

علم هک کردن انسان

مهندسی
اجتماعی

مجید جعفریان، محمدرهبان، شیرین سجودی

گريستوفر هدنكي



بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ



The mark of
responsible forestry
FSC® C009732

سرشناسه: هدنگی، کریستوفر Hadnagy, Christopher
عنوان و نام پدیدآور: مهندسی اجتماعی؛ علم هک کردن انسان / کریستوفر هدنگی
مترجمان: مجید جعفریان، محمد رهبان، شیرین سجودی
مشخصات نشر: تهران: راه پرداخت، ۱۴۰۰.
مشخصات ظاهری: ۳۹۲ ص
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۹-۴
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: Social engineering: the art of human hacking, c2011.
عنوان دیگر: مهندسی اجتماعی هنر هک کردن انسان.
موضوع: مهندسی اجتماعی
موضوع: Social engineering
موضوع: هکرها
موضوع: Hackers
موضوع: کامپیوترها - ایمنی اطلاعات
موضوع: Computer security
شناسه افزوده: جعفریان، مجید، ۱۳۶۱-مترجم
شناسه افزوده: رهبان، محمد، ۱۳۶۷-مترجم
شناسه افزوده: سجودی، شیرین، ۱۳۶۹-مترجم
شناسه افزوده: سرلک، بهار، ۱۳۶۷-ویراستار
رده بندی کنگره: HM۶۶۸
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۸۷۵۱۰۰۵

علم هک کردن انسان

مهندسی
اجتماعی

مجید جعفریان، محمدرهبان، شیرین سجودی

گریستوفر هدنگی





عنوان: مهندسی اجتماعی؛ علم هک کردن انسان

ناشر: راه پرداخت

نویسنده: کریستوفر هدنکی

مترجمان: مجید جعفریان، محمد رهبان، شیرین سجودی

ویراستار ارشد: مینا والی

ویراستار محتوایی: بهار سرلک

ویراستار فنی: محدثه گودرزنی

بازبینی نهایی متن: رضا قربانی

صفحه آرا: بهناز سعیدی

ناظر چاپ: قادر شهبازی

نوبت چاپ: اول ۱۴۰۰

شمارگان: ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۹-۴

تلفن: ۰۲۱-۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل: info@way2pay.press

وبسایت: way2pay.shop

لایتوگرافی: هنر اشکان

چاپ و صحافی: واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و ...) بدون اجازه کتبی ناشر ممنوع است.

فروشگاه انتشارات راه پرداخت نشانی: تهران، جنت آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

۱۶	فصل اول: نگاهی به دنیای جدید مهندسی اجتماعی حرفه‌ای
۱۹	چه چیزی تغییر کرده است؟
۲۱	چرا باید این کتاب را بخوانید؟
۲۲	ارجاع به پادکست مهندس اجتماعی
۲۴	نگاهی اجمالی به مهندسی اجتماعی
۲۶	واقعیت بی‌مصرف
۲۷	ارجاع به پادکست مهندس اجتماعی
۳۱	اطلاعات بیشتر
۳۳	در این کتاب چه می‌خوانید؟
۳۵	خلاصه
۳۸	فصل دوم: آنچه من می‌بینم تو هم می‌بینی؟
۳۹	نمونه‌ای واقعی از جمع‌آوری اطلاعات منبع‌باز
۴۴	مستند کردن یا نکردن؛ مسئله این است
۴۵	اطلاعات منبع‌باز غیرفنی
۴۷	مهارت‌های مشاهده‌ای چه مهارت‌هایی هستند؟
۵۹	اطلاعات منبع‌باز فنی
۸۴	دو مسئله دیگر
۹۵	ابزارهای مهم
۹۷	خلاصه
۹۹	فصل سوم: پروفایل‌بندی افراد از طریق ارتباط
۱۰۱	اطلاعات بیشتر
۱۰۴	برخورد اول
۱۰۷	دیسک وارد می‌شود
۱۲۲	خلاصه

۱۲۵	فصل چهارم: تبدیل شدن به هرکسی که می خواهید
۱۲۸	اصول ایجاد دستاویز
۱۳۵	محض اطلاع شما
۱۴۵	خلاصه

	فصل پنجم: می دانم چطور کاری کنم که دوستم داشته باشی
۱۵۱	ذهنیت قبیله ای
۱۵۴	ایجاد رابطه دوستانه به عنوان یک مهندس اجتماعی
۱۶۶	مثالی در مورد رئیس جمهور
۱۷۵	ماشین رابطه
۱۷۶	خلاصه

	فصل ششم: تحت تأثیر
۱۸۱	درس مهارت ها
۱۸۳	اصل اول: عمل متقابل
۱۸۶	اصل دوم: مسئولیت
۱۹۰	اصل سوم: پذیرش
۱۹۴	اصل چهارم: کمیابی
۱۹۸	اصل پنجم: قدرت
۲۰۴	اصل ششم: سازگاری و تعهد
۲۰۸	اصل هفتم: دوست داشتن
۲۱۲	اصل هشتم: تأیید اجتماعی
۲۱۳	داستانی جالب
۲۱۵	مقایسه تأثیرگذاری با فریب کاری

	فصل هفتم: خلق اثر هنری
۲۲۷	قوانین متغیر چهارچوب بندی
۲۳۸	فراخوانی
۲۴۸	اظهارات غلط به علاوه شیوه بده بستان
۲۵۸	خلاصه

	فصل هشتم: می توانم آنچه را نگفتی ببینم
۲۶۱	رفتارهای غیرکلامی ضروری اند
۲۶۵	تمام احساسات مبنای شما به درد ما می خورد
۲۶۵	در مورد این داستان فکر کنید
۲۷۶	دانستن اصول اولیه رفتارهای غیرکلامی
۲۷۸	راحتی در مقابل عدم راحتی

فصل نهم: هک کردن انسان‌ها

۳۰۹

۳۱۱

۳۱۲

۳۱۸

۳۲۲

۳۲۳

۳۳۱

۳۳۳

۳۳۳

۳۳۹

۳۴۴

۳۵۰

این شرایط همه را به یک اندازه قربانی می‌کند

اصول تست نفوذ

فیشینگ

واقعیتی عجیب و غریب

ویشینگ

اسمیشینگ

جعل هویت

روش‌های حملات جعل هویت مهندسی اجتماعی در مقابل تیم قرمز

گزارش‌دهی

سؤال‌های رایج مهندسان اجتماعی که تست نفوذ انجام می‌دهند

خلاصه

فصل دهم برنامه کاهش اثر و پیشگیری دارید؟

۳۵۱

۳۵۴

۳۵۷

۳۶۱

۳۶۳

۳۶۵

۳۶۶

۳۶۸

۳۷۰

۳۷۳

گام اول: یادگیری نحوه شناسایی حمله‌های مهندسی اجتماعی

گام دوم: تدوین دستورالعمل‌های عملیاتی و واقع‌بینانه

گام سوم: انجام ارزیابی‌های منظم در محیط واقعی

گام چهارم: پیاده‌سازی برنامه‌های آگاهی‌رسانی امنیتی کاربردی

همه گام‌ها در کنار هم

به روزرسانی مستمر

اشتباه‌های همتایان‌تان را سرلوحه قرار دهید

فرهنگ حساس به امنیت ایجاد کنید

خلاصه

فصل یازدهم: حالا چی؟

۳۷۶

۳۷۷

۳۷۹

۳۸۱

۳۸۲

۳۸۴

۳۸۶

مهارت‌های نرم مورد نیاز مهندس اجتماعی شدن

اطلاعات بیشتر

مهارت‌های فنی

تحصیلات

چشم‌انداز شغلی

آینده مهندسی اجتماعی

[یادداشت مترجم]

گسترش روزافزون نقش تکنولوژی در تعاملات اجتماعی، کسب و کارها، اقتصاد، مناقشات سیاسی و به صورت کلی در تمامی جوانب زندگی بشری شمشیر دولبه‌ای است که از یک سو سهولت و سرعت انجام کار را در پی داشته و از سوی دیگر هراس از وابستگی افسارگسیخته تمام امور به تکنولوژی. در این میان یکی از مهم‌ترین عناصر اطمینان‌بخش و تسکین‌دهنده این هراس، امنیت سایبری و نقش آن در راستای تضمین تداوم خدمات‌دهی کارآ و کامل است. تصور عمومی فعالان حوزه تکنولوژی از امنیت، ارتقای سخت‌افزاری و نرم‌افزاری سیستم‌ها و سامانه است؛ به این صورت که نقش عامل انسانی به عنوان یکی از بخش‌های اصلی سیستم اطلاعاتی همواره نادیده گرفته می‌شود. واقعیت این است که انسان در اصل ضعیف‌ترین عنصر حلقه زنجیره امنیت سایبری و در عین حال مغفول‌ترین آن است.

این کتاب تازه‌ترین اثر چاپ‌شده از کریستوفر هدنگی است که از محدود آثار جامع و دقیق در زمینه شناخت عنصر انسانی در حوزه امنیت سایبری به‌شمار می‌رود. هدنگی با زبانی ساده، روان و مملو از شوخ‌طبعی‌های دلنشین سعی بر بررسی تکنیک‌ها و روش‌های نفوذ بر عامل انسانی سیستم‌های اطلاعاتی دارد. او از اولین متخصصانی بود که موضوع مهندسی اجتماعی و علم نفوذ بر افراد را به عنوان یک عامل مستقل و بسیار حائز اهمیت در حوزه سایبری بررسی کرد و در ویراست اول همین کتاب گنجانده و نویسنده در ویرایش دوم کتاب

با به روزرسانی تکنیک‌ها، فرآیندها و همچنین بررسی نمونه‌های رخ داده در دنیای واقعی، عامل گذر زمان و پیشرفت تکنولوژی را نیز مورد بررسی قرار داده است. پس از خواندن این نسخه از کتاب به دلیل ویژگی‌های منحصر به فرد آن، درصدد ترجمه کتاب برآمدیم تا شاید از این طریق گام کوچکی در راستای شناسایی هرچه بیشتر روش‌های مهندسی اجتماعی در زیست‌بوم امنیت سایبری کشور برداریم.

هدنگی در این اثر به بهترین شیوه ممکن تکنیک‌های مختلف این حوزه را مورد بررسی قرار داده و تشریح می‌کند که هر چه تقویت حلقه‌های امنیت اطلاعات از شما فردی نفوذناپذیر و سرسخت ساخته باشد، کماکان به ساده‌ترین روش‌ها امکان نفوذ به شما وجود دارد.

نکته حائز اهمیت دیگر این است که برای لذت بردن از این اثر نیازی نیست در حوزه امنیت تخصص ویژه‌ای داشته باشید. بدیهی است متخصصان این حوزه بهره بیشتری از کتاب خواهند برد اما به دلیل ویژگی‌های مثال‌زدنی این اثر، همچون زبان ساده و عاری از پیچیدگی‌های تخصصی و داستان‌پردازی جذاب رویدادهای به وقوع پیوسته در دنیای واقعی (شامل سناریوهای موفق و ناموفق که به شیوه مهندسی اجتماعی ثبت شده‌اند)، خواندن این اثر برای هر مخاطبی آموزنده و لذت‌بخش خواهد بود.

مجید جعفریان

پیشگفتار

در سال ۱۹۷۶، وقتی همراه با استیو جابز «اپل» را تأسیس کردم، نمی دانستم این اختراع جهان را به کدام سو می برد. می خواستم کاری بی سابقه انجام بدهم؛ کامپیوتری شخصی بسازم. کامپیوتری که هرکسی بتواند از آن استفاده کند، لذت ببرد و بهره مند شود. فقط ۴۰ سال گذشته و آن رؤیا به واقعیت تبدیل شده است.

در حالی که میلیاردها کامپیوتر شخصی در سراسر جهان وجود دارند و تلفن های هوشمند، دستگاه های هوشمند و فناوری با همه ابعاد زندگی ما عجین شده اند، خوب است از نمایی دورتر به این شرایط نگاه کنیم و ببینیم چطور می توانیم هم زمان با حفظ ایمنی و امنیت، همچنان به نوآوری و رشد ادامه بدهیم و با نسل بعد همکاری کنیم.

از همکاری با جوانان امروزی و ترغیب شان به نوآوری و رشد لذت می برم؛ از جریان ایده ها در میان آنها در راه رسیدن به روش های جدید و خلاقانه برای استفاده از فناوری لذت می برم و همچنین اینکه می بینم این فناوری چطور می تواند زندگی افراد را بهبود بخشد نیز واقعاً برایم لذت بخش است.

با این حال باید با جدیت درمورد حفظ امنیت این آینده فکر کنیم. در سال ۲۰۰۴، وقتی به عنوان سخنران اصلی در «کنفرانس هوپ» (HOPE Conference) صحبت می کردم، گفتم هک های زیادی اتفاق می افتند که با زندگی افراد بازی و آنها را وادار می کنند کارهایی عجیب انجام دهند.

دوستم، «کوین میتنیک» (Kevin Mitnick)، در طول سال ها، در یکی از حوزه های امنیت به نام «مهندسی اجتماعی» به تبحر و خبرگی رسیده است.

کتاب کریس ماهیت و جوهره مهندسی اجتماعی را بیرون می کشد و آن را به نحوی تعریف می کند و شکل می دهد که همه آن را درک کنیم. کریس کتاب مهندسی اجتماعی را بازنویسی کرده است تا آن دسته از اصول و فرایندهای محوری تأثیرگذار بر تصمیم گیری ما انسان ها را تعریف کند و نشان دهد افراد چطور از این فرایندها سوءاستفاده می کنند.

هک کردن چند دهه ای است که به وجود آمده، اما هک کردن انسان از ابتدای خلقت وجود داشته است. این کتاب می تواند شما را آماده کند، از شما محافظت کند و به شما

آموزش بدهد که چطور خطرهای ناشی از مهندسی اجتماعی را شناسایی کنید، آثارشان را کاهش دهید و از خودتان در برابرشان دفاع کنید.

استیو ورنیاک / هم‌بنیان‌گذار اپل

[

مقدمه

]

زمانی را به یاد می‌آورم که حاصل جست‌وجوی عبارت «مهندسی اجتماعی» در اینترنت یا صرفاً پیدا کردن ویدئوهایی در مورد روش به دست آوردن همبرگر مجانی بود یا چگونگی قرار گذاشتن با کسی که به او علاقه‌مندیم. اما اکنون به نظر می‌رسد تقریباً عبارتی شناخته‌شده و آشناست. همین چند روز پیش یکی از دوستان خانوادگی‌مان که اصلاً در این صنعت کار نکرده است در مورد یک کلاهبرداری ایمیلی حرف می‌زد و در آخر گفت: «بله، این مثال بسیار خوبی از مهندسی اجتماعی است.»

ابتدا غافل گیر شدم، اما بعد واقعیتی را فهمیدم؛ تنها بعد از هشت سال که تصمیم گرفتم شرکتی تأسیس کنم که فقط بر مهندسی اجتماعی متمرکز باشد، مهندسی اجتماعی به صنعتی کاملاً شکوفا و عبارتی شناخته‌شده تبدیل شده است.

اگر بدون پیش‌زمینه این کتاب را بخوانید ممکن است در مورد اهدافم به اشتباه بیفتید. شاید فکر کنید هیچ مشکلی ندارم که آدم‌های بدسرشست را برای انجام کارهای نادرست مجهز و آماده کنم. این تصور فرسنگ‌ها با واقعیت فاصله دارد.

وقتی اولین کتابم را نوشتم، افراد زیادی بودند که در مصاحبه‌ها به شدت از من ناراحت می‌شدند و می‌گفتند با نوشته‌هایم مهندسان اجتماعی مخرب را تجهیز می‌کنم. آن موقع نیز همین احساسی را داشتم که اکنون دارم؛ تا وقتی از همه ابعاد چگونگی استفاده از مهندسی اجتماعی آگاه نباشید نمی‌توانید در برابر آن از خودتان دفاع کنید. مهندسی اجتماعی ابزاری مانند چکش، بیل، چاقو یا حتی اسلحه است. هر کدام از این ابزارها برای هدفی ساخته شده‌اند و می‌توان از آن‌ها برای ساختن، نجات دادن، تغذیه کردن یا زنده ماندن استفاده کرد، در عین حال هم برای آسیب زدن، کشتن، خراب کردن و نابود کردن. برای اینکه درک کنید چطور می‌توان از مهندسی اجتماعی برای اهداف خوب استفاده کرد، باید هر دو نوع استفاده را درک کنید. این حرف به‌ویژه زمانی درست است که هدف‌تان دفاع کردن باشد. برای محافظت از خودتان و دیگران در برابر استفاده مخرب از مهندسی اجتماعی، ابتدا باید سمت تاریک آن را بشناسید تا تصویری روشن از نحوه بهره‌مندی از آن به دست بیاورید.

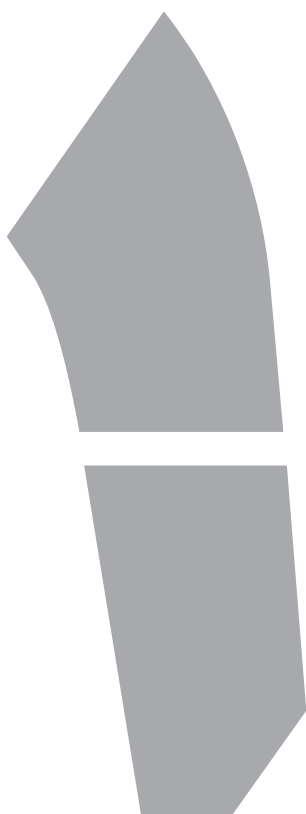
به‌تازگی با «ای جی کوک» (AJ Cook) در مورد کارش در سریال ذهن‌های جنایت‌کار (Criminal Minds) حرف می‌زدم که گفت اغلب به‌منظور آماده شدن برای ایفای نقش «جی جی» (JJ) در این سریال باید با مأموران فدرالی گفت‌وگو کند که روی پرونده‌های مربوط

به قتل‌های سریالی کار می‌کنند. این ایده به‌طور مستقیم به این کتاب هم مربوط می‌شود. این کتاب را با ذهنی باز و بدون تعصب بخوانید. با تمام توانم تلاش کرده‌ام دانش، تجربه و بینش به‌دست‌آمده از فعالیت‌هایم در طول دهه گذشته را در این صفحات به اشتراک بگذارم. بدون شک اشتباه‌هایی وجود دارند یا مواردی که با سلیقه شما هم‌خوانی ندارند، یا ممکن است احساس کنید صد درصد شفاف نیستند. بیا بید درموردشان بحث کنیم؛ با من تماس بگیرید تا درباره‌شان حرف بزنیم. می‌توانید در توییتر از طریق حساب @humanhacker با من در ارتباط باشید. یا می‌توانید از طریق یکی از وب‌سایت‌های www.social-engineer.org و www.social-engineer.com برایم ایمیل بفرستید. وقتی در دوره‌های پنج‌روزه‌ام تدریس می‌کنم، از دانشجویان می‌خواهم با من مانند فردی عاری از خطا و اشتباه تعامل نکنند و اگر دانش، فکر یا حتی احساسی دارند که با حرف‌هایم در تعارض‌اند، درموردش حرف بزنند. دوست دارم بیشتر یاد بگیرم و درکم از این موضوعات را گسترش دهم. از شما هم درخواست می‌کنم همین کار را بکنید.

در آخر می‌خواهم از شما تشکر کنم؛ ممنون که زمان ارزشمندتان را با خواندن صفحات این کتاب سپری می‌کنید. ممنون که کمک می‌کنید در طول سال‌ها بهتر شوم. ممنون به‌خاطر همه بازخوردها، ایده‌ها، نقدها و توصیه‌های تان.

واقعاً امیدوارم از مطالعه این کتاب لذت ببرید.

کریستوفر هدنکی (Christopher Hadnagy)



فصل اول
نگاهی به دنیای جدید
مهندسی اجتماعی حرفه‌ای

فکر می‌کنم امنیت شما دلیل موفقیت‌تان است و کلید موفقیت شما ذائقه ناب‌تان.
«گوردون رمزی» (Gordon Ramsay)، آشپز و شخصیت تلویزیونی معروف

هنوز به وضوح زمانی را به یاد دارم که روبه‌روی صفحه‌نمایش کامپیوترم نشسته بودم و می‌خواستم نگارش اولین پاراگراف کتاب مهندسی اجتماعی: هنر هک کردن انسان (Social Engineering: The Art of Human Hacking) را شروع کنم. سال ۲۰۱۰ بود. دوست داشتم به شوخی بگویم: «آن قدیم‌ها باید با ماشین تایپ می‌نوشتیم، کاری که خیلی سخت بود»، ولی نمی‌خواستم بیخودی شلوغش کنم.

آن موقع وقتی عبارت «مهندسی اجتماعی» را در اینترنت جست‌وجو می‌کردید، چند صفحه درمورد «کوبین میتنیک»، چهره برجسته مهندسی اجتماعی، پیدا می‌کردید و چند ویدئو درباره چگونگی قرار گذاشتن با کسی که به او علاقه‌مند بودید یا اینکه چطور همبرگر مجانی از مک‌دونالد بگیرید. الان، یعنی هشت سال بعد، عبارت مهندسی اجتماعی تقریباً عبارتی آشناست. در سه یا چهار سال گذشته مهندسی اجتماعی را در حوزه امنیت، دولت، آموزش، فلسفه، ارتش و هر کاربرد دیگری که تصورش را بکنید مشاهده کرده‌ام.

این تحول وادارمان می‌کند پرسیم چرا. یکی از همکارانم می‌گفت: «تقصیر توست کریس». فکر می‌کنم قصد داشت به من توهین کند، اما این جمله باعث می‌شود کمی احساس غرور کنم. با این حال احساس نمی‌کنم فقط من مسئول فراگیری تقریباً کامل عبارت مهندسی اجتماعی باشم. معتقدم دلیل اینکه می‌بینیم همه از آن استفاده می‌کنند این است که علاوه بر اینکه آسان‌ترین شیوه حمله است (همان‌طور که هفت سال پیش هم بود)، بیشترین بسته‌های اطلاعاتی را هم برای مهاجمان فراهم می‌کند.

هزینه حمله مهندسی اجتماعی کم است. خطرش از آن هم کمتر است و بازده بالقوه‌اش بسیار زیاد. با توجه به اینکه تیم من مشغول جمع‌آوری مقاله‌های خبری مربوط به حمله‌های مهندسی اجتماعی و جست‌وجوی اینترنت برای یافتن آمارهای این حوزه بوده است، با اطمینان می‌گویم در سال ۲۰۱۷ در بیش از ۸۰ درصد همه نفوذهای عنصر مهندسی اجتماعی وجود داشته است.

«مطالعه هزینه نشت داده ۲۰۱۷» (Cost of Data Breach Study 2017) شرکت

«آی بی ام» نشان می دهد که میانگین هزینه هر نشت داده ۳/۶۲ میلیون دلار آمریکا بوده است. وقتی بازده بالقوه این چنین زیاد است، به راحتی می توان متوجه شد که چرا مهاجمان به دنبال بهره برداری از مهندسی اجتماعی اند.

نکته تخصصی تا سال ۲۰۱۷ «مطالعه هزینه نشت داده» آی بی ام ۱۲ بار انجام شده است. می توانید آن را در <https://www.ibm.com/security/data-breach> ببینید یا به راحتی عبارت «Cost of Data Breach Study» را وارد هر موتور جست و جویی کنید تا گزارش کامل و به روز را مشاهده و دانلود کنید.

همچنین یکی از اولین مصاحبه هایم بعد از انتشار کتاب مهندسی اجتماعی: هنر هک کردن انسان، در سال ۲۰۱۰ را به یاد می آورم که مصاحبه گر پرسید: «نگران نیستید که آدم های بدسرشست را مجهز کنید؟» از نظر من مهندسی اجتماعی مانند هر نوع جنگ افزار دیگری است.

فکر کردن به ماجرای ورود «بروس لی» به آمریکا در دهه ۱۹۶۰ کمک می کند این موضوع را بهتر توضیح بدهم. در آن زمان تبعیض نژادی زیاد بود و بروس لی کاری می کرد که هیچ کس دیگری انجام نمی داد؛ به مردم با هر نژاد، رنگ یا ملیتی «جیت کان دو» آموزش می داد: یکی از هنرهای رزمی باستانی چین. با شاگردانش که فکر می کردند از مبارزه خیلی می دانند مبارزه می کرد، پشت سر هم حریفانش را شکست می داد و برخی از این حریفان در نهایت دوست یا حتی شاگرد بروس لی شدند.

چه نتیجه ای می گیریم؟ افراد باید نوع جدیدی از مبارزه را یاد می گرفتند و گرنه مدام شکست می خوردند. آیا این خطر وجود داشت که یکی از شاگردان بروس لی از مهارت های جدیدش برای آسیب زدن به دیگران یا انجام کارهای شرورانه استفاده کند؟ بله، اما بروس لی احساس می کرد باید به افراد آموزش بدهد تا بتوانند از خودشان محافظت کنند.

بنابراین پاسخ من به پرسش «نگران نیستید که آدم های بدسرشست را مجهز کنید؟» همان پاسخی است که هشت سال پیش دادم: «نمی توانم نحوه استفاده شما از این اطلاعات را کنترل کنم.» می توانید این کتاب را بخوانید و سپس برای حمله به افراد و سرقت پول شان

از آن استفاده کنید یا می‌توانید آن را بخوانید و یاد بگیرید چگونه مدافع خوبی‌ها شوید. انتخاب با شماست، اما افراد خوب به فردی نیاز دارند که به آن‌ها آموزش بدهد. یادگیری دفاع در برابر این سبک جدید حمله فقط شامل یادگیری واکنش مناسب به حمله‌ها نیست، بلکه مانند جیت کان دو مستلزم ایجاد تعادل میان یاد گرفتن شیوه حمله، یاد گرفتن شیوه دفاع و آگاهی از زمان مناسب انجام هر کدام است. در حالی که یاد می‌گیرید چگونه یک مهندس اجتماعی باشید، باید بتوانید مانند آدم‌های بد فکر کنید و در عین حال از یاد نبرید که آدم خوب داستان هستید. به عبارت دیگر باید بتوانید بر این نیرو مسلط شوید و به سمت تاریکی نیز کشیده نشوید.

حال ممکن است بپرسید: «اگر پاسخ تغییر چندان‌ی نکرده، چه نیازی به نسخه دومی از کتاب قبلی داریم؟» اجازه بدهید بگویم.

چه چیزی تغییر کرده است؟

در بحث مهندسی اجتماعی این سؤال نقشی اساسی دارد. در ظاهر پاسخ این است: «تغییر چندان‌ی اتفاق نیفتاده است.» می‌توانید به گذشته‌های خیلی دور بروید و حکایت‌هایی از مهندسی اجتماعی پیدا کنید. به عنوان مثال یکی از اولین داستان‌های مستندی که می‌توانم در این مورد تعریف کنم در کتاب پیدایش، از کتاب‌های مقدس، آمده و حدود سال ۱۸۰۰ پیش از میلاد اتفاق افتاده است. «یعقوب» به دنبال مقام پیامبری بود که قرار بود به برادرش «عیسو» برسد. بنابراین از آنجا که می‌دانست چشمان اسحاق، پدرش، ضعیف شده و برای اینکه بفهمد با چه کسی حرف می‌زند از حواس دیگرش استفاده می‌کند، لباس‌های عیسو را پوشید و غذایی مانند آنچه عیسو قرار بود آماده کند، آماده کرد. جالب‌ترین بخش داستان اینجاست: عیسو بسیار پرمو بود، اما یعقوب این‌طور نبود، پس پوست دوبر را به بازوها و پشت گردنش بست. وقتی اسحاق با یعقوب روبه‌رو شد، با استفاده از حواس بویایی، لامسه و چشایی‌اش به این نتیجه رسید که نه با یعقوب بلکه با عیسو حرف می‌زند. طبق روایت کتاب پیدایش، حمله مهندسی اجتماعی یعقوب موفقیت‌آمیز بود.

از ابتدای ثبت تاریخ همواره شاهد حيله‌گری، فریب، شیادی و کلاهبرداری انسان‌ها بوده‌ایم. ظاهراً اتفاقی تازه در زمینه مهندسی اجتماعی نیفتاده است، اما نمی‌توان گفت

هیچ چیز هیچ وقت تغییر نمی کند.

یکی از مثال ها در این مورد «ویشینگ» (vishing) یا «فیشینگ صوتی» است. اولین باری را که از این واژه استفاده کردم، به خوبی به یاد می آورم. افراد جوری به من نگاه می کردند انگار به زبان ساختگی «کلینگان» صحبت می کردم. با این حال ویشینگ از سال ۲۰۱۵ به فرهنگ انگلیسی آکسفورد اضافه شده است.

نکته تخصصی کلینگان زبانی ساختگی است، اما مؤسسه ای واقعی (www.kli.org) برای آموزش، ترجمه و حرف زدن به این زبان وجود دارد. همچنین می توانید مترجم های زیادی پیدا کنید که این زبان را برای تان ترجمه کنند. تا امروز نشنیده ام که فردی به کمک زبان کلینگان از شیوه های مهندسی اجتماعی استفاده کرده باشد.

چرا اضافه شدن ویشینگ به فرهنگ واژگان اهمیت دارد؟ زیرا نشان می دهد شیوه های مهندسی اجتماعی چقدر روی جهان تأثیر گذاشته اند. واژه هایی که زمانی به نظر می رسید متعلق به زبانی ساختگی اند، اکنون بخشی از واژگان روزمره شده اند. فقط هم واژه ها نیستند که رایج شده اند؛ اکنون سرویس هایی وجود دارند که به صورت تخصصی به آدم های بد کمک می کنند در بد بودن بهتر شوند. به عنوان مثال وقتی برای یکی از مشتریان کاری انجام می دادم، به سرویسی برخوردیم که خدماتی تخصصی برای نمونه خوانی و غلط گیری ایمیل های فیشینگ مخرب عرضه می کرد. این شرکت، پشتیبانی شبانه روزی به زبان انگلیسی داشت. کافی است چنین مسائلی را با تبدیل شدن دستگاه های موبایل به ابررایانه های کوچک تلفیق کنید و سپس اعتیاد به شبکه های اجتماعی در دنیای جدید را به آن بیفزایید. حاصل، دستورالعملی برای یک چشم انداز حمله جدید به سبک مهندسی اجتماعی است.

علاوه بر تغییر چشم انداز، من هم تغییر کرده ام. عنوان جلد اول این کتاب مهندسی اجتماعی: هنر هک کردن انسان بود. دلیل انتخاب چنین نامی این بود که احساس می کردم آنچه در کتاب تشریح می کنم، بسیار شبیه هنر است. هنر نسبی و سلیقه ای است؛ در ذهن افراد مختلف معانی متفاوتی دارد. می توان به روش های متفاوتی آن را به کار گرفت و به

دلایلی کاملاً متفاوت از آن استفاده کرد، به آن نگاه کرد، آن را دوست داشت و از آن متنفر بود.

عنوان جلد دوم مهندسی اجتماعی: علم هک کردن انسان است. فرهنگ واژگان مریام وبستر، علم را این‌گونه تعریف کرده است: «حالت دانستن: دانش در مقابل نادانی یا کژفهمی.» هشت سال پیش بیشتر کارهایی که در حوزه امنیت انجام می‌دادم جدید بودند و همین‌طور که پیش می‌رفتم یاد می‌گرفتم. اکنون به واسطه چند سال تجربه بیشتر در «حالت دانستن» قرار دارم.

فرقی نمی‌کند یک متخصص امنیت هستید که می‌خواهد مهندسی اجتماعی را درک کند، یا فردی علاقه‌مند که می‌خواهد افق‌های پیش رویش را گسترش بدهد، یا مربی و معلمی که می‌خواهد مسائل را درک کند تا در درس‌هایش به کار بگیرد، در هر صورت امیدوارم تجربه چندساله‌ام در این زمینه، کتاب را برای شما مفیدتر کند. به هر دلیلی که این کتاب را مطالعه می‌کنید، امیدوارم با دیدگاهی علمی بتوانم این اطلاعات را مفیدتر و کامل‌تر منتقل کنم.

چرا باید این کتاب را بخوانید؟

فکر می‌کنم در این فصل ابتدا باید از همان الگویی پیروی کنم که در کتاب اول پی گرفتم، بنابراین می‌خواهم کمی در این باره بحث کنم که چرا فکر می‌کنم باید این کتاب را بخوانید. می‌دانم که شاید دیدگاهی جانب‌دارانه داشته باشم، اما به حرف‌هایم گوش کنید.

آیا انسان هستید؟ حدس می‌زنم اگر این کتاب پیش روی‌تان است و این پاراگراف را می‌خوانید، نوع پیشرفته‌ای از هوش مصنوعی یا انسان هستید. حتی به جرئت می‌گویم ۹۹/۹۹۹۹۹۹ درصد مخاطبان این کتاب انسان‌اند. مهندسی اجتماعی به فرایندهای طبیعی تصمیم‌گیری انسان‌ها متوسل می‌شود و از آسیب‌پذیری‌های موجود در این فرایندها سوءاستفاده می‌کند.

هدف مهندس اجتماعی این است که کاری کند شما بدون فکر کردن تصمیم بگیرید. هرچه بیشتر فکر کنید، بیشتر محتمل است که متوجه شوید در حال فریب خوردن هستید که بدون شک به نفع مهاجم نیست. در اپیزودهای ۷ و ۷۰ پادکست مهندس اجتماعی

(Social-Engineer Podcast) افتخار داشتم با دکتر «الن لنگر» (Ellen Langer) مصاحبه کنم. او در مورد موضوعی با من گفت و گو کرد که حالت‌های آلفا و بتا می‌خواند.

ار جاع به پادکست مهندس اجتماعی

آدرس دو اپیزود پادکست مهندس اجتماعی که در آن‌ها با دکتر لنگر مصاحبه کردم در ادامه آمده‌اند:

- اپیزود ۷ اولین مصاحبه من با دکتر لنگر است که در مورد پژوهش‌ها و کتاب‌هایش بحث می‌کنیم:

<https://www.social-engineer.org/podcasts/episode-007-using-persuasion-on-the-mindless-masses>

- اپیزود ۷۰ پنج سال بعد از مصاحبه اولم با دکتر لنگر ضبط شده است. به پادکست برگشته بود تا به ما بگوید در طول این چند سال چه چیزهایی یاد گرفته است، چه تغییراتی اتفاق افتاده و چه پیشرفت‌هایی حاصل شده‌اند:

<https://www.social-engineer.org/podcasts/ep-070-thinking-without-a-box>

حالت آلفا زمانی است که مغز با سرعت ۸ تا ۱۳ چرخه بر ثانیه فعالیت می‌کند. ویژگی شاخص این حالت معمولاً «خیال‌بافی» یا آن‌طور که دکتر لنگر می‌گفت، «تمرکز کامل در حالت آرامش» است.

حالت بتا زمانی است که مغز با سرعت ۱۴ تا ۱۰۰ چرخه بر ثانیه فعالیت می‌کند. در این حالت مغز در خصوص اتفاق‌های پیرامون، هشیار، آماده و آگاه است.

کدام حالت بیشتر برای مهندس اجتماعی مناسب است؟ البته که پاسخ حالت آلفاست، زیرا سطح تفکر و خودآگاهی کاهش یافته است. کاربرد این حالت فقط برای اهداف نیست. در این حالت فریب و برخی انواع تأثیرگذاری موجب می‌شوند شما بدون فکر عمل کنید. برای مثال، به احتمال زیاد چنین تبلیغی را مشاهده کرده‌اید: تصویر خواننده خانم معروفی را می‌بینیم و موسیقی بسیار غم‌انگیزی هم در پس زمینه پخش می‌شود. سپس

تصاویری از بچه‌گربه‌ها و سگ‌هایی پخش می‌شود که ضربه خورده‌اند، آسیب دیده‌اند، سوءتغذیه دارند، ظاهرشان چرک و کثیف است و به نظر می‌رسد رو به مرگ‌اند. سپس آن هنرمند دوباره برمی‌گردد در حالی که حیواناتی سالم اطرافش را گرفته‌اند و او به آن‌ها عشق می‌ورزد. پیام این تبلیغ چیست؟ می‌توانید با پرداخت فقط چند دلار حیوانات دچار سوءتغذیه و رو به مرگ را به حیواناتی خانگی، دوست‌داشتنی، سالم و شاد برای خودتان تبدیل کنید. تصاویر این نوع تبلیغات شبیه تصویر شکل ۱-۱ هستند.



شکل ۱-۱ این تصویر چه احساسی به شما می‌دهد؟
عکس متعلق به «پناهگاه حیوانات آمازون» (Amazon Community Animal Rescue) به آدرس www.flickr.com/photos/amazoncares/2345707195 است.

آیا سازندگان این تبلیغ شما را برای اهداف خودخواهانه فریب می‌دهند؟ نه کاملاً. آن‌ها یاد

گرفته‌اند که اگر احساسات شما را تحریک کنند، بیشتر محتمل خواهد بود که کمک مالی کنید یا کار موردنظر را انجام دهید. نرخ موفقیت چنین روشی بسیار بیشتر از این است که فقط به دانش یا منطق متوسل شوند؛ هرچه احساسات تان بیشتر تحریک شوند، کمتر منطقی فکر خواهید کرد. هرچه کمتر منطقی فکر کنید، سریع‌تر صرفاً بر اساس احساسات تحریک شده تصمیم خواهید گرفت.

پس برمی‌گردیم به نکته قبلی، اینکه اگر انسان هستید، پس این کتاب می‌تواند به شما کمک کند درک کنید چه نوع حمله‌هایی وجود دارند. می‌توانید بفهمید آدم‌های بد چطور از احساسات انسانی شما بر ضدتان استفاده می‌کنند و یاد بگیرید که چطور در برابر این حمله‌ها از خود دفاع کنید و اجازه ندهید عزیزان تان قربانی چنین حمله‌هایی شوند. اجازه بدهید با نگاهی اجمالی به مهندسی اجتماعی شروع کنم.

نگاهی اجمالی به مهندسی اجتماعی

هروقت می‌خواهم درمورد مهندسی اجتماعی بحث کنم، معمولاً با تعریفی شروع می‌کنم که در ده سال گذشته از آن استفاده کرده‌ام. با گذشت زمان فقط کمی آن را تغییر داده‌ام. اما پیش از تعریف مهندسی اجتماعی باید به نکته‌ای بسیار مهم اشاره کنم: مهندسی اجتماعی از مفهوم نزاکت سیاسی تبعیت نمی‌کند (منظور از نزاکت سیاسی پیروی از آداب و ملاحظات است که از اهانت به اقلیت‌های نژادی و مذهبی یا آزار آن‌ها پیشگیری می‌کنند). ممکن است درک این حقیقت برای بسیاری از افراد دشوار باشد، اما واقعیت دارد. مهندسی اجتماعی از سوگیری‌های جنسیتی، نژادی، سنی و موقعیتی (و همچنین ترکیبی از این سوگیری‌ها) سوءاستفاده می‌کند.

به‌عنوان مثال تصور کنید باید به ساختمان یکی از مشتریان نفوذ کنید. بدین منظور باید دستاویزی برای ورود آسان ایجاد کنید. تیم‌تان از چند فرد متفاوت تشکیل شده است. اگر به این نتیجه برسید که بهترین دستاویز برای ورود این است که فردی را به‌عنوان مستخدم ساختمان جا بزنید، کدام یک از اعضای تیم برای این کار مناسب‌ترند؟

- مرد سفیدپوست ۴۰ ساله با موی بلوند

- زن آسیایی ۴۳ ساله

• زن لاتین تبار ۲۷ ساله

از طرف دیگر اگر به این نتیجه برسید که بهترین دستاویز استفاده از فردی در نقش کارگر آشپزخانه است، کدام یک از اعضای تیم برای این کار مناسب‌ترند؟ واقعیت این است که مهندس اجتماعی ماهر می‌تواند در هر کدام از این نقش‌ها ظاهر شود و به موفقیت برسد. اما کدام فرد کمتر دیگران را به فکر وامی‌دارد؟ به یاد داشته باشید که فکر کردن هدف یا همان قربانی، دشمن مهندس اجتماعی است. با در نظر گرفتن این نکته برگردیم به تعریف من از مهندسی اجتماعی:

«مهندسی اجتماعی هر کاری است که روی فردی تأثیر می‌گذارد تا اقدامی را انجام دهد که ممکن است به نفعش باشد یا نباشد.»

می‌پرسید چرا تعریفم بسیار گسترده و کلی است؟ زیرا معتقدم مهندسی اجتماعی همیشه بد نیست.

زمانی بود که می‌توانستید بگویید «من هکر هستم» و باعث نشوید افراد عادی از شما فرار کنند و همه دستگاه‌های الکترونیکی را از برق بکشند. هکر در گذشته به معنای فردی بود که باید می‌فهمید وسیله یا دستگاهی چگونه کار می‌کند. هکرها به دانش پایه‌ای راضی نمی‌شدند، می‌خواستند عمیق‌تر شوند و سازوکار درونی و پنهان هر چیزی را بفهمند. سپس وقتی می‌فهمیدند، بررسی می‌کردند که آیا راهی وجود دارد که بتوان آن ابزار را دور زد، بهبود بخشید، از آن بهره‌برداری کرد یا هدف اولیه‌اش را تغییر داد.

وقتی نگارش اولین کتابم را شروع کردم می‌خواستم اطمینان حاصل کنم می‌توانم مهندسی اجتماعی را به نحوی تعریف کنم که این‌طور القا نکند که همیشه پای کلاهبردار، حقه‌باز یا شایادی در میان است. می‌توان از همان اصولی که آدم‌های بد از شان استفاده می‌کنند، برای رسیدن به اهداف خوب استفاده کرد و می‌خواستم افراد این را بدانند.

اغلب از این تصویرسازی استفاده می‌کنم: اگر به من مراجعه می‌کردید و می‌گفتید: «کریس، می‌خواهم به مهمانی چای شاهزاده خانم دعوت کنم؛ یعنی اینکه اینجا بنشینم و در حالی که روسری صورتی سر کرده‌ای، من ناخن‌هایت را لاک بزنم و درمورد شاهزاده خانم‌های دیزنی صحبت کنیم»، نه فقط به شما می‌خندیدم، بلکه به آرامی از شما دور می‌شدم و به دنبال اولین راه خروج می‌گشتم. با این حال باید اعتراف کنم چنین اتفاقی

برایم افتاده است.

چطور ممکن است؟ دخترم من را به مهمانی چای شاهزاده خانم دعوت کرد. پیش از آنکه بگویید: «این مقایسه منصفانه نیست؛ معلوم است که عاشق دخترت هستی و به همین دلیل پذیرفتی»، اذعان می‌کنم که این موضوع نقش زیادی در تصمیم داشت، اما به اصول روان‌شناسانه‌ای فکر کنید که در اتخاذ این تصمیم نقش داشتند. برای اینکه درخواستی را بپذیرم که اگر فرد دیگری از من خواسته بود، در یک نانو ثانیه رد می‌کردم، می‌باید فرایند تصمیم‌گیری عادی‌ام را دور می‌زدم.

واقعیت بی‌مصرف

با توجه به اینکه یک نانو ثانیه یک میلیاردیم ثانیه است و هر فرد عادی با سرعت ۱۴۵ واژه در هر دقیقه صحبت می‌کند، در عمل نمی‌توانستم در یک نانو ثانیه پاسخ منفی بدهم. از طرف دیگر، نور که ۱۸۶ هزار مایل بر ثانیه سرعت دارد، می‌تواند در یک نانو ثانیه یک فوت جابه‌جا شود.

وقتی سازوکار تصمیم‌گیری را درک کنید، به‌مرور می‌توانید بفهمید که مهاجمی مخرب چطور می‌تواند با استفاده از محرک‌های احساسی، اصول روان‌شناسی و به‌کارگیری هنر و علم مهندسی اجتماعی کاری کند که شما «کاری را انجام بدهید که به نفع‌تان نیست». دکتر «پل زک» (Paul Zak) در اپیزود ۴۴ پادکست مهندس اجتماعی حضور داشت. او نویسنده کتاب مولکول اخلاق (The Moral Molecule) (انتشارات داتون، ۲۰۱۲) است. دکتر زک در این کتاب و در پادکست ما در مورد پژوهشش درباره هورمونی به نام «اکسی‌توسین» حرف می‌زند. پژوهش او به ما کمک کرده است که بفهمیم اکسی‌توسین چه رابطه نزدیکی با اعتماد دارد، زیرا نظر بسیار مهمی درباره این مسئله دارد که چطور وقتی احساس می‌کنیم فردی به ما اعتماد دارد، این هورمون در خون‌مان آزاد می‌شود. لطفاً این نکته بسیار حیاتی را درک کنید: مغز ما نه فقط وقتی به فردی اعتماد می‌کنیم، بلکه وقتی احساس می‌کنیم فرد دیگری به ما اعتماد کرده نیز اکسی‌توسین آزاد می‌کند. بر اساس پژوهش دکتر زک، این پدیده در ارتباط حضوری، تلفنی، اینترنتی و حتی وقتی نمی‌توانیم

فرد «اعتمادکننده» را ببینیم، بروز می‌کند.

ارجاع به پادکست مهندس اجتماعی

اپیزود ۴۴ پادکست مهندس اجتماعی شامل گفت‌وگویی جذاب با دکتر زک درباره این دستاورد مهم زندگی‌اش است. می‌توانید این اپیزود را در این آدرس پیدا کنید:
www.social-engineer.org/podcast/ep-044-do-you-trust-me

ماده شیمیایی دیگری که مغز ما تولید می‌کند «دوپامین» است. دوپامین انتقال‌دهنده‌ای عصبی است که در اوقات لذت، شادی و تحریک آزاد می‌شود. با ترکیب اکسی‌توسین و دوپامین، یک مغز مستعد مهندسی اجتماعی ایجاد می‌شود که هر دری را که بخواهید باز می‌کند.

دوپامین و اکسی‌توسین در زمان برقراری روابط خودمانی آزاد می‌شوند، اما ممکن است هنگام گفت‌وگوهای عادی هم آزاد شوند. این گفت‌وگوها اساس مهندسی اجتماعی‌اند. معتقدم هر روز (بارها و ناخودآگاه) از این اصول در ارتباط با همسر، رئیس، همکاران، کشیش، مشاور و تعمیرکاران و هر فرد دیگری که می‌بینیم استفاده می‌کنیم. در نتیجه، درک مهندسی اجتماعی و نحوه برقراری ارتباط با هم‌نوعان یکی از ضروریات زندگی امروز است.

در دنیایی که فناوری برقراری ارتباط را با استفاده از شکلک‌ها یا با یک توییت آسان کرده، یادگیری نحوه استفاده از مهارت‌های گفت‌وگو دشوارتر شده است، چه برسد به اینکه بخواهیم بفهمیم از این مهارت‌ها چه زمانی علیه ما استفاده می‌شود. وضعیت زمانی بدتر شد که شبکه‌های اجتماعی جامعه‌ای ایجاد کردند که گفتن همه‌چیز به همه درمورد خودمان پذیرفتنی و حتی ترویج شد.

وقتی درمورد مهندسی اجتماعی مخرب حرف می‌زنم، آن را به چهار شیوه زیر تفکیک می‌کنم:

- «اسمیشینگ» (SmiShing): بله، چنین عبارتی وجود دارد و معادل فیشینگ پیامکی یا فیشینگ از طریق پیام‌های متنی است. در سال ۲۰۱۶،

وقتی هکرها به شرکت «ولز فارگو» (Wells Fargo) نفوذ کردند، پیامک حمله اسمیشینگ به نمایش درآمده در شکل ۱-۲ را دریافت کردم.

(ولز-فارگو) پیام مهمی از طرف
واحد امنیت!
به حساب‌تان وارد شوید
vigourinfo.com/secure.
well5farg0card.html

شکل ۱-۲ این حمله اسمیشینگ افراد زیادی را به دام انداخت

نکته جالب این است که من اصلاً در ولز فارگو حساب ندارم، اما باز هم هدف این حمله قرار گرفتم (و نه خیر، نمی‌گویم در چه بانکی حساب دارم!). هکرها می‌توانستند با یک کلیک ساده نام کاربری و رمز عبور را سرقت یا بدافزاری را روی دستگاه موبایل بارگذاری کنند و گاهی اوقات هر دو را انجام دهند.

- «**ویشینگ**»: همان‌طور که پیش از این گفتم، این عبارت معادل فیشینگ صوتی است. کاربرد این شیوه از سال ۲۰۱۶ به شدت افزایش یافته و برای مهاجم نیز آسان، ارزان و بسیار سودآور است. همچنین با توجه به اینکه مهاجمان از شماره‌های جعلی خارج از کشور تماس می‌گیرند، پیدا کردن مکان‌شان تقریباً غیرممکن است.

- «**فیشینگ**»: پربحث‌ترین موضوع در حوزه مهندسی اجتماعی فیشینگ است. در واقع ویراستار فنی این کتاب، یعنی «میشل» و من کتابی در این مورد با عنوان ابعاد پنهان فیشینگ: جنبه‌های تهاجمی و تدافعی ایمیل‌های مخرب (Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails) (انتشارات وایلی، ۲۰۱۶) نوشته‌ایم (بله، درست متوجه شدید؛ خیلی بی‌شرمانه یکی دیگر از کتاب‌هایم را تبلیغ کردم). از فیشینگ برای

توقف کار کارخانه‌ها، هک کردن کمیته ملی حزب دموکرات، نفوذ به کاخ سفید و همچنین ده‌ها شرکت بزرگ و سرقت میلیون‌ها دلار در شیادی‌های گوناگون استفاده شده است. فیشینگ، با اختلاف، خطرناک‌تر از سه شیوه حمله دیگر است.

• «جعل هویت»: می‌دانم که انتظار داشتید این مورد هم با کلمه‌ای هم‌وزن کلمات فوق تمام شود، اما تنها کاری که می‌توانستم انجام دهم این بود که این مورد را در انتهای فهرست قرار دهم. با این حال جایگاه جعل هویت در این فهرست به هیچ‌وجه به این معنی نیست که نباید به اندازه سایر موارد نگران آن باشیم. در ۱۲ ماه گذشته صدها گزارش جمع‌آوری کرده‌ایم مبنی بر اینکه افراد با جعل هویت پلیس، مأموران فدرال و همکاران‌شان دست به جنایت‌هایی واقعاً وحشتناک زده‌اند. در آوریل ۲۰۱۷ گزارشی درباره مردی منتشر شد که اقدام به جعل هویت پلیس کرده و دستگیر شده بود. این فرد در پورنوگرافی کودکان دست داشت و از جعل هویت برای کسب سود استفاده می‌کرد.

اطلاعات بیشتر

هنگام نگارش این صفحات می‌توانستید آن گزارش منجرکننده را در این آدرس مشاهده کنید:

www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn-20170418-story.html

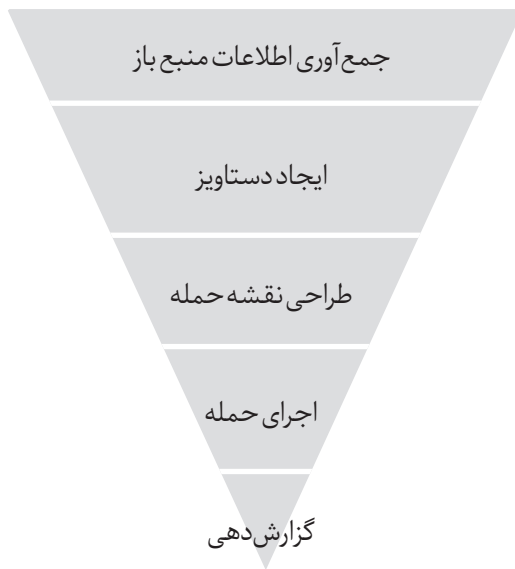
هر حمله مبتنی بر مهندسی اجتماعی را می‌توان در یکی از این چهار طبقه‌بندی قرار داد. به تازگی شاهد حمله‌هایی هستیم که «حمله ترکیبی» می‌خوانیم و در آن‌ها مهندسان اجتماعی مخرب، از ترکیبی از این شیوه‌ها در یک حمله استفاده می‌کنند تا به اهداف‌شان دست یابند.

وقتی این حمله‌ها را تحلیل می‌کنم، الگوهایی را می‌بینم که فقط انواع ابزارها و فرایندهایی را شناسایی می‌کنند که مهاجمان از آن‌ها استفاده کرده‌اند، اما همین اطلاعات نیز می‌توانند به یک متخصص امنیت کمک کنند نحوه اجرای این حمله‌ها را با وضوحی بیشتر بفهمد و

سپس از نتایج برای آموزش و حفاظت استفاده کند. با این کار در واقع از مقوله‌ای استفاده می‌شود که هرم مهندسی اجتماعی می‌خوانم.

هرم مهندسی اجتماعی

اجازه بدهید در همین ابتدا هرم را ببینیم و بعد توضیح بدهم که چرا آن را تعریف کردم و هر بخش چه معنایی دارد. هرم در شکل ۱-۳ نشان داده شده است.



شکل ۱-۳ هرم مهندسی اجتماعی

همان‌طور که می‌بینید هرم به چند بخش تقسیم شده است و به مهندسی اجتماعی از دیدگاه یک مهندس اجتماعی حرفه‌ای نگاه می‌کند؛ یعنی نه فردی که از مهندسی اجتماعی برای اهداف شرورانه استفاده می‌کند، بلکه فردی که می‌خواهد در این زمینه به مشتریان کمک کند. در ادامه هر بخش را تعریف می‌کنم و در فصل‌های بعدی کتاب با جزئیات بیشتری به هر لایه می‌پردازم.

جمع‌آوری اطلاعات منبع‌باز

جمع‌آوری اطلاعات منبع‌باز رکن حیاتی هرگونه فعالیت مهندسی اجتماعی است. همچنین آن بخشی است که باید بیشترین زمان را صرفش کرد؛ به همین دلیل اولین و بزرگ‌ترین بخش از هرم را به خود اختصاص داده است. یکی از تکه‌های این بخش از هرم به‌ندرت موردتوجه قرار می‌گیرد، یعنی مستندسازی. چطور اطلاعاتی را که پیدا می‌کنید، مستند، ذخیره و فهرست‌بندی می‌کنید؟ در فصل بعد بیشتر درمورد این عامل کلیدی بحث می‌کنم.

ایجاد دستاویز

گام منطقی بعدی این است که بر اساس همه یافته‌ها در مرحله جمع‌آوری اطلاعات، شروع کنید به ایجاد دستاویزها. این بخش حیاتی است و باید با در نظر گرفتن اطلاعات منبع‌باز انجام شود. در این مرحله متوجه می‌شوید که چه تغییراتی باید انجام و چه چیزهایی باید اضافه شوند تا اطمینان حاصل کنید موفق می‌شوید. در این مرحله همچنین معلوم می‌شود که به چه لوازم و ابزارهایی نیاز دارید.

طراحی نقشه حمله

داشتن دستاویز به معنی آماده بودن نیست. مرحله بعدی پاسخ‌گویی به پرسش‌های چه، چه زمانی و چه کسی است.

- نقشه چیست؟ به دنبال دستیابی به چه چیزی هستیم؟ مشتری چه می‌خواهد؟ این پرسش‌ها به ایجاد بخش بعدی کمک می‌کنند.
- چه موقع بهترین زمان حمله است؟
- چه فرد یا افرادی باید در کمترین زمان ممکن برای پشتیبانی یا کمک در دسترس باشند؟

اجرای حمله

حالا نوبت به بخش هیجان‌انگیز یعنی اجرای حمله می‌رسد. طبق نقشه آماده‌اید که با تمام توان جلو بروید. باید آماده باشید، در عین حال نباید همه‌چیز آن‌قدر از پیش تعیین شده و مکتوب باشد که نتوانید پویا باشید. کاملاً موافقم که باید نقشه‌ای مکتوب وجود داشته باشد و فکر می‌کنم در ادامه می‌تواند از دردسرهای زیادی پیشگیری کند. اما نگرانی‌ام این

است که اگر همه حرف‌ها و کارهایی را که فکر می‌کنید مورد نیازند از پیش مشخص کنید، ممکن است وقتی اتفاق‌هایی بیفتند که از قبل پیش‌بینی نشده‌اند، با مشکل روبه‌رو شوید. ذهن‌تان متوجه می‌شود که در آن موقعیت هیچ برنامه مکتوبی ندارید که از آن کمک بگیرید و دچار درماندگی و اضطراب می‌شوید و نشانه‌های ترس در شما نمایان می‌شود. این اتفاق می‌تواند واقعاً توانایی‌تان برای موفقیت را از بین ببرد. به جای اینکه همه چیز را از پیش تعیین کنید، پیشنهاد می‌کنم طرحی کلی داشته باشید که مسیری را پیش روی شما قرار دهد، اما دست شما را هم باز بگذارد و امکان بداهه‌پردازی را هم برای‌تان فراهم کند.

گزارش‌دهی

صبر کنید! نخوانده از این بخش عبور نکنید. درست است که دادن گزارش، کاری جذاب نیست، اما می‌توانید این‌طور به آن فکر کنید: مشتری‌تان پولی به شما پرداخت کرده است تا خدماتی را به او بدهید و به احتمال زیاد در حمله‌ها بسیار موفق بوده‌اید. اما مشتری فقط برای این کار به شما پول نداده است، به شما پول داده که بفهمد چه کاری می‌تواند انجام دهد تا مشکل را برطرف کند. به همین دلیل مرحله گزارش‌دهی در نوک هرم قرار دارد و بقیه هرم بر آن تکیه کرده است.

اگر از پنج مرحله این هرم پیروی کنید، هم به عنوان مهندس اجتماعی و هم به عنوان متخصصی که به مشتریان خدمات مهندسی اجتماعی می‌دهد، به موفقیت می‌رسید. واقعیت این است که مهندسان اجتماعی مخرب نیز از همین گام‌ها، به جز گام گزارش‌دهی، پیروی می‌کنند.

«دارک ریدینگ» (Dark Reading) در سال ۲۰۱۵ از حمله‌ای خبر داد که در آن از همین هرم پیروی شده بود (می‌توانید این مقاله را با عنوان حمله کریربیلدر رزومه‌های حاوی بدافزار را به کسب‌وکارها می‌فرستد را در آدرس

<https://www.darkreading.com/vulnerabilities---threats/careerbuilder-attack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236> مشاهده کنید).

۱. مهاجمان در مورد حمله به چند هدف تحقیق کرده و هنگام جمع‌آوری اطلاعات منبع‌باز متوجه شده بودند که اهداف از سایت کاریابی پرطرفداری به نام کریربیلدر

استفاده می‌کنند.

۲. مهاجمان بعد از تکمیل مرحله جمع‌آوری اطلاعات منبع‌باز ایجاد دستاویز را شروع کرده بودند. در نتیجه دستاویزی را به‌عنوان پذیرفتن نقش کارجویی برنامه‌ریزی کردند که می‌خواهد در جایی استخدام شود که شرکت‌های هدف برای آن استخدام می‌کردند. فهمیدند که ابزارهای مورد نیازشان فایل‌های کدگذاری شده مخرب و رزومه‌هایی با ظاهر واقع‌بینانه است.

۳. با پاسخ دادن به پرسش‌های چه، چه زمانی و چه کسی، شروع کرده بودند به طراحی نقشه حمله.

۴. بعد حمله‌ها را با آپلود کردن اسناد مخرب، نه در وب‌سایت هدف، بلکه در وب‌سایت کریربیلدر اجرا کرده بودند. شرکت‌هایی که درخواست استخدام داده بودند از طریق ایمیل خبردار می‌شدند که متقاضی جدیدی وجود دارد و ایمیل حاوی پیوست‌هایی بود که مهاجم آپلود کرده بود.

۵. مهاجمان مرحله گزارش‌دهی عملیاتی را انجام نداده بودند، اما به لطف پژوهشگرانی در «پروف‌پوینت» (Proofpoint) گزارشی عملیاتی درمورد این حمله وجود دارد.

این حمله به این دلیل موفق بود که سوژه، ایمیلی به همراه پیوستی از منبعی قابل اعتماد و معتبر (کریربیلدر) دریافت می‌کرد. در نتیجه بدون فکر کردن پیوست را باز می‌کرد. خواسته مهندس اجتماعی مخرب نیز دقیقاً همین بود؛ کاری کند که سوژه بدون فکر کردن و در نظر گرفتن خطرهای بالقوه دست به اقدامی بزند که به نفعش نیست.

در این کتاب چه می‌خوانید؟

وقتی برنامه‌ریزی برای نوشتن این کتاب را شروع کردم، می‌خواستم حتماً طبق طرح کلی نسخه اول کتاب مهندسی اجتماعی پیش بروم تا افرادی که از آن کتاب بهره‌برده بودند، از این کتاب هم بهره‌برند. هم‌زمان می‌خواستم آن کتاب را تغییر بدهم و به‌روز کنم تا به برخی از حمله‌ها و پدیده‌های جدیدی بپردازم که در کتاب قبلی بررسی نکرده بودم. می‌خواستم اطمینان حاصل کنم که از همه توصیه‌های طرف‌داران، پژوهشگران،

خوانندگان و منتقدان استفاده می‌کنم، با این امید که این کتاب را بسیار بهتر از کتاب قبلی بنویسم. اجازه بدهید ساختار و قالب این کتاب را به صورتی کلی مرور کنیم تا بدانید چه در پیش دارید.

در فصل دوم، «آنچه من می‌بینم تو هم می‌بینی؟»، درمورد جمع‌آوری اطلاعات منبع‌باز بحث می‌کنم و همچنین برخی از روش‌های مورد استفاده که تاریخ انقضایی ندارند. از بررسی مفصل ابزارها خودداری می‌کنم، اما به چند ابزار اشاره می‌کنم که از دهه گذشته در جعبه‌ابزار من باقی مانده‌اند.

در فصل سوم، «پرو فایل بندی افراد از طریق ارتباط»، موضوعی را بررسی می‌کنم که در نسخه اول کتاب چندان مطرح نشد؛ یعنی ابزارهای پیشرفته مدل سازی و پرو فایل بندی ارتباطات را عمیق و موشکافانه بررسی می‌کنم.

از فصل چهارم، «تبدیل شدن به هرکسی که می‌خواهید»، پرداختن به ایجاد دستاویز شروع می‌شود. خارج از حوزه مهندسی اجتماعی، افراد زیادی درباره این موضوع بحث نمی‌کنند. به نکته‌ها، ترفندها و بسیاری از تجربه‌های (موفق و شکست خورده‌ای) می‌پردازم که در طول سال‌ها به دست آورده‌ام.

در فصل پنجم، «می‌دانم چطور کاری کنم که دوستم داشته باشی»، اطلاعاتی را از پادکست‌ها، خبرنامه‌ها و گفت‌وگوهای با برخی از افراد برجسته این حوزه در جهان، مثل «رابین دریک» (Robin Dreeke)، جمع‌آوری کرده‌ام و درباره چگونگی به کارگیری اصول اعتمادسازی در مهندسی اجتماعی بحث می‌کنم. رابین دریک رئیس «واحد تحلیل رفتاری» (Behavioral Analysis Unit) «اف بی آی» و یکی از دوستان خوب من است. در اعتمادسازی تبحر زیادی دارد و گام‌های مورد نیاز برای انجام این کار را تعریف کرده است.

در فصل ششم، «تحت تأثیر»، از مطالعات «رابرت چالدینی» (Robert Cialdini)، یکی از رهبران حوزه پژوهش در مورد تأثیرگذاری بر مهندسی اجتماعی استفاده کرده‌ام. این فصل نشان می‌دهد که مهندسان اجتماعی چطور می‌توانند از اصولی که چالدینی در طول سال‌ها پژوهش، تدوین کرده است استفاده کنند و استفاده می‌کنند.

در فصل هفتم، «خلق اثر هنری»، چهارچوب بندی و استخراج اطلاعات را تعریف می‌کنم و نشان می‌دهم که چطور هر فردی می‌تواند در هر دو حوزه متبحر شود.

در فصل هشتم، «می‌توانم آنچه را نگفتی ببینم»، سراغ یکی از موضوع‌های مورد علاقه‌ام، یعنی ارتباطات غیرکلامی، رفته‌ام.

در کتاب دیگرم با عنوان برداشتن نقاب مهندس اجتماعی: عنصر انسانی امنیت (Unmasking the Social Engineer: The Human Element of Security) (انتشارات وایلی، ۲۰۱۴) این موضوع را کاملاً موشکافی کرده‌ام، اما این فصل راهنمایی مقدماتی برای آشنایی با ارتباطات غیرکلامی است.

در فصل نهم، «هک کردن انسان‌ها»، محتوای هشت فصل قبلی درمورد پنج نوع متفاوت از حمله‌های مهندسی اجتماعی را به کار می‌گیرم. این فصل نشان می‌دهد به کارگیری اصول این کتاب چقدر برای شما به عنوان مهندس اجتماعی حرفه‌ای مهم است.

کمی مانده به انتهای کتاب، در فصل دهم، «برنامه کاهش اثر و پیشگیری دارید؟» به پیشگیری از حمله‌های مهندسی اجتماعی و کاهش تأثیرگذاری آن‌ها پرداخته‌ام. در این فصل چهار گام یادگیری نحوه مقابله با همه حمله‌های مهندسی اجتماعی را توضیح داده‌ام. سپس این کتاب هم باید مانند هر چیز خوب دیگری به پایان برسد، پس کتاب با فصل یازدهم، «حالا چی؟»، تمام می‌شود.

چند قولی که درمورد این کتاب به شما می‌دهم:

- قول می‌دهم به‌ویژه هنگام اشاره به پژوهش‌ها به ویکی‌پدیا به عنوان منبعی معتبر ارجاع ندهم (از اشتباه‌هایم درس گرفته‌ام).
- قول می‌دهم داستان‌های زیادی از تجربه‌های حدود هفت سال اخیرم تعریف کنم. گاهی داستانی را از چندین زاویه تعریف می‌کنم تا چند نکته کاملاً در ذهن‌تان تثبیت شوند.
- وقتی از پژوهش‌ها و مطالعه‌های برخی از برجسته‌ترین افراد در هر حوزه‌ای استفاده می‌کنم، حتماً به کارهای آن‌ها ارجاع می‌دهم تا بتوانید درمورد هر موضوعی که می‌خواهید مفصل‌تر تحقیق کنید.
- درست مانند کتاب اولم، با روی باز از همه تماس‌ها، نظرها، پیشنهادهای و انتقادهای استقبال می‌کنم.

اگر تازه‌کارید، این کتاب می‌تواند به شما کمک کند بفهمید به چه چیزهایی نیاز دارید

تا به یک مهندس اجتماعی حرفه‌ای تبدیل شوید. اگر باتجربه‌اید، امیدوارم با به اشتراک گذاشتن چند داستان، نکته و ترفند ابزارهای جدیدی را در اختیارتان قرار دهم. اگر صرفاً به این حوزه علاقه‌مندید، می‌خواهم این کتاب را با همان هیجانی بخوانید که من هنگام نگارش آن داشتم. اگر هم فردی بدبین هستید، این کتاب را با این دیدگاه بخوانید که ادعا نمی‌کنم بهترین و تنها منجی مهندسی اجتماعی هستم. فقط مهندس اجتماعی مشتاقی با چندین سال تجربه‌ام که می‌خواهد دانش و تجربه‌اش را به اشتراک بگذارد تا شاید این دنیا را کمی امن‌تر کند.

خلاصه

هیچ کتابی به قلم من وجود ندارد که بدون تشبیهی به آشپزی کامل باشد، پس این شما و این تشبیه، بفرمایید! مهندسی اجتماعی مانند هر غذای خوش مزه‌ای نیازمند برنامه‌ریزی زیاد، دستورالعملی عالی با استفاده از مواد تازه و پخت یا اجرای هنرمندانه و علمی است. هرچند مهندسی اجتماعی در ذات خود ساده است، دستورالعملی دارد که برای تازه‌کارها مناسب نیست. در مهندسی اجتماعی باید درک کنید انسان‌ها چطور تصمیم می‌گیرند، چه چیزهایی به آن‌ها انگیزه می‌دهد و شما چطور در عین حال که از فرایندهای احساسی دیگران بهره‌برداری می‌کنید، احساسات‌تان را کنترل کنید.

موضوع این کتاب امروز همان قدر مهم و مرتبط است که هشت سال پیش بود، شاید اکنون حتی مهم‌تر باشد. در هشت سال گذشته شاهد پیشرفت و مطرح شدن افراد زیادی به‌عنوان مهندس اجتماعی حرفه‌ای بوده‌ام. ظهور و افول مهندسان اجتماعی مخرب زیادی را هم دیده‌ام.

با توجه به گرایش زیاد ماهیت حمله‌ها به سمت عنصر انسانی، درک مهندسی اجتماعی برای همه متخصصان امنیت ضروری است. اما این موضوع بسیار گسترده‌تر از این حرف‌هاست. یادم می‌آید وقتی (سال‌ها پیش، قبل از ورود به حوزه مهندسی اجتماعی) کارم را به‌عنوان آشپز شروع کردم، مربی‌ام از من می‌خواست تمام مواد تشکیل‌دهنده هر غذا را کمی بچشم. چرا چنین خواسته‌ای از من داشت؟

می‌گفت اگر مزه هر کدام از مواد را به‌خوبی درک نکنم، امکان ندارد بفهمم «چشیدن»

به چه معناست. وقتی می‌دانم در دستور پخت غذا کمی ترب کوهی وجود دارد و می‌خواهم غذا کمی تندتر شود، می‌فهمم می‌توانم کمی بیشتر ترب کوهی اضافه کنم. وقتی می‌دانم ماده خاصی خودش کمی شور است، مقدار نمک غذا را طوری تنظیم می‌کنم که مواد بیش از حد طعم‌دار نشوند. خودتان دیگر منظور را متوجه می‌شوید.

حتی اگر در حوزه امنیت فعال نیستید، باید «مزه» هرکدام از این عناصر را بفهمید تا بتوانید از خودتان محافظت کنید. اعتمادسازی به چه معناست و چطور می‌توان با استفاده از آن کاری کرد که فرد از پولش بگذرد؟ (این موضوع در فصل پنجم بررسی شده است). چطور استفاده از تأثیرگذاری در گفت‌وگوی استخراج اطلاعات باعث می‌شود فردی رمز عبورش را پشت تلفن به فردی دیگر بدهد؟ (در فصل‌های ششم و هفتم به این موضوع پرداخته‌ام). هرکدام از این عناصر می‌توانند به شما کمک کنند «مزه» را بفهمید. اگر با آن‌ها آشنا شوید، وقتی فردی از آن‌ها علیه‌تان استفاده کند، می‌توانید تشخیص بدهید و در نتیجه امنیت بیشتری داشته باشید. می‌توانید بفهمید مشکلی وجود دارد و تدابیر دفاعی اتخاذ کنید.

آیا تابه‌حال مسابقات آشپزی با گوردون رمزی را تماشا کرده‌اید؟ وقتی غذای شرکت‌کننده‌ای را می‌خورد و دوست ندارد، دقیقاً مشکل را تشخیص می‌دهد. به عنوان مثال می‌گوید: «این غذا خیلی فلفل دارد و از روغن زیادی برای پختش استفاده شده است.» در مقابل، فردی تازه‌کار ممکن است بگوید: «خیلی تند و چرب است.» آیا این دو توصیف یکسان‌اند؟ من این‌طور فکر نمی‌کنم. می‌خواهم به شما کمک کنم به یک گوردون رمزی در دنیای مهندسی اجتماعی تبدیل شوید.

اکنون با همه این حرف‌ها بیایید به سراغ فصل پرمحتوای بعدی برویم و درمورد جمع‌آوری اطلاعات منبع‌باز بحث کنیم.



فصل دوم
آنچه من می بینم
تو هم می بینی؟



به یاد داشته باشید که ناکامی یک رویداد است و چیزی به نام انسان ناکام وجود ندارد.
زیگ زیگلار (Zig Ziglar)

جمع آوری اطلاعات منبع باز رکن اساسی مهندسی اجتماعی است. اطلاعات نقطه شروع و تکیه گاه هر تعاملی اند. جمع آوری اطلاعات منبع باز برای ما مهندسان اجتماعی اهمیت زیادی دارد، در نتیجه ضروری است با انواع روش های کسب اطلاعات در مورد سوژه هایمان آشنا شویم. صرف نظر از نحوه جمع آوری اطلاعات منبع باز باید تصویری روشن از آنچه می خواهید داشته باشید. شاید در ظاهر آسان باشد، اما آن قدر که به نظر می رسد آسان نیست. نمی توانید به سادگی بگویید: «همه اطلاعات مربوط به سوژه را می خواهم.» هر نوع اطلاعاتی ارزشی متفاوت دارد و ارزشمند بودن هر اطلاعاتی ممکن است به نوع حمله ای بستگی داشته باشد که می خواهید انجام دهید.

نمونه ای واقعی از جمع آوری اطلاعات منبع باز

اجازه بدهید تصویری کلی به شما بدهم؛ طبق اطلاعات سایت www.worldwidewebsite.com بیش از ۴/۴۸ میلیارد وب سایت فهرست شده وجود دارند. این رقم شامل وب سایت های موجود در «دارک وب» و «دیپ وب» نمی شود. ترافیک اینترنت سالانه جهان به ۱/۳ زتابایت (یعنی ۱,۳۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰ بایت) رسیده است. حتی منبعی مدعی است که اینترنت می تواند در مجموع تا ۱۰ یوتابایت داده داشته باشد (۱۰ یوتابایت یعنی ۱۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰ بایت).

نکته جالب

یوتابایت که در کمال تعجب بعد از زتابایت قرار دارد، با الهام از شخصیت «یودا» (Yoda) در مجموعه فیلم های جنگ ستارگان نام گذاری شده است. واحدهای دیگری هم وجود دارند که از یوتابایت بزرگ ترند و نام هایی عجیب تر هم دارند، از جمله می توان به «شیلنتنوبت» (shilentnobyte) و «دامجمگروتنا بایت» (domegemegrottebyte) اشاره کرد.

اساساً درک مقدار ترافیک اینترنت چه اهمیتی دارد؟ به عنوان مثال اگر بخواهید ایمیل فیشینگ ارسال کنید، شاید بهتر باشد دنبال این موارد بگردید: سرگرمی های شخصی سوژه، مقوله هایی که به آنها علاقه دارد، از آنها بیزار است، یا برایش ارزشمند است. اما اگر بخواهید از طریق ویشینگ به سوژه حمله کنید، شاید بهتر باشد جزئیاتی در مورد شغل و نقشش در سازمان پیدا کنید و ببینید او انتظار دارد از کدام منابع داخلی و خارجی با او تماس بگیرند. اگر هدف شما ورود به محلی باشد، باید بفهمید آیا سوژه با افراد ملاقات می کند یا خیر و همچنین با چه افرادی قرار می گذارد.

بیش از ۴/۴۸ میلیارد وب سایت وجود دارند که در آنها باید دنبال داده هایی بگردید که ممکن است مفید باشند. بنابراین پیش از شروع جست و جو باید برای جمع آوری داده های منبع باز برنامه ریزی کنید. به منظور تعیین محدوده برای جست و جوی تان از فهرست پرسش های جدول ۲-۱ استفاده کنید.

جدول ۲-۱ نمونه پرسش های جمع آوری اطلاعات منبع باز

نوع سازمان	آنچه باید پرسید
شرکت	شرکت مورد نظر چطور از اینترنت استفاده می کند؟
	شرکت مورد نظر چطور از شبکه های اجتماعی استفاده می کند؟
	آیا شرکت مورد نظر برای محتوایی که کارمندان تولید و در اینترنت منتشر می کنند، قانونی تعیین کرده است؟
	شرکت مورد نظر با چند وندور همکاری می کند؟
	شرکت مورد نظر از کدام وندورها استفاده می کند؟
	شرکت مورد نظر پرداخت ها را از طریق چه روش هایی می پذیرد؟
	شرکت مورد نظر چطور پرداخت های خودش را انجام می دهد؟
	آیا شرکت مورد نظر مرکز تماس دارد؟
	ساختمان های مرکزی، مراکز تماس و سایر شعبه های شرکت مورد نظر کجا واقع شده اند؟
	آیا شرکت مورد نظر اجازه می دهد افراد دستگاه های خودشان را داخل شرکت ببرند؟
	آیا شرکت مورد نظر یک ساختمان دارد یا چند ساختمان؟
	آیا چارت سازمانی وجود دارد؟

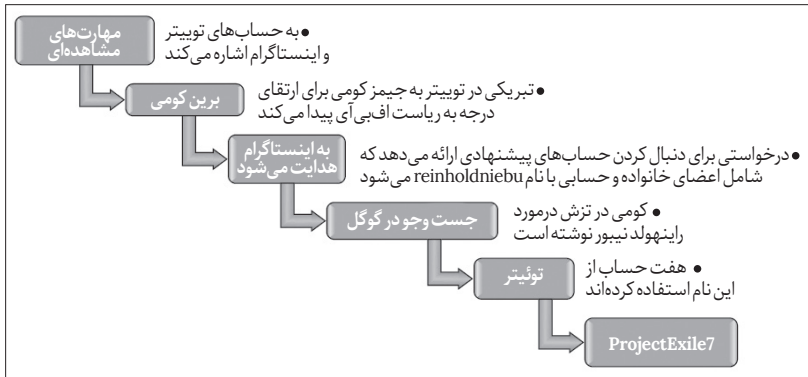
فرد مورد نظر از کدام حساب‌های شبکه‌های اجتماعی استفاده می‌کند؟ فرد مورد نظر چه سرگرمی‌هایی دارد؟ فرد مورد نظر برای تعطیلات کجا می‌رود؟ فرد مورد نظر به کدام رستوران‌ها علاقه دارد؟ پیشینه خانوادگی فرد مورد نظر (شامل بیماری‌ها، کسب و کارها و غیره) چیست؟ فرد مورد نظر تا چه سطحی و در چه رشته‌ای تحصیل کرده است؟ فرد مورد نظر چه نوع شغلی دارد، از جمله اینکه در خانه برای شرکت کار می‌کند، برای خودش کار می‌کند و به چه کسی گزارش می‌دهد؟ آیا سایت دیگری وجود دارد که به فرد مورد نظر اشاره کند (شاید سخنرانی می‌کند، برای انجمن‌های اینترنتی مطلب می‌فرستد یا عضو باشگاهی است)؟ آیا فرد مورد نظر صاحب خانه است؟ اگر بله، مالیات، وثیقه و سایر اطلاعات مربوط به این ملک به چه صورت است؟ نام اعضای خانواده فرد مورد نظر (و همچنین همه اطلاعات پرسش‌های قبل درمورد این افراد) چیست؟	فرد
--	------------

البته پاسخ این پرسش‌ها فقط اطلاعاتی سطحی‌اند. می‌توانید پرسش‌های دیگری را درمورد انواع کامپیوترهای مورد استفاده، برنامه زمانی کارمندان، زبان‌های مورد استفاده، نوع آنتی‌ویروس و بسیاری از مسائل دیگر اضافه کنید.

بیا بید به ماجرای زیر بپردازیم که از عناوین خبری سال ۲۰۱۷ استخراج شده است (می‌توانید روایتی از آن را در آدرس <https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitteraccount-1793843641> مشاهده کنید).

محور داستان رئیس سابق اف‌بی‌آی، «جیمز کومی» (James Comey) است. بلاگر و پژوهشگری اینترنتی قصد داشت ببیند آیا می‌تواند حساب‌های جیمز کومی را در شبکه‌های اجتماعی پیدا کند. چون کومی رئیس اف‌بی‌آی بود، مشخصات حساب‌هایش در شبکه‌های اجتماعی در دسترس عموم نبود، همچنین اساساً مشخص نبود حسابی در شبکه‌های اجتماعی دارد یا خیر. اینجا نقطه شروع ماجرای جمع‌آوری اطلاعات منبع‌باز است.

طرح کامل اقدام‌های این بلاگر برای رسیدن به نتیجه در شکل ۱-۲ نشان داده شده است. نگاهی به آن بیندازید تا بعد سراغ بررسی مفصل هر گام برویم.



شکل ۱-۲ جمع‌آوری جالب اطلاعات منبع‌باز درمورد سوژه

این پژوهشگر ابتدا باید تعیین می‌کرد چه اطلاعاتی را می‌خواهد آشکار کند: آیا جیمز کومی در شبکه‌های اجتماعی حساب دارد؟ اگر دارد، آدرس‌شان چیست؟ از قرار معلوم تحقیق در این مورد صرفاً با استفاده از اینترنت بسیار دشوار بوده است. در سال ۲۰۱۶، یکی از وب‌سایت‌ها «۶۰ پلتفرم برتر شبکه‌های اجتماعی» را فهرست کرده بود. پیدا کردن یک نفر در این تعداد پلتفرم در دسترس (که هر کدام قوانین و روش‌هایی متفاوت دارند) بسیار سخت است.

خوشبختانه یکی از روش‌های قدیمی جمع‌آوری اطلاعات، یعنی گوش دادن، به سود این پژوهشگر عمل کرده بود؛ جیمز کومی در یکی از اظهارنظرهای عمومی‌اش اشاره کرده بود که حساب توییتر و اینستاگرام دارد.

این اظهارنظر به پژوهشگر ما کمک کرده بود که جست‌وجو را از بیش از ۶۰ پلتفرم شبکه اجتماعی به فقط دو پلتفرم محدود کند. مدیریت تحقیق درمورد دو پلتفرم بسیار راحت‌تر است.

او ابتدا هیچ حسابی را پیدا نکرده بود که به‌طور مستقیم به کومی مرتبط باشد، اما بعد حساب توییتر «برین کومی» (Brien Comey)، پسر رئیس اف‌بی‌آی را یافته بود. او زمانی توانسته بود ارتباط میان برین کومی و جیمز کومی را بفهمد که متوجه شده بود برین به‌خاطر انتصاب به سمت رئیس اف‌بی‌آی به جیمز کومی تبریک گفته است.

یکی از کارهایی که کاربران می‌توانند انجام دهند این است که حساب‌های مختلف‌شان در شبکه‌های اجتماعی را به یکدیگر لینک کنند. در این مورد برین حساب اینستاگرامش را به حساب توئیترش لینک کرده بود. این بلاگر به حساب اینستاگرام برین مراجعه کرده بود، اما برین حسابش را خصوصی کرده و در نتیجه فقط افرادی می‌توانستند پست‌هایش را ببینند که برین به آن‌ها اجازه داده بود.

وی تصمیم می‌گیرد برای برین درخواست دنبال کردن بفرستد. یکی از قابلیت‌های اینستاگرام این است که وقتی منتظرید کاربری درخواست دنبال کردن شما را بپذیرد، فهرستی از افرادی در همان حلقه را به شما پیشنهاد می‌دهد تا اگر خواستید بتوانید یکی از آن‌ها را دنبال کنید. اینستاگرام چند کاربر را پیشنهاد داده بود که اعضای خانواده برین (به غیر از جیمز کومی) و حسابی با نام کاربری reinholdniebuhr بودند.

اگر در اینترنت کمی درباره «راینهولد نیبور» (Reinhold Niebuhr) جست‌وجو کنید، خیلی سریع متوجه می‌شوید که الهی‌دان و مفسر مسائل سیاسی اهل آمریکا بوده است. البته در سال ۱۹۷۱ از دنیا رفته، پس بعید است که حساب اینستاگرام داشته باشد. اما این پژوهشگر با کمی تحقیق متوجه شده بود کومی در تز دانشگاهش درمورد راینهولد نیبور نوشته است.

با داشتن این اطلاعات توئیتر را جست‌وجو و هفت حساب پیدا کرده بود که از این نام استفاده کرده بودند. یکی از این هفت حساب با آیدی ProjectExile7@ از این نام به صورت عمومی استفاده کرده بود.

با کمی جست‌وجوی بیشتر فهمیده بود «Project Exile» (پروژه تبعید) نام برنامه‌ای بوده که کومی زمانی آن را آغاز کرده که دادستان ایالات متحده بوده و در «ریچموند» (Richmond) زندگی می‌کرده است.

این پژوهشگر با دنبال کردن سرنخ‌ها و بدون دسترسی به هیچ‌گونه اطلاعات غیرقانونی، بدون هک کردن و صرفاً با نگاه کردن به منابع اطلاعات منبع‌باز به آنچه می‌خواست رسیده بود. این تحقیقات نمونه‌ای عالی از تلفیق اطلاعات منبع‌باز غیرفنی و فنی و درس خوبی برای همه مهندسان اجتماعی است. از این رو، مبنای ادامه این فصل انواع متفاوت اطلاعات منبع‌باز و نحوه استفاده از آن‌ها در نقش مهندس اجتماعی است. انواع اطلاعات منبع‌باز

را به دو دسته اصلی اطلاعات منبع باز غیرفنی و فنی تقسیم کرده‌ام.

مستند کردن یا نکردن؛ مسئله این است

پیش از آنکه سراغ انواع اطلاعات منبع باز برویم، می‌خواهم کمی درباره افکارم درمورد مستندسازی بگویم.

پرسش اصلی در واقع مستند کردن یا نکردن نیست. پرسش‌های اصلی این‌ها هستند: برای مستند کردن از چه ابزارهایی استفاده و چقدر مستند کنیم.

به حرفی که در ابتدای این فصل زدم فکر کنید: وقتی در ۱۰ یوتایپت داده جست‌وجو می‌کنید، اطلاعات زیادی درمورد اهداف‌تان می‌یابید. مهم نیست چقدر باهوش باشید، در هر صورت نمی‌توانید همه جزئیات را به خاطر بسپارید مگر اینکه حافظه تصویری داشته باشید. حتی افراد دارای حافظه تصویری نیز نمی‌توانند فقط با اتکا به حافظه‌شان گزارش‌دهی حرفه‌ای را انجام دهند.

نمی‌توانم به شما بگویم دقیقاً چطور باید مستندسازی کنید زیرا عوامل بسیار زیادی در این زمینه وجود دارند. به عنوان مثال وقتی این مسیر شغلی را شروع کردم و همه کارها را خودم به تنهایی انجام می‌دادم، از نرم‌افزارهای یادداشت‌برداری پیشرفته‌ای استفاده می‌کردم که امکان ایجاد پوشه یا یادداشت جدید برای هر مشتری را فراهم می‌کردند. بعد می‌توانستم یادداشت‌ها را به بخش‌های متفاوت، مثل بخش شخصی، کاری، خانوادگی، شبکه‌های اجتماعی و... تقسیم کنم. وقتی اطلاعات منبع‌بازی پیدا می‌کردم، آن‌ها را در بخش مناسب مستند می‌کردم که پیدا کردن داده‌ها را هنگام نوشتن گزارش آسان‌تر می‌کرد. از ترفندهای ساده‌ای مثل به کارگیری رنگ‌های خاص برای موارد مربوط به حمله‌ها استفاده می‌کردم: از رنگی برای یافته‌های معمولی و از رنگی دیگر برای یافته‌های حیاتی.

بعد به مرور تعداد اعضای تیم افزایش یافت و افراد زیادی را داشتم که روی یک پروژه کار می‌کردند. در نتیجه متوجه این موضوع شدم که ردوبدل کردن یادداشت‌ها به هیچ وجه بهترین راه حل نیست. باید به راه‌حلی می‌رسیدم که به اعضای تیم امکان می‌داد یادداشت‌ها را به اشتراک بگذارند.

ابتدا به ابزارهایی مثل گوگل درایو فکر کردم. به اپلیکیشن‌های یادداشت مبتنی بر ابر و سایر ابزارهای ابری دیگر هم فکر کردم. این راه‌حل‌ها چند مشکل داشتند:

- وظیفه داشت شماره‌های تأمین اجتماعی، داده‌های بانکی و سایر اطلاعات خصوصی و شخصی زندگی افراد را جمع‌آوری کنم. اگر راه‌حلی که از آن استفاده می‌کردم هک می‌شد، چه اتفاقی می‌افتاد؟ (این اتفاق در سال ۲۰۱۳ و با نفوذ به نرم‌افزار «اورنوت» (Evernote) افتاد که بیش از ۵۰ میلیون نفر را مجبور کرد رمزهای عبورشان را تغییر دهند).
- نمی‌توانستم نحوه دسترسی به راه‌حل‌ها و نحوه مدیریت داده‌ها را کنترل کنم.
- خود واژه «ابری» اغلب باعث می‌شد برخی از مشتریان پاسخ منفی بدهند.

در نتیجه شروع کردم به ایجاد سرور اختصاصی. در ساختمان میزبان سروری فضایی گرفتیم که ارزیابی شده و امن بود. سرور مجازی خصوصی خودمان را ایجاد کردیم و نرم‌افزار انتخابی‌مان را روی سروری متعلق به خودمان نصب کردیم که پشت فایروال‌ها، روترها و سرور مجازی شخصی‌مان قرار داشت.

به این ترتیب نحوه ذخیره‌سازی، مدیریت، پشتیبان‌گیری، انتقال و تأمین امنیت داده‌ها در کنترل خودمان بود. این راه‌حل به من اجازه می‌داد شب با خیال راحت بخوابم زیرا از نحوه مدیریت داده‌های مشتریان‌مان اطمینان داشتم. شاید شما راه‌حلی متفاوت داشته باشید. مهم این است که ذخیره‌سازی، مدیریت، پشتیبان‌گیری، انتقال و تأمین امنیت هرگونه داده جمع‌آوری شده از مشتریان‌تان را جدی بگیرید.

اطلاعات منبع باز غیرفنی

اطلاعات منبع باز غیرفنی را هر اطلاعاتی می‌دانم که به تماس مستقیم مهندس

اجتماعی و استفاده از کامپیوتر نیازمند نیست. شاید در حالی که سوژه از کامپیوتر استفاده می‌کند، مخفیانه از پشت شانه‌اش اطلاعاتی درباره‌اش به دست بیاورید، اما این شما (به عنوان مهندس اجتماعی) نیستید که از کامپیوتر استفاده می‌کنید. این اطلاعات را با استفاده از روشی غیرفنی به دست آورده‌اید.

شیوه‌های خاص زیادی وجود دارند که می‌توان در اینجا بررسی‌شان کرد، اما همه آن‌ها را با تسامح ذیل مهارت‌های مشاهده‌ای تعریف می‌کنم و در بخش زیر چند مثال درباره‌شان می‌آورم.

مهارت‌های مشاهده‌ای

شاید به نظر برسد مهارت‌های مشاهده‌ای مشهودند و استفاده از آن‌ها آسان است، اما استفاده موفقیت آمیز از آن‌ها، به ویژه در عصر رواج رسانه‌های دیجیتال، مهارتی معمولی نیست. در واقع روش‌های بازاریابی امروزی باعث شده‌اند ما به جزئیات توجه نکنیم. مطالعه «امیلی دراگو» (Emily Drago) از دانشگاه «الون» (Elon University) در سال ۲۰۱۵ (با عنوان «تأثیر فناوری بر ارتباط چهره‌به‌چهره» نشان می‌دهد کیفیت ارتباط چهره‌به‌چهره به واسطه فناوری کاهش یافته است. از میان افرادی که در این مطالعه تحت نظر قرار گرفتند، ۶۲ درصد هنگام گفت‌وگو با دیگران از یک دستگاه موبایل استفاده می‌کردند، در حالی که می‌دانستند این کار کیفیت ارتباط را کاهش می‌دهد.

توجه برای مطالعه متن کامل پژوهش «تأثیر فناوری بر ارتباط چهره‌به‌چهره» به

آدرس /[www.elon.edu/docs/e-web/academics/communications/](http://www.elon.edu/docs/e-web/academics/communications/research/vol6no1/02DragoEJSpring15.pdf)

[research/vol6no1/02DragoEJSpring15.pdf](http://www.elon.edu/docs/e-web/academics/communications/research/vol6no1/02DragoEJSpring15.pdf) مراجعه کنید.

در جامعه‌ای زندگی می‌کنیم که بیشتر ارتباطات در آن از طریق پیام‌های ۲۸۰ کاراکتری، شکلک‌ها و میم‌ها یا پست‌های شبکه‌های اجتماعی برقرار می‌شوند. پیشرفت‌هایی که این ارتباطات را ممکن می‌سازند حیرت‌انگیزند، اما وضعیتی را به وجود آورده‌اند که در آن افراد هنگام برقراری ارتباط کمتر حواس‌شان به طرف مقابل است. به همین دلیل است که در بخش اطلاعات منبع‌باز غیرفنی مهارت‌های مشاهده‌ای در صدر فهرست من قرار دارند.

شاید بپرسید:

- مهارت‌های مشاهده‌ای چه مهارت‌هایی هستند؟
 - برای به دست آوردن این مهارت‌ها چه کاری می‌توانیم انجام دهیم؟
 - چه انتظاری باید از این مهارت‌ها داشته باشیم؟
- بیایید در مورد هر کدام از این پرسش‌ها بحث کنیم و ببینیم چه چیزهایی را می‌توانید مشاهده کنید و یاد بگیرید.

مهارت‌های مشاهده‌ای چه مهارت‌هایی هستند؟

سناریوهای زیر مثال‌هایی از نحوه استفاده از مهارت‌های مشاهده‌ای در دنیای واقعی‌اند.

سناریوی یک

مأموریت شما ورود به اتاق نامه‌ها در یک مرکز درمانی بزرگ است. این کار را باید در روز روشن انجام دهید. نمی‌توانید دزدکی قفل‌ها را باز کنید، از دیوارها بالا بروید یا از پنجره‌ها وارد شوید. بنابراین پیشخوان و کارمندان حراست را امتحان می‌کنید تا ببینید آیا به شما اجازه می‌دهند وارد محدوده امن شوید یا خیر. پس باید از بخش کارمندان حراست مرکز درمانی عبور کنید.

آنچه در ادامه می‌آید فقط چند مورد از مهارت‌های مشاهده‌ای هستند که باید داشته باشید:

- **لباس و پوشش:** این قسمت مهم ساده است اما گاهی اوقات مغفول می‌ماند. در فصل اول، «نگاهی به دنیای جدید مهندسی اجتماعی حرفه‌ای»، گفتم هدف مهندس اجتماعی این است که کاری کند بدون فکر کردن تصمیم بگیرد. اگر به مکانی نفوذ کنید که همه در آنجا لباس غیررسمی پوشیده باشند و شما با کت و شلوار و جلیقه باشید، توجه افراد را به خودتان جلب می‌کنید. عکس این وضعیت نیز همین‌طور است، پس باید بدانید کارمندان چطور لباس می‌پوشند تا بتوانید پوششی مناسب انتخاب کنید.
- **ورودی‌ها و خروجی‌ها:** پیش از ورود به ساختمان بفهمید نقاط خروج کجا قرار دارند. آیا دری وجود دارد که افراد سیگاری برای سیگار کشیدن پشت آن جمع

شوند؟ آیا تدابیر امنیتی یکی از ورودی‌ها بیشتر از ورودی دیگر است؟ آیا شیفت تغییر می‌کند که باعث شود محل نگهبانی خاصی در زمانی از روز بدون نگهبان باشد یا نگهبان کمتری داشته باشد؟

• **الزامات ورود:** برای ورود به ساختمان یا محوطه آن چه الزاماتی وجود دارند؟ آیا کارمندی می‌بینید که آرم سینه (badge) داشته باشند؟ چه نوع آرمی دارند؟ آیا برای ورود باید کدی را هم بدانند؟ آیا فردی بازدیدکننده‌ها را مشایعت می‌کند؟ آیا بازدیدکننده‌ها آرم ورود دریافت می‌کنند؟ آیا در چرخان، میز نگهبانی یا تمهید امنیتی دیگری در محل ورود وجود دارد؟

• **امنیت محدوده:** ببینید بیرون از ساختمان چه خبر است. آیا دوربین امنیتی وجود دارد؟ آیا نگهبانان در محوطه گشت می‌زنند؟ آیا درهای زباله‌دانی‌ها قفل شده‌اند؟ آیا زنگ هشدار یا سیستم حفاظتی حساس به حرکتی وجود دارد؟

• **کارمندان حراست:** آیا مشغول نگاه کردن به دستگاه‌های موبایل یا صفحه کامپیوترشان هستند یا هشیارند و به اطراف‌شان توجه می‌کنند؟ آیا بیش از حد خسته و کسل به نظر می‌رسند یا سرحال و علاقه‌مند به کارشان؟

• **وضعیت سالن انتظار:** آیا دستگاه امنیتی یا صفحه کلیدی وجود دارد که بتوانید مخفیانه از پشت سر و روی شانه افراد رمز عبورشان را سرقت کنید؟ (به عبارت دیگر آیا می‌توانید آن قدر نزدیک شوید که از پشت شانه افراد رمز عبورشان را هنگام وارد کردن ببینید؟)

البته ممکن است موارد بسیار بیشتری وجود داشته باشند که بخواهید مشاهده کنید و موارد یادشده مقدماتی باشند.

برای اینکه کمک کنم بفهمید چرا این معیارها مهم‌اند، داستانی واقعی را تعریف می‌کنم که شامل لباس و پوشش، ورودی‌ها و خروجی‌ها، الزامات ورود و امنیت محدوده می‌شود. همان سناریویی که در ابتدای این بخش مطرح کردم، به میشل (ویراستار فنی این کتاب) و من سپرده شده بود. باید مقدار نسبتاً زیادی اطلاعات منبع باز فنی جمع‌آوری می‌کردیم که در ادامه این فصل به آن می‌پردازم، در عین حال مقدار زیادی اطلاعات منبع باز غیرفنی وجود داشتند که به موفقیت ما منجر شدند.

تصمیم گرفتیم از این دستاویز استفاده کنیم که شرکت سم‌پاشی و کنترل آفاتی هستیم که انتخاب شده تا در مورد سم‌پاشی اضطراری برای از بین بردن عنکبوت‌ها قیمتی پیشنهاد بدهد. نام شرکت مان را شرکت کنترل آفات «بیگ بلو» (Big Blue) گذاشتیم و با لباس‌هایی با لوگوی بیگ بلو و ظرف‌های سم‌پاشی حاوی «سم» آبی ویژه‌ای مراجعه کردیم تا در فرایند اعلام قیمت هر عنکبوتی را که دیدیم بکشیم. این سم در واقع فقط نوشابه غیرگازدار آبی‌رنگ از برند «گیترید» (Gatorade) در ظرف‌های سم‌پاشی بود.

نکته جالب استفاده از گیترید آبی در پوشش سم‌روشی عالی برای همراه داشتن نوشیدنی انرژی‌زا و طراوت بخشی است که وقتی در عملیات نفوذ به ساختمان مضطرب شده‌اید و به شدت عرق می‌ریزید، می‌تواند به رفع تشنگی‌تان کمک کند. با این حال اگر داخل آسانسور در حال نوشیدن از «ظرف سم‌پاشی» باشید و ناگهان فردی وارد شود، احتمالاً باید نگاه‌هایی متعجب را تحمل کنید.

با رانندگی پیرامون محدوده شروع کردیم. به ورودی‌ها، خروجی‌ها، مکان دوربین‌ها، مکان تجمع سیگاری‌ها و ورودی‌های شلوغ‌تر در برابر ورودی‌های خلوت‌تر توجه کردیم. همچنین توجه کردیم ببینیم کارمندانی که وارد و خارج می‌شوند آرم سینه دارند یا خیر و چطور لباس پوشیده‌اند. سپس نقطه ورود اول مان را انتخاب کردیم و به آهستگی به سمت در قدم زدیم. دلیل قدم زدن آهسته این بود که تا حد ممکن ببینیم افراد چطور به داخل راه داده می‌شوند.

دو نگهبان دیدیم. وقتی افراد کارت‌هایشان را به استندی فلزی فشار می‌دادند و اجازه ورود می‌گرفتند، این نگهبان‌ها بر کارشان نظارت می‌کردند. همچنین میز حراستی در سمت راست بود که در آنجا فردی برای نظارت بر دفتر ورود و خروج حضور داشت.

تصمیم گرفتیم سرمان را پایین بیندازیم و از کنار نگهبان‌ها رد شویم و جمعیت را به سمت داخل دنبال کنیم. این نقشه اصلاً موفق نبود؛ یکی از نگهبان‌ها ما را نگه داشت و پرسید چه کار می‌کنیم و چرا آنجا هستیم. به نامش که بروی پیراهنش حک شده بود، نگاه کردم و بعد گفتم: «ببین اندرو، از ما خواسته شده به اینجا بیاییم و برای سم‌پاشی اضطراری

عنکبوت‌ها پیشنهاد قیمت بدهیم...» نگهبان وسط حرفم پرید و گفت: «باشد، برو جلوی میز و دفتر را امضا کن.»

فکر کردم اجازه ورود را گرفتیم و دیگر می‌توانیم وارد شویم، اما وقتی به میز نزدیک شدیم، مردی که آنجا بود نام‌های مان را پرسید. نام‌های جعلی مان را گفتیم و او در فهرستی دنبال‌شان گشت. وقتی نام مان را در فهرست پیدا نکرد گفت: «متأسفم، در فهرست بازدیدکنندگان امروزمان نیستید. بدون اجازه نمی‌توانید وارد شوید.»

سعی کردیم توضیح بدهیم، رویش تأثیر بگذاریم و حتی با فشار و درخواست کمک کارمان را راه بیندازیم. اما هیچ‌کدام کارساز نبودند. از در جلو خارج شدیم. در حین قدم زدن در آن حوالی درمورد گام بعدی صحبت می‌کردیم که چند نفر را بیرون در حال استراحت و سیگار کشیدن دیدیم. به میشل گفتم دنبال‌م بیاید و به سمت آن‌ها رفتیم. به نحوی رفتار می‌کردیم که انگار باید آنجا باشیم و در حال بررسی محیط بیرون ساختمان هستیم. وانمود کردم در حال نوشتن یادداشت روی تخته‌شاسی‌ام هستم.

دوباره آرام قدم زدیم تا اینکه دیدیم چند نفر به سمت در می‌روند و درست پشت سرشان حرکت کردیم. بعد از ورود به ساختمان دنبال‌شان می‌کردیم که به سرعت متوجه شدم مستقیم به سمت همان دری می‌رویم که مأموران حراستی آنجا هستند که همین چند لحظه پیش به ما اجازه ورود نداده بودند. آسانسوری را سمت راست دیدم، اما هیچ دکمه‌ای نداشت. با خودم فکر کردم: «عجب شائسی! آسانسوری که تحت کنترل حراست است.» در همین حین ناگهان در آسانسور باز شد. بی‌درنگ وارد شدم و امیدوار بودم میشل هم ببیند و پشت سرم بیاید.

خوشبختانه میشل در این کارها بسیار عالی است، در نتیجه نه گم شده بود و نه اضطراب خیلی زیادی داشت. چند نفر داخل آسانسور بودند و میشل بلافاصله با صدای بلند گفت: «رئیس، می‌شود کار را زودتر تمام کنیم؟ خیلی گرسنه‌ام و گفتید نمی‌توانیم تا پایان کار چیزی بخوریم.»

خانمی که داخل آسانسور بود نگاهی ناراضی به من انداخت و گفت: «به این زن بیچاره غذا بدهید.» پاسخ دادم: «خودم هم می‌خواهم، اما فقط یک طبقه دیگر مانده. هرچه زودتر کار را تمام کنیم، زودتر می‌تواند غذا بخورد.»

آن خانم آهی کشید و گفت: «بسیار خب، پس بگویند کجا می‌روید تا آسانسور را در همان طبقه نگه داریم...» وسط حرفش پریدم و گفتم: «به اتاق نامه‌ها می‌رویم.»، چند دکه را فشار داد و گفت: «شما را آنجا پیاده می‌کنم.»

خوشبختانه به خاطر مهارت‌های مشاهده‌ای عالی میشل و سرعت عمل من، دست‌مان رو نشده بود و حتی توانسته بودیم خانمی خوش‌برخورد را متقاعد کنیم که ما را به آن طبقه امن ببرد (در ضمن میشل فقط تا حدی تظاهر می‌کرد چون در واقع همیشه گرسنه است). در طبقه اتاق نامه‌ها از آسانسور بیرون آمدیم و فهمیدیم در اتاق نامه‌ها قفل است. زنگی با برج‌سیبی وجود داشت که رویش نوشته شده بود: «برای کمک زنگ بزنید.» زنگ را زدیم و منتظر ماندیم.

خانمی آمد و گفت: «چطور می‌توانم کمک‌تان کنم؟» دست‌اویزمان، یعنی قیمت دادن، را مطرح کردیم. آن خانم پاسخ داد: «در هر صورت باید به حراست زنگ بزنم تا تأییدیه بگیرم.»

اگر به حراست زنگ می‌زد، لو می‌رفتیم، پس گفتم: «اگر بخواهید می‌توانید زنگ بزنید، اما خود اندرو ما را به اینجا فرستاد تا کار را انجام دهیم.»

گفت: «اندرو شما را فرستاده؟ پس بفرمایید داخل.» اجازه داد به اتاق نامه‌ها وارد شویم و گفت: «فقط به نامه‌ها دست نزنید» سقف‌پوش‌ها، کابل‌های شبکه و مقدار زیادی نامه را جابه‌جا کردیم و سپس سقف را گشتیم.

همان‌طور که در طول این داستان متوجه شدید، اتفاق‌های زیادی افتاد چون مشاهداتی سریع داشتیم و اطلاعات را برای استفاده بعدی ذخیره کردیم (و اینجا تازه شروع داستان بود).

نمی‌دانستم به نام اندرو نیاز خواهم داشت، میشل نمی‌دانست با خانمی دل‌سوز در آسانسور روبه‌رو خواهیم شد و هیچ‌کدام نمی‌دانستیم با چند سیگاری بی‌تفاوت برخورد خواهیم کرد که اهمیتی نمی‌دهند دنبال‌شان وارد ساختمان شویم. اما مشاهدات این امکان را برای مان فراهم کردند که برای موفقیت از این افراد استفاده کنیم.

سناریوی دوم

مأموریت دارید و کیلی برجسته در یک شرکت آمریکایی بزرگ را با حمله فیشینگ هدف

قرار دهید. اجازه دارید از هر اطلاعاتی که درباره‌اش پیدا می‌کنید بهره ببرید. وقتی به بخش اطلاعات منبع باز فنی برسیم، اطلاعات بیشتری از این داستان آشکار خواهند شد، اما برای تأکید بر درسی بسیار ارزشمند اجازه بدهید به شما بگویم چطور در این مورد به شکلی مفترضانه شکست خوردم.

با بهره‌گیری از اطلاعات منبع باز به این نتیجه رسیدیم که این وکیل به مسائلی در ماساچوست رسیدگی می‌کند. متوجه به‌روزرسانی تازه‌ای در قانون مالیات ماساچوست شدیم که می‌توانست توجه او را جلب و مجابش کند روی یک لینک یا باز کردن پیوستی بسیار مخرب کلیک کند.

شروع کردم به نوشتن ایمیلی درباره تغییرات در ایالت ماساچوست و همه ابعاد حمله فیشینگ را برنامهریزی کردم. ایمیل به شکلی حرفه‌ای نوشته شده بود، تهدید نمی‌کرد، شامل بسته اطلاعاتی موردنظرمان بود، مهلتی واقع‌بینانه برای مطالعه و پاسخ‌گویی تعیین می‌کرد و به اندازه‌ای اطلاعات می‌داد که اطمینان حاصل شود برای گرفتن اطلاعات بیشتر مجبور است روی لینک کلیک کند.

چند دقیقه پس از ارسال ایمیل لورفتیم و گزارش شدیم و مأموریت کاملاً شکست خورد. آیا در همان پاراگراف قبلی متوجه نقص حمله شدید؟ پیش از آنکه نقص را بگویم، چند ثانیه فرصت می‌دهم تا به عقب برگردید و پاسخ را پیدا کنید. وقت تمام شد!

ماساچوست ایالت نیست، مشترک‌المنافع است. این وکیل که نقطه قوتش توجهش به جزئیات بود، ایمیلی درباره تغییرات در قانون مالیات «ایالت ماساچوست» دریافت کرده و با خودش گفته بود: «اگر ایمیل واقعی بود، باید می‌دانستند که ماساچوست ایالت نیست، مشترک‌المنافع است.» این اشتباه باعث شده بود به آدرس «فرستنده» و آن یو آر آل (URL) نگاه کند و به قدری مشکوک شود که ایمیل را گزارش کند. در نتیجه پوشش مان لورفت.

این جزئیات کوچک را مشاهده نکردیم و بابت این مشاهده نکردن هزینه دادیم. درس این سناریو این است که باید همه چیزهای ممکن را مشاهده کنید. مانند فردی فکر کنید که می‌خواهید مهندسی اجتماعی را درموردش به کار بگیرید. تلاش کنید بفهمید انتظار دارد چه ببیند و همان را عرضه کنید. در غیر این صورت جزئیات کوچک بعداً

در درس ساز می شوند.

برای به دست آوردن این مهارت ها چه کاری می توانیم انجام دهیم؟

پرداختن به این موضوع در بخش کوچکی از یک کتاب دشوار است. توانایی های ذاتی و توانایی های اکتسابی هر فردی می توانند یادگیری این مهارت ها را بسیار آسان یا بسیار دشوار کنند. از آنجا که شما را نمی شناسم، فقط می توانم بگویم خودم چه کار کردم تا مهارت هایم را بهبود بخشم.

یک بازی مشابه بازی تسخیر پرچم انجام می دهم (در این بازی هر کدام از تیم ها سعی می کنند پرچم تیم دیگر را بگیرند و به سلامت به زمین شان برگردند). اگر قرار بود وارد ساختمانی شوم (برای مثال مطب یک پزشک) با خودم می گفتم: «پرچم ها این موارد هستند: به خاطر سپردن دو نفر اولی که می بینم، رنگ پیراهن شان و مجله ای که می خوانند یا کاری که می کنند.»

محدودیت هایی مشابه موارد زیر تعیین می کردم:

- این افراد نمی توانند افراد مربوط به آن سرویس باشند که پشت پیشخوان هستند.

- در عین حال باید مأموریت بررسی را هم انجام بدهم و نمی توانم متوقفش کنم یا از آن منحرف شوم.

- نمی توانم چیزی یادداشت کنم.

بعد وارد ساختمان می شدم، مشاهده می کردم و با تمام توان تلاش می کردم مشاهداتم را تا زمان ترک ساختمان از یاد نبرم. آن چیزهایی که به خاطر می سپردم شبیه موارد زیر بودند:

- زن مسن تر که پیراهن آبی پوشیده و سمت راست نشسته بود مجله وومنز دی (Woman's Day) می خواند.

- کودک، مذکر، تی شرت راه راه، در حال بازی با بلوک ها روی زمین.

مشاهدات را در ذهنم ثبت می کردم و تمام توانم را به کار می گرفتم تا آن ها را از یاد نبرم. از چند ترفند ثبت حافظه استفاده می کردم، برای مثال چیزی را چند بار با خودم تکرار می کردم تا در ذهنم تثبیتش کنم.

وقتی احساس می کردم می توانم بدون اینکه زیاد فکر کنم، یادداشت برداری ذهنی

انجام دهم، پیچیدگی را افزایش می‌دادم. در نهایت فهرست پرچم‌ها شبیه فهرست زیر می‌شدند:

- جنسیت X تعداد از افراد؛
- چه پوشیده بودند؛
- اولین باری که این افراد را دیدم، مشغول چه فعالیت‌هایی بودند؛
- تصورم از پروفایل ارتباط (در فصل سوم، «پروفایل بندی افراد از طریق ارتباط» بیشتر به این موضوع می‌پردازم)؛
- زبان بدن مشکوک.

همیشه با استفاده از این اطلاعات تلاش می‌کنم داستانی در ذهنم بسازم که چرا این افراد در مکانی بودند که من بودم و از جزئیات داستان برای یادآوری آن‌ها استفاده می‌کنم. صادقانه می‌گویم این روش (حتی با حافظه ضعیف من) آن‌قدر خوب است که می‌توانم دفتر کاری را به یاد بیاورم که سه یا چهار سال پیش واردش شدم و در آنجا دو خانم را دیدم که دامن مشکی و پیراهن دکمه‌ای پوشیده بودند و روی آپید چیزی می‌خواندند. به نظر می‌رسید خانم سمت چپ از خانم سمت راست خوشش نمی‌آید اما او را تحمل می‌کند. با توجه به اینکه پایین تنه خانم سمت چپ از خانم سمت راست فاصله داشت، به این نتایج رسیدم.

مردی با پوشش نگهبانی (کت و شلوار مشکی، پیراهن سفید و کراوات مشکی) پشت پیشخوان بود. ساعتی طلا به مچ دست راستش بسته بود که نشان می‌داد چپ‌دست است. موهایی مرتب و ریشی آراسته داشت. با خودکار روی دفترچه چیزی می‌نوشت. هم من و هم سالن انتظار را زیر نظر داشت.

مرد جوانی آنجا بود که جلوی پیشخوان روی صندلی نشسته بود. به روزنامه‌ای نگاه می‌کرد، اما به نظر می‌رسید تظاهر به خواندن می‌کند. به فضا خیره شده بود و لبه‌های روزنامه می‌لرزیدند. داستانی را در ذهنم ساختم مبنی بر اینکه برای مصاحبه شغلی به آنجا آمده و مضطرب است، اما تلاش می‌کند خودش را آرام نشان بدهد و حواسش را با روزنامه پرت کند.

انگار همین الان هم آن سالن انتظار را در ذهنم می‌بینم. این مشاهدات کوچک نقش

مهمی در دستیابی شما، به عنوان مهندس اجتماعی، به اهداف تان دارند. پیشنهاد می‌کنم دنبال نقاط ضعف خودتان بگردید و از کارهای کوچک شروع و به مرور سخت ترشان کنید. این نکته را از یاد نبرید که باید تمرین کنید. بارها پیش می‌آید افرادی را می‌بینم که می‌خواهند بلافاصله به موفقیت صد درصدی برسند، اما این کار زمان بر است.

اگر اجازه بدهیم، شکست می‌تواند خیلی بیشتر از موفقیت به ما درس بدهد. به همین دلیل است که باید در مورد انتظارات حرف بزنم.

چه انتظاری باید از این مهارت‌ها داشته باشیم؟

در کتاب برداشتن نقاب مهندس اجتماعی که به همراه دکتر «پل اکمن» (Paul Ekman) نوشته‌ام، فقط روی سرخ‌های غیرکلامی، یعنی زبان بدن و حالت چهره، تمرکز کردم. وقتی تازه داشتم یاد می‌گرفتم که چطور ابتدا متوجه این نشانه‌ها شوم و بعد رمزگشایی‌شان کنم، احساس می‌کردم نوعی ابرقهرمان با قدرت ذهن خوانی‌ام. می‌توانستم به فردی نگاه کنم و احساساتی را ببینم که او سعی می‌کرد پنهان کند و سپس این نشانه‌ها را با زبان بدن و اعمال دیگری ترکیب می‌کردم تا تقریباً از پیش بفهمم چطور به پرسش‌ها یا موقعیت‌ها واکنش نشان خواهد داد.

نکته جالب این است که پیش‌بینی‌هایم در بیش از ۵۰ درصد مواقع درست بودند. آنجا بود که مشکل شروع شد. فرض کنید در ۷۵ درصد مواقع درست حدس می‌زنم که یعنی در ۲۵ درصد مواقع اشتباه می‌کنم. علاوه بر این، روی تصورم از توانایی‌هایم تأثیر گذاشت. بیشتر از آنچه در واقعیت بود، احساس می‌کردم می‌بینم، درک می‌کنم و در نتیجه مهندسی اجتماعی می‌کنم.

یکی از درس عبرت‌هایم را هنگام کار با دکتر اکمن گرفتم، درسی که باعث شد بسیار متواضع شوم. او مدام اشتباه‌هایم را اصلاح می‌کرد و می‌گفت: «کریس، چون چیستی را می‌بینی، به این معنی نیست که چرایی را هم می‌دانی.»

پیش از بحث در مورد انتظارات، احساس می‌کنم باید این گزاره را چند بار بشنوید: چون چیستی را می‌بینی، به این معنی نیست که به‌طور خودکار چرایی را هم می‌دانی. چطور می‌توان ارتباطی میان چیستی و چرایی برقرار کرد؟ چند راه شامل پرسیدن، کسب اطلاعات بیشتر و مشاهده طولانی‌تر وجود دارد.

به این مثال توجه کنید: در کلاسی درس می‌دادم و درباره یک داستان مهندسی اجتماعی از تجربیاتم حرف می‌زدم. یکی از دانشجویان چهره‌ای خشمگین به خود گرفت. زبان بدنش از باز به بسته تغییر کرد.

دست به سینه و با پاهایی رو به بیرون به صندلی تکیه داده بود. با این تصور که داستانم را باور نمی‌کند، توجه شخصی بیشتری به او کردم. به نظر می‌رسید این کار هم تأثیری بر بی‌اعتمادی او ندارد و داستان را نمی‌پذیرد. بعد از چند دقیقه اجازه گرفت و از کلاس بیرون رفت.

مات و مبہوت بودم. همه کارها را درست انجام داده بودم. چرا همچنان از من عصبانی بود؟

کمی بعد وقت استراحت رسید. به سمت سرویس بهداشتی می‌رفتم و به این مسئله و راه‌حلی برایش فکر می‌کردم.

همان دانشجو به من نزدیک شد و گفت: «واقعاً متأسفم که کلاس را ترک کردم. رئیس وسط کلاس پیام داد و گفت موردی اضطراری سر کار پیش آمده. سعی کردم برایش توضیح بدهم که نمی‌توانم کاری کنم چون در کلاس حضور دارم، اما دستور داد کلاس را ترک کنم و در تماس گروهی مسخره‌ای شرکت کنم. آیا می‌توانم درسی را که از دست دادم جبران کنم؟»

خنده‌ام گرفت. مجبور بودم خیلی سریع علت خنده‌ام را توضیح بدهم و به او گفتم که چطور مشاهداتم را اشتباه تفسیر کرده بودم. می‌توانستم صدای دکتر اکمن را در سرم بشنوم که می‌گفت: «کریس، چی گفته بودم؟» درس بزرگی در زمینه رابطه علت و معلولی برای من بود.

این مسئله در مورد جمع‌آوری اطلاعات منبع باز و مشاهده هم صدق می‌کند. فرض نکنید همه چیزهایی که می‌خواهیم به شما نشان بدهم نتیجه «حماقت انسان‌ها» هستند. ترجیح می‌دهم فکر کنم افراد در مورد خطرهای بالقوه آموزش ندیده‌اند نه اینکه احمق باشند.

نگاهی کوتاه به تصویر شکل ۲-۲ بیندازید و یادداشتی ذهنی از مشاهدات تان بردارید. اگر مانند یک مهندس اجتماعی فکر کنید، در این تصویر چه می‌بینید که می‌تواند



شکل ۲-۲ چه می بینید؟



شکل ۲-۳ مشاهده آسان تر شد؟

این برچسب ها چه تصویری از این فرد به شما می دهند؟ اینکه از فعالیت های خیریه حمایت می کند و کدام فعالیت ها برای او مهم اند. آیا دلیل حمایت او این است که خودش یا یکی از اعضای خانواده اش به سرطان یا در کودکی به بیماری سختی مبتلا شده اند؟ همچنین نظری قاطع و محکم درباره قوانین حمل سلاح و

جرائم مسلحانه دارد. آیا به این دلیل چنین احساسی دارد که خودش قربانی جرائم مسلحانه بوده یا فردی را می‌شناسد که قربانی این جرائم بوده است؟ آیا فکر می‌کنید با آگاهی از این اطلاعات می‌توانید گفت‌وگوی استخراج اطلاعات را ترتیب بدهید؟

احتیاط کنید! دانشجویان زیادی داشته‌ام که شتاب‌زده پاسخ داده‌اند: «درمورد قوانین حمل سلاح و دلیل اشتباه بودن‌شان حرف می‌زنیم.» یا گفت‌وگویی مشابه ترتیب می‌دهیم. اما به این فکر کنید که تغییر عقیده شما از یک باور به باوری دیگر در یک گفت‌وگو چقدر دشوار است.

این فرد هم تفاوتی نخواهد داشت. این مسئله را با خواسته‌تان (اینکه فرد فکر نکند) ترکیب کنید و به یاد داشته باشید که می‌خواهید درمورد علایق او، نه علایق خودتان، گفت‌وگو کنید. در فصل هفتم، «خلق اثر هنری» بیشتر به این موضوع می‌پردازیم.

حالا به شکل ۴-۲ نگاه کنید.



شکل ۴-۲ با توجه به این عکس چه می‌توانید بگویید؟

در این عکس چه چیزی توجه‌تان را جلب می‌کند؟ به‌عنوان مهندس اجتماعی چه

چیزی مشاهده می‌کنید؟ به جزئیات کوچک این عکس ساده فکر کنید:

- می‌توانید نوع محیط کاری را ببینید.
- می‌توانید سیستم‌عاملی را ببینید که این فرد از آن استفاده می‌کند.
- می‌توانید متوجه شوید که این فرد از چه نوع تبلتی استفاده می‌کند.
- می‌توانید بفهمید این فرد طرفدار سریال کمدی خاصی است.
- می‌توانید متوجه مرورگر و ایمیل مورد استفاده این فرد هم بشوید؟
- آیا نشانه‌ای می‌بینید که ممکن است جزئیات دیگری درباره این فرد به شما نشان دهد؟

- چه جزئیات دیگری را تشخیص می‌دهید؟

این موارد فقط فهرستی سطحی و شتاب‌زده‌اند. شاید متوجه مواردی بسیار بیشتر شده باشید. آیا می‌توانید با توجه به این مشاهدات پروفایلی تشکیل بدهید که برای نوشتن یک یا دو ایمیل فیشینگ کافی باشند و بتوانند واکنشی احساسی را برانگیزند؟

با این حال گاهی یک عکس یا حتی تعاملی حضوری کافی نیست. در این شرایط اطلاعات منبع باز فنی می‌توانند خلأ را پر کنند.

اطلاعات منبع باز فنی

پیش از اینکه شروع کنید به نوشتن نقدی بد برای این کتاب و به دنیا بگویید چقدر افتضاحم چون این فصل شامل فهرستی جامع از همه ابزارهای موجود برای جمع‌آوری اطلاعات منبع باز نمی‌شود، اجازه بدهید مسئله‌ای را روشن کنم:

این فصل شامل فهرستی کامل از همه ابزارها، همه فرایندها و همه شیوه‌های جمع‌آوری اطلاعات منبع باز از طریق فنی نمی‌شود.

می‌توانم این را به شما بگویم: این فصل به ابزارها و روش‌هایی می‌پردازد که هر روز در کسب‌وکارم از آن‌ها استفاده می‌کنم. نوابغی در حوزه جمع‌آوری اطلاعات منبع باز وجود دارند که از طریق آن‌ها می‌توانید دانشی عمیق‌تر در این زمینه به دست بیاورید. اینجا دو نفر را معرفی می‌کنم که شانس آشنایی نزدیک با آن‌ها را داشته‌ام:

• «**نیک فرنو**»: سفری هوایی به بریتانیا داشتم تا در دوره چهارروزه نیک شرکت کنم و واقعاً تحت تأثیر قرار گرفتم. اطلاعاتی که در این دوره درمورد کارهایی که با ای پی آی ها می توان انجام داد و درکی که از سازوکار اپلیکیشن های شبکه های اجتماعی به دست آوردیم واقعاً آموزنده و روشنگر بودند. آدرس وبسایت نیک www.csitech.co.uk است.

• «**مایکل بزل**»: در زمینه ناپدید شدن از فضای اینترنت مایکل بهترین است، در عین حال مجموعه ای فوق العاده از ابزارها را برای شاغلان در حوزه جمع آوری اطلاعات منبع باز توسعه داده که می تواند به این افراد کمک کند شبکه های اجتماعی و موتورهای جست و جو را بگردند. وبسایت مایکل را می توانید در آدرس inteltechniques.com مشاهده کنید.

این چهره های برجسته هر دو از دوستانم هستند و شخصاً از آن ها آموخته ام، مشاوره گرفته ام و کمک دریافت کرده ام. با اطمینان خاطر می گویم که استاد حوزه جمع آوری اطلاعات منبع باز هستند (تبلیغ بی شرمانه: هر دو نفر مهمان پادکست مهندس اجتماعی بوده اند. با جست و جوی عبارت اطلاعات منبع باز (OSINT) می توانید این اپیزودها را پیدا کنید).

در حوزه جمع آوری اطلاعات منبع باز تمرکز روی استفاده عملی روزانه برای کارهای مربوط به شغل است. این کارها را می توان به چهار موضوع ساده، شامل شبکه های اجتماعی، موتورهای جست و جو، گوگل و سایر ابزارها، تقسیم کرد. به همه این موضوع ها می پردازم تا کمی با نحوه استفاده من از آن ها آشنا شوید و بعد می توانید از این دانش به عنوان زیربنای خودآموزی بیشتر استفاده کنید.

شبکه های اجتماعی

هیچ فصلی درمورد اطلاعات منبع باز بدون دست کم اشاره ای سطحی به مبحث شبکه های اجتماعی کامل نخواهد بود. نکته عجیب این است که زمانی را به یاد می آورم که خواندن دفترچه خاطرات خواهرت به کتک خوردن منجر می شد. اما اکنون خاطرات شخصی نه فقط آنلاین شده اند بلکه اگر آن ها را نخوانید، درموردشان نظر ندهید و لایک شان نکنید، توهین محسوب می شود.

شبکه‌های اجتماعی در عمل به بخشی از زندگی روزمره ما تبدیل شده‌اند و فعلاً به نظر می‌رسد ماندگار خواهند بود.

آمار زیر برگرفته از «وی آر سوشال» (We Are Social) هستند و به ما پیش‌زمینه‌ای در این مورد می‌دهند (<https://wearesocial.com/special-reports/>) (digital-in-2017-globaloverview).

در سال ۲۰۱۷:

- جمعیت جهان ۷/۴۷۶ میلیارد نفر بود.
 - تعداد کل کاربران اینترنت ۳/۷۷۳ میلیارد نفر بود.
 - تعداد کاربران فعال در شبکه‌های اجتماعی ۲/۷۸۹ میلیارد نفر بود.
 - تعداد کاربران منحصربه‌فرد موبایل ۴/۹۱۷ میلیارد نفر بود.
 - تعداد کاربران موبایل فعال در شبکه‌های اجتماعی ۲/۵۴۹ نفر بود.
- درک این آمارها برای شما به عنوان مهندس اجتماعی مهم است. بیایید برخی از برترین پلتفرم‌های شبکه‌های اجتماعی را بررسی کنیم:

لینکدین با بیش از ۱۰۶ میلیون کاربر اطلاعات زیر را در مورد شما به افراد می‌گوید:

- چه سابقه شغلی‌ای دارید.
- در کدام مؤسسه عالی درس خوانده‌اید.
- به کدام دبیرستان رفته‌اید.
- در کدام انجمن‌های علمی و دستاوردهای پژوهشی مشارکت داشته‌اید.
- چه افرادی مهارت‌های شما را تأیید می‌کنند.

فیس‌بوک با بیش از ۱/۸ میلیارد کاربر موارد زیر را به افراد می‌گوید:

- موسیقی‌های مورد علاقه‌تان؛
- فیلم‌های مورد علاقه‌تان؛
- انجمن‌هایی که در آن‌ها عضو هستید؛
- دوستان‌تان؛
- اعضای خانواده‌تان؛
- مکان‌هایی که تعطیلات‌تان را در آن‌ها گذرانده‌اید؛

- غذاهای مورد علاقه‌تان؛
 - جاهایی که در آن‌ها زندگی کرده‌اید؛
 - و بسیاری اطلاعات دیگر.
- توییت‌ر با ۳۱۷ میلیون کاربر موارد زیر را به افراد می‌گوید:
- اکنون چه کار می‌کنید؛
 - عادت‌های غذایی‌تان؛
 - مکان جغرافیایی‌تان؛
 - وضعیت روحی و عاطفی‌تان (فقط با استفاده از ۲۸۰ کاراکتر).
- می‌توانم ادامه بدهم، اما حتماً مفهوم کلی را فهمیده‌اید. همین سه اپلیکیشن می‌توانند اطلاعات زیادی درباره سوزدهایتان به شما بدهند.
- به جرئت می‌گویم با این اطلاعات می‌توانید پروفایلی بسیار جامع در مورد سوزده‌تان ایجاد کنید.

نکته جالب

در اپیزود ۸۷ پادکست مهندس اجتماعی با دکتر «جیمز پنی‌بیکر» (James Pennebaker) گفت‌وگو کردیم. ابزاری (www.analyzewords.com) طراحی کرده که می‌تواند حساب توییت‌ر هر فردی را بر اساس سبک و ادبیات مورد استفاده تحلیل کند. حساب توییت‌ر میشل با آی دی @SultryAsian را با این ابزار بررسی کرده و او را به عنوان دختری حواس‌پرت، سرخوش و خوش‌بین با سبک زندگی در لحظه ارزیابی کرده بود. وقتی این توصیف را خواندم به شدت خنده‌ام گرفت چون برعکس شخصیت واقعی میشل بود، اما دقیقاً همان شخصیتی بود که می‌خواست در شبکه‌های اجتماعی به نمایش بگذارد.

ارزیابی فرد بر اساس شبکه‌های اجتماعی نباید با ایجاد پروفایل روان‌شناختی واقعی اشتباه گرفته شود. همان‌طور که در بخش نکته جالب اشاره کردم، افرادی وجود دارند که نحوه تعامل‌شان در فضای آنلاین با محیط واقعی فرق می‌کند. هرچند این مسئله درست است، به هر حال شبکه‌های اجتماعی برای مهندسان اجتماعی

ارزشمندند زیرا بسیاری از حمله‌ها بر اساس شخصیت «آنلاین» انجام می‌شوند و یاد گرفتن شیوه برقراری ارتباط با این بُعد از شخصیت هدف می‌تواند به نفوذ منجر شود.

با توجه به وجود صدها پلتفرم شبکه اجتماعی و میلیاردها کاربری که از آن‌ها استفاده می‌کنند، شبکه‌های اجتماعی گنجینه داده‌ای برای مهندسان اجتماعی به شمار می‌آیند.

یکی از راه‌های بسیار خوب استخراج اطلاعات از پلتفرم‌های شبکه اجتماعی استفاده از موتورهای جست‌وجوست که در بخش بعدی به آن می‌پردازیم.

موتورهای جست‌وجو

اینترنت مدام در حال تغییر است، همچنین همواره راه‌هایی جدید و بهبودیافته برای پیدا کردن اطلاعات در چندین یوتابایت داده ذخیره‌شده عرضه می‌شوند. این تغییرات مستمر می‌توانند برای بیشتر افراد نقطه‌قوت، اما برای مهندسان اجتماعی نقطه‌ضعف باشند زیرا موتور جست‌وجویی که امروز کار می‌کند ممکن است فردا کار نکند.

زمانی را به یاد دارم که «اسپوکیو» (Spokeo) تازه راه‌اندازی شده و منبعی فوق‌العاده برای به دست آوردن اطلاعاتی عالی بود. با افزایش محبوبیت این وب‌سایت، تعداد تبلیغاتش هم افزایش یافت. سپس از کاربران خواست برای اطلاعات هزینه پرداخت کنند و به نظر می‌رسید اطلاعات غیرقابل اعتماد زیاد نمایش داده می‌شوند.

نمی‌گویم اسپوکیو چیز مفیدی ندارد، اما برای من به عنوان مهندس اجتماعی زمان، پول است و اگر قرار باشد همه اطلاعات دریافتی را با استفاده از منبع دیگری اعتبارسنجی کنم، هزینه زیادی برایم دارد.

در کتاب اولم و بسیاری از کتاب‌های بعدی به این نتیجه رسیدم که عرضه فهرست‌هایی از ابزارها تقریباً برای خواننده بی‌فایده است. اغلب، اتفاقات زیر می‌افتند:

- روز عرضه کتاب، ابزارها منسوخ شده‌اند و ایده‌هایی که به خوانندگان

داده‌ام، دیگر قدیمی‌اند.

- ابزارهایی جدید و بهتر عرضه شده‌اند.
- ترکیبی از هر دو اتفاق می‌افتد.

به جای دادن فهرستی از وب‌سایت‌ها و ابزارها می‌خواهم شما را گام به گام در فرایند جمع‌آوری اطلاعات منبع‌باز درباره یک سوژه راهنمایی کنم. به وب‌سایت‌ها و ابزارهای مورد استفاده‌ام اشاره می‌کنم، اما تمرکز بیشتر روی نحوه بررسی همه ابعاد این بخش از مهندسی اجتماعی بودن است.

سوژه‌ام دوستم نیک فرنو است (بیایید دعا کنیم بعد از انتشار این کتاب همچنان دوستم بماند).

باید توجه کنید که هیچ قصد بدی در مورد نیک ندارم. صرفاً از او استفاده می‌کنم تا نشان بدهم افرادی که می‌دانند چطور بپرسند، می‌توانند در اینترنت رازهایی در مورد کسی پیدا کنند که بسیار آگاه، بسیار هشیار و بسیار حساس به امنیت است.

داکس (dox) کردن نیک فرنو

داکس کردن یک نفر به چه معناست؟ واژه داکس عبارتی در ادبیات هکری و به این معناست که سندی در مورد سوژه‌ای تنظیم کنیم که حاوی جزئیاتی درباره زندگی شخصی او باشد. از این جزئیات اغلب برای حمله به هدف، تحقیر او یا ارتکاب جرائم دیگر استفاده می‌شود.

در این مورد به دنبال هیچ کدام از این کارها نیستیم. فقط می‌خواهیم قدرت اطلاعات منبع‌باز و نحوه استفاده از آن را نشان دهیم. اغلب با وب‌سایت پپیل (pipl.com) شروع می‌کنم.

پپیل را چیزی شبیه حاصل جفت‌گیری کتابچه راهنمای تلفن و سایت‌های اسکرپینگ شبکه‌های اجتماعی می‌دانم.

قابلیت بسیار خوب این سایت این است که در آن می‌توانید نام، نام کاربری، نام مستعار یا هرگونه اطلاعات دیگری را که در مورد سوژه‌تان می‌خواهید، جست‌وجو کنید.

با گشتی کوتاه در اینترنت می‌توانیم بفهمیم آی‌دی حساب توییتر نیک

«nickfx» است. بیا ببینیم با این اسم مستعار چه چیزهایی می‌توانیم پیدا کنیم. شکل ۵-۲ را ببینید.

The screenshot shows the Pipl search interface. At the top, the Pipl logo is on the left, and a search bar contains 'nickfx'. To the right of the search bar is a 'Location (optional)' field and a magnifying glass icon. Further right is a 'LOGIN' link. Below the search bar, on the left, is a 'Search By' section with a 'Username' field containing 'nickfx' and a '+ MORE OPTIONS' button. The main area is titled 'Results for nickfx' and displays a row of six profile picture thumbnails. Below these is an 'ALL MEDIA' link. On the right side of the results, there is a vertical 'Feedback' button. Below the thumbnails, there are four search results listed. Each result includes a small profile picture, a name, a description of associations, and a 'SPONSORED' section with links to 'Personal Info', 'Distant Relatives', 'Contact Info', and 'Online Photos'. The results are for Nicola Effe, Nick Harlow, Nick Stuhler, and Nick Furneaux. At the bottom, there is a result for 'nickfx, Nick Fusco' with a link to 'Sign up. Log in. Pinterest • The world's catalog ...'.

شکل ۵-۲ او را می‌بینید؟

با نگاهی اجمالی می‌توانیم ببینیم که اولین تصویر همان «نیک» مورد نظر ماست و چهار خط پایین‌تر می‌بینیم که نیک فرنوبه «کریس اچ» (Chris H) مرتبط شده (که نمی‌دانم کیست) و آن نام کاربری کاملاً متفاوتی از نیک نمایش داده شده است. پیش از اینکه به کریس اچ و آن نام کاربری بپردازیم، بیا ببینیم اگر روی تصویری که می‌دانیم نیک است کلیک کنیم چه اتفاقی می‌افتد. نتیجه در شکل ۶-۲ نشان داده شده است.

فقط با یک کلیک تأیید می‌شود که به فرد درست و مکانش رسیده‌ایم. با اطلاعات منبع باز فهمیدیم کجا زندگی می‌کند.

اکنون یک صفحه عقب می‌رویم و روی لینک چهارم کلیک می‌کنیم. این لینک چه