علم هک کردن انسان

مهندسی اجتماعی

کریستوفر هدنگی

مجید جعفریان، محمد رهبان، شیرین سجودی

چاپ دوم

انتشارات راه پرداخت


بسم الله
الرحمن
الرحيم

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: ٤-۱۹-۷۷۰۲-٦۲۲-۹۷۸
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

کریستوفر هدنگی

مجید جعفریان، محمد رهبان، شیرین سجودی

۱

چاپ دوم

عنوان : مهندسی اجتماعی؛ علم هک کردن انسان
ناشر : راه پرداخت
نویسنده: کریستوفر هدنگی
مترجمان: مجید جعفریان، محمد رهبان، شیرین سجودی
ویراستار ارشد : مینا والی
ویراستار محتوایی : بهار سرلک
ویراستار فنی: محدثه گودرزنیا
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا : بهناز سعیدی
ناظر چاپ : قادر شهبازی
نوبت چاپ: دوم ۱۴۰۴
شمارگان : ۱۰۰ نسخه
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۹-٤
تلفن : ۰۲۱-٤٤٤٤٣٩٦٦
دورنگار: ۸۹۷۸۴۹۰۲
ایمیل : info@way2pay.press
وب‌سایت : way2pay.shop
لیتوگرافی: هنر اشکان
چاپ و صحافی: واژه

فروشگاه انتشارات راه‌پرداخت نشانی: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

way2pay.press w2ppress.ir way2paypress

فهرست

[یادداشت مترجم]

گسترش روزافزون نقش تکنولوژی در تعاملات اجتماعی، کسب‌وکارها، اقتصاد، مناقشات سیاسی و به‌صورت کلی در تمامی جوانب زندگی بشری شمشیر دو لبه‌ای است که از یک‌سو 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 به‌عنوان 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 معدود 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 به‌عنوان یک عامل مستقل و بسیار حائز اهمیت در حوزه سایبری بررسی کرد و در ویراست اول همین کتاب گنجاند. نویسنده در ویرایش دوم کتاب

با به‌روزرسانی تکنیک‌ها، فرآیندها و همچنین بررسی نمونه‌های رخ‌داده 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 منحصربه‌فرد 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 به‌وقوع 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، نمی‌دانستم این اختراع جهان را به کدام‌سو می‌برد. می‌خواستم کاری بی‌سابقه انجام بدهم؛ کامپیوتری شخصی بسازم. کامپیوتری که هرکسی بتواند از آن استفاده کند، لذت ببرد و بهره‌مند 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 تلفن‌های هوشمند، دستگاه‌های هوشمند و فناوری با همه ابعاد زندگی ما عجین شده‌اند، خوب است از نمایی دورتر به این شرایط نگاه کنیم و ببینیم چطور می‌توانیم هم‌زمان با حفظ ایمنی و امنیت، همچنان به نوآوری و رشد ادامه بدهیم و با نسل بعد همکاری کنیم.

از همکاری با جوانان امروزی و ترغیب‌شان به نوآوری و رشد لذت می‌برم؛ از جریان ایده‌ها در میان آن‌ها در راه رسیدن به روش‌های جدید و خلاقانه برای استفاده از فناوری لذت می‌برم و همچنین اینکه می‌بینم این فناوری چطور می‌تواند زندگی افراد را بهبود بخشد نیز واقعاً برایم لذت‌بخش است.

با این حال باید با جدیت درمورد حفظ امنیت این آینده فکر کنیم. در سال ۲۰۰۴، وقتی به‌عنوان سخنران اصلی در «کنفرانس هوپ» (HOPE Conference) صحبت می‌کردم، گفتم هک‌های زیادی اتفاق می‌افتند که با زندگی افراد بازی و آن‌ها را وادار می‌کنند کارهایی عجیب انجام دهند.

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

کتاب کریس ماهیت و جوهره مهندسی اجتماعی را بیرون می‌کشد و آن را به‌نحوی تعریف می‌کند و شکل می‌دهد که همه آن را درک کنیم. کریس کتاب مهندسی اجتماعی را بازنویسی کرده است تا آن دسته از اصول و فرایندهای محوری تأثیرگذار بر تصمیم‌گیری ما انسان‌ها را تعریف کند و نشان دهد افراد چطور از این فرایندها سوءاستفاده می‌کنند.

هک کردن چند دهه‌ای است که به وجود آمده، اما هک کردن انسان از ابتدای خلقت وجود داشته است. این کتاب می‌تواند 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 وزنیاک / هم‌بنیان‌گذار اپل

مقدمه

زمانی را به یاد می‌آورم که حاصل جست‌وجوی عبارت «مهندسی اجتماعی» در اینترنت یا صرفاً پیدا کردن ویدئوهایی درمورد 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 درمورد یک کلاهبرداری ایمیلی حرف می‌زد و در آخر گفت: «بله، این مثال بسیار خوبی از مهندسی اجتماعی است.»

ابتدا غافل‌گیر 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 درمورد اهدافم به اشتباه بیفتید. شاید فکر کنید هیچ مشکلی ندارم که آدم‌های بدسرشت 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 به‌شدت 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. هرکدام 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 «ای‌جی کوک» (AJ Cook) درمورد کارش در سریال ذهن‌های جنایت‌کار (Criminal Minds) حرف می‌زدم که گفت اغلب به‌منظور آماده شدن برای ایفای نقش «جی‌جی» (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 صددرصد شفاف نیستند. بیایید 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 توصیه‌های‌تان.

واقعاً امیدوارم از مطالعه این کتاب لذت ببرید.

کریستوفر هدنگی (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 به‌وضوح 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 به‌شوخی 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 «کوین 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 بپرسیم 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 نفوذها عنصر مهندسی اجتماعی وجود داشته است.

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

«آی‌بی‌ام» نشان می‌دهد که میانگین هزینه هر نشت داده ۳٫۶۲ میلیون دلار آمریکا بوده است. وقتی بازده بالقوه این‌چنین زیاد است، به‌راحتی می‌توان متوجه شد که چرا مهاجمان به دنبال بهره‌برداری از مهندسی اجتماعی‌اند.

نکته تخصصی تا سال ۲۰۱۷ «مطالعه هزینه نشت داده» آی‌بی‌ام ۱۲ بار انجام شده است. می‌توانید آن را در https://www.ibm.com/security/data-breach ببینید یا به‌راحتی عبارت «Cost of Data Breach Study» را وارد هر موتور جست‌وجویی کنید تا گزارش کامل و به‌روز را مشاهده و دانلود کنید.

همچنین یکی از اولین مصاحبه‌هایم بعد از انتشار کتاب مهندسی اجتماعی: هنر هک کردن انسان، در سال ۲۰۱۰ را به یاد می‌آورم که مصاحبه‌گر پرسید: «نگران نیستید که آدم‌های بدسرشت را مجهز کنید؟» از نظر من مهندسی اجتماعی مانند هر نوع جنگ‌افزار دیگری است.

فکر کردن به ماجرای ورود «بروس لی» به آمریکا در دهه ۱۹۶۰ کمک می‌کند این موضوع را بهتر توضیح بدهم. در آن زمان تبعیض نژادی زیاد بود و بروس لی کاری می‌کرد که هیچ‌کس دیگری انجام نمی‌داد؛ به مردم با هر نژاد، رنگ یا ملیتی «جیت کان دو» آموزش می‌داد: یکی از هنرهای رزمی باستانی چین. با شاگردانش که فکر می‌کردند از مبارزه خیلی می‌دانند مبارزه می‌کرد، پشت‌سر هم حریفانش را شکست می‌داد و برخی از این حریفان در نهایت دوست یا حتی شاگرد بروس لی شدند.

چه نتیجه‌ای می‌گیریم؟ افراد باید نوع جدیدی از مبارزه را یاد می‌گرفتند وگرنه مدام شکست می‌خوردند. آیا این خطر وجود داشت که یکی از شاگردان بروس لی از مهارت‌های جدیدش برای آسیب زدن به دیگران یا انجام کارهای شرورانه استفاده کند؟ بله، اما بروس لی احساس می‌کرد باید به افراد آموزش بدهد تا بتوانند از خودشان محافظت کنند.

بنابراین پاسخ من به پرسش «نگران نیستید که آدم‌های بدسرشت را مجهز کنید؟» همان پاسخی است که هشت سال پیش دادم: «نمی‌توانم نحوه استفاده شما از این اطلاعات را کنترل کنم.» می‌توانید این کتاب را بخوانید و سپس برای حمله به افراد و سرقت پول‌شان

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 هرکدام 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. به‌عبارت دیگر باید بتوانید بر این نیرو مسلط شوید و به سمت تاریکی نیز کشیده نشوید.

حال ممکن است بپرسید: «اگر پاسخت 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. به‌عنوان 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 دو بز 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 حیله‌گری، فریب، شیادی و کلاهبرداری انسان‌ها بوده‌ایم. ظاهراً اتفاقی تازه در زمینه مهندسی اجتماعی نیفتاده است، اما نمی‌توان گفت

هیچ‌چیز هیچ‌وقت تغییر نمی‌کند.

یکی از مثال‌ها در این مورد «ویشـینگ» (vishing) یا «فیشینگ صوتی» است. اولین باری را که از این واژه استفاده کردم، به‌خوبی به یاد می‌آورم. افراد جوری به من نگاه می‌کردند انگار به زبان ساختگی «کلینگان» صحبت می‌کردم. با این حال ویشینگ از سال ۲۰۱۵ به فرهنگ انگلیسی آکسفورد اضافه شده است.

نکته تخصصی کلینگان زبانی ساختگی است، اما مؤسسه‌ای واقعی (www.kli.org) برای آموزش، ترجمه و حرف زدن به این زبان وجود دارد. همچنین می‌توانید مترجم‌های زیادی پیدا کنید که این زبان را برای‌تان ترجمه کنند. تا امروز نشنیده‌ام که فردی به کمک زبان کلینگان از شیوه‌های مهندسی اجتماعی استفاده کرده باشد.

چرا اضافه شدن ویشینگ به فرهنگ واژگان اهمیت دارد؟ زیرا نشان می‌دهد شیوه‌های مهندسی اجتماعی چقدر روی جهان تأثیر گذاشته‌اند. واژه‌هایی که زمانی به نظر می‌رسید متعلق به زبانی ساختگی‌اند، اکنون بخشی از واژگان روزمره شده‌اند.

فقط هم واژه‌ها نیستند که رایج شده‌اند؛ اکنون سرویس‌هایی وجود دارند که به‌صورت تخصصی به آدم‌های بد کمک می‌کنند در بد بودن بهتر شوند. به‌عنوان مثال وقتی برای یکی از مشتریان کاری انجام می‌دادم، به سرویسی برخوردم که خدماتی تخصصی برای نمونه‌خوانی و غلط‌گیری ایمیل‌های فیشینگ مخرب عرضه می‌کرد. این شرکت، پشتیبانی شبانه‌روزی به زبان انگلیسی داشت. کافی است چنین مسائلی را با تبدیل شدن دستگاه‌های موبایل به ابررایانه‌های کوچک تلفیق کنید و سپس اعتیاد به شبکه‌های اجتماعی در دنیای جدید را به آن بیفزایید. حاصل، دستورالعملی برای یک چشم‌انداز حمله جدید به سبک مهندسی اجتماعی است.

علاوه بر تغییر چشم‌انداز، من هم تغییر کرده‌ام. عنوان جلد اول این کتاب مهندسی اجتماعی: هنر هک کردن انسان بود. دلیل انتخاب چنین نامی این بود که احساس می‌کردم آنچه در کتاب تشریح می‌کنم، بسیار شبیه هنر است. هنر نسبی و سلیقه‌ای است؛ در ذهن افراد مختلف معانی متفاوتی دارد. می‌توان به روش‌های 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 به‌واسطه 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 به‌جرئت می‌گویم ۹۹٫۹۹۹۹۹۹۹ 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 درمورد موضوعی با من گفت‌وگو کرد که حالت‌های آلفا و بتا می‌خواند.

ارجاع 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 درمورد 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-with-out-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، به‌احتمال زیاد چنین تبلیغی را مشاهده کرده‌اید: تصویر خواننده خانم معروفی را می‌بینیم و موسیقی بسیار غم‌انگیزی هم در پس‌زمینه 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 احساسات‌تان بیشتر تحریک شوند، کمتر منطقی فکر خواهید کرد. هرچه کمتر منطقی فکر کنید، سریع‌تر صرفاً بر اساس احساسات تحریک‌شده 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 عزیزان‌تان 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 ملاحظاتی 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، کدام‌یک از اعضای تیم برای این کار مناسب‌ترند؟

- مرد سفیدپوست ۴۰ ساله با موی بلوند
- زن آسیایی ۴۳ ساله

- زن لاتین‌تبار ۲۷ ساله

از طرف دیگر اگر به این نتیجه برسید که بهترین دستاویز استفاده از فردی در نقش کارگر آشپزخانه است، کدام‌یک از اعضای تیم برای این کار مناسب‌ترند؟

واقعیت این است که مهندس اجتماعی ماهر می‌تواند در هرکدام 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 به‌معنای فردی بود که باید می‌فهمید وسیله یا دستگاهی چطور کار می‌کند. هکرها به دانش پایه‌ای راضی نمی‌شدند، می‌خواستند عمیق‌تر شوند و سازوکار درونی و پنهان هرچیزی 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 به‌نحوی تعریف کنم که این‌طور القا نکند که همیشه پای کلاهبردار، حقه‌باز یا شیادی در میان است. می‌توان از همان اصولی که آدم‌های بد ازشان 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 شاهزاده‌خانم دعوتت کنم؛ یعنی اینکه اینجا بنشینی و در حالی که روسری صورتی سر کرده‌ای، من ناخن‌هایت را لاک بزنم و درمورد شاهزاده‌خانم‌های دیزنی صحبت کنیم»، نه‌فقط به شما می‌خندیدم، بلکه به‌آرامی 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 شاهزاده‌خانم 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 تصمیمم 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 نانوثانیه رد می‌کردم، می‌باید فرایند تصمیم‌گیری عادی‌ام را دور می‌زدم.

واقعیت بی‌مصرف

با توجه به اینکه یک نانوثانیه یک میلیاردم ثانیه است و هر فرد عادی با سرعت ۱۴۵ واژه در هر دقیقه صحبت می‌کند، در عمل نمی‌توانستم در یک نانوثانیه پاسخ منفی بدهم. از طرف دیگر، نور که ۱۸۶هزار مایل بر ثانیه سرعت دارد، می‌تواند در یک نانوثانیه 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 درمورد 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 نه‌فقط 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 تعمیرکارمان 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 شـرکت «ولز فارگـو» (Wells Fargo) نفوذ کردنـد، پیامک حمله اسمیشینگ به‌نمایش‌درآمده در شکل ۲-۱ را دریافت کردم.

