صداوسیمای جمهوری اسلامی ایران

معاونت سیاسی

اداره پژوهش‌های سیاسی

مهندسی اجتماعی و تکنