نقش مهندسی اجتماعی در امنیت سایبری

هک کردن سیستم عامل انسانی

پیشرفت‌های فناورانه اخیر، به‌واسطه افزایش استفاده و وابستگی مردم به اینترنت روزبه‌روز کامل‌تر شده‌اند، امکانات و فرصت‌های جدید و نامحدودی را در اختیار کاربران قرار داده است. پیشرفت‌هایی که می‌توانند به‌عنوان ابزاری برای انجام طیفی از جرائم اینترنتی به کار گرفته شوند. جرائمی که با بهره‌گیری و بهبود کیفی اینترنت متصل به دستگاه‌های آسیب‌پذیر و فریب کاربران فرصت دسترسی به اطلاعات حساس و محرمانه را فراهم می‌کنند. نفوذ رو به رشد اینترنت در کنار ظهور فناوری‌های جدیدی از قبیل اینترنت اشیا علاوه بر اینکه رفتارهای آنلاین مردم را تغییر داده است، مسیری جدید پیش روی حملات سایبری قرار داده است. بنا بر گزارش سازمان اروپایی ارزیابی جرائم اینترنتی، تکنیک‌های مهندسی اجتماعی یکی از کلیدی‌ترین راه‌های مورد توجه مجرمانی از این دست است.

در حال حاضر، مجرمان سایبری برای رسیدن به مقاصد خود لزوماً نیازی به دانش پایه‌ای انجام این کار ندارند. بعضی از ابزارهای مخرب به‌راحتی و از طریق ارسال یک ایمیل به کار گرفته می‌شوند و تعداد قابل توجهی از کاربران را تحت تأثیر قرار می‌دهند؛ در چنین مواردی آلوده کردن کامپیوترهای قربانیان بیش از هر چیز به‌واسطه دست‌کاری روانی میسر می‌شود. این شیوه‌های روانی به‌سادگی و راحتی قربانیان را به کلیک کردن روی پیوست ایمیل‌ها قانع می‌کند.

در حال حاضر استفاده از تکنیک‌های مهندسی اجتماعی به یکی از ابزارهای رایج در حمله مهاجمان سایبری بدل شده است، شیوه‌ای که دست‌یابی به اطلاعات حساس و طبقه‌بندی‌شده رقبا، دولت و سایرین را امکان‌پذیر می‌کند. یکی از روندهای اخیری که در حمله‌های سایبری به وجود آمده است، هدف قرار دادن ذات خود حمله است: مجرمان با استفاده از شیوه‌های پیچیده، مناسب و اغلب از طریق ایمیل‌های فیشینگ به مقصد موردنظر نفوذ می‌کنند. یکی دیگر از نمونه‌های

به‌کارگیری این شیوه whaling است، روشی که مجرمان برای نفوذ به پروفایل شخصی افراد خاصی از برخی گروه‌ها انتخاب می‌کنند. درحالی‌که بعضی گروه‌های سازمان‌یافته ممکن است در مقیاسی بزرگ و از طریق ارسال طعمه و پذیرش آن از جانب قربانی موردحمله یا کلاه‌برداری سایبری قرار بگیرند. برخی هم از روش‌های پیچیده‌تر تهاجم سایبری بهره می‌گیرند و بدین واسطه به سازمان، نهاد دولتی یا مؤسسه مالی موردنظرشان نزدیک می‌شوند. متخاصمان به‌صورتی هدفمند اطلاعاتی در مورد اهداف خود به دست می‌آورند و از این راه برنامه طراحی‌شده خود برای دست‌کاری و دسترسی به اطلاعات حساس را اجرا می‌کنند.

با توجه به ظهور بی‌اندازه جعل و تقلب سایبری در سال‌های اخیر، پیگیری اثرات مخرب و تأثیرات مالی چنین حمله‌هایی به توجه هر دو بخش خصوص و عمومی در کنار سایر اعضای یک اجتماع نیاز دارد. ازآنجایی که این روزها شاهد افزایش تأثیرگذاری این تکنیک‌های جعلی هستیم و با توجه به این واقعیت که انسان ضعیف‌ترین حلقه امنیت سیستم است نگاهی کوتاه به شیوه‌هایی که می‌تواند کاربـــران را تحت تأثیر قرار دهد می‌اندازیم.

در حال حاضر ما با تعداد گسترده‌ای فیشینگ، حفره در وب‌سایت‌ها، پیام کوتاه متنی (smishing)، آی‌پی تلفن همراه یا سایر وسایل مواجه هستیم. ابزارهایی که امکان حمله برای مهاجم بدون دانش پایه‌ای خاص را فراهم می‌کند. درواقع، اگر جرم را به‌عنوان یک الگوی خدماتی در نظر بگیریم، به این نتیجه می‌رسیم که اشاعه استفاده از این الگو در اقتصاد جرائم سایبری تبهکاری را به پدیده‌ای آسان و قابل‌دسترس بدل کرده است. افزایش تعداد حمله‌های سایبری در سال ۲۰۱۴ گواهی بر این مدعاست. به‌عنوان نمونه، در اروپا شاهد افزایش تعداد قربانیانی هستیم که فیشینگ به سازمان آن‌ها ضربه زده است. اتفاقی که در میان افراد یا شرکت‌های قدیمی و ناآشنا با تهدیدهای اینترنتی رواج بیشتری دارد.

از منظر قانونی، مبارزه با تکنیک‌های مهندسی اجتماعی به دلیل درگیر کردن چندین بخش از سیستم قضایی و بهره گرفتن از فناوری‌های ردیاب یک چالش بزرگ به‌حساب می‌آیند. بااین‌حال، در سیستم قانونی اروپا موفق شده‌اند راهکارهایی برای مبارزه گروه‌های جرائم اینترنتی و تکنیک‌های به‌کاررفته توسط آن‌ها دست یابند. سیستمی که توسط کشورهای بلژیک و آلمان طرح‌ریزی و از جانب اتحادیه‌های قضایی اروپایی حمایت می‌شود. در کنار حمایت‌های قانونی، همکاری بخش خصوصی با سیستم‌های قضایی ابزاری است در جهت کاهش جرائم اینترنتی که از طریق مهندسی اجتماعی رخ می‌دهند. اولین پله این همکاری شناخت درست و کافی بخش خصوصی از اتفاقات در حال جریان محیط پیرامونشان است. از همین رو، تلاش شـــده است در این گزارش نگاهی اجمالی به چیستی و چگونگی مهندسی اجتماعی شود تا افراد حقیقی و حقوقی بتوانند بینش جامع‌تری نسبت به تهدیدهای سایبری با عاملی انسانی پیدا کنند.

مرکز جرائم اینترنتی اروپا

شیوع استفاده از مهندسی اجتماعی در بسیاری از جوامع نشان از ضعفی ذاتی در این سیستم‌ها دارد؛ این نقطه‌ضعف بیش از هر چیز به عدم توانایی قربانی در تشخیص ارتباطات مخرب بازمی‌گردد


FedEx
FedEx Billing Online - Ready for Payment
fedex.com

Hello
You have a new not paid invoice(s) from FedEx that is ready for payment.

The following ivoice(s) are to be paid now :

Invoice Number
8957-31879

To pay or review these invoices, please sign in to your FedEx Billing Online account by clicking on this link: http://www.fedex.com/us/accountfbo

Note: Please do not use this email to submit payment. This email may not be used as a remittance notice. To pay your invoices, please visit FedEx Billing Online, http://www.fedex.com/us/accountfbo

Thank you,
Revenue Services
FedEx

مقدمه

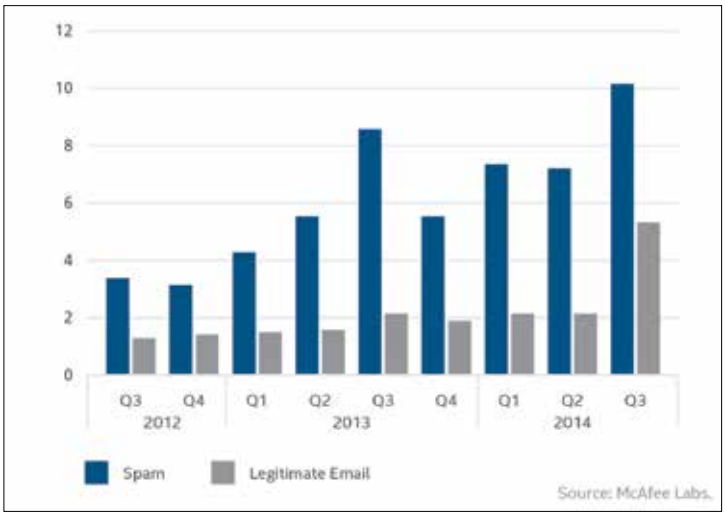
در جولای ۲۰۱۴، بیش از هزار شرکت انرژی در امریکای شمالی و اروپا از اینکه موردحمله سایبری قرار گرفتند خبر دادند. در مقایسه با دیگر انواع حملات (مانند حمله تروی، های رولر و اژدهای شب) این روش صورتی متفاوت در روش‌های حمله به خود می‌گیرد. بااین‌حال، یک پیش‌زمینه مشترک در میان تمامی روش‌های مهندسی اجتماعی وجود دارد. چه هدف حمله مشتریان باشد چه یک شرکت بزرگ، شیوه‌ای که برای اغلب جرائم سایبری به کار گرفته می‌شود شکلی از مهندسی اجتماعی است؛ در این شیوه قربانی مجبور به انجام کاری می‌شود که نفوذ و آلوده کردن سیستم را آسان می‌کند.

شیوع استفاده از مهندسی اجتماعی در بسیاری از جوامع نشان از ضعفی ذاتی در این سیستم‌ها دارد؛ این نقطه‌ضعف بیش از هر چیز به عدم توانایی قربانی در تشخیص ارتباطات مخرب بازمی‌گردد. هرچند نباید فراموش کرد که مجرمان نیز از راه‌هایی به‌شدت پیچیده جهت دور زدن سیستم‌های امنیتی استفاده می‌کنند. گرچه گزارش‌های بشماری از رفتارهای ناسالم کاربران وجود دارد، اما اینکه قربانی را مقصر اصلی بدانیم بی‌انصافی است. زیرا مجرمان به حدی زیرک و باهوش هستند که شناخت روش‌های به کار گرفته توسط آن‌ها دشوار و گاهی غیرممکن است. درواقع، مهاجمان تلاش می‌کنند از ناهشیاری اهداف خود سوءاستفاده و سیستم او را دست‌کاری کنند.

این گزارش هم‌چنین به‌مرور مفهوم مهندسی اجتماعی می‌پردازد. تلاش می‌شود در مجالی اندک آخرین تکنیک‌های به کار گرفته توسط مهاجمان، تأثیرات آن‌ها بر قربانی‌ها، کانال‌های ارتباطی، راه‌های کنترلی و شیوه‌های کاهش خطرات معرفی شود.

تعریف مهندسی اجتماعی

تعاریف مختلفی برای اصطلاح مهندسی اجتماعی بیان‌شده است. این تعاریف از طرح‌ریزی یک برنامه اقناعی با هدف جلب رضایت قربانی برای انتشار و در اختیار گذاشتن اطلاعات از طریق



وارونه جلوه دادن واقعیت تا به‌کارگیری روشی با قدرت تأثیرگذاری در سطحی وسیع را شامل می‌شود. در اینجا با توجه سرفصل‌های در نظر گرفته‌شده تنها به بیان عناصر کلیدی که در سایر مغفول مانده‌اند می‌پردازیم.

برنامه‌ای کاربردی که به‌صورتی عامدانه با استفاده از روش‌های فریب آمیز به دست‌کاری سیستم‌های اطلاعاتی می‌پردازد؛ این دست‌کاری‌ها نتیجه‌ای جز افشای اطلاعات ندارد.

در حین حمله مهندسی اجتماعی، قربانی از اینکه چه کارهای مخاطره‌آمیزی انجام می‌دهد آگاهی ندارد. مهندسی اجتماعی به‌صورتی غریزی تنها قربانیان بی‌خبر و بی‌گناه را هدف می‌گیرد. مهاجمان راه‌های مختلفی برای کلک زدن به قربانی به کار می‌گیرند، این راه‌ها قربانی را به افشای اطلاعات یا کلیک کردن روی یک لینک خطرناک ترغیب می‌کند. در مهندسی اجتماعی مهاجمان با طفره‌روی‌های مختلف هدف را بدون اینکه متوجه شود وادار به افشای اطلاعات می‌کنند. در مقابل آنچه گفته شد برخی روش‌ها مانند: رشوه‌خواری یا تهدید به خشونت به‌صورت مستقیم منجر به سرقت اطلاعات می‌شوند.

حمله در مهندسی اجتماعی می‌تواند هدفمند یا فرصت‌طلبانه باشد. حملات معطوف به هدف، غالباً روی افراد خاصی تمرکز می‌کنند، درحالی‌که حملات فرصت‌طلبانه با هدف جمع‌آوری اطلاعات از منابع مختلف در یک موقعیت خاص انجام می‌شوند.

تعریف حمله مهندسی اجتماعی

دسته‌بندی‌های مهندسی اجتماعی

حملات در مهندسی اجتماعی می‌تواند به دو دسته تقسیم شود: شکار و کشت.

- در شکار هدف استخراج اطلاعات با استفاده از تعامل محدود است. در این رویکرد به‌صورت معمول تنها یک هدف و مهاجم نقش‌آفرینی می‌کنند و ارتباط میان آن‌ها معطوف به دوره‌ای خاص و برای رسیدن به اطلاعاتی مشخص است.
- در حمله کشت، مقصود بنا نهادن ارتباط وسیع‌تر با هدف و استمرار این ارتباط به‌منظور دسترسی به اطلاعات در طولانی‌مدت است.

با گذشت زمان، رابطه میان هدف و مهندس اجتماعی ممکن است تغییر کند. به‌عنوان‌مثال: هدف ممکن است از حمله بو ببرد و درخواست پاداش بکند یا احتمال دارد مهندس اجتماعی از Blackmail استفاده کند. بنابراین، تغییر جهت از مهندسی اجتماعی به سمت رفتارهای مجرمانه اتفاقی محتمل در این نوع حمله‌ها است.

مثال‌هایی از شکار

مثال زیر نمونه‌ای ایمیلی است از جانب FedEx، این ایمیل با هدف اقناع قربانی برای کلیک روی لینک ارسال‌شده است. در اینجا به‌خوبی یک ارتباط محدود مرسوم در حمله شکار به نمایش گذاشته می‌شود.

ایمیل یک شاخصه مهم در حملات مهندسی اجتماعی است. گزارش سال ۲۰۱۴ McAfee که با هدف بررسی جهانی ایمیل‌های اسپم انجام شد نشان داد» حدود دوسوم ایمیل‌های جهانی ازاین‌دست هستند.

اسپم جهانی و حجم ایمیل
(هزاران میلیارد پیام)

- اسپم
- ایمیل‌های معتبر

در مهندسی اجتماعی مهاجمان با طفره‌روی‌های مختلف هدف را بدون اینکه متوجه شود وادار به افشای اطلاعات می‌کنند. در مقابل آنچه گفته شد برخی روش‌ها مانند: رشوه‌خواری یا تهدید به خشونت به‌صورت مستقیم منجر به سرقت اطلاعات می‌شوند

اگرچه تمامی ایمیل‌های ناخواسته با هدف استخراج اطلاعات ارسال نمی‌شوند، بااین‌حال هیچ شکی نیست که ایمیل‌ها یک ابزار مهم در مهندسی اجتماعی هستند. همان‌گونه که در تصویر زیر مشاهده می‌شود، این تلاش‌ها اغلب در دسته حمله‌های شکار جای می‌گیرند.

نمونه ذکرشده نشان می‌دهد، چگونه مهاجمان از طریق جعل هویتی مشروع، قربانی را به باز کردن پیوست‌های ارسالی قانع می‌کنند. در این مثال، تعاملی محدود اما مستقیم میان قربانی و مهاجم دیده می‌شود که به‌احتمال‌قوی پس از رسیدن به هدف موردنظر منتفی می‌شود.

مثالی از کشت

مثال‌های زیر نشان می‌دهد، چگونه حمله کشت در اجرای قانون مخفی مورداستفاده قرار گرفت. عملیاتی که در آن عامل FBI نقش مدیر وب‌سایت DarkMarket را ایفا می‌کرد.

DarkMarket که این روزها به‌عنوان یک وب‌سایت مزایده اینترنتی شناخته می‌شود، همچون eBay محملی است که سارقان هویت می‌توانند در آن به خریدوفروش بی‌نهایت کارت اعتباری، هویت آنلاین و ابزارهایی که کارت اعتباری جعلی درست می‌کنند بپردازند. در اواخر ۲۰۰۶، نماینده ویژه FBI، به‌نوعی مدیریت این وب‌سایت را در دست گرفت. این نماینده نه‌تنها کنترل اطلاعات تکنیکی موجود را تحت کنترل داشت، بلکه از قدرت شکستن هویت سارقان یا حتی استفاده از آن‌ها به‌واسطه دسترسی به بخش مدیریتی وب‌سایت نیز بهره‌مند بود.

همان‌گونه که این نمونه نشان می‌دهد، مهندسی اجتماعی بدون پهن کردن دامی زیرکانه برای قربانی امکان‌پذیر نیست. برخلاف حمله شکار، تعامل میان افراد در ارتباط کشت در طول زمان بیشتر می‌شود. البته نباید فراموش کرد حمله کشت در مهندسی اجتماعی چندان رایج نیست. تفاوت اساسی میان شکار و حمله در کمیت تعامل میان مهندس اجتماعی و هدف است. شکار با هدف کسب اطلاعات از یک ارتباط واحد صورت می‌گیرد، درحالی‌که کشت از تعاملات در حال جریان و پیش‌رونده بهره می‌جوید.

چرخه عمر حمله مهندسی اجتماعی

حمله مهندسی اجتماعی از هر نوعی که باشد عموماً شامل چهار مرحله می‌شود، در این میان مرحله اول که تحقیق است انتخابی است؛ به این دلیل که حمله مهندسی اجتماعی بیش از آنکه هدفمند و برنامه‌ریزی‌شده باشد به‌صورت

تصادفی اتفاق می‌افتد.

چرخه عمر مهندسی اجتماعی

- نزدیک شدن
- فهمیدن
- تنظیم
- استخراج

۱- تحقیقات (انتخابی)

با هدف فهم کافی در راستای برنامه‌ریزی برای یک تله هوشمندانه انجام می‌شود.

- اطلاعات پیش‌زمینه‌ای در مورد افراد یا سازمان کسب کنید.
- بهترین فرد را برای موردحمله قرار دادن انتخاب کنید.
- برای مشارکت با هدف برنامه مشخص داشته باشید، تا بتوانید اهرم‌های در دسترس او را شناسایی کنید.

۲- تله

با هدف تنظیم امور برای یک ایفای نقش موفق انجام می‌شود.

- تعامل با هدف
- داستان‌سرایی
- ایجاد سطحی از صمیمیت
- کنترل بر تعامل شکل گرفته

۳- بازی

با هدف استخراج اطلاعات و حفظ ارتباط در طولانی‌مدت انجام می‌شود.

- حفظ معماگونگی داستان
- افزایش کنترل بر رابطه
- استخراج اطلاعات

۴- خروج

با هدف تعامل نزدیک انجام می‌شود. در حالت ایده آل، بدون برانگیختن سوءظن.

- معمای طرح‌شده به طبیعی‌ترین شکل ممکن به پایان می‌رساند.
- یک دلیل منطقی برای خارج شدن از این تعامل در نظر بگیرد.
- نشانی‌های به‌جامانده را مخفی کنید.

مهندسی اجتماعی ممکن است تنها بخش کوچکی از یک برنامه دست‌یابی به اطلاعات باشد. به‌عنوان‌مثال، مهاجم ممکن است تنها یک حمله شکار داشته باشد، اطلاعات را استخراج کند و سپس ناپدید شود. یا احتمال دارد مهاجم حملات متعددی

یک حمله مهندسی اجتماعی ممکن است تنها یک تلفن کوتاه، ایمیل یا پیام مستقیم باشد (روش شکار)، یا ممکن است حمله‌ای طولانی‌مدت همراه با تعاملات پیچیده و چندوجهی باشد

داشته باشد و با اطلاعات جمع‌آوری‌شده پایه‌های یک حمله کشت را ایجاد کند. اگرچه، حملات مهندسی اجتماعی اغلب به‌صورت خطی دیده می‌شوند؛ اما یک حمله ممکن است منجر به حمله دیگری شود، ازاین‌رو چرخه عمر مهندسی اجتماعی چهار مرحله دارد. یک نمونه از این چرخه را می‌توان در حمله اخیر Operation Dragonfly مشاهده کرد:

این واقعیت که Dragonfly اطلاعاتی در مورد سرور OPC و اتصالات VPN به PLCs جمع‌آوری می‌کند ممکن است اثباتی بر این مدعا باشد که هدف نهایی دسترسی به PLCs است. این موضوع قدرت تغییر، آسیب یا اختلال در فرایندهای حیاتی و اجرایی سازمان هدف را به مهاجم می‌دهد.

هرچند Operation Dragonfly از مهندسی اجتماعی (شکار در شکل فیشینگ‌های گسترده) استفاده کرد، اما این تنها می‌تواند مقدمه‌ای برای حمله‌ای وسیع با هدف تحت تأثیر قرار دادن کل یک سیستم باشد. هیچ الگوی زمانی مشخصی برای مراحل یادشده وجود ندارد. یک حمله مهندسی اجتماعی ممکن است تنها یک تلفن کوتاه، ایمیل یا پیام مستقیم باشد (روش شکار)، یا ممکن است حمله‌ای طولانی‌مدت همراه با تعاملات پیچیده و چندوجهی باشد.

مرحله۱: تحقیق

مقصود اصلی از مرحله تحقیق شناسایی پتانسیل ذاتی برای طرح‌ریزی یک دام یا جمع‌آوری اطلاعات است، مهاجم در این مرحله می‌تواند از طریق پی بردن به اشتباهات شخص یا سازمان زمینه اولیه آغاز یک رابطه مؤثر را فراهم کند. یک مهندس اجتماعی می‌تواند از منابع مختلفی برای تحقیق استفاده کند:

- اطلاعات آنلاین:

وب‌سایت‌های مشارکتی، پروفایل‌های شبکه‌های اجتماعی، جست‌وجو در اینترنت و ...

- مستندات عمومی

اطلاعاتی در مورد گزینشگران، میزان بازدهی شرکت و ...

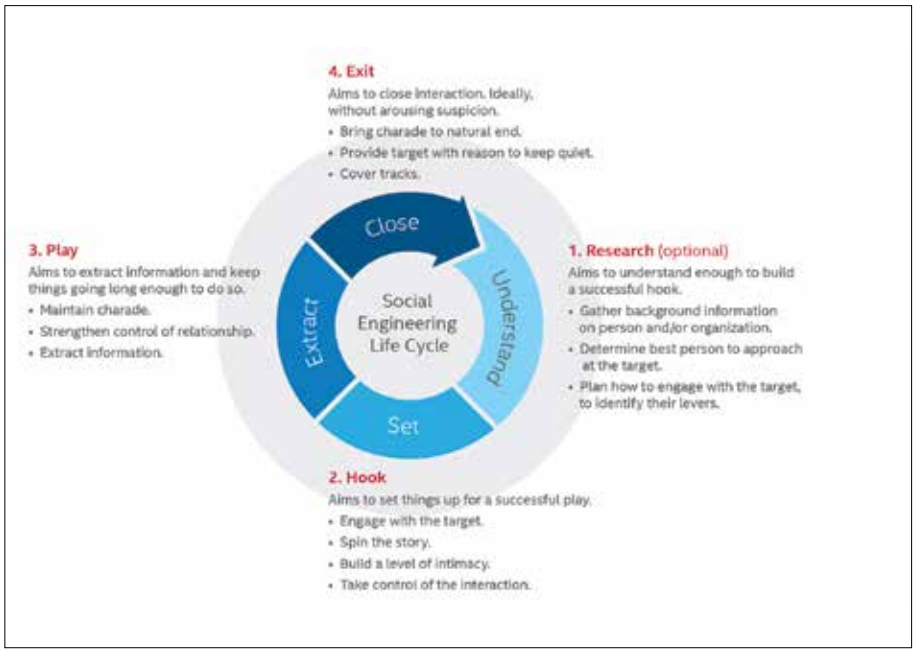
- تعامل فیزیکی

ارتباط اجتماعی با هدف در نظر گرفته‌شده، همکاران یا دوستان.

هم‌زمان با ظهور اینترنت، قابلیت انجام تحقیقات خودکار، ساده و کم‌هزینه افزایش‌یافته است. گاهی اوقات، مهندسی اجتماعی حمله‌ای فرصت‌طلبانه را تدارک می‌بیند که به‌هیچ‌وجه در طول تحقیقات نامی از آن برده نشده است. به‌عنوان‌مثال: تحقیق در مورد افراد اگر قصد استفاده گسترده از ایمیل‌های فیشینگ داشته باشیم ممکن است غیرضروری باشد. استفاده از یک نام تجاری معروف با پیام‌های عمومی به‌اندازه کافی می‌تواند بر دریافت‌کنندگان بی‌خبر و ناآگاه اثرگذار باشد.

مرحله۲: دام

هدف از یک تله موفقیت در بازی است. در اینجا مهاجم ضمن زیر نظر گرفتن اهداف به تهیه یک پیش متن به‌منظور افزایش سطح تعامل مشغول می‌شود. مهندسان اجتماعی تلاش خواهند کرد از توانایی‌های اثرگذاری‌شان در این مرحله استفاده کنند. روان‌شناسان ۶ مرحله برای تأثیرگذاری



عمیق بر دیگران مطرح می‌کنند، مراحلی که با هدف نشانه رفتن بخش ناخودآگاه ذهن افراد طی می‌شوند.

این فرایندهای اثرگذاری برای اهداف مختلفی، ازجمله: فروش، اقناع (تلاش برای گرفتن پول از مردم) و مهندسی اجتماعی استفاده می‌شوند. در بعضی از مثال‌های آورده شده اگرچه هدف دست‌یابی به اطلاعات نبوده است ولی از تئوری سطوح تأثیرگذاری بهره برده‌اند.

• **عمل متقابل:** زمانی که مردم ارائه‌دهنده خدمتی هستند در مقابل آن چیز احساس وظیفه می‌کنند و در تلاش هستند تا به‌نوعی تعهد خود را نسبت به آنچه عرضه می‌کنند نشان دهند.

به‌عنوان‌مثال: کارمندی با تلفنی از جانب شخصی که خودش را با عنوان یکی از اعضای بخش فناوری اطلاعات معرفی می‌کند مواجه می‌شود. تماس‌گیرنده این‌چنین توضیح می‌دهد که بعضی از کامپیوترهای مجموعه به‌وسیله برخی ویروس‌های جدید که آنتی‌ویروس قادر به شناسایی آن‌ها نیست آلوده‌شده‌اند، ویروس‌هایی که آسیب جدی به فایل‌های موجود در کامپیوتر وارد کرده‌اند. این شخص تقاضا دارد با فردی صحبت کند که در چند گام بتواند از بروز برخی مشکلات جلوگیری کند. پس‌ازاین، تماس‌گیرنده از فرد پشت خط می‌خواهد بار دیگر کاربری نرم‌افزار را که به‌تازگی و به‌منظور تغییر رمز عبور به‌روزرسانی شده است آزمایش کند. در چنین شرایطی، کارمند به‌سختی این درخواست را رد می‌کند، به دلیل اینکه تماس‌گیرنده به دنبال راهی است تا بتواند در مقابل ویروس‌ها از خودش محافظت کند. بنابراین او عملی مطابق با خواست تماس‌گیرنده انجام می‌دهد.

در حال حاضر، شبکه‌های اجتماعی همچون: لینکدین و توییتر برای افزایش شمار کاربران و دنبال کنندگانش از اهرم‌های عمل متقابل استفاده می‌کنند.

• **کمبود:** تمایل مردم به موافقت کردن با امری هنگام احساس کمبود و فقدان بیشتر می‌شود. به‌عنوان‌مثال: در یک ایمیل جعلی ادعا می‌شود که متن پیش رو از جانب بانک امریکا ارسال‌شده است. این ایمیل شامل لوگو بانک است که به دریافت‌کننده می‌گوید: اطلاعات حسابش را از همین طریق ارسال کند. علاوه بر این، در متن ایمیل ذکر می‌شود که در صورت عدم توجه به آنچه گفته‌شده است حساب به‌سرعت غیرفعال می‌شود.

استفاده از حربه کمبود یک شیوه رایج میان مهاجمانی است که از کانال‌های دیجیتال استفاده می‌کنند. نمونه این شیوه در ایمیل زیر به‌خوبی مشخص است

• **ثبات:** هنگامی که اهداف متعهد به انجام کاری می‌شوند، غالباً برای اینکه در نظر دیگران غیرقابل‌اعتماد جلوه نکنند پیگیر آنچه متعهد شده‌اند هستند.

به‌عنوان‌مثال: در اغلب اوقات مهاجم تلاش می‌کند با کارکنان جدید ارتباط برقرار کند و پایداری به سیاست‌های امنیتی و فرایندی را به‌عنوان شرط استفاده از اطلاعات سیستم مطرح کند. پس از بحث پیرامون برخی شیوه‌های امنیتی، تماس‌گیرنده از کاربر می‌خواهد که رمز عبورش را به‌منظور بررسی انطباق یا عدم انطباق باسیاست‌هایی که حدس زدن رمز عبور را دشوار می‌کند در اختیار او قرار دهد. اگر یک‌بار کارمندی رمز عبور خودش را افشا کند، درواقع این فرصت را در اختیار مهاجم قرار می‌دهد که بر مبنای همان ساختار رمزهای عبور آینده او را حدس بزند. درواقع، کارمند در اینجا قربانی تعهد ابتدایی می‌شود که در راستای پایداری به سیاست‌های شرکت ملزم به رعایت آن شده است.

• **علاقه:** احتمال موافقت اهداف انتخابی با مهندس اجتماعی زمانی بیشتر می‌شود که فرد مهاجم مورد علاقه و توجه آن‌ها باشد.

به‌عنوان‌مثال: برنارد مدوف، یکی از بزرگ‌ترین بازرگانان آمریکایی، با تکیه‌بر اعتبار، شهرت، جذابیت، اعتمادبه‌نفس خدشه‌ناپذیر و تصویر بدون ایرادی که از خودش به نمایش گذاشته بود توانست بزرگ‌ترین طرح معاملات هرمی دنیا را اجرایی کند و چیزی حدود ۵۰ بیلیون دلار از این طرح به دست بیاورد. معروف است که همه امریکا آرزو دارند در هواپیما کنار مدوف بنشینند.

• **اقتدار:** احتمال موافقت مردم با درخواستی زمانی که در قالب یکی از اشکال قدرت مطرح شود افزایش می‌یابد.

به‌عنوان‌مثال: در یکی از آخرین گزارش‌های ارائه‌شده جزئیات یک شیوه کلاهبرداری جدید به نام «AIG» مطرح‌شده است. در این روش کلاهبرداران خود را به‌عنوان یکی از اعضای مهم سازمان یا مجموعه معرفی (رئیس شرکت، مدیرعامل اجرایی یا مدیر ارشد مالی) و تلاش می‌کنند با یکی از کارمندانی که احتمال می‌دهند از قدرت اجرایی کردن درخواست‌های محرمانه و فوری برخوردار است تماس برقرار کنند. این عملیات می‌تواند به‌واسطه ایمیل انجام شود، ایمیلی جعلی و با آدرسی ویژه و طراحی حرفه‌ای که امکان تشخیص تقلبی بودن آن بسیار سخت است.

برای ایمیل‌های فیشینگ‌های معمولی، اغلب از تکنیک‌های اقتدار مرسوم استفاده می‌شود؛ ارسال ایمیل‌هایی ازاین‌دست تحت عنوان یک مجموعه بانکی نیز یکی از اتفاقات رایج است. علاوه بر این، اغلب از نام برندهای معروف برای ارسال ایمیل‌های تقلبی استفاده می‌شود. نتایج آخرین تست فیشینگ انجام‌شده در شرکت مکافی نشان داده است: نمونه ایمیل فیشینگ‌های موفق از جانب UPS ارسال می‌شوند. این روش از تغییر وجهه و چهره علی‌رغم مشترک و معمول بودن

قابلیت تأثیرگذاری بالایی دارد. بر همین اساس توصیه می‌شود، تمامی ایمیل‌هایی که با دامنه UPS.com فرستاده می‌شوند جدی گرفته شوند و از باز کردن پیوست ایمیل‌هایی با دامنه این‌چنینی به‌شدت پرهیز شود؛ به‌احتمال‌زیاد تمامی این ایمیل‌ها از طرف یک کلاهبردار ارسال‌شده‌اند.

• **اعتبار اجتماعی:** زمانی که کاری توسط جمع کثیری انجام شود گونه‌ای اعتبار اجتماعی پیدا می‌کند؛ همین اصل احتمال پیوستن به گروه انجام دهنده این کار را افزایش می‌دهد.

برای مثال: شما با ایمیلی مواجه می‌شوید که نه‌تنها برای شخص شما، بلکه برای تعداد زیادی از افراد آشنا و همکار نیز فرستاده‌شده است. اما این ایمیل نباید شما را به اشتباه بیندازد؛ چون یک سارق اینترنتی با هک کردن ایمیل شما به لیست آدرس ایمیل‌های دسترسی پیدا کرده است. در این مثال، دیدن اسامی آشنا در نوار دریافت‌کنندگان این حس خوب را به شما می‌دهد که می‌توانید با خیالی آسوده ایمیل جدید، هر لینک و پیوست‌های آن را باز کنید. فرایندی که از آن به‌عنوان قدرت نفوذ اعتبار اجتماعی یاد می‌شود و یکی از عناصر اصلی اقتدار است.


RBS
The Royal Bank of Scotland
Make it happen
Digital Banking

Dear Valued Customer,
Due to the recent amount of fraudlent messages that targeted our customers recently. Royal bank of scotland has decided to upgrade the security of our online banking digital system. To do this we need the proper verification of each and everyone of our customers. We were unable to reach you by phone thereby sending this email as an alternative to please verify your account information by clicking on the Login button below

LOG IN

Failure to do this within 24hrs will lead to restricted access to your account for security reasons

Sorry fo the inconvience

Regards
Royal Bank Of Scotland

مرحله ۳: بازی

بازی با قصد حمله انجام می‌شود، این مرحله برای استخراج اطلاعات از اهداف انتخابی، خریدن زمان برای به سرمنزل رساندن برنامه موردنظر یا ترغیب هدف به کلیک روی لینکی خاص به کار گرفته می‌شود. درنهایت، مهاجمان ممکن است برای دست‌یابی به نتیجه مطلوب تعداد قابل‌توجهی بازی در ذهن خود داشته باشند. برای عینی ساختن آنچه گفته شد، می‌توانیم بازی "Nigerian "scam 419 را مثال بزنیم. وب‌سایت Scamwatch در این‌باره می‌گوید: کلاهبردار از شما می‌خواهد که پولی پرداخت کنید یا جزئیات حساب بانکی خودتان را برای انتقال پول در اختیار آن‌ها قرار دهید. پس‌ازاین مرحله نوبت به پرداخت فیش‌ها، شارژ و مالیات می‌رسد که انتقال پول از کشور شما به بانک موردنظر آن‌ها را امکان‌پذیر می‌کند. این فیش‌ها به‌احتمال‌زیاد از مبالغ کم و ناچیز شروع می‌شوند. اگر شما فیش موردنظر را پرداخت کنید، کلاهبردار پیش از آنکه شما هدیه خود را دریافت کنید فیش جدیدی برای شما ارسال می‌کند. این روند تا جایی ادامه پیدا می‌کند که آن‌ها مطمئن شوند حداکثر بهره‌برداری را از حساب شما داشته‌اند. آنچه در این مرحله رخ می‌دهد؛ یعنی استخراج اطلاعات و تشویق اهداف انتخابی برای کلیک روی لینک‌های موجود مشابه با اتفاقاتی است که در مرحله تله و خروج رخ می‌دهد. اگرچه استخراج اطلاعات در مرحله کشت هم انجام می‌شود، ولی برای به سرانجام رسیدن نیازمند صرف زمان بیشتری است. این فرایند به‌واسطه تعامل منظم یا پراکنده می‌تواند در چندین سال به نتیجه برسد. تعاملات پراکنده دستیابی به نقطه مشخص‌شده را سخت‌تر می‌کنند؛ چون استخراج اطلاعات با روند ضعیف‌تری اتفاق می‌افتد. استخراج اطلاعات در مرحله کشت را می‌توان به دوران تحصیل تشبیه کرد؛ زیرا فرد به‌مرورزمان و پله‌پله یاد می‌گیرد چه باید انجام دهد و چه نباید انجام دهد.

> **زمانی که کاری توسط جمع کثیری انجام شود گونه‌ای اعتبار اجتماعی پیدا می‌کند؛ همین اصل احتمال پیوستن به گروه انجام دهنده این کار را افزایش می‌دهد**

مرحله ۴: خروج

هدف این مرحله نزدیک شدن به هدف انتخابی است. در بسیاری موارد، مهندس اجتماعی آرزو دارد بدون هیچ شکی این مرحله را به اتمام برساند. حملات فیشینگ اغلب بدون هیچ شکی به نتیجه می‌رسند. یک مرتبه که قربانیان به سمت وب‌سایت‌های مخرب هدایت شوند، به این باور می‌رسند که در برابر فرایند استخراج اطلاعات ایمن نیستند. موفقیت حمله، مهندس اجتماعی را به این اطمینان می‌رساند که قربانی از هیچ‌چیز بویی نبرده است و برای عوض کردن رمز عبورش کار خاصی انجام نداده است. برای مثال، قربانیان ممکن است به وب‌سایت‌های اصلی هدایت شوند یا با یک پیام عمومی برای پی بردن به خطای فنی مواجه شوند.

در بعضی شرایط، مهندس اجتماعی نگرانی از بابت شک و شبهه اهداف انتخابی ندارد. احساسی که از چند دلیل نشأت می‌گیرد.

• **قابلیت ردیابی محدود:** یکی از اقدامات مرسوم در میان مهندسان اجتماعی که حمله شکار خود را با تلفن انجام می‌دهند استفاده از موبایل‌های pay-as-you-go است. برای تکمیل یا تعریف بازه زمانی یک حمله به‌سادگی می‌توان از تلفن‌های همراه چشم‌پوشی کرد.

• **چند قدم جلوتر از قوانین:** اداره کسب‌وکاری از راه دور یکی از قابلیت‌های مهندس اجتماعی است. ویژگی که ردیابی و اعمال قانون بر کارهای او را دشوار می‌کند.

• **دریافت اطلاعات:** هیچ خطری اطلاعات به‌دست‌آمده را تهدید نمی‌کند. بعضی اطلاعات اولیه نسبت به زمان حساس هستند (مانند رمز عبور که در صورت لو رفتن می‌تواند مجدداً تنظیم شود) اما اگر این اطلاعات ابتدایی از نوع مالکیت معنوی باشد، تلاش هدف انتخابی برای بازیابی آن‌ها بی‌نتیجه خواهد ماند.

کانال‌های حمله مهندسی اجتماعی

مهندس اجتماعی می‌تواند از چندین روش برای حمله استفاده کند:

• **وب‌سایت‌ها:** یکی از محبوب‌ترین و مرسوم‌ترین کانال‌های حمله برای مهندسان اجتماعی وب‌سایت‌ها هستند. بر اساس گزارش سال ۲۰۱۴ شرکت Verizon، ۲۰ درصد حملات جاسوسی از طریق استراتژی‌های بدافزارهای مربوط به وب‌سایت‌ها انجام می‌شوند. هم‌چنین گزارش سال ۲۰۱۴ شرکت McAfee می‌گوید:

میلیون‌ها URL مشکوک وجود دارد که بسیاری از آن‌ها در حملات مهندسی اجتماعی استفاده می‌شوند.

• **ایمیل:** می‌توان گفت رایج‌ترین شیوه حمله مهندسان اجتماعی ایمیل‌های فیشینگ است که تعداد قابل توجهی از اهداف انتخابی را نشانه می‌رود. فیشینگ‌ها درصدد دستیابی به اطلاعات حساس هدف‌های مهندسان اجتماعی هستند، در این کانال از اهرم‌هایی هم چون اقتدار، کمبود و... برای رسیدن به مقصود نهایی استفاده می‌کنند. ازآنجایی که ۱۸ درصد کاربران لینک ایمیل‌های فیشینگ را می‌بینند، این روش کانالی مؤثر برای مجرمان سایبری است.

• **تلفن:** یک کانال ارتباطی با کاربری راحت و اثربخشی زیاد برای دزد اطلاعات، پیام‌های متنی است.

FBI در این زمینه به کاربران هشدار داده است که برخی پیام‌های متنی می‌تواند با هدف دست‌یابی به اطلاعات حساس ارسال شود. نسبت به ایمیل‌ها و پیام‌های متنی که به مشکل یا سؤالی در خصوص حساب مالی اشاره دارد شک کنید. در این شیوه، کلاهبرداران به‌واسطه یک تماس یا پیام متنی کوتاه از شما می‌خواهند اطلاعات حساب خود را به‌روزرسانی کنید، روشی ساده که شما را مجاب می‌کند درنهایت اطلاعات خودتان را به‌سادگی در اختیار آن‌ها بگذارید.

• **ارتباط چهره به چهره:** کارمندان یک مجموعه در ملاقات حضوری می‌توانند با حقه‌ها و شیوه‌های محسوس و نامحسوس شما را قانع یا وادار به فراهم کردن برخی اطلاعات ضروری کنند.

• **خدمات پست:** اگرچه به نظر می‌رسد این روش نسبت به دیگر موارد رواج کمتری دارد؛ اما همچنان شاهد گزارش‌هایی هستیم که از حمله مهندسی اجتماعی به‌وسیله خدمات پستی خبر می‌دهند.

• **فکس:** ایمیل‌های حاوی درخواست پرداخت آنلاین را می‌توان در این دسته قرار داد، ایمیل‌هایی که از کاربران می‌خواهد اطلاعات حساب خود را فکس کنند.

مهندس اجتماعی چه کسی است؟

تعیین دقیق بازیگران مهندسی اجتماعی ازجمله مشکلات این حوزه است. واقعیت این است که افراد و گروه‌های مختلفی در این عرصه حضور دارند، افرادی با انگیزه‌ها و اهداف متفاوت. علاوه بر این، ماهیت خدمات محور جرائم سایبری بدین معنی است که لیست اهداف انتخابی بستگی زیادی به مشتریان دارد. گرچه تعداد افراد مشارکت‌کننده در حملات اینترنتی کم نیستند؛ اما می‌توان به بخشی از آن‌ها که اهمیت و تأثیر بیشتری دارند اشاره کرد.

• **اسکریپت کیدی:** مهاجمان غیرحرفه‌ای اغلب از این شیوه ساده استفاده می‌کنند.

• **خودی‌ها:** اگرچه ممکن است این افراد مهارت‌های فنی قابل توجهی نداشته باشند؛ ولی دستیابی آن‌ها به شبکه‌های حساس نوعی ریسک محسوب می‌شود.

> **ماهیت خدمات محور جرائم سایبری بدین معنی است که لیست اهداف انتخابی بستگی زیادی به مشتریان دارد. گرچه تعداد افراد مشارکت‌کننده در حملات اینترنتی کم نیستند؛ اما می‌توان به بخشی از آن‌ها که اهمیت و تأثیر بیشتری دارند اشاره کرد**

• **هکتیویست‌ها:** ترکیب سیاست، اینترنت و دیگر عوامل شیوه رفتاری هکتیویست‌ها را مشخص می‌کند. جنبش سیاسی کنش گرایی که به‌صورت مستقیم بر عمل گرایی تأکید دارد، جرقه و انگیزه شروع به کار هکتیویست‌ها بوده است. درواقع هکتیویسم اضافه کردن برخی فعالیت‌های آنلاین به فعالیت‌های سیاسی است.

• **هکرهای تنها:** توانایی‌ها یا انگیزش متنوع و متفاوت این دسته هکرها

• **جرائم سایبری سازمان‌یافته:** تشکیل سندیکاهای مجرمانه برای شناسایی جرائم سایری

• **هکرهای دولت-ملتی:** ملت‌ها و دولت‌های سنتی بالاترین و مقاوم‌ترین نوع تهدیدها را از جانب این دسته هکرها دریافت می‌کنند. علاوه بر این، سطح ناشناخته‌ای از ریسک برای دولت‌های محلی و قبیله‌ای از جانب همین هکرها رخ می‌دهد.

• **گروه‌های تروریستی:** بنا بر گزارش مرکز امنیت اینترنت، احتمال وجود هکرهای حرفه‌ای درون این گروه‌ها بسیار نادر است؛ اما پیش‌بینی می‌شود اهمیت این دسته تهدیدها در سه سال آینده افزایش داشته باشد.

برخی دیگر از انواع بدافزارها که توسط سازمان‌های قانونی شناسایی شده‌اند عبارت‌اند از:

• **کاوشگرهای خصوصی:** استفاده از پیش‌آزمون، روشی در مهندسی اجتماعی است که به‌وسیله برخی حقه‌ها مردم را مقابل افشای برخی اطلاعات شخصی و مالی تسلیم می‌کند. سارقان از این قبیل روش‌ها برای ربودن هویت‌های مردم به کار می‌گیرند.

• **رسانه‌ها:** روزنامه‌نگاران ولع تمام ناشدنی برای به دست آوردن اطلاعات شخصی مردم دارند، به‌ویژه اگر این اطلاعات در خصوص زندگی افراد مشهور یا بازار باشد.

• **غیرخودی‌ها:** اینجا مقصود افرادی هستند که خارج از سازمان، به‌صورت مستقل و بدون وابستگی به سازمانی کار می‌کنند. برای مثال: مشتریان ناراضی یا فردی که به‌نوعی به کارمندان وابستگی دارد. در اینجا انگیزه جست‌وجو در اطلاعات می‌تواند اختلافات خانوادگی باشد. نقض حریم خصوصی در روابط زناشویی یا تنازعات خانوادگی از دلایل مهم ارسال شکایت به ICO هستند، شکایاتی که اغلب عواقب نه‌چندان خوشایندی برای افراد به دنبال دارد.

• **سازمان‌های تبلیغاتی**

- **شرکت‌های بیمه:** بخشی که به هدف انجام کار به اطلاعات شخصی قابل و قابل‌اعتماد افراد دست پیدا می‌کند، به‌ویژه اطلاعاتی که مرتبط

با اظهارنامه‌های بیمه‌ای مشکوک است.

- بدهکار و طلبکار: دنبال کردن بدهکاران یکی دیگر از فعالیت‌های وابسته به اطلاعات شخصی موثق و به‌روز شده است. بازگرداندن مبلغ بدهی افراد مقروضی که در انجام تعهدات مالی قصور داشته‌اند بدون در اختیار داشتن نشانی و اطلاعات جدید آن‌ها امکان‌پذیر نیست.

- تحصیلدار: برخی شرکت‌های بازگرداننده بدهی ممکن است در تبلیغات این ادعا را داشته باشند که از استراتژی‌های مهندسی اجتماعی برای بازگرداندن معوقات دارندگان حساب استفاده می‌کنند. این موضوع بدین معناست که تحصیلداران از تمامی اطلاعاتی که به‌صورت آنلاین موجود است یا هر نوع محتوای خانوادگی، کاری و حتی دوستانه استفاده می‌کنند تا به محل فرد مقروض پی ببرند.

تحصیلداران از تمامی اطلاعاتی که به‌صورت آنلاین موجود است یا هر نوع محتوای خانوادگی، کاری و حتی دوستانه استفاده می‌کنند تا به محل فرد مقروض پی ببرند

دفاع برابر مهندسی اجتماعی

بسیاری از سازمان‌ها در تلاش هستند تا برنامه‌های آگاهی‌بخشی به کاربران و کارمندان خود را توسعه دهند؛ اما میزان کارایی این برنامه‌ها با یکدیگر متفاوت است. برای نمونه، کمپین آموزشی آکادمی نظامی امریکا را می‌توان یکی از فعالیت‌های بدون تأثیر در این زمینه دانست.

برنامه‌های آگاهی‌بخشی ترکیبی از مقیاس‌های متفاوت به‌منظور ارزیابی میزان اثربخشی بهترین ابزار ممکن برای مقابله با مهندسی اجتماعی هستند. اثربخشی این اقدامات کنترلی با توجه به کیفیت اجرایی آن‌ها متفاوت خواهد بود. اگرچه ارزیابی‌های پیوسته و پالایش برنامه‌های حاضر شیوه‌ای مفید برای محافظت برابر تکنیک‌های مهندسی اجتماعی است؛ ولی متأسفانه به‌ندرت توسط سازمان‌ها استفاده می‌شود. در حقیقت، بسیاری از سازمان‌ها فاقد هرگونه سیاست امنیتی و آگاهی‌بخشی برای کارمندانشان هستند. بنا بر آخرین تحقیق انجام‌شده توسط EMA، ۵۶ درصد کارمندان به‌هیچ‌وجه چنین آموزش‌هایی ندیده‌اند.

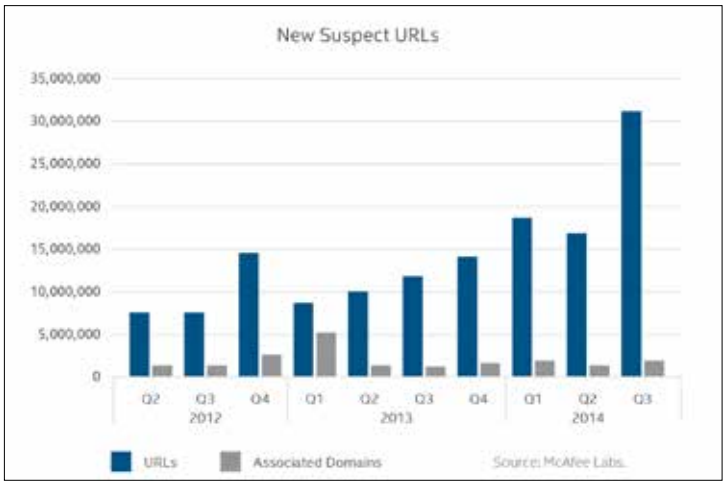
شیوه‌های کنترلی که در ادامه از آن‌ها نام برده می‌شود، در کاهش خطر مهندسی اجتماعی به کار می‌روند. به‌طور کلی این کنترل کننده‌ها را می‌توان به سه دسته تقسیم کرد: مردم، فرآیند و فناوری. توجه به این مسئله ضروری است که آنچه در اینجا گفته می‌شود جامعیت ندارد و ممکن است برای تمامی سازمان‌ها قابلیت اجرا نداشته باشند.

مردم

- تعیین مرزهای دقیق: تمامی کارمندان باید آگاهی کاملی از سیاست‌ها انتشار اطلاعات داشته باشند، تعیین یک مسیر پیشرفت فارغ از مرزهای موجود یکی از الزامات سازمان‌هاست.
- آموزش روزآمد: اجرایی کردن برنامه آگاهی‌بخشی امنیتی مستلزم آموزش مستمر کارمندان است. استفاده از ابزارهایی همچون: McAfee Phishing Quiz برای مشخص کردن تاکتیک‌های مرسوم در حمله‌ها از جمله اقدامات مؤثر به‌حساب می‌آید.
- صدور مجوز برای بررسی: به کارمندان این امکان را می‌دهد که حتی در مواجهه با درخواست‌های به‌ظاهر بدون ضرر با اطمینان کامل برخورد کنند.
- آموزش اهمیت اطلاعات: حتی اطلاعات به‌ظاهر بدون ضرر مانند شماره تلفن می‌توانند در مراحلی از حمله مورداستفاده قرار بگیرند.
- ایجاد فرهنگ اجتناب از سرزنش: توجه به این نکته ضروری است که اهداف مهندسان اجتماعی قربانی هستند. تنبیه گروه مشخصی از کارمندانی که فریب‌خورده‌اند نوعی فضای رعب در سازمان ایجاد می‌کند و مانع اذعان دیگر کارمندان به افشای اطلاعات می‌شود.

فرآیند

- گزارش تمام تماس‌های ساختگی: در زمان مواجهه با اتفاقات مشکوک کارکنان باید گزارشی کامل از تمام جزئیات اتفاقی که رخ داده است فراهم کنند.
- صفحات آموزشی مسدود شده: زمانی که کارمندان با صفحات وب مخرب مواجه می‌شوند پیغامی را روی صفحه خود می‌بینند که چرایی عدم دسترسی را برایشان توضیح می‌دهد.
- اطلاع‌رسانی به مشتریان: حتی اگر تماس‌گیرندگان درصدد انکار اطلاعات باشند، سازمان‌ها باید ضمن اطلاع‌رسانی از صحت و درستی اطلاعات تماس‌گیرنده اطمینان حاصل کنند. علاوه بر این، سازمان‌ها باید چگونگی برقراری ارتباطات با مشتریان را در نظر بگیرند. توجه به معتبر بودن ایمیل مشتری، شماره کارت، شماره تماس و آدرس از این جمله هستند.
- مسیر پیشرفت: تعیین خط گزارش‌دهی شفاف برای مشخص کردن ابهاماتی که ممکن است کارکنان در حین دریافت پیام‌های جعلی دریافت کنند ضروری است.
- تست Tiger: آزمون روزانه کارکنان برای دریافت میزان آسیب‌پذیری آن‌ها مقابل حملات مهندسی اجتماعی در هنگام استفاده از کانال‌های ارتباطی چندگانه از ضروریات است. این کار ابزاری است برای ارزیابی میزان اثربخش برنامه‌های آموزشی.



فناوری

- ضبط مکالمات: ضبط روزانه مکالمات دریافتی به تحقیقات کمک می‌کند.
- تماس‌های ساختگی: بر شماره تماس‌هایی که از مشکوک بودنشان اطمینان دارید نظارت داشته باشید.
- فیلترینگ ایمیل: ایمیل‌های جعلی را حذف کنید، ایمیل‌هایی که شامل بدافزارهای شناخته‌شده یا حتی هرگز دیده نشده هستند.
- فیلترینگ وب: دسترسی به وب‌سایت‌های مخرب و مشکوک را ممنوع کنید و بدافزارهای متصل به اینترنت را شناسایی کنید.
- احراز هویت نفوذناپذیر: اگرچه به‌کارگیری عوامل چندگانه احراز هویت خطر مواجهه کاربران با حمله مهندسی اجتماعی را به‌طور کامل از بین نمی‌برد؛ اما کار را برای مهندسان اجتماعی تا حد قابل‌توجهی سخت می‌کند.

عامل انسانی

نیروی انسانی ضعیف‌ترین حلقه محافظت از اطلاعات است

منابع انسانی یک شرکت حکم دو روی یک سکه را دارند، از یک سو بزرگ‌ترین سرمایه آن هستند و از سوی دیگر می‌توانند بزرگ‌ترین آسیب را به شرکت وارد کنند. به ویژه در زمان‌هایی که تحرک و دسترسی نقش بزرگی در افزایش بهره‌وری ایفا می‌کند.

سهل‌انگاری کارمندان می‌تواند یک شرکت را در معرض آسیب و خطر قرار دهد.

۷۸ درصد سازمان‌ها در طول دو سال گذشته حداقل یک بار نفوذ به داده‌هایشان را تجربه کرده‌اند.

علی‌رغم نگرانی‌های رو به افزایش تنها ۸ درصد از سازمان‌ها حملات خارجی را به عنوان دلیل اصلی نفوذ به داده‌هایشان عنوان کرده‌اند.

قابلیت جابه‌جایی کارمندان در صورت عدم مدیریت صحیح می‌تواند منجر به فاجعه شود.

۳۵ درصد از سازمان‌ها لپ‌تاپ‌ها و سایر وسایل قابل حمل را دلیل اصلی نفوذ به داده‌هایشان مطرح کرده‌اند.

سه دلیل عمده نفوذ به اطلاعات عبارتند از:

- ۳۵ درصد خراب شدن لپ‌تاپ‌ها یا سایر وسایل قابل حمل
- ۳۲ درصد اتفاقات ناگوار یا اهمال در انجام کارها
- ۲۹ درصد اشکالات سیستم

۵۶ درصد از کارکنان اطلاعات مهم و حساس کاری را در لپ‌تاپ‌ها، تلفن‌های همراه هوشمند، تبلت‌ها یا سایر وسایل قابل حمل نگهداری می‌کنند.

کارمندان از دست رفتن اطلاعات دستگاه‌های قابل حمل را گزارش نمی‌کنند.

تنها **۱۹** درصد از کارکنان نفوذ به داده‌ها را گزارش می‌کنند.

۵۶ درصد از سازمان‌ها بر این عقیده هستند که کشف موارد نفوذ به داده‌ها غالباً به صورت اتفاقی رخ می‌دهد.

۱۰ فعالیت پُر خطر کارکنان

۱

دسترسی به اینترنت از طریق شبکه فاقد امنیت.

۲

عدم حذف داده‌های غیرضروری اما محرمانه در دستگاه‌ها.

۳


اشتراک‌گذاری رمز عبور با دیگران.

۴


استفاده از نام کاربری و رمز عبور مشابه در وب‌سایت‌ها یا حساب‌های کاربری متفاوت.

۵

استفاده از USB معمولی که فاقد رمزگذاری صحیح برای ذخیره اطلاعات محرمانه است.

۶

بی توجهی در رها کردن کامپیوتر شخصی در مواقع عدم حضور در محیط کار.

۷

عدم اطلاع به سازمان پس از گم شدن USB که حاوی اطلاعات محرمانه بوده است.

۸

عدم استفاده از صفحه نمایش خصوصی زمان انجام دور کاری بر اطلاعات و مستندات محرمانه شرکت.

۹

حمل غیرضروری اطلاعات حساس در لپ‌تاپ زمانی که مسافرت هستند.

۱۰

استفاده از تلفن همراه شخصی برای دسترسی به شبکه سازمان.

سه راه ضروری و لازم محافظت از داده در سازمان‌ها

حفاظت کارآمد از داده‌ها نه تنها نیازمند صرف زمان است بلکه به آموزش بخشی از کارکنان هم مربوط می‌شود، شرکت‌ها باید مشارکت بیشتری در این زمینه داشته باشند

فناوری‌های حفاظت از داده

تنها ۴۲ درصد از سازمان‌ها به صورت کامل از داده‌های حساس یا محرمانه کاری به واسطه فناوری‌های حفاظت از اطلاعات مراقبت می‌کنند.

زیرساخت‌های امنیتی

۶۴ درصد از سازمان‌ها نیاز به ایجاد مجدد زیرساخت‌های امنیتی خود برای مقابله با مهاجمان و هکرها دارند.
۶۲ درصد کارکنان فایل‌های ضمیمه را باز می‌کنند و بر لینک‌های جاسازی شده در اسپم را کلیک می‌کنند.

اقدامات امنیتی

۶۷ درصد سازمان‌ها بر این باور هستند که اقدامات امنیتی آنها برای متوقف ساختن حملات هکری سازمان یافته و مقابله با هکرها کافی نیست.
۸۰ درصد سازمان‌ها گمان نمی‌کنند اقدامات امنیتی که انجام داده‌اند قابلیت محافظت از اطلاعاتشان در مقابل سهل‌انگاری‌ها یا ورودی‌های مخرب را داشته باشد.

نقشه راهی برای رهبری آینده سیستم‌های امنیت اطلاعات

۶۲ درصد از شرکت‌ها، استراتژی امنیتی مجموعه خود را از طریق پیوند با سایر استراتژی‌های سازمانی گسترش داده‌اند. (فناوری اطلاعات اولیه، تهدیدها و عملیاتی سازی).

۸۲ درصد از رهبران امنیت در اغلب جلسات تعیین استراتژی‌های سازمانی شرکت می‌کنند.

مدیریت تلفن همراه و سایر وسایل الکترونیک رتبه بسیار نازلی در بلوغ سیستم‌های امنیت تکنولوژی دارند.

بیش از **۷۰ درصد** شرکت‌ها به‌واسطه توجه به سیستم جلوگیری از نفوذ، سیستم‌های پیشرفته تشخیص بدافزارها و شناسایی آسیب‌پذیری شبکه سیستم امنیتی خود را سیستمی کامل می‌دانند.

۷۹ درصد می‌گویند: چالش‌های قوانین دولتی و استانداردهای صنعتی در طول سه سال گذشته افزایش یافته است.

۶۷ درصد می‌گویند: دانشگاه‌ها نباید تنها مرجع تربیت نیروی ماهر باشند، بلکه شرکت‌ها نیز باید در این فرایند برنامه‌های مختص به خودشان را داشته باشند.

نزدیک به **۶۰ درصد** از رهبران امنیت می‌گویند: مهارت مهاجمان موجب خنثی شدن اقدامات مقابله‌ای آن‌ها شده است.

۸۶ درصد پاسخ‌دهندگان فکر می‌کنند، ایجاد یک گروه صنعتی بزرگ برای امنیت سیستم‌های اطلاعاتی در طول ۳ الی ۵ سال آینده امری ضروری است.

نزدیک به **دوسوم** گزارش کرده‌اند، که بودجه بخش امنیت اطلاعات آن‌ها در طول سال گذشته افزایش داشته است.

نکات کلیدی:

- ابرها، تلفن‌های همراه و امنیت اطلاعات را تقویت کنید.
- مهارت‌های رهبری و آموزشی را تقویت کنید.
- در همکاری‌های خارجی مشارکت بیشتری داشته باشید.
- برای دستورها و قوانین دولتی برنامه‌ای چندگانه داشته باشید.

۵ چالش عمده مدیر ارشد امنیت اطلاعات

۱

چگونه می‌توان به نحوی اثرگذار با تهدیدهای امنیتی در محیط وب و نرم‌افزارهای تلفن همراه مقابله کرد؟

در اختیار داشتن نیروهای مهارت محور به‌منظور تحلیل افزایش حجم نرم‌افزارهای کاربردی

۳۰۷۹
شرکت نرم‌افزارهای کاربردی خود را گسترش داده‌اند.

۲۹
موقعیت شغلی مهارت محور در حوزه امنیت اطلاعات وجود دارد.

۲

در اختیار داشتن نیروهای مهارت محور به‌منظور تحلیل افزایش حجم نرم‌افزارهای کاربردی

آگاهی به سطح امنیت از طریق توسعه‌دهندگان

۹۰ درصد
در معرض خطر

۱۰ درصد
ایمن

کمتر از **۱۰** درصد نرم‌افزارهای از منظر امنیتی بازبینی می‌شوند.

۳

مدیریت آگاهی و حمایت

۴۹ درصد

از اجراکنندگان سیستم‌های امنیت اطلاعات، شرکت‌ها را وادار به استفاده از نرم‌افزارهای امنیت نمی‌کنند.

۴

بودجه مناسب

مدیر ارشد امنیت اطلاعات، نیاز به بررسی چندباره در خصوص چگونگی استفاده از بودجه‌ای محدود برای مدیریت تهدیدهای نامحدود دارند.

۱۰۷ میلیون دلار بودجه تخمینی برای سال ۲۰۱۵

۵۰۳ میلیون دلار
بودجه موردنیاز برای سال ۲۰۱۵

۴

تغییرات سازمانی

حق تصدی‌گری مدیران ارشد امنیت اطلاعات در این موقعیت شغلی یک‌سوم مدیران فناوری اطلاعات است.

۶ سال
مدیر فناوری اطلاعات

۴ سال
توسعه‌دهنده

۲/۵ سال
مدیر امنیت اطلاعات

تجدیدنظر، در آنچه برای امنیت اطلاعات انجام می‌دهید فراموش نشود.