(ولز-.فارگـو) پیـام مهمـی از طـرف
واحد امنیت!
به حساب‌تان وارد شوید
vigourinfo.com/secure.
well5farg0card.html

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

نکته جالب این اسـت که من اصلاً در ولز فارگو حساب ندارم، اما باز هم هدف این حمله قرار گرفتم (و نه‌خیر، 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.

- **«ویشـینگ»**: همان‌طور که پیش از ایـن گفتم، این عبارت معادل فیشـینگ صوتی است. کاربرد این شیوه از سال ۲۰۱۶ به‌شدت افزایش یافته و برای مهاجم نیز آسـان، ارزان و بسیار سـودآور اسـت. همچنین با توجه به اینکه مهاجمان از شـماره‌های جعلی خارج از کشـور تماس می‌گیرند، پیدا کردن مکان‌شان تقریباً غیرممکن است.
- **«فیشـینگ»**: پربحث‌ترین موضوع در حوزه مهندسـی اجتماعی فیشینگ است. در واقع ویراستار فنی این کتاب، یعنی «میشـل» 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)» (انتشـارات وایلی، ۲۰۱۶) نوشـته‌ایم (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 به‌هیچ‌وجه به این معنی نیست که نباید به‌اندازه 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 منزجرکننده را در این آدرس مشاهده کنید:
www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn-20170418-story.html

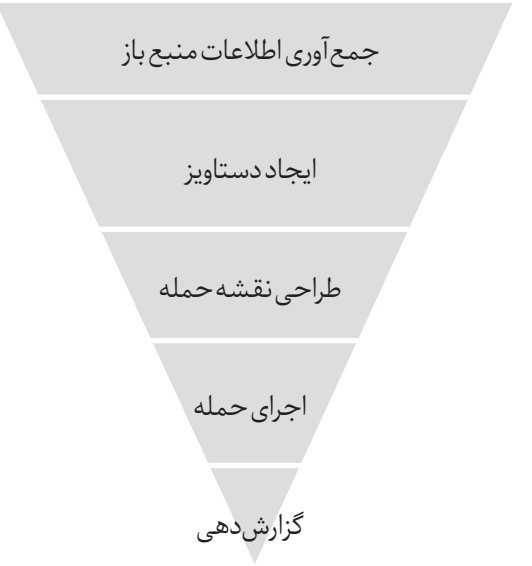
هر حمله مبتنی بر مهندسی اجتماعی را می‌توان در یکی از این چهار طبقه‌بندی قرار داد. به‌تازگی شاهد حمله‌هایی هستیم که «حمله ترکیبی» می‌خوانیم و در آن‌ها مهندسان اجتماعی مخرب، از ترکیبی از این شیوه‌ها در یک حمله استفاده می‌کنند تا به اهداف‌شان دست یابند.

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 ۳-۱ نشان داده شده است.



شکل ۳-۱ 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 به‌معنی 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 تعیین‌شده 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. به‌جای اینکه همه‌چیز 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 به‌احتمال 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 به‌عنوان مهندس اجتماعی و هم به‌عنوان متخصصی که به مشتریان خدمات مهندسی اجتماعی می‌دهد، به موفقیت می‌رسید. واقعیت این است که مهندسان اجتماعی مخرب نیز از همین گام‌ها، به‌جز 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 درمورد 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 کدگذاری‌شده 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 قابل‌اعتماد 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 بهره برده بودند، از این کتاب هم بهره ببرند. 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 به‌صورتی 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، «پروفایل‌بندی افراد از طریق ارتباط»، موضوعی را بررسی می‌کنم که در نسخه اول کتاب چندان مطرح نشد؛ یعنی ابزارهای پیشرفته مدل‌سازی و پروفایل‌بندی 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 شکست‌خورده‌ای) 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 گفت‌وگوهایی با برخی از افراد برجسته این حوزه در جهان، مثل «رابین دریک» (Robin Dreeke)، جمع‌آوری کرده‌ام و درباره چگونگی به‌کارگیری اصول اعتمادسازی در مهندسی اجتماعی بحث می‌کنم. رابین دریک رئیس «واحد تحلیل رفتاری» (Behavioral Analysis Unit) «اف‌بی‌آی» 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، «تحت‌تأثیر»، از مطالعات «رابرت چالدینی» (Robert Cialdini)، یکی از رهبران حوزه پژوهش درمورد 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»، چهارچوب‌بندی 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 به‌کارگیری اصول این کتاب چقدر برای شما به‌عنوان 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 هرچیز 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 به‌عنوان 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، پیشنهادها و انتقادها 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 خوش‌مزه‌ای 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 همان‌قدر 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 هرکدام از مواد را به‌خوبی درک نکنم، امکان ندارد بفهمم «چشیدن»

به چه معناست. وقتی می‌دانم در دستورپخت 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. به‌عنوان 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 می‌بینم
تو هم می‌بینی؟

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

جمع‌آوری اطلاعات منبع‌باز رکن اساسی مهندسی اجتماعی است. اطلاعات نقطه شروع و تکیه‌گاه هر تعاملی‌اند. جمع‌آوری اطلاعات منبع‌باز برای ما مهندسان اجتماعی اهمیت زیادی دارد، در نتیجه ضروری است با انواع روش‌های کسب اطلاعات درمورد سوژه‌هایمان آشنا شویم. صرف‌نظر از نحوه جمع‌آوری اطلاعات منبع‌باز باید تصویری روشن از آنچه می‌خواهید، داشته باشید. شاید در ظاهر آسان باشد، اما آن‌قدر که به نظر می‌رسد آسان نیست. نمی‌توانید به‌سادگی بگویید: «همه اطلاعات مربوط به سوژه را می‌خواهم.» هر نوع اطلاعاتی ارزشی متفاوت دارد و ارزشمند بودن هر اطلاعاتی ممکن است به نوع حمله‌ای بستگی داشته باشد که می‌خواهید انجام دهید.

نمونه‌ای واقعی از جمع‌آوری اطلاعات منبع‌باز

اجازه بدهید تصویری کلی به شما بدهم؛ طبق اطلاعات سایت www.worldwidewebsize.com بیش از ۴٫۴۸ میلیارد وب‌سایت فهرست‌شده وجود دارند. این رقم شامل وب‌سایت‌های موجود در «دارک وب» و «دیپ وب» نمی‌شود. ترافیک اینترنت سالانه جهان به ۱٫۳ زتابایت (یعنی ۱،۳۰۰،۰۰۰،۰۰۰،۰۰۰،۰۰۰،۰۰۰ بایت) رسیده است. حتی منبعی مدعی است که اینترنت می‌تواند درمجموع تا ۱۰ یوتابایت داده داشته باشد (۱۰ یوتابایت یعنی ۱۰،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 فیلم‌های جنگ ستارگان نام‌گذاری شده است. واحدهای دیگری هم وجود دارند که از یوتابایت بزرگ‌ترند و نام‌هایی عجیب‌تر هم دارند، از جمله می‌توان به «شیلنتنوبات» (shilentnobyte) و «دامجمگروتابایت» (domegemegrottebyte) اشاره کرد.

اساساً درک مقدار ترافیک اینترنت چه اهمیتی دارد؟ به‌عنوان مثال اگر بخواهید ایمیل فیشینگ ارسال کنید، شاید بهتر باشد دنبال این موارد بگردید: سرگرمی‌های شخصی سوژه، مقوله‌هایی 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 درمورد 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 می‌کند یا خیر و همچنین با چه افرادی قرار می‌گذارد.

بیش از ۴٫۴۸ میلیارد وب‌سایت وجود دارند که در آن‌ها باید دنبال داده‌هایی بگردید که ممکن است مفید باشند. بنابراین پیش از شروع جست‌وجو باید برای جمع‌آوری داده‌های منبع‌باز برنامه‌ریزی کنید. به‌منظور تعیین محدوده برای جست‌وجوی‌تان از فهرست پرسش‌های جدول ۱-۲ استفاده کنید.

جدول ۱-۲ نمونه پرسش‌های جمع‌آوری اطلاعات منبع‌باز

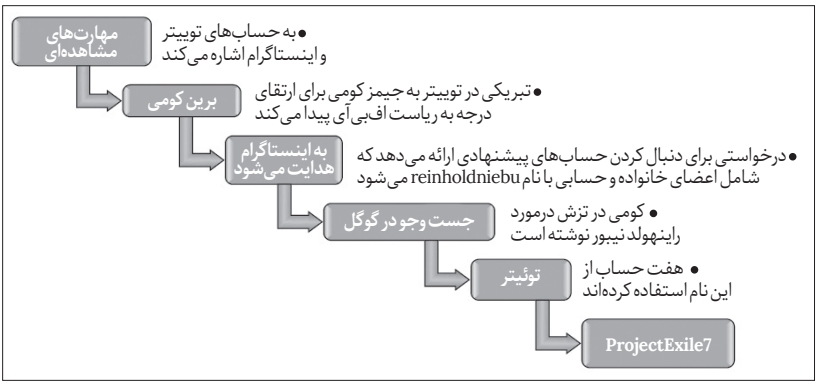
نوع سازمان	آنچه باید بپرسید
شرکت	شرکت موردنظر چطور از اینترنت استفاده می‌کند؟ شرکت موردنظر چطور از شبکه‌های اجتماعی استفاده می‌کند؟ آیا شرکت موردنظر برای محتوایی که کارمندانش تولید و در اینترنت منتشر می‌کنند، قانونی تعیین کرده است؟ شرکت موردنظر با چند وندور همکاری می‌کند؟ شرکت موردنظر از کدام وندورها استفاده می‌کند؟ شرکت موردنظر پرداخت‌ها را از طریق چه روش‌هایی می‌پذیرد؟ شرکت موردنظر چطور پرداخت‌های خودش را انجام می‌دهد؟ آیا شرکت موردنظر مرکز تماس دارد؟ ساختمان‌های مرکزی، مراکز تماس و سایر شعبه‌های شرکت موردنظر کجا واقع شده‌اند؟ آیا شرکت موردنظر اجازه می‌دهد افراد دستگاه‌های خودشان را داخل شرکت ببرند؟ آیا شرکت موردنظر یک ساختمان دارد یا چند ساختمان؟ آیا چارت سازمانی وجود دارد؟

فرد	فرد موردنظر از کدام حساب‌های شبکه‌های اجتماعی استفاده می‌کند؟ فرد موردنظر چه سرگرمی‌هایی دارد؟ فرد موردنظر برای تعطیلات کجا می‌رود؟ فرد موردنظر به کدام رستوران‌ها علاقه دارد؟ پیشینه خانوادگی فرد موردنظر (شامل بیماری‌ها، کسب‌وکارها و غیره) چیست؟ فرد موردنظر تا چه سطحی و در چه رشته‌ای تحصیل کرده است؟ فرد موردنظر 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 موردنظر اشاره کند (شاید سخنرانی می‌کند، برای انجمن‌های اینترنتی مطلب می‌فرستد یا عضو باشگاهی است)؟ آیا فرد موردنظر صاحب خانه است؟ اگر بله، مالیات، وثیقه و سایر اطلاعات مربوط به این ملک به چه صورت است؟ نام اعضای خانواده فرد موردنظر (و همچنین همه اطلاعات پرسش‌های قبل درمورد این افراد) چیست؟

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.

بیایید 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 پلتفرمِ در دسترس (که هرکدام 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 توییترش 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 (به‌غیر 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 توییتر 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 به‌صورت 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 منبع‌باز غیرفنی و فنی تقسیم کرده‌ام.

مستند کردن یا نکردن؛ مسئله این است

پیش از آنکه سراغ انواع اطلاعات منبع‌باز 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 یوتابایت 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. به‌عنوان مثال وقتی این مسیر شغلی را شروع کردم و همه کارها را خودم به‌تنهایی 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 به‌کارگیری رنگ‌های خاص برای موارد مربوط به حمله‌ها استفاده می‌کردم: از رنگی برای یافته‌های معمولی و از رنگی دیگر برای یافته‌های حیاتی.

بعد به‌مرور 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 به‌هیچ‌وجه بهترین راه‌حل 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 داشتم 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 جمع‌آوری‌شده از مشتریان‌تان را جدی بگیرید.

اطلاعات منبع‌باز غیرفنی

اطلاعات منبع‌باز 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 (به‌عنوان 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 موفقیت‌آمیز از آن‌ها، به‌ویژه 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 ارتباطات چهره‌به‌چهره به‌واسطه فناوری کاهش یافته است. از میان افرادی که در این مطالعه تحت‌نظر 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/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 درمورد هرکدام 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 بگیرید. اگر به مکانی نفوذ کنید که همه در آنجا لباس غیررسمی پوشیده باشند و شما با کت‌وشلوار 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 کارمندانی 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 صفحه‌کلیدی وجود دارد که بتوانید مخفیانه از پشت‌سر و روی شانه افراد رمز عبورشان را سرقت کنید؟ (به‌عبارت دیگر آیا می‌توانید آن‌قدر 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 منبع‌باز فنی جمع‌آوری می‌کردیم که در ادامه این فصل به آن می‌پردازم، در عین حال مقدار زیادی اطلاعات منبع‌باز 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 درمورد سم‌پاشی اضطراری برای از بین بردن عنکبوت‌ها قیمتی پیشنهاد بدهد. نام شرکت‌مان 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 سم روشی عالی برای همراه داشتن نوشیدنی انرژی‌زا و طراوت‌بخشی است که وقتی در عملیات نفوذ به ساختمان مضطرب شده‌اید و به‌شدت 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 اول‌مان را انتخاب کردیم و به‌آهستگی 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 چه‌کار 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 نام‌های‌مان را پرسید. نام‌های جعلی‌مان را گفتیم و او در فهرستی دنبال‌شان گشت. وقتی نام‌مان 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. به‌نحوی 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 پشت‌سرشان حرکت کردیم. بعد از ورود به ساختمان دنبال‌شان می‌کردیم که به‌سرعت 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 راستم دیدم، اما هیچ دکمه‌ای نداشت. با خودم فکر کردم: «عجب شانسی! آسانسوری که تحت کنترل حراست است.» در همین حین ناگهان در آسانسور باز شد. بی‌درنگ وارد شدم و امیدوار بودم میشل هم ببیند و پشت‌سرم 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 بگویید کجا می‌روید تا آسانسور را در همان طبقه نگه داریم...» وسط حرفش پریدم و گفتم: «به اتاق نامه‌ها می‌رویم.»، چند دکمه را فشار داد و گفت: «شما را آنجا پیاده می‌کنم.»

خوشبختانه به‌خاطر 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 درِ اتاق نامه‌ها قفل است. زنگی با برچسبی 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 برای‌مان فراهم کردند که برای موفقیت از این افراد استفاده کنیم.

سناریوی دوم

مأموریت دارید وکیلی 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 منبع‌باز 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 به‌شکلی مفتضحانه شکست خوردم.

با بهره‌گیری از اطلاعات منبع‌باز 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 به‌شکلی حرفه‌ای نوشته شده بود، تهدید نمی‌کرد، شامل بسته اطلاعاتی موردنظرمان بود، مهلتی واقع‌بینانه برای مطالعه و پاسخ‌گویی تعیین می‌کرد و به‌اندازه‌ای اطلاعات می‌داد که اطمینان حاصل شود برای گرفتن اطلاعات بیشتر مجبور است روی لینک کلیک کند.

