano ormai in grado di riconoscere, bloccare e segnalare un’aggressione attiva alla loro organizzazione, e questo grazie alla formazione che avevamo fatto con loro. Uno dei miei allievi mi confessò che quello che aveva imparato durante il mio corso di cinque giorni aveva salvato il suo matrimonio. Anche se salvare matrimoni non è mai stata la mia principale motivazione a tenere lezioni di ingegneria sociale, mi fa piacere che questo studente sia stato talmente influenzato da quello che ha imparato sulla comunicazione, sui legami e sull’influenzamento da applicarlo in famiglia tanto da riuscire a sistemare la sua relazione.

Sono stato anche coinvolto nel salvataggio di molti bambini dallo sfruttamento, sia nel mio lavoro come azienda, sia in quello che sto facendo con la mia nuova organizzazione non profit, la Innocent Lives Foundation (`www.innocentlivesfoundation.org`). Sfruttare le stesse abilità che insegno ogni giorno, per smascherare coloro che sfruttano i bambini è la cosa più gratificante.

Infine, un’ultima annotazione molto personale. Ho potuto insegnare ai miei figli queste stesse abilità, il che li rende più auto-consapevoli, meno suscettibili agli attacchi e (questa è la mia, assolutamente non umile, opinione) fra le persone più equilibrate e straordinarie che conosca.

Imparare a usare queste abilità è gratificante non solo per la carriera ma anche nella vita di tutti i giorni. Spero che questo libro vi motivi a volerne sapere sempre di più. Se avete già appreso alcune di queste abilità, spero che questo libro vi abbia dato almeno una o due nuove idee sulle quali riflettere. Se siete scettici o appassionati, spero che questo libro promuova una sana discussione su queste abilità e sul modo in cui usarle.

Apprezzo il vostro contributo e le vostre opinioni su questo argomento. Vi incoraggio quindi a rendere queste abilità parte della vostra cassetta degli attrezzi quotidiana.

State al sicuro.

Indice

Prefazione

Ringraziamenti

Premessa

Capitolo 1 - Uno sguardo al nuovo mondo dell’ingegneria sociale professionale

- Che cosa è cambiato?
- Perché dovreste leggere questo libro?
- Una panoramica sull’ingegneria sociale
- La piramide SE
- Di che cosa parla questo libro?
- Riepilogo

Capitolo 2 - Vedi anche tu quel che vedo io?

- Un esempio reale di raccolta di OSINT
- OSINT non tecnica
- OSINT tecnica
- Strumenti del mestiere
- Riepilogo

Capitolo 3 - Profilare le persone attraverso la comunicazione

- L’approccio
- Il sistema DISC
- Riepilogo

Capitolo 4 - Impersonare chiunque
I principi del pretexting
Riepilogo

Capitolo 5 - Come cercare di farsi accettare
La tribe mentality
L’ingegneria sociale per la costruzione del legame
I 10 principi per la costruzione del legame
La macchina del legame
Riepilogo

Capitolo 6 - Sotto la mia influenza
Principio 1 – La reciprocità
Principio 2 – L’obbligo
Principio 3 – La concessione
Principio 4 – La rarità
Principio 5 – L’autorità
Principio 6 – La coerenza e l’impegno
Principio 7 – L’apprezzamento
Principio 8 – La prova sociale
Influenza vs manipolazione
La manipolazione in azione
Riepilogo

Capitolo 7 - Realizzare la propria opera d’arte
Le regole dinamiche del quadro di riferimento
La sollecitazione
Riepilogo

Capitolo 8 - Vedo anche quello che non mi hai detto
La comunicazione non verbale è essenziale
I nostri specifici elementi di base
Comprendere le basi della comunicazione non verbale

Comfort vs disagio
Riepilogo

Capitolo 9 - Hacking degli esseri umani

Un aggressore con “pari opportunità”
I principi del pen-test
Il phishing
Il vishing
Lo SMiShing
L’impersonificazione
I report
Le grandi domande per il pen-tester dell’ingegneria sociale
Riepilogo

Capitolo 10 - Avete un MAPP?

Passaggio 1 – Imparate a identificare gli attacchi di ingegneria sociale
Passaggio 2 – Adottate politiche attuabili e realistiche
Passaggio 3 – Svolgete regolari controlli in tempo reale
Passaggio 4 – Implementate efficaci programmi di sensibilizzazione sulla sicurezza
Per ricapitolare
Aggiornatevi continuamente
Imparate dagli errori dei vostri pari
Create una cultura di consapevolezza della sicurezza
Riepilogo

Capitolo 11 - E ora?

Soft skill di un ingegnere sociale
Competenze tecniche
Formazione scolastica
Prospettive di lavoro
Il futuro dell’ingegneria sociale