چند دقیقه پس از ارسال ایمیل لو رفتیم 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 یوآرال (URL) نگاه کند و به‌قدری مشکوک شود که ایمیل را گزارش کند. در نتیجه پوشش‌مان لو رفت.

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

دردسرساز می‌شوند.

برای به دست آوردن این مهارت‌ها چه کاری می‌توانیم انجام دهیم؟

پرداختن به این موضوع در بخش کوچکی از یک کتاب دشوار است. توانایی‌های ذاتی و توانایی‌های اکتسابی هر فردی می‌توانند یادگیری این مهارت‌ها را بسیار آسان یا بسیار دشوار کنند. از آنجا که شما را نمی‌شناسم، فقط می‌توانم بگویم خودم چه‌کار کردم تا مهارت‌هایم را بهبود بخشم.

یک بازی مشابه بازی تسخیر پرچم انجام می‌دهم (در این بازی هرکدام از تیم‌ها سعی می‌کنند پرچم تیم دیگر را بگیرند و به‌سلامت به زمین‌شان برگردند). اگر قرار بود وارد ساختمانی شوم (برای مثال مطب یک پزشک) با خودم می‌گفتم: «پرچم‌ها این موارد هستند: به خاطر سپردن دو نفر اولی که می‌بینم، رنگ پیراهن‌شان و مجله‌ای که می‌خوانند یا کاری که می‌کنند.»

محدودیت‌هایی مشابه موارد زیر تعیین می‌کردم:

- این افراد نمی‌توانند افراد مربوط به آن سرویس باشند که پشت پیشخوان هستند.
- در عین حال باید مأموریت بررسی را هم انجام بدهم و نمی‌توانم متوقفش کنم یا از آن منحرف شوم.
- نمی‌توانم چیزی یادداشت کنم.

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

- زن مسن‌تر که پیراهن آبی پوشیده و سمت راست نشسته بود مجله وومنز دی (Woman's Day) می‌خواند.
- کودک، مذکر، تی‌شرت راه‌راه، در حال بازی با بلوک‌ها روی زمین.

مشاهدات را در ذهنم ثبت می‌کردم و تمام توانم را به کار می‌گرفتم تا آن‌ها را از یاد نبرم. از چند ترفند ثبت حافظه استفاده می‌کردم، برای مثال چیزی را چند بار با خودم تکرار می‌کردم تا در ذهنم تثبیتش کنم.

وقتی احساس می‌کردم می‌توانم بدون اینکه زیاد فکر کنم، یادداشت‌برداری 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، «پروفایل‌بندی 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 آیپد چیزی می‌خواندند. به نظر می‌رسید خانم سمت چپ از خانم سمت راست خوشش نمی‌آید اما او را تحمل می‌کند. با توجه به اینکه پایین‌تنه خانم سمت چپ از خانم سمت راست فاصله داشت، به این نتایج رسیدم.

مردی با پوشش نگهبانی (کت‌وشلوار 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، به‌عنوان مهندس اجتماعی، به اهداف‌تان دارند. پیشنهاد می‌کنم دنبال نقـاط ضعف خودتـان بگردیـد و از کارهـای کوچک شـروع و به‌مرور سخت‌ترشـان کنید. این نکته را از یاد نبرید که باید تمرین کنید. بارها پیش می‌آید افرادی را می‌بینم که می‌خواهند بلافاصله به موفقیت صددرصدی برسند، اما این کار زمان‌بر است.

اگر اجازه بدهیم، شکست می‌تواند خیلی بیشتر از موفقیت به ما درس بدهد. به همین دلیل است که باید درمورد 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 سرنخ‌های غیرکلامی، یعنی زبان بدن و حالت چهره، تمرکز کردم. وقتی تازه داشـتم یاد می‌گرفتم که چطور ابتدا متوجه این نشانه‌ها شـوم و بعد رمزگشایی‌شان کنم، احساس می‌کردم نوعی ابرقهرمان با قدرت ذهن‌خوانی‌ام. 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. بیشـتر از آنچـه در واقعیـت بـود، احسـاس می‌کـردم می‌بینـم، درک می‌کنـم و در نتیجه مهندسی اجتماعی می‌کنم.

یکی از درس عبرت‌هایم را هنگام کار با دکتر اکمن گرفتم، درسـی که باعث شـد 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 درمورد انتظارات، احساس می‌کنم باید این گزاره را چند بار بشنوید: چون چیسـتی را می‌بینی، به این معنی نیسـت 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 مـی‌زدم. یکی از دانشـجویان چهره‌ای خشـمگین به خـود گرفت. زبان بدنش از باز به بسته تغییر کرد.

دست‌به‌سینه و با پاهایی رو به بیرون به صندلی تکیه داده بود. با این تصور که داستانم را باور نمی‌کند، توجه شخصی بیشـتری 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.

مات‌ومبهوت بودم. همه کارها را درسـت 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. رئیسم 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 شـرکت کنم. آیا می‌توانم درسـی 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 اشـتباه تفسـیر کرده بودم. می‌توانسـتم 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 درمورد جمع‌آوری اطلاعات منبع‌باز و مشاهده هم صدق می‌کند. فرض نکنید همه چیزهایی که می‌خواهم به شـما نشـان بدهم نتیجه «حماقت انسـان‌ها» هستند. ترجیح می‌دهم فکـر کنم افراد درمـورد خطرهای بالقـوه آموزش ندیده‌اند نـه اینکه احمق باشند.

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

شکل ۲-۲ چه می‌بینید؟

شکل ۳-۲ مشاهده آسان‌تر شد؟

این برچسب‌ها چه تصوری از این فرد به شما می‌دهند؟ اینکه از فعالیت‌های خیریه حمایت می‌کند و کدام فعالیت‌ها برای او مهم‌اند. آیا دلیل حمایت او این است که خودش یا یکی از اعضای خانواده‌اش به سرطان یا در کودکی به بیماری سختی مبتلا شده‌اند؟ 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 منبع‌باز فنی می‌توانند خلأ را پر کنند.

اطلاعات منبع‌باز 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 منبع‌باز نمی‌شود، اجازه بدهید مسئله‌ای را روشن کنم:

این فصل شامل فهرستی کامل از همه ابزارها، همه فرایندها و همه شیوه‌های جمع‌آوری اطلاعات منبع‌باز 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 منبع‌باز 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 تحت‌تأثیر قرار گرفتم. اطلاعاتی که در این دوره درمورد کارهایی که با ای‌پی‌آی‌ها می‌توان انجام داد و درکی که از سازوکار اپلیکیشن‌های شبکه‌های 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 مجموعه‌ای فوق‌العاده از ابزارها را برای شاغلان در حوزه جمع‌آوری اطلاعات منبع‌باز توسعه داده که می‌تواند به این افراد کمک کند شبکه‌های اجتماعی و موتورهای جست‌وجو را بگردند. وب‌سایت مایکل را می‌توانید در آدرس inteltechniques.com مشاهده کنید.

این چهره‌های برجسته هر دو از دوستانم هستند و شخصاً از آن‌ها آموخته‌ام، مشاوره گرفته‌ام و کمک دریافت کرده‌ام. با اطمینان خاطر می‌گویم که استاد حوزه جمع‌آوری اطلاعات منبع‌باز هستند (تبلیغ بی‌شرمانه: هر دو نفر مهمان پادکست مهندس اجتماعی بوده‌اند. با جست‌وجوی عبارت اطلاعات منبع‌باز (OSINT) می‌توانید این اپیزودها را پیدا کنید).

در حوزه جمع‌آوری اطلاعات منبع‌باز تمرکزم روی استفاده عملی روزانه برای کارهای مربوط به شغلم است. این کارها را می‌توان به چهار موضوع ساده، شامل شبکه‌های اجتماعی، موتورهای جست‌وجو، گوگل و سایر ابزارها، تقسیم کرد. به همه این موضوع‌ها می‌پردازم تا کمی با نحوه استفاده من از آن‌ها آشنا شوید و بعد می‌توانید از این دانش به‌عنوان زیربنای خودآموزی بیشتر استفاده کنید.

شبکه‌های اجتماعی

هیچ فصلی درمورد اطلاعات منبع‌باز بدون دست‌کم اشاره‌ای سطحی به مبحث شبکه‌های اجتماعی کامل نخواهد بود. نکته عجیب این است که زمانی را به یاد می‌آورم که خواندن دفترچه خاطرات خواهرت به کتک خوردن منجر می‌شد. اما اکنون خاطرات شخصی نه‌فقط آنلاین شده‌اند بلکه اگر آن‌ها را نخوانید، درموردشان نظر ندهید و لایک‌شان نکنید، توهین محسوب می‌شود.

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 به‌عنوان 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 چه‌کار 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 سوژه‌هایتان به شما بدهند.

به‌جرئت می‌گویم با این اطلاعات می‌توانید پروفایلی بسیار جامع درمورد سوژه‌تان 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 آی‌دی SultryAsian@ را با این ابزار بررسی کرده و او را به‌عنوان دختری حواس‌پرت، سرخوش و خوش‌بین با سبک زندگی در لحظه ارزیابی کرده بود. وقتی این توصیف را خواندم به‌شدت 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 غیرقابل‌اعتماد زیاد نمایش داده می‌شوند.

نمی‌گویم اسپوکیو چیز مفیدی ندارد، اما برای من به‌عنوان 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.

به‌جای دادن فهرستی از وب‌سایت‌ها و ابزارها می‌خواهم شما را گام‌به‌گام در فرایند جمع‌آوری اطلاعات منبع‌باز درباره یک سوژه راهنمایی کنم. به وب‌سایت‌ها و ابزارهای مورد استفاده‌ام اشاره می‌کنم، اما تمرکزم بیشتر روی نحوه بررسی همه ابعاد این بخش از مهندس 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 درمورد نیک ندارم. صرفاً از او استفاده می‌کنم تا نشان بدهم افرادی که می‌دانند چطور بپرسند، می‌توانند در اینترنت رازهایی درمورد 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 درمورد 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.

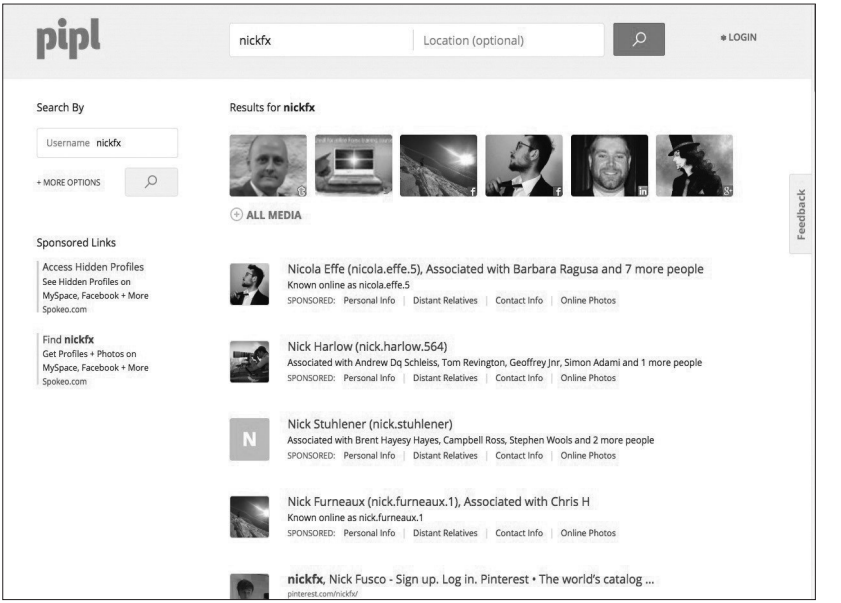
در این مورد به دنبال هیچ‌کدام از این کارها نیستیم. فقط می‌خواهیم قدرت اطلاعات منبع‌باز و نحوه استفاده از آن را نشان دهیم. اغلب با وب‌سایت پیپل (pipl.com) شروع می‌کنم.

پیپل 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 درمورد سوژه‌تان می‌خواهید، جست‌وجو کنید.

با گشتی کوتاه در اینترنت می‌توانیم بفهمیم آی‌دی حساب توییتر نیک

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



شکل ۵-۲ او را می‌بینید؟

با نگاهی اجمالی می‌توانیم ببینیم که اولین تصویر همان «نیک» موردنظر ماست و چهار خط پایین‌تر می‌بینیم که نیک فرنو به «کریس اچ» (Chris H) مرتبط شده (که نمی‌دانم کیست) و نام کاربری کاملاً متفاوتی از نیک نمایش داده شده است.

پیش از اینکه به کریس اچ و آن نام کاربری بپردازیم، بیایید 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 منبع‌باز فهمیدیم کجا زندگی می‌کند.

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

اطلاعاتی را آشکار می‌کند؟ نگاهی به شکل ۷-۲ بیندازید.

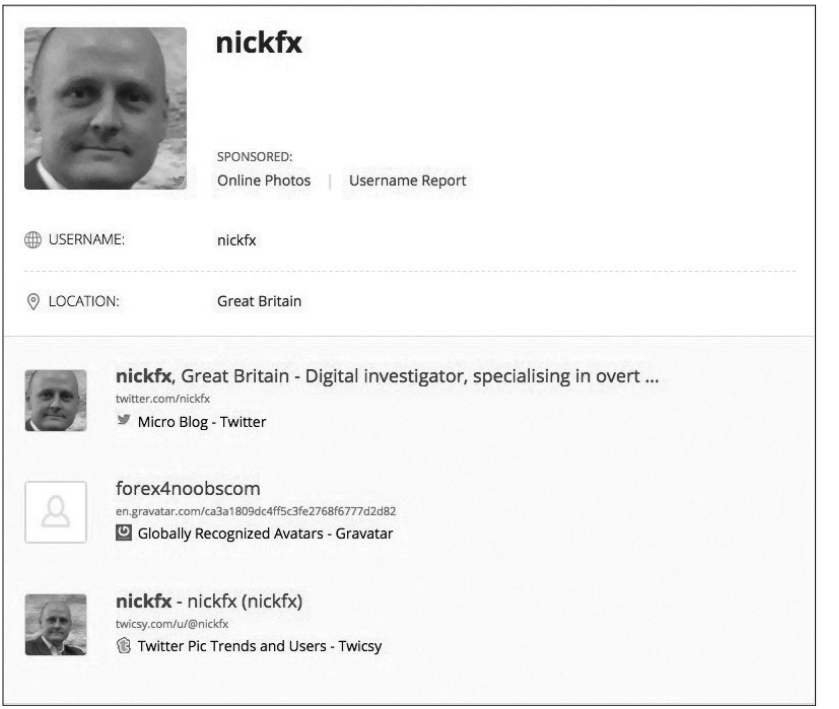
اطلاعات منبع‌باز بسیار خوبی می‌بینیم، این‌طور نیست؟

صفحه فیس‌بوک و سرگرمی خاصی که قبلاً نمی‌دانستیم نیک به آن علاقه دارد.

نیک اسنوبردسوار است. به‌علاوه، حتماً علاقه زیادی به کریس اچ دارد؛ ظاهراً همه‌جا هست.

وقتی روی لینک فیس‌بوک کلیک می‌کنم، با اطلاعات منبع‌باز بیشتری مواجه می‌شوم.

- در شهر بریستول بریتانیا زندگی می‌کند.
- فهرستی از دوستانش می‌بینم.
- نام کاربری جدیدی پیدا می‌کنم: nick.furneaux.1



شکل ۶-۲ تأییدیه

شکل ۷-۲ اطلاعات منبع‌باز بیشتر

وقتی دوباره به pipl.com برمی‌گردم و فقط نام و محل زندگی‌اش، یعنی بریستول انگلستان، را وارد می‌کنم، به جزئیات بیشتری درباره او می‌رسم:

- شغل سابقش؛
- پروفایل لینکدینش؛
- نام کاربری دیگری از او؛
- مدرسه‌ای که رفته است.

با چند کلیک به مقدار مناسبی اطلاعات از نیک دست پیدا می‌کنم که بدون شک در ایجاد پروفایل برای او مفید خواهد بود. آیا می‌توانم اطلاعات بیشتری به دست بیاورم؟

سپس به سایت دیگری به نام وبمی (webmii.com) می‌روم. هدف وبمی این است که به ما کمک کند رؤیت‌پذیری افراد را ببینیم. جست‌وجوی نام «Nick Furneaux» در این وب‌سایت نتایجی را به نمایش می‌گذارد که در شکل ۸-۲ می‌بینید.

بلافاصله متوجه چند مسئله می‌شوم: امتیاز رؤیت‌پذیری نیک ۴٫۲۲ است (که خیلی زیاد نیست چون از ۱۰ محاسبه می‌شود). اما کلیک کردن روی این امتیاز به ما نشان می‌دهد چه زمانی بیشتر رؤیت‌پذیر بوده است (شکل ۹-۲ را ببینید). به‌عنوان فردی که اطلاعات منبع‌باز جمع‌آوری می‌کند، زمانی که نیک بیشتر محبوب بوده کنجکاوی‌ام را برمی‌انگیزد. می‌خواهم بدانم در این زمان‌ها چه اتفاقی در زندگی‌اش در جریان بوده است.

اگر برگردیم به تصویری که در شکل ۸-۲ نشان داده شده بود، می‌بینیم داده‌های دیگری هم وجود دارند:

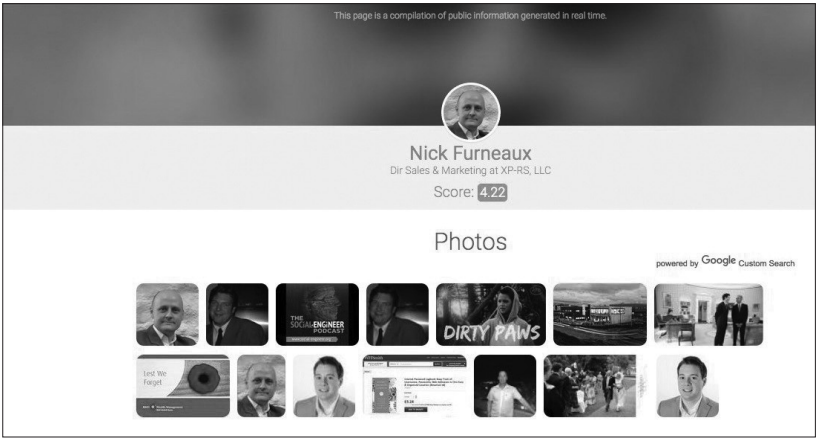
- تصویر اول به توییتر لینک می‌شود.
- تصویر سوم به پادکستی لینک می‌شود که نیک در آن مهمان بوده است. پادکست مهندس اجتماعی است و شنیده‌ام واقعاً عالی است (باز هم تبلیغ بی‌شرمانه).
- بسیاری از تصاویر دیگر به صفحاتی در لینکدین کانادایی‌ها لینک می‌شود که به نیک فرنو موردنظر ما مربوط نیستند.
- تصویر پنجم عجیب است: مردی جوان که نوعی لباس سرهمی و غیرعادی پوشیده است. ماجرا چیست؟

با کلیک روی لینک پنجم به موزیک‌ویدئویی از شرکتی به نام «ای‌اف‌بی پروداکشنز» (AFB Productions) می‌رسیم. وقتی بیشتر روی دکمه کلیک می‌کنم، تصویری را می‌بینم که در شکل ۱۰-۲ نشان داده شده است.

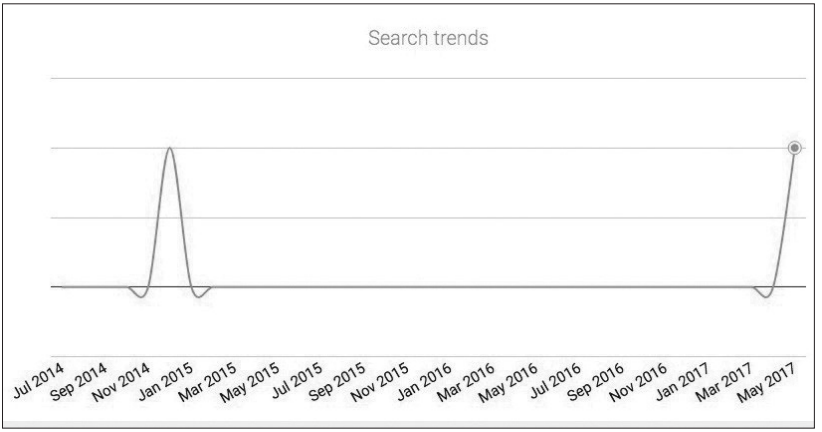
به نظر می‌رسد ویدئو را فردی (با فامیل یکسان) به نام توبی فرنو (Toby Furneaux) ساخته است و در این ویدئو راننده کسی نیست جز نیک فرنو.

البته این یافته مسیر دیگری را باز می‌کند که ببینم توبی کیست و شرکت ای‌اف‌بی چیست و چه‌کار می‌کند.

طولی نمی‌کشد (فقط دو یا سه کلیک) که می‌فهمم توبی پسر نیک است و شرکت تولید موسیقی کوچکی به نام «انی فیوچر باکس» (Any Future Box) یا به‌اختصار ای‌اف‌بی را مدیریت می‌کند.



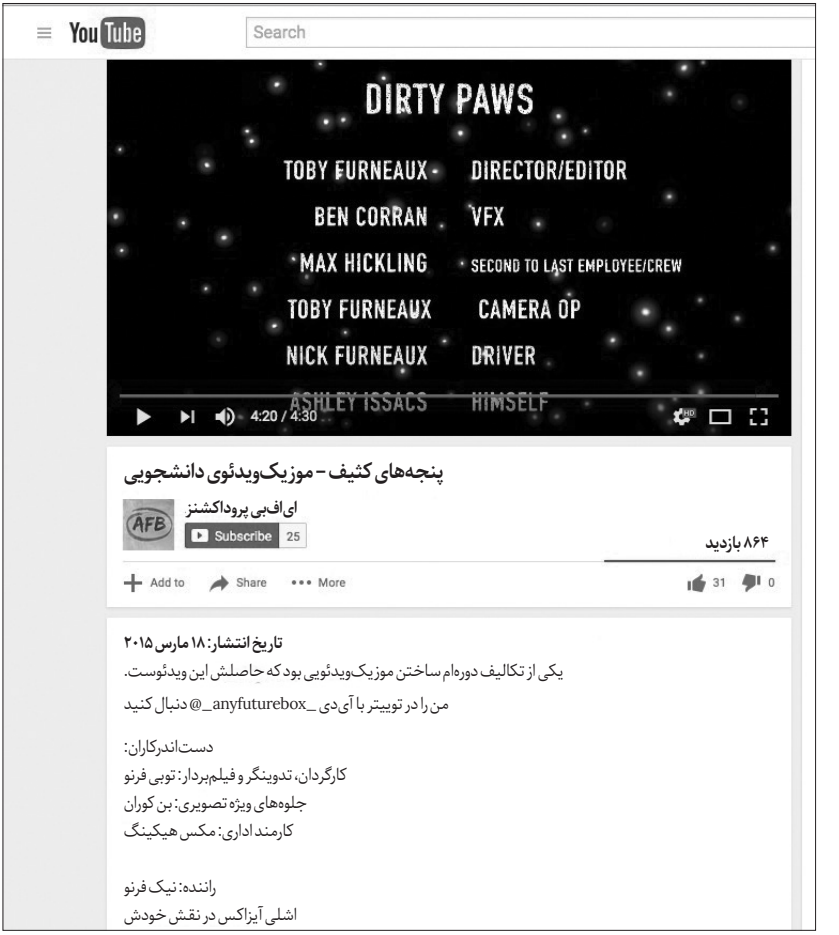
شکل ۸-۲ اطلاعات بسیار بیشتر درمورد نیک



شکل ۹-۲ چه زمانی نیک محبوب بوده است؟

فردی ماهر در جمع‌آوری اطلاعات منبع‌باز همه این جزئیات را در اطلاعات جمع‌آوری‌شده می‌آورد زیرا اعضای خانواده (به‌ویژه فرزندان سوژه) اغلب منابع بسیار خوبی برای رسیدن به شیوه‌های مناسب حمله‌اند.دوباره به شکل ۸-۲ مراجعه کنید. این عکس نیک را چند جا دیده‌ام. این عکس شاید به منابع بیشتری منتهی شود، پس یوآرال (URL) اصلی عکس

را برمی‌دارم و آن را وارد موتور جست‌وجوی تصویر معکوس می‌کنم. می‌توانید این کار را با دنبال کردن گام‌های زیر انجام دهید:



شکل ۱۰-۲ باز هم اطلاعات منبع‌باز بیشتر

۱. روی تصویر کلیک‌راست کنید.

۲. روی نمایش تصویر (View Image) کلیک کنید.

۳. دوباره کلیک‌راست و بعد روی کپی کردن نشانی تصویر (Copy Image Location)

کلیک کنید.

۴. به www.google.com بروید و روی تصاویر (Images) کلیک کنید.

۵. روی جاگذاری نشانی وب تصویر (Paste Image by URL) کلیک و یوآرالی را جاگذاری کنید که در گام سوم کپی کرده بودید.

با صفحه‌ای شبیه شکل ۱۱-۲ مواجه می‌شوید.

شکل ۱۱-۲ چه‌قدر نیک!

```
Domain name:
    csitech.co.uk

Registrant:
    CSI Technologies

Registrant type:
    UK Individual

Registrant's address:
    The registrant is a non-trading individual who has opted to have their
    address omitted from the WHOIS service.

Data validation:
    Nominet was able to match the registrant's name and address against a 3rd party data source on 10-Dec-2012

Registrar:
    Easily Limited t/a easily.co.uk [Tag = WEBCONSULTANCY]
    URL: http://www.easily.co.uk

Relevant dates:
    Registered on: 31-Mar-2004
    Expiry date:  31-Mar-2019
    Last updated:  14-Oct-2013

Registration status:
    Registered until expiry date.

Name servers:
    dns0.easily.co.uk          185.83.100.31
    dns1.easily.co.uk          185.83.102.32

WHOIS lookup made at 02:27:34 19-May-2017
```

شکل ۱۲-۲ تو کی هستی؟

علاوه بر تکرار زیاد این تصویر چهره، متوجه شدم که نیک صفحه‌ای در «بلاگ‌اسپات» (Blogspot) دارد و در صفحه‌ای مربوط به جرم‌شناسی هم مطلب می‌نویسد. وقتی لینک صفحه جرم‌شناسی را دنبال کردم، مصاحبه چند سال پیش نیک را پیدا کردم که با ایمیل و آدرس وب‌سایتش تمام می‌شود.

وقتی درمورد نام دامنه وب‌سایت نیک جست‌وجوی «هوئیز» (WHOIS) انجام دادم، به اطلاعات شکل ۱۲-۲ رسیدم.

نیک مدت زیادی صاحب این وب‌سایت بوده است. جالب است که نیک هوشمندانه دامنه‌اش را خصوصی کرده و در نتیجه هیچ اطلاعاتی به‌جز نام شرکتش (که از قبل می‌دانستیم) و محل سکونتش در بریتانیا وجود ندارد.

نکته‌ای درباره اطلاعات منبع‌باز

برای جست‌وجوی هوئیز چند راه وجود دارد. اگر از لینوکس یا مک استفاده می‌کنید، می‌توانید با وارد کردن whois DOMAIN (و قرار دادن نام دامنه به‌جای DOMAIN) در ترمینال این کار را انجام دهید. می‌توانید از وب‌سایتی رایگان هم استفاده کنید. چند انتخاب دارید، اما سایتی که بیشتر از آن استفاده می‌کنم www.whois.net است.

نوع جمع‌آوری اطلاعاتی که اکنون برای‌تان تشریح کردم در دنیای مهندسی اجتماعی بسیار متداول است.

فکر می‌کنید چرا این‌طور است؟ با فقط چند کلیک توانستم مقدار نسبتاً زیادی اطلاعات مفید درباره سوژه پیدا کنم.

درست است که (خدا را شکر) لینکی از همه رمز عبورها یا عکس‌های خصوصی‌اش پیدا نکردم، اما به‌قدری اطلاعات پیدا کردم که اگر می‌خواستم حمله‌ای فیشینگی یا ویشینگی علیه نیک ترتیب بدهم، واقعاً مفید باشند.

یعنی دیگر تمام شد؟ قطعاً این‌طور نیست. حالا تازه به مهم‌ترین منبع جمع‌آوری اطلاعات منبع‌باز می‌رسیم.

گوگل

گوگل! همین نام به‌تنهایی کافی است که خنده‌ای شیطنت‌آمیز بر لب هر مهندس اجتماعی بیاورد. درست است، این تصویرسازی ذهنی کمی آزاردهنده بود.

پس شاید بهتر باشد تصویر خنده شیطنت‌آمیز را کنار بگذارید و بیشتر آن را لبخندی به‌واسطه شادی ناشی از دانش در نظر بگیرید.

چرا؟ چون گوگل مانند پیشگویی همه‌چیزدان است.

می‌داند چه کارهایی انجام داده‌اید، آن‌ها را ذخیره می‌کند و حتی اگر بخواهید اطلاعات را پاک کنید، آن‌ها را کش می‌کند (می‌دانید که برای حفاظت از آن‌ها).

نکاتی درباره گوگل

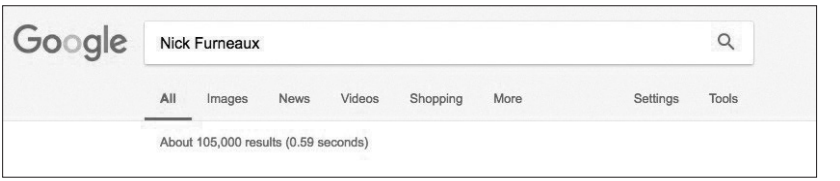
گوگل قدرتمند است؛ حدود ۸۸ درصد سهم بازار را در تبلیغات موتور جست‌وجو در دست دارد. بر اساس اطلاعات گوگل، این موتور جست‌وجو بیش از ۱۰۰٫۰۰۰٫۰۰۰ گیگابایت وب‌سایت را فهرست کرده است (www.google.com/search/howsearchworks/crawling-indexing).

با این‌همه قدرت و تریلیون‌ها صفحه وب فهرست‌شده، یک مهندس اجتماعی ساده چطور آن مقادیر کم داده موردنظرش را پیدا کند؟ پیش از پاسخ باید توضیحی کوتاه درمورد سازوکار گوگل (و در واقع هر موتور جست‌وجوی دیگری) بدهم.

اسرار موتورهای جست‌وجو برملا می‌شود!

در این بخش واقعاً رازی برملا نمی‌شود. عنوان گمراه‌کننده است. احتمالاً همین حالا هم می‌دانید موتورهای جست‌وجو چطور کار می‌کنند، اما اگر نمی‌دانید، این توضیح کوتاه و ساده را بخوانید. موتورهای جست‌وجو از برنامه‌هایی کوچک به نام خزنده وب استفاده می‌کنند. این خزنده‌ها در تمام صفحات موجود در وب «می‌خزند» و چیزهایی را کش می‌کنند که اجازه دسترسی به آن‌ها را دارند. فایل‌های خاصی مثل فایل robots.txt وجود دارند که به خزنده‌ها اجازه نمی‌دهند برخی بخش‌ها را فهرست کنند، اما بیشتر حوزه‌های دیگر فهرست و کش می‌شوند.

این کش در پایگاه داده‌ای ذخیره می‌شود و وقتی عبارتی را در کادر جست‌وجو وارد می‌کنید، نتایجی مانند شکل ۱۳-۲ ارائه می‌دهد.



شکل ۱۳-۲ دوباره نیک

اجازه بدهید به چند نکته کلیدی در شکل ۱۳-۲ اشاره کنم: اول اینکه جست‌وجو در عرض ۰٫۵۹ ثانیه ۱۰۵٫۰۰۰ نتیجه را به نمایش گذاشته است. چطور گوگل می‌تواند در عرض ۰٫۵۹ ثانیه در ۳۰ تریلیون صفحه وب جست‌وجو کند؟ به یاد داشته باشید این صفحات در پایگاه داده‌ای کش شده‌اند که سرعت فوق‌العاده زیاد در جست‌وجو را ممکن می‌کند.

اسکرپینگ ۱۰۵٫۰۰۰ صفحه نه‌تنها نامحتمل بلکه به‌احتمال زیاد ناممکن است. پس اجازه بدهید شما را با عملگرهای جست‌وجو آشنا کنم.

عملگرهای جست‌وجو

گوگل مجموعه‌ای از عبارت‌های جست‌وجو را با نام عملگر ایجاد کرده است که دامنه جست‌وجو را محدود می‌کنند. این مفهوم را در قالب تفاوت استفاده از ذره‌بین و میکروسکوپ ببینید.

هر دو شما را به شیئی که می‌خواهید بررسی کنید نزدیک‌تر می‌کنند، اما اگر می‌خواهید جزئیات بیشتری را مشاهده کنید، میکروسکوپ برای شما مناسب است.

این عملگرها میکروسکوپ جست‌وجو هستند.

دو وب‌سایت زیر همه عملگرهای مفید گوگل (و حتی شماری از عملگرهای مفید «یاهو» و «بینگ») را فهرست کرده‌اند:

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

برای راحتی شما، فهرست زیر را آماده کرده‌ام که فکر می‌کنم مفیدترین عملگرها هستند:

- **Intext**: این عملگر به دنبال هرچیزی «در متن» صفحه وب یا سند مورد جست‌وجو می‌گردد که بعد از این عملگر می‌آید. به‌عنوان مثال اگر intext:csitech را وارد کنید، گوگل به دنبال تمام تکرارهای این عبارت می‌گردد.

- **Site:** این عملگر عبارت‌هایی را که وارد سایت و جست‌وجو کرده‌اید، محدود می‌کند. به‌عنوان مثال اگر site:csitech.co.uk را وارد کنید، گوگل فقط در آن دامنه جست‌وجو می‌کند.
- **inurl:** شاید این عملگر شبیه عملگر site به نظر برسد، اما جست‌وجوی‌تان را به هر یوآرالی محدود می‌کند که در آن عبارت جست‌وجوی شما وجود دارد. اگر inurl:csitech.co.uk را وارد کنید، جست‌وجوی هر وب‌سایتی را که در یوآرال خود دارای عبارت ccistech.co.uk است، در بر می‌گیرد. به‌عنوان مثال اگر سایتی با آدرس forensicsmag.com/csitech.co.uk/interviews وجود داشته باشد، در این جست‌وجو نمایش داده می‌شود، اما در جست‌وجویی با عملگر سایت نمایش داده نمی‌شود.
- **filetype:** این عملگر دقیقاً همان کاری را می‌کند که از عنوانش پیداست؛ جست‌وجوی شما را به نوع فایل انتخابی محدود می‌کند.
- **cache:** این عملگر نسخه‌های کش دامنه، فایل یا هر موردی را جست‌وجو می‌کند که شما وارد کنید.
- **info:** این عملگر درمورد دامنه‌ای که وارد می‌کنید به شما اطلاعات می‌دهد.

درمورد هرچیزی که شامل نرم‌افزار می‌شود، قوانینی وجود دارد. جست‌وجوی گوگل نیز از این موضوع مستثنی نیست.

- عبارت جست‌وجو بعد از عملگر با دو نقطه و بدون فاصله می‌آید. به‌عنوان مثال اگر site:whitehouse.gov را جست‌وجو کنید، جست‌وجو را به whitehouse.gov محدود کرده‌اید. اما اگر site: whitehouse.gov را جست‌وجو کنید، جست‌وجو را به فاصله بعد از دو نقطه محدود کرده‌اید که بی‌اثر است.
- می‌توانید پیش از عملگر از خط فاصله (-) استفاده کنید تا آن نتایج را از جست‌وجوی‌تان حذف کنید. به‌عنوان مثال اگر می‌دانید که می‌خواهید همه ارجاع‌ها به csitech را پیدا کنید، اما نتایج موجود در فضای com. را

نمی‌خواهید، می‌توانید با جست‌وجوی این عبارت نتایج را محدود کنید: inurl:csitech.co.uk -site.com.

- اگر عبارت جست‌وجویی دارید که بیشتر از یک واژه است و می‌خواهید همه واژه‌ها در جست‌وجو باشند، باید از گیومه استفاده کنید. به‌عنوان مثال اگر بخواهم Nick Furneaux را جست‌وجو کنم، می‌توانم intext:"Nick Furneaux" را وارد کنم تا در این جست‌وجو نام و نام خانوادگی هر دو باشند.
- به‌گفته گوگل (https://support.google.com/gsa/answer/4411411# requests)، درمورد تعداد مجاز عبارت‌های جست‌وجو محدودیتی وجود دارد. پیش‌فرض ۵۰ و سقف تعداد عبارت‌ها ۱۵۰ است (اما صادقانه می‌گویم اگر در جست‌وجوی‌تان بیش از ۱۰۰ عبارت وجود دارد، شاید مشکلی دارید).

باور کنید خیلی بیشتر از آنچه اینجا فهرست کردم، عملگر جست‌وجو و نکته‌های دیگر وجود دارند.

گوگل ابزاری قدرتمند است و می‌توانم چند جلد کتاب درباره جزئیات و ریزه‌کاری‌هایش بنویسم و تشریحش کنم. اما باید به مبحث اطلاعات منبع‌باز برگردیم.

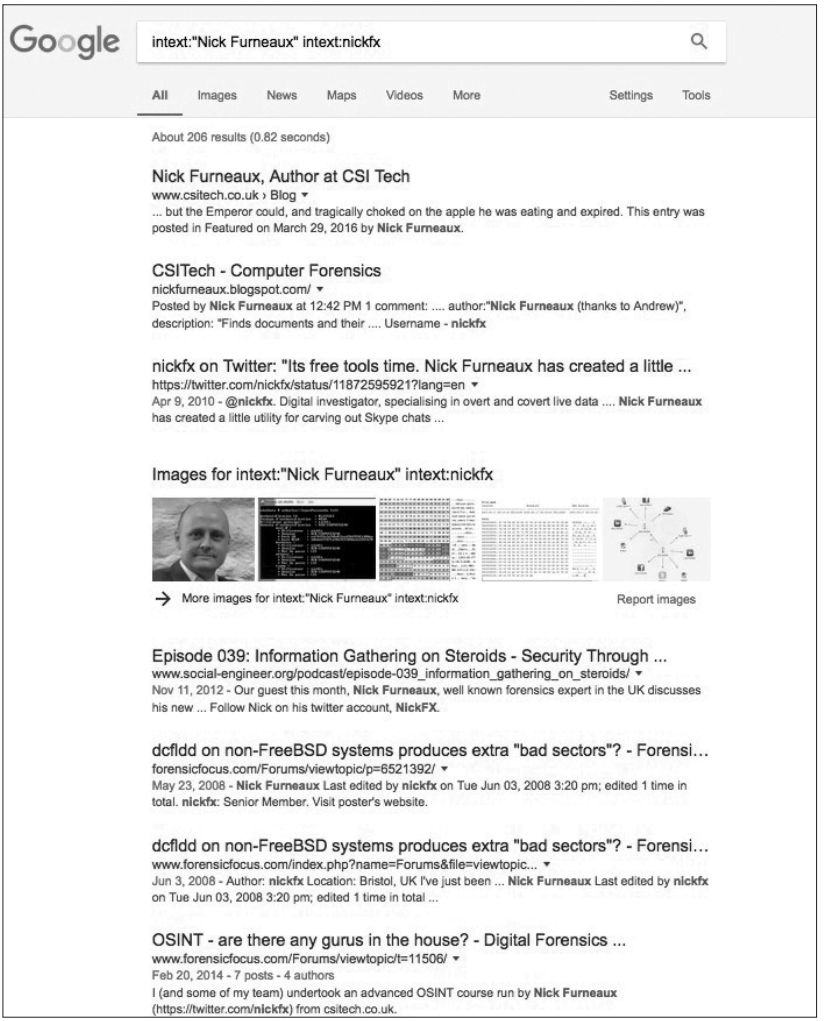
بیایید چند مثال را بررسی کنیم و ببینیم چه چیزهایی می‌توانیم پیدا کنیم.

محدود کردن برای موفق شدن

وقتی از وسط جست‌وجویم درباره نیک فرنو موضوع عوض شد، در حال ایجاد پروفایلی کوچک درمورد او بودم. آیا گوگل می‌تواند یافته‌هایم را تأیید کند یا حتی اطلاعاتی بیشتر بدهد؟

اطلاعاتی مثل نام و نام مستعاری را که از آن استفاده می‌کرد در دست‌کم یک شبکه اجتماعی پیدا کرده بودم. چطور است این دو را در کنار هم جست‌وجو کنم تا ببینیم چه چیزهایی پیدا می‌شوند.

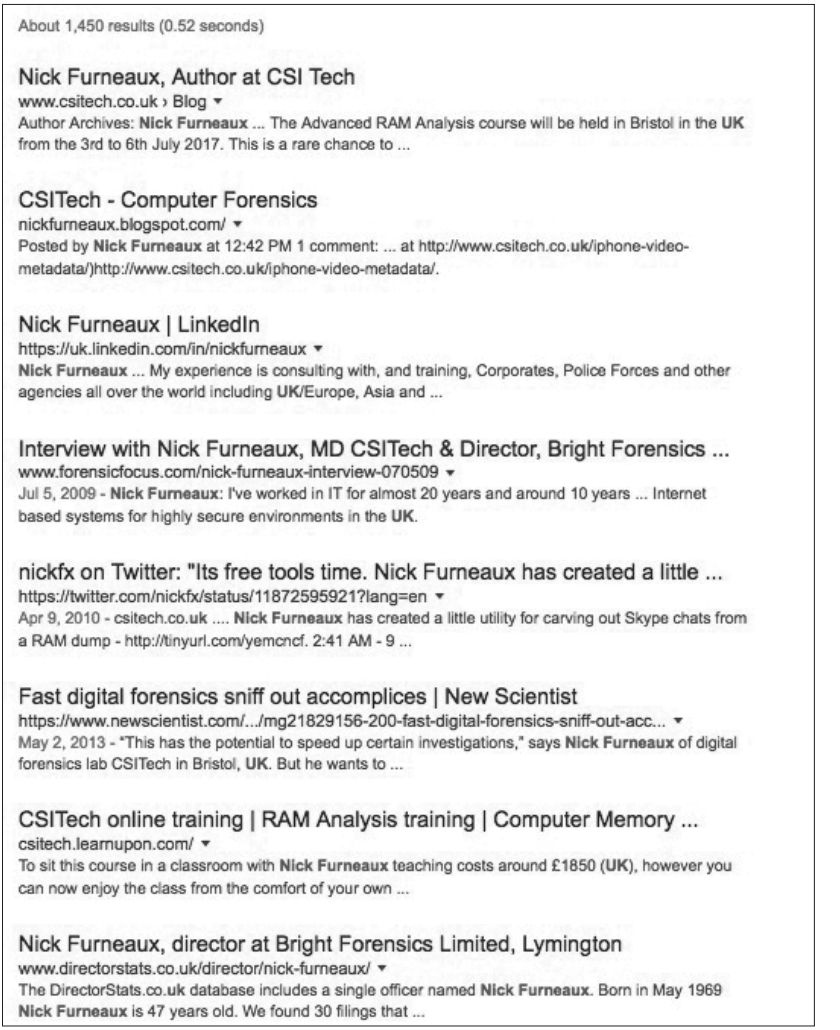
با وارد کردن intext:nickfx intext:"Nick Furneaux" در کادر جست‌وجوی گوگل نتایجی را که نشان داده شدند، در شکل ۱۴-۲ مشاهده می‌کنید.



شکل ۱۴-۲ صفر تا ۲۰۶ نتیجه در دقیقاً ۰٫۸۲ ثانیه

در کمتر از یک ثانیه ۲۰۶ نتیجه درمورد سوژه دریافت می‌کنم. یکی از قابلیت‌های جست‌وجوی گوگل امکان مشاهده تصاویر مربوط به جست‌وجوست. کلیک روی لینک «تصاویر بیشتر» (More Images For) نتایجی جذاب را به شما نشان می‌دهند. در این مورد

تصاویر می‌توانند من را به صفحاتی ببرند که درمورد نیک هستند. اما تا پیش از این اطلاعات زیادی درباره نیک داشتم، پس بیایید ببینیم چه اطلاعات دیگری می‌توانیم پیدا کنیم. عبارت جست‌وجو را به intext:UK intext:"Nick Furneaux" تغییر می‌دهم. نتایج در شکل ۱۵-۲ نشان داده شده‌اند.


About 1,450 results (0.52 seconds)

Nick Furneaux, Author at CSI Tech
www.csitech.co.uk › Blog
Author Archives: **Nick Furneaux** ... The Advanced RAM Analysis course will be held in Bristol in the **UK** from the 3rd to 6th July 2017. This is a rare chance to ...

CSITech - Computer Forensics
nickfurneaux.blogspot.com/
Posted by **Nick Furneaux** at 12:42 PM 1 comment: ... at http://www.csitech.co.uk/iphone-video-metadata/)http://www.csitech.co.uk/iphone-video-metadata/.

Nick Furneaux | LinkedIn
https://uk.linkedin.com/in/nickfurneaux
Nick Furneaux ... My experience is consulting with, and training, Corporates, Police Forces and other agencies all over the world including **UK**/Europe, Asia and ...

Interview with Nick Furneaux, MD CSITech & Director, Bright Forensics ...
www.forensicfocus.com/nick-furneaux-interview-070509
Jul 5, 2009 - **Nick Furneaux**: I've worked in IT for almost 20 years and around 10 years ... Internet based systems for highly secure environments in the **UK**.

nickfx on Twitter: "Its free tools time. Nick Furneaux has created a little ...
https://twitter.com/nickfx/status/11872595921?lang=en
Apr 9, 2010 - csitech.co.uk .... **Nick Furneaux** has created a little utility for carving out Skype chats from a RAM dump - http://tinyurl.com/yemcncf. 2:41 AM - 9 ...

Fast digital forensics sniff out accomplices | New Scientist
https://www.newscientist.com/.../mg21829156-200-fast-digital-forensics-sniff-out-acc...
May 2, 2013 - "This has the potential to speed up certain investigations," says **Nick Furneaux** of digital forensics lab CSITech in Bristol, **UK**. But he wants to ...

CSITech online training | RAM Analysis training | Computer Memory ...
csitech.learnupon.com/
To sit this course in a classroom with **Nick Furneaux** teaching costs around £1850 (**UK**), however you can now enjoy the class from the comfort of your own ...

Nick Furneaux, director at Bright Forensics Limited, Lymington
www.directorstats.co.uk/director/nick-furneaux/
The DirectorStats.co.uk database includes a single officer named **Nick Furneaux**. Born in May 1969 **Nick Furneaux** is 47 years old. We found 30 filings that ...

شکل ۱۵-۲ آیا به پاسخ نزدیک می‌شویم؟

اولین نتیجه نشان می‌دهد در شهری به نام بریستول آموزش می‌دهد. آخرین نتیجه نام شرکتی را نشان می‌دهد که ممکن است نیک هنوز یکی از اعضای آن باشد. همچنین تاریخ دقیق تولد و حتی آدرسی از نیک می‌دهد (که همان‌طور که حدس می‌زنید در بریستول است).

این صفحه همچنین شامل فهرستی از نام‌های اعضای خانواده و دوستانی می‌شود که ممکن است با نیک در آن شرکت همکار باشند. گنجینه اطلاعاتی مهمی است.

با قرار دادن «بریستول» به‌جای «بریتانیا» در عبارت جست‌وجوی قبلی، به اطلاعاتی مثل کد پستی و حتی نام برخی دیگر از اعضای خانواده می‌رسیم که احتمالاً با نیک زندگی می‌کنند.

پیش از عبور از این بخش بیایید این مثال را بررسی کنیم. فکر می‌کنید اگر جست‌وجوی زیر را در گوگل انجام دهید، اولین نتیجه چه خواهد بود؟

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

نتیجه اولی که با این جست‌وجو پیدا کردم، صفحه لینکدین نیک بود. با استفاده از عملگرهای گوگل می‌توانید اطلاعاتی از جست‌وجوهای قبلی‌تان اضافه کنید تا به اطلاعات دقیق مورد نیازتان نزدیک و نزدیک‌تر شوید و در نهایت آن‌ها را پیدا کنید.

می‌خواهم نکته‌های بیشتری درباره قدرت گوگل به شما بگویم، اما چون نیک هنوز دوستم است (دست‌کم آخرین باری که بررسی کردم بود)، از تمرکز روی اطلاعات مربوط به او فاصله می‌گیرم و بیشتر به جست‌وجوهای عمومی می‌پردازم.

اما در خود عنوان نوشته شده «خصوصی»

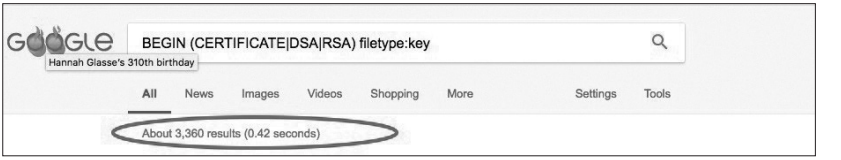
آیا با مفهوم کلید خصوصی «آراس‌ای» (RSA) آشنا هستید؟ کلید آراس‌ای کلیدی مبتنی بر الگوریتمی انحصاری است و دو بخش دارد: کلید عمومی که به تعیین هویت آن کمک می‌کند و کلید خصوصی که قفل موردنظر را باز می‌کند.

طبق این تعریف، از کلیدهای خصوصی آراس‌ای برای برقراری ارتباط امن استفاده می‌شود.

پس احتمالاً فکر می‌کنید اگر کلیدهای خصوصی آراس‌ای را جست‌وجو کنید، به هیچ نتیجه‌ای نمی‌رسید، درست است؟ اما استفاده از عبارت جست‌وجوی زیر

BEGIN (CERTIFICATE|DSA|RSA) filetype:key

بیش از ۳٫۰۰۰ نتیجه می‌دهد که در شکل ۱۶-۲ می‌بینید.



شکل ۱۶-۲ پس چرا می‌گویید خصوصی؟

اما نشان محرمانه دارد

نهادهای دولتی معمولاً اسناد را با طبقه‌بندی‌هایی خاص نشان‌دار می‌کنند تا نشان بدهند که عموم مردم می‌توانند این اسناد را ببینند یا خیر. نشان‌هایی مثل «محرمانه» و «فوق‌محرمانه» معمولاً به این معنی‌اند که مردم عادی نباید این اسناد را ببینند. در نتیجه فرض می‌کنیم که نمی‌توان این اسناد را در فضای آنلاین پیدا کرد (ولی همیشه از این فرض‌ها پرهیز کنید).

اما از آنجا که زندگی خارج از زندان را بیشتر دوست دارم، بیایید فرض کنیم فقط می‌خواهیم ببینیم اسنادی با رمز عبور که باید محرمانه باشند وجود دارند یا خیر.

چه اتفاقی می‌افتد اگر site:gov.ir intext:password filetype:xls را جست‌وجو کنم؟ با این کار جست‌وجویم به همه دامنه‌های gov.ir محدود می‌شود و فقط دنبال فایل‌هایی با فرمت XLS می‌گردد که در آن‌ها واژه password وجود دارد. نتایج در شکل ۱۷-۲ نشان داده شده‌اند.

برای جست‌وجوی شما site:gov.ir intext:password filetype:xls نتیجه‌ای پیدا نشد.
پیشنهادها:

- اطمینان حاصل کنید که املای واژه‌ها درست است.
- کلیدواژه‌های دیگری را امتحان کنید.
- کلیدواژه‌های کلی‌تری را امتحان کنید.
- کلیدواژه‌های کمتری را امتحان کنید.

شکل ۱۷-۲ چه مشکلی پیش آمد؟

درست به نظر نمی‌آید. چرا سندی در سروری دولتی در ایران باید حاوی واژه انگلیسی password باشد؟ اما چطور است از سایت translate.google.com استفاده کنیم تا واژه password را به فارسی ترجمه کنیم؟ آیا فایده‌ای دارد؟ شکل ۱۸-۲ نتیجه را نشان می‌دهد.

شکل ۱۸-۲ جست‌وجوهای چندزبانه در گوگل

قدرت گوگل اینجا به‌خوبی نشان داده شده است؛ نیازی نیست فارسی بلد باشم یا حتی به فارسی جست‌وجو کنم، فقط کافی است به گوگل بگویم دنبال این واژه بگردد تا اسناد را پیدا کنم.

وبکم‌ها: وقت آن رسیده که دیگر با لباس زیر نرقصید

زمانی شاهد افزایش گرایش شدید افراد به داشتن وبکم در خانه‌های‌شان بودیم. افراد برای حفظ امنیت یا هدفی دیگر از وبکم‌ها جهت نظارت بر کودکان، پرستاران کودکان و حیوانات خانگی‌شان استفاده می‌کردند.

بسیاری از این دوربین‌ها با تنظیماتی پیش‌فرض به فروش می‌رسیدند که آن‌ها را آسیب‌پذیر و بدون محافظ می‌کردند.

گاهی اوقات نرم‌افزاری که همراه با این دوربین‌ها فروخته می‌شد نیز ایمنی چندانی نداشت. به این ترتیب کار برای کاربر آسان می‌شد، اما حمله کردن نیز برای مهاجمان راحت بود.

«وبکم‌اکس‌پی» (webcamXP) یکی از این نوع نرم‌افزارها بود. به‌نحوی طراحی شده بود که روی همه ویندوزها قابل‌اجرا باشد. طبق اطلاعات وب‌سایت این نرم‌افزار، آخرین به‌روزرسانی آن در سال ۲۰۱۶ بوده است. با توجه به این نکته به نظر می‌رسد اکنون نباید چندان پرکاربرد باشد، پس احتمالاً تصور می‌کنید جست‌وجو در این زمینه نتیجه‌ای خاص نخواهد داشت، درست است؟

پس intitle:"Webcam 7" inurl:8080 -intext:8080 را جست‌وجو می‌کنم. شکل ۱۹-۲ نتایج را نشان می‌دهد.

درست است که قرار بوده بسیاری از این وبکم‌ها آنلاین باشند و برای مشاهده عموم در دسترس قرار گرفته‌اند و بسیاری از آن‌ها تصاویر دوربین‌های ترافیکی، اسکله‌ها یا مکان‌های دیگر را پخش می‌کنند، اما افرادی هستند که برای استفاده شخصی وبکم‌هایی را راه‌اندازی می‌کنند و در حیاط‌ها یا درون خانه‌های‌شان قرار می‌دهند. منظور این است که اگر این وبکم‌ها به‌درستی ایمن نشده باشند، هر فردی با کمی مهارت می‌تواند بدون اینکه دیگران بفهمند، تصاویر این دوربین‌ها را تماشا کند.

دیگر منابع اطلاعات

معمولاً وقتی به این بخش می‌رسم، افراد هم می‌ترسند و هم کنجکاو می‌شوند که با جست‌وجوی گوگل چه اطلاعات دیگری می‌توان به دست آورد. نمی‌خواهم همه جست‌وجوهای گوگلم را ردیف کنم، اما می‌توانم به برخی از یافته‌هایی اشاره کنم که به‌سادگی و صرفاً با استفاده از جست‌وجوی گوگل به دست آورده‌ام:

- وبکم فردی که در حال تماشای رشد گیاهان ماری‌جوانایش بود؛
- تصاویر شخصی افراد در تلفن‌های‌شان؛
- فهرست‌های موسیقی و فیلم‌هایی که افراد به اشتراک گذاشته بودند؛
- اسناد حاوی رمز عبور، تاریخ تولد و شماره تأمین اجتماعی افراد؛
- هزاران شماره کارت اعتباری در قالب فایل‌های مختلف؛
- پایگاه‌های داده اس‌کیوال کاملاً باز با اطلاعات فراوان؛
- دسترسی آزاد به دوربین‌های ترافیکی؛
- دسترسی آزاد به شبکه‌های انرژی و سیستم‌های کنترل؛

- تعدادی محل تحویل محتوای پورنوگرافی کودکان.

این فهرست می‌تواند همین‌طور ادامه پیدا کند.

شکل ۱۹-۲ مهمانی وبکم‌ها

دو مسئله دیگر

این بخش به‌تنهایی می‌تواند یک کتاب مجزا باشد، اما کوتاهی کرده‌ام اگر پیش از اتمام این فصل به دو مسئله دیگر اشاره نکنم.

ربات‌ها باحال هستند

وقتی بچه بودم خیلی دوست داشتم یکی از ربات‌های «آرتودی‌تو» (R2D2) را داشته باشم. فکر می‌کردم اگر یکی از این ربات‌ها را داشته باشم، بهترین دوستم خواهد بود. در این بخش درمورد این نوع ربات‌ها حرف نمی‌زنم بلکه به فایل‌های robots.txt می‌پردازم.

فایل robots.txt چیست؟ فایلی است که صاحبان وب‌سایت‌ها از آن استفاده می‌کنند تا به ربات‌های خزنده و اسکرپر سایت‌ها بگویند اجازه دارند چه کارهایی را انجام دهند و برعکس. به‌عنوان مثال در برخی از فایل‌های robots.txt «گزاره‌های غیرمجاز» وجود دارند که نشان می‌دهند ربات‌ها اجازه ندارند فولدری را کش کنند. برای مثال شکل ۲۰-۲ فایل robots.txt وب‌سایت whitehouse.gov را نشان می‌دهد.

اکنون لحظه‌ای مانند یک مهندس اجتماعی فکر کنید. فایل شکل ۲۰-۲ به شما چه می‌گوید؟

می‌توانید ببینید چه مدخل‌هایی وجود دارند، در عین حال می‌توانید ببینید به کدام مدخل‌ها نمی‌خواهند دسترسی پیدا کنید یا نمی‌خواهند گوگل آن‌ها را کش کند.

به‌علاوه، فایل‌هایی مثل mysql یا pgpsql نشانه‌هایی از نوع فناوری مورد استفاده برای ایجاد این سایت فراهم می‌کنند.

اکنون اگر این سایت واقعاً هدف بود (که با تأکید می‌گویم نیست)، وارد تک‌تک مدخل‌ها می‌شدیم تا مطمئن شویم به‌نحوی مناسب پیکربندی شده‌اند و به ما اجازه نمی‌دهند بدون مجوز به آن‌ها دسترسی داشته باشیم. آن لاگ‌ها و فایل‌ها را، اگر دسترسی‌پذیر باشند، بررسی می‌کنیم تا ببینیم در سرورها اشتباهی در پیکربندی

وجود دارد یا خیر.

زمانی کاری را برای شرکتی انجام می‌دادم. از آن آزمایش‌های کم‌نظیری بود که از ما می‌خواست «هر کاری می‌توانیم انجام دهیم و ببینیم چه می‌توانیم پیدا کنیم و بعد بدون هیچ ملاحظه‌ای به آن‌ها حمله کنیم». با جمع‌آوری مقدماتی اطلاعات منبع‌باز و جست‌وجوی گوگل شروع کردم و دیدم در فایل robots.txt این سایت گزاره‌ای غیرمجاز برای مدخلی به نام ادمین وجود دارد.

صرفاً از سر کنجکاوی آدرس www.company.com/admin را وارد کردم و غافل‌گیر شدم، چون فهمیدم بدون نیاز به هیچ نام کاربری یا رمز عبوری می‌توانم وارد شوم. این مدخل حاوی مخزن فایل خصوصی مدیرعامل بود و به نظر می‌رسید از این مدخل برای به اشتراک گذاشتن فایل‌های مورد نیاز هنگام سفر استفاده کرده است. قراردادها، داده‌های بانکی، تصویری از گذرنامه مدیرعامل و داده‌های حساس بی‌شمار دیگری در این مدخل وجود داشتند.

قراردادی پیدا کردم که در چند روز گذشته امضا شده بود. دامنه‌ای خریدم که نامش فقط یک یا دو کاراکتر با نام واقعی شرکت دیگر طرف قرارداد فرق داشت، ایمیلی برای فرد امضاکننده قرارداد ساختم و حمله فیشینگ را با ارسال فایلی مخرب و ایمیلی به مدیرعامل شروع کردم که در آن آمده بود: «در بخش 14.1a قرارداد پرسشی وجود دارد. لطفاً آن را ببینید و به من پاسخ بدهید.»

```
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/
```

شکل ۲۰-۲ موارد زیادی غیرمجاز شمرده شده‌اند

در عرض ۱۵ دقیقه مدیرعامل ایمیل را باز کرد و در دام افتاد. سپس برای آن آدرس جعلی ایمیلی فرستاد و گفت قرارداد باز نمی‌شود و مدام متوقف می‌شود. آزمون نفوذ که قرار بود یک هفته طول بکشد، در عرض فقط سه ساعت تمام شد.

با مدیرعامل تماس گرفتم. گفت‌وگوی‌مان این‌طور پیش رفت:

مدیرعامل: «سلام.»

من: «سلام پل. کریس هستم از شرکت «سوشال انجینیر» (Social-Engineer). زنگ زدم تا درمورد آزمون نفوذ حرف بزنم.»

مدیرعامل: «به این زودی تسلیم شدی کریس؟ می‌دانستم نفوذ به شرکت ما خیلی دشوار است.»

من: «حقیقتش پل، ما همین حالا گذرنامه و تاریخ تولدت، دسترسی به بانک‌هایت و دسترسی از راه دوری (remote shell) با نام کاربری و رمز عبور ادمین در شبکه داریم. با خودم گفتم باید تماس بگیرم و ببینم آیا هنوز هم می‌خواهی تا یک هفته به کارم ادامه بدهم؟»

مدیرعامل: «بس کن! داری شوخی می‌کنی! تازه چند ساعت پیش شروع شد. بگو آن بی‌عرضه‌ای که کلیک کرده و دسترسی را داده کیست؟ می‌خواهم با او حرف بزنم.»

من: «حقیقتش پل... (آب دهانم را قورت دادم، نمی‌دانستم جای مناسبی برای شوخی درون ذهنم است یا نه) جای تو بودم خیلی به او سخت نمی‌گرفتم؛ آدم خیلی خوبی است.»

مدیرعامل: «که این‌طور. واقعاً؟ کی بود که دسترسی داد؟»

من: «پل، آن فرد تو هستی.»

بعد همه جزئیات را برایش توضیح دادم و خیلی زود متوجه شد چه اتفاقی افتاده است. موفقیت این آزمون نفوذ تا حد زیادی مدیون فایل robots.txt و مدخلی با پیکربندی اشتباه بود.

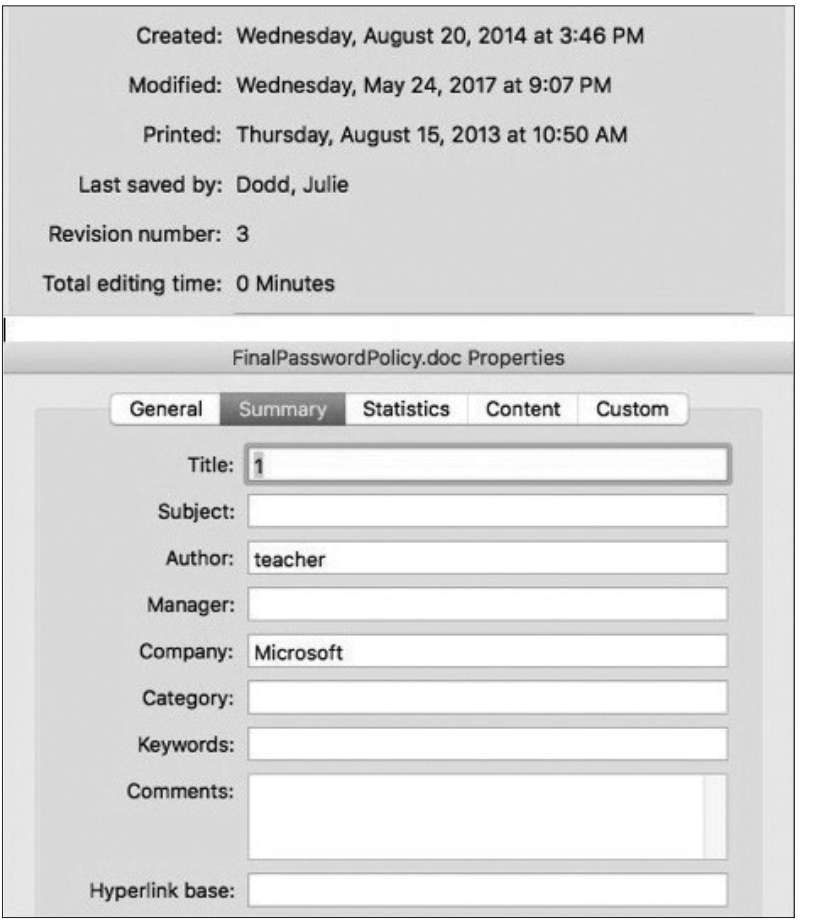
همه‌چیز به فراداده برمی‌گردد

طبق تعریف فرهنگ آکسفورد، «متا» (meta) به‌معنی «ارجاع به خود یا به قواعد گونه خود؛ خودارجاعی» است. بنابراین فراداده به‌معنی داده‌ای درباره داده است.

اجازه بدهید ساده‌تر توضیح بدهم. فراداده اطلاعاتی درباره یافته‌ای است که در جست‌وجو

پیدا می‌کنید. این داده‌ها در بسیاری از موارد واقعیت‌هایی بسیار جالب را فاش می‌کنند و بسیاری از این واقعیت‌ها آگاهانه در آنجا قرار داده نشده‌اند.

فرض کنید جست‌وجویی بسیار بی‌خطر در گوگل انجام می‌دهم تا آن دسته از فایل‌های دارای فرمت .doc را پیدا کنم که اطلاعاتی درباره رمزهای عبور دارند. به سندی با نام «فاینال‌پسوردپالیسی» (FinalPasswordPolicy) برخورد می‌کنم. متاداده این فایل چه اطلاعاتی را آشکار می‌کند؟ به شکل ۲۱-۲ نگاهی بیندازید.



شکل ۲۱-۲ فراداده به ما چه می‌گوید؟

این فراداده تاریخ و زمان ایجاد فایل، آخرین فردی که آن را ذخیره کرده، نام و عنوان پدیدآورنده، تعداد تغییراتی که در فایل اعمال شده و اطلاعات دیگری را به ما می‌دهد که اینجا به آن‌ها اشاره نمی‌کنم. شاید بپرسید: «خب که چی؟»

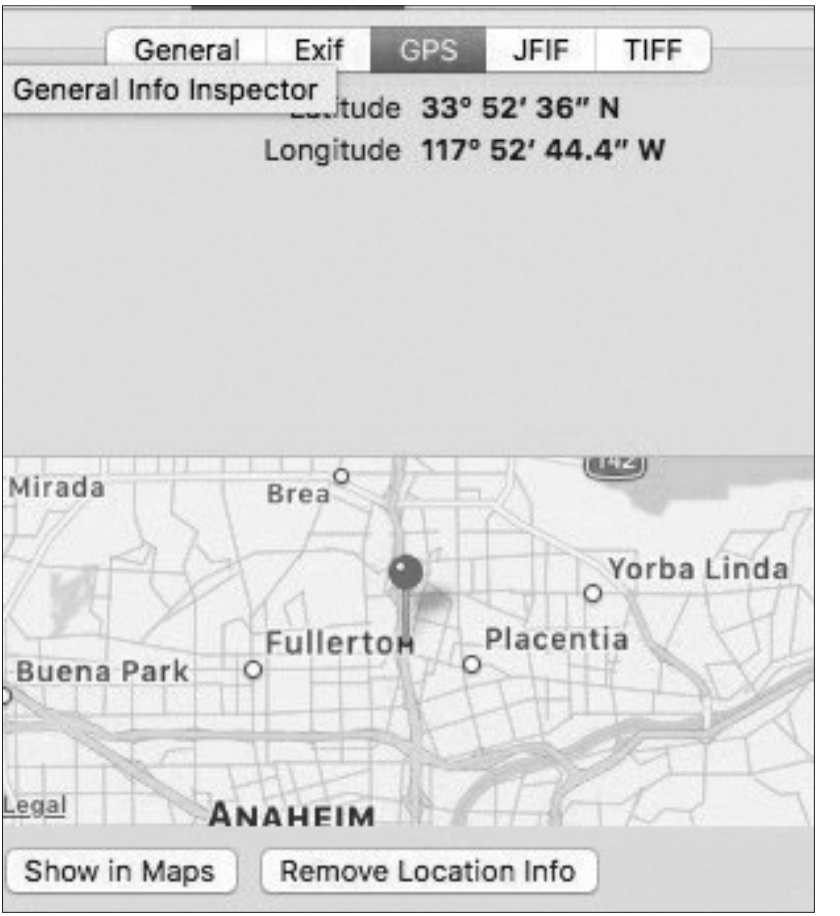
همین نام و نوع سند می‌توانند اطلاعاتی بسیار مهم برای یک مهندس اجتماعی باشند. به این فکر کنید که چه می‌شود اگر یک مهندس اجتماعی مقررات منابع انسانی جدیدی را پیدا کند که تازه منتشر کرده‌اید؟ فراداده نشان می‌دهد این مقررات آخرین بار چه زمانی تغییر کرده‌اند (در این مورد حتی یک ماه هم نمی‌گذرد)، چه کسی آن را نوشته و چه زمانی منتشر شده است. البته اطلاعات این مقررات در سند هم وجود دارد. فکر می‌کنید ایمیل فیشینگی که ظاهراً از طرف فردی ارسال شده که مقررات را نوشته و به نظر می‌رسد درباره به‌روزرسانی مقررات است، ممکن است چند کلیک بخورد؟

شکل ۲۲-۲ را ببینید.

شکل ۲۲-۲ «نه، واقعاً می‌پرسم! این فراداده به ما چه می‌گوید؟»

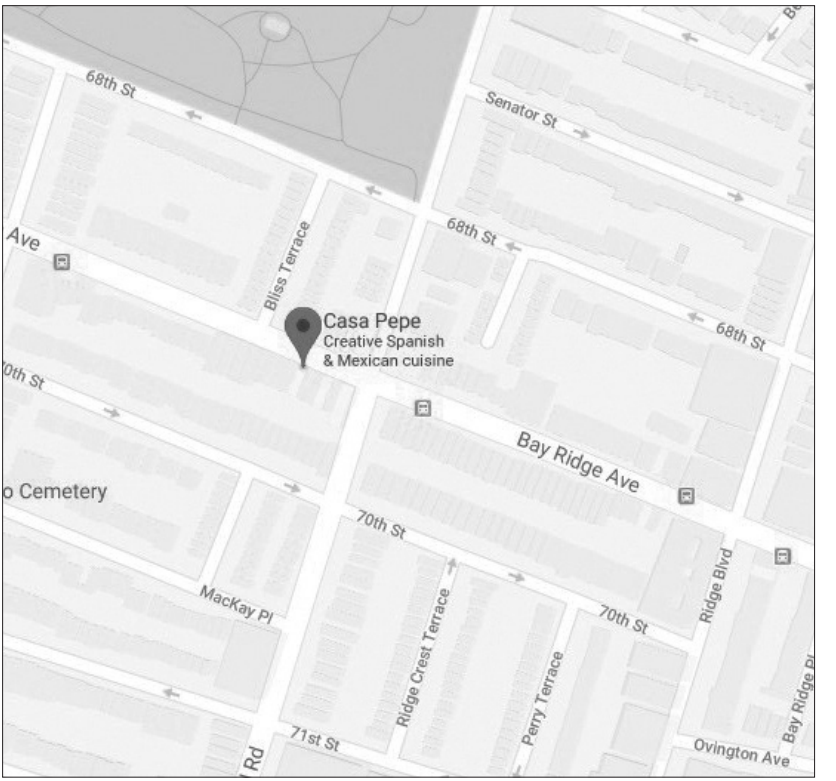
در نگاه اول شاید فکر کنید: «آیا قرار است با ارسال کد تخفیف سس تند به این فرد حمله

فیشینگ کنیم؟» خیر. اما به فراداده‌ای نگاه کنید که در شکل ۲۳-۲ نشان داده شده است.



شکل ۲۳-۲ پاسخ این است که...

وقتی عکسی به‌ظاهر بی‌اهمیت را در فضای آنلاین پیدا می‌کنید، فراداده عکس اطلاعاتی درباره نوع دوربین، تاریخ و زمان ثبت عکس و مختصات جی‌پی‌اس محل ثبت عکس را به ما نشان می‌دهد. وقتی این مختصات را وارد نقشه گوگل کنید، شکل ۲۴-۲ را به شما نشان می‌دهد.



شکل ۲۴-۲ اگر از من بپرسید، می‌گویم خیلی جذاب است

نقشه پارکینگ رستوران «په‌په» (Pepe) را نشان می‌دهد که یکی از مصرف‌کنندگان بزرگ این برند سس تند است.

بنابراین فردی از تلفن هوشمندش برای عکس گرفتن استفاده کرده است. جی‌پی‌اس تلفنش روشن بوده و به اپلیکیشن دوربین اجازه داده همه این فراداده‌را در قسمت پنهان فایل عکس ثبت کند. وقتی این فرد عکس را در حسابش در شبکه‌ای اجتماعی آپلود کرده، فایل حاوی همه این اطلاعات بوده و در نتیجه برای همه جهان منتشر شده است.

آیا متوجه پیامدهای این مسئله می‌شوید؟ تصور کنید کسی که با او شام می‌خورید دوست‌تان نیست، یکی از افراد زیر است:

- مدیرعامل یک شرکت بزرگ خدمات شهری (آب، برق، گاز و غیره) که هدف حمله هک دولتی است.
- منشی فردی میلیاردر که اطلاعاتی درباره حساب‌های بانکی رئیسش و همچنین اجازه انتقال وجه دارد.
- دختر ۱۵ ساله‌تان که عکس‌هایی شیطنت‌آمیز از خودش می‌گیرد.

حالا متوجه پیامدها شدید؟ فرقی نمی‌کند به کدام سناریو فکر کرده باشید، در هر صورت اطلاعاتی که به‌راحتی در دسترس همه قرار دارند، به‌سرعت خطرناک می‌شوند.

به همراه تیمم مأموریت داشتیم درمورد سوژه‌ای سطح بالا در حوزه نظامی و دفاعی اطلاعات منبع‌باز جمع‌آوری و سپس به او حمله کنیم. نمی‌خواستیم به او آسیب بزنیم، بلکه می‌خواستیم میزان تمایلش به انجام عملی را بسنجیم که نباید انجام می‌داد. باید همه تماس‌ها و کلیک‌ها را برای اهداف آموزشی ثبت و ضبط می‌کردیم.

با جمع‌آوری اطلاعات منبع‌باز اولیه به صفحاتش در شبکه‌های اجتماعی رسیدیم. وقتی فهمیدیم زیاد توییت می‌کند و معمولاً هنگام استفاده از آیفون جدیدش جی‌پی‌اس را روشن می‌گذارد، متوجه شدیم به گنجینه‌ای از اطلاعات دست یافته‌ایم. چرا این مسئله خیلی مهم بود؟ توییتر به ما اجازه می‌داد نموداری از تغییر مکانش در طول روز و هنگام توییت کردن از هر مکانی ترسیم کنیم. در عرض چند ساعت اطلاعات زیر را به دست آوردیم:

- مکانی که معمولاً هر روز صبح برای خریدن قهوه به آنجا می‌رفت؛
- باشگاه ورزشی‌ای که بعد از کار و قبل از رفتن به خانه به آنجا می‌رفت؛
- دو رستوران مورد علاقه‌اش؛
- نشانی خانه‌اش؛
- اینکه چقدر از ترافیک شهری متنفر بود.

اطلاعات منبع‌باز بسیار بیشتری وجود داشتند، اما اطلاعات موجود در این فهرست نقشی بسیار مهم در حمله‌های ما پیدا کردند. ابتدا نام دامنه‌ای را پیدا کردیم که فقط یک حرف با نام دامنه باشگاهش تفاوت داشت. خیلی سریع ایمیلی نوشتیم که به او می‌گفت در حال به‌روزرسانی همه حساب‌ها هستیم و اطلاعات کارت اعتباری‌اش دیگر معتبر نیستند. از او خواستیم «همین حالا وارد حسابش شود تا اطلاعات کارت اعتباری

را وارد کند»، خیلی سریع روی لینک کلیک کرد.

از آنجا که می‌دانستیم با خطای ۴۰۴ (صفحه پیدا نشد) مواجه می‌شود، صبر کردیم تا روی لینک کلیک کند و بعد به تلفنش زنگ زدیم. گفت‌وگوی‌مان شبیه زیر بود:

تماس‌گیرنده: «سلام. آقای اسمیت؟»

سوژه: «بله، بفرمایید. شما؟»

تماس‌گیرنده: «سارا هستم از باشگاه «کلد» (Cold). امروز ایمیلی درباره به‌روزرسانی سیستم ارسال کردیم. لینک موجود در ایمیل خراب بود. به همین دلیل برای عذرخواهی با مشتریان‌مان تماس می‌گیریم. می‌توانم لینک جدیدی برای‌تان ارسال کنم یا اطلاعات کارت اعتباری‌تان را بگیرم و خودم به‌جای شما اطلاعات را به‌روزرسانی کنم. کدام برای شما آسان‌تر است؟»

سوژه: «مشکلی نیست سارا. بفرمایید این هم شماره کارتم.»

تماس‌گیرنده: «ممنون آقای اسمیت! فعلاً خدانگهدار!»

این حمله به این دلیل موفق شد که برای هدف آشنا و باورپذیر بود. با کمی اطلاعات منبع‌باز، یک ایمیل فیشینگ و یک تماس، به یک کلیک، شماره کارت اعتباری و پنج شیوه حمله آماده دیگر دست یافتیم که در صورت نیاز می‌توانستیم از آن‌ها استفاده کنیم.

فراداده قدرتمند و برای مهندسان اجتماعی مفید است، بنابراین توصیه می‌کنم در هر فایلی که در فرایند جمع‌آوری اطلاعات منبع‌باز به دست می‌آورید، فراداده را بررسی کنید.

این کار، به‌ویژه وقتی با تعداد زیادی فایل سروکار دارید، ممکن است بسیار دشوار باشد. خودم شخصاً از ابزارهایی مثل «فوکا» (FOCA) (www.elevenpaths.com/labstools/foca/index.html) و «مالتیگو» (Maltego) (www.paterva.com/web7) استفاده می‌کنم تا این کار را آسان‌تر کنم. هرچند قول دادم که در این کتاب هیچ ابزاری را به‌شکل مفصل بررسی نکنم، احساس می‌کنم ضرورت دارد دست‌کم به‌صورت اجمالی این دو ابزار مفید دیگر را بررسی کنم. در بخش زیر این کار را انجام می‌دهم.

ابزارهای مهم

همان‌طور که در فصل اول گفتم، چون ابزارها زیاد تغییر می‌کنند، تصمیم گرفته‌ام در این کتاب خیلی روی آن‌ها متمرکز نشوم.

با این حال چهار ابزار وجود دارند که از پنج تا ده سال گذشته در جعبه‌ابزارم باقی مانده‌اند و احساس کردم دست‌کم باید به آن‌ها اشاره کنم. هرچند این ابزارها مدت زیادی ماندگار بوده‌اند، رابط‌ها و کارکردهای‌شان تغییر کرده‌اند.

اگر بخواهم وقت زیادی را برای بررسی جداگانه همه قابلیت‌ها صرف کنم، این اطلاعات تا زمان رسیدن کتاب به دست شما کهنه و قدیمی خواهند شد. در عوض آدرس وب‌سایت‌های این ابزارها را به شما می‌دهم و در این وب‌سایت‌ها می‌توانید با دریافت خودآموزها از تازه‌ترین و مهم‌ترین تحولات باخبر شوید.

قول می‌دهم که این بخش کوتاه باشد، اما بخش مهمی از پازل است که نباید از دست بدهید.

اس‌ای‌تی (SET)

به یاد می‌آورم که زمانی با دوست خوبم «دیوید کندی» (David Kennedy) گپ می‌زدم. به او گفتم دوست دارم ابزاری داشته باشم که با آن بتوانم به فردی حمله فیشینگ کنم و نام کاربری و رمز عبور به دست بیاورم یا هر صفحه وبی را شبیه‌سازی کنم.

دیوید پاسخ داد: «فکر می‌کنم بتوانم این کار را انجام بدهم.»

هنوز ۲۴ ساعت هم نگذشته بود که نمونه اولیه را آماده کرد. از آن زمان دیوید آن‌چنان مشغول اس‌ای‌تی یا «جعبه‌ابزار مهندس اجتماعی» (Social-Engineer Toolkit) شد که انگار رسالت زندگی‌اش است.

مدام (به نظر می‌رسد هر روز) به‌روزرسانی می‌کند و قابلیت‌هایی ایجاد کرده است که باعث می‌شوند ایده کوچک اولیه من بسیار خام به نظر برسد. این ابزار فوق‌العاده بیش از دو میلیون بار دانلود شده است.

می‌توانید این ابزار و دستورالعمل‌های مربوط به آن را از www.trustedsec.com/socialengineer-toolkit دریافت کنید.

اینتل‌تکنیکس (IntelTechniques)

این مورد «ابزار» نیست و در واقع مجموعه‌ای فوق‌العاده از موتورهای جست‌وجوست که دوست خوبم مایکل بزل جمع‌آوری کرده است.

مایکل در چند زمینه متخصص است، اما در دو زمینه واقعاً استادی بی‌بدیل است: یکی پیدا کردن افراد در اینترنت و دیگری پنهان شدن از افرادی که در اینترنت دنبال شما می‌گردند. مایکل زمانی به من گفت برای خرید از آمازون بهتر است شرکتی صوری در مکزیک تأسیس کنم تا بتوانم کارت‌های اعتباری‌ای بگیرم که ارتباطی با من نداشته باشند.

مایکل مجموعه‌ای فوق‌العاده از ابزارها را ایجاد کرده که می‌توانند شبکه‌های اجتماعی، شماره‌های تلفن و آدرس‌های آی‌پی را جست‌وجو کنند و حتی جست‌وجوی معکوس تصویر را انجام دهند.

این ابزارها را می‌توانید در https://inteltechniques.com/menu.html ببینید و توصیه می‌کنم زمانی قابل‌توجه را صرف بررسی این سایت کنید.

فوکا

فوکا مخفف «انگشت‌نگاری سازمان‌ها با آرشیوهای گردآوری‌شده» (Fingerprinting Organizations with Collected Archives) است. در سال ۲۰۱۰، گروهی کوچک از هکرهای برزیلی با عرضه این ابزار به‌سرعت توجه کاربران اینترنت را به خود جلب کردند.

تا امروز هیچ ابزاری شبیه فوکا عرضه نشده است. ابزاری اختصاصی برای ویندوز است که در طول سال‌ها فرازونشیب‌های زیادی داشته است. زمانی آن را کنار گذاشتم زیرا از آخرین به‌روزرسانی‌اش چند وقت می‌گذشت و هیچ راهی برای تماس با سازندگانش وجود نداشت (و در ضمن منبع‌باز هم نبود).

بعد شرکت «ایلون‌پث» (ElevenPaths) مسئولیت این پروژه را بر عهده گرفت، فوکا را به‌روز و در وب‌سایتش https://www.elevenpaths.com/labstools/foca/index.html منتشر کرد. متأسفانه فوکا همچنان فقط نسخه ویندوز دارد، اما اگر از ویندوز استفاده نمی‌کنید، می‌ارزد که برای استفاده از این ابزار سرور مجازی

راه‌اندازی کنید.

سرعت دریافت فایل‌ها و استخراج فراداده از آن‌ها در فوکا حیرت‌انگیز است. امتحانش کنید.

مالتیگو: بابابزرگ همه این ابزارها

با پذیرش این ریسک که این تصور در شما ایجاد شود که من تبلیغات‌چی مالتیگو هستم، می‌گویم عاشق این ابزارم. واقعاً عاشقش هستم. شرکت «پاتروا» (Paterva)، سازنده مالتیگو، کاری واقعاً کم‌نظیر انجام می‌دهد؛ ابزاری فوق‌العاده ساخته، نسخه رایگان کوچک‌تری عرضه کرده (که واقعاً عالی است) و نسخه تجاری را هم مدام به‌روز می‌کند. بنابراین همواره در حال پیشرفت و بسیار کاربردی است.

احتمالاً می‌پرسید مالتیگو چیست. ابزاری است که به شما کمک می‌کند داده‌ها را از منابع آنلاین جمع‌آوری کنید و سپس برای نمایش این داده‌ها نموداری تعاملی به شما می‌دهد. می‌تواند به شما کمک کند منابع عمومی اطلاعات را فهرست‌بندی و شناسایی کنید، درموردشان تحقیق و با آن‌ها ارتباط برقرار کنید.

مالتیگو کارم را بسیار آسان‌تر می‌کند و استفاده از آن راحت و سرگرم‌کننده است. به‌علاوه، پاتروا ویدئوها و دوره‌های آموزشی بسیار مفیدی دارد. در نهایت اینکه مالتیگو برای همه پلتفرم‌ها در دسترس است. می‌توانید آن را از وب‌سایت پاتروا در www.paterva.com/web7/downloads.php#tab-2 دانلود کنید. توصیه می‌کنم با نسخه «مالتیگو کلاسیک» (Maltego Classic) شروع کنید.

خلاصه

بدون شک دانش قدرت است و احتمالاً هیچ منبع دانشی بهتر از اطلاعات منبع‌باز درمورد هدف‌های‌تان وجود ندارد. اگر از اصول این فصل پیروی و تمرین کنید و این مهارت‌ها را بهبود ببخشید می‌توانید در این زمینه استاد شوید و کوچک‌ترین جزئیات پنهان‌شده در اینترنت را پیدا کنید.

کار جمع‌آوری اطلاعات منبع‌باز را تمام کرده‌اید. همه قطعات اطلاعات را فهرست‌بندی، جمع‌آوری و مستند کرده و به این نتیجه رسیده‌اید که قطعه اطلاعاتی

مناسب شیوه حمله‌تان را پیدا کرده‌اید و باید آماده‌سازی بهانه (pretext) را شروع کنید. تحلیل داده‌های جمع‌آوری‌شده و جست‌وجوی نشانه‌های کلیدی درباره سبک ارتباط سوژه چطور به شما کمک می‌کند؟ این موضوع فصل بعدی است.

هیچ‌کس هیچ‌چیز هنوز

کوین میتنیک، یکی از مشـهورترین مهندسان اجتماعی جهان، عبارت «مهندسـی اجتماعی» را ابداع کرد. او می‌گوید فریب دادن آدم‌ها برای اینکه خودشان رمز عبور سیستم‌شان را به شما بدهند راحت‌تر از تلاش برای هکِ سیستم آنهاست.

مهندسی اجتماعی ابزاری مثل چکش، بیل، چاقو یا حتی اسلحه است. هرکدام از این ابزارها برای هدفی ساخته شده‌اند و می‌توان از آن‌ها برای ساختن، نجات دادن، تغذیه یا بقا استفاده کرد، در عین حال هم برای آسیب زدن، کشتن، خراب و نابود کردن. برای درک اینکه چطور می‌توان از مهندسی اجتماعی برای ساختن، تغذیه و بقا یا نجات استفاده کنید، باید هر دو نوع استفاده را یاد بگیرید. صحت این گفته زمانی مشخص می‌شـود که هدف‌تان دفاع کردن باشـد. برای محافظـت از خودتان و دیگران در برابر استفاده مخرب از مهندسـی اجتماعی، ابتدا باید سویه تاریک آن را بشناسید تا تصویری روشن از نحوه بهره‌مندی از آن به دست بیاورید.

چند دهه بیشتر از عمر هک کردن نمی‌گذرد، اما قدمت هک کردن انسان به ابتدای خلقت بازمی‌گردد. این کتاب می‌تواند آماده‌تان کند، از شـما محافظت کند و به شما آموزش بدهد چطور خطرهای ناشی از مهندسی اجتماعی را شناسایی کنید، آثارشان را کاهش دهید و از خودتان در برابر این خطرات دفاع کنید. این کتاب روش‌های مختلفی را برای فریب دادن قربانی‌های بی‌دفاع برمی‌شمرد و از سوی دیگر روش‌هایی را برای خنثی کردن تهدیدهای مهندسی اجتماعی می‌آموزد.

WILEY

ناشـر اصلی کتـاب مهندسـی اجتماعی انتشـارات وایلی است

ISBN 978-622-7702-19-4

۹۰۰ هـزار تومـان

انتشارات راه پرداخت

ناشر فناوری و نوآوری

way2pay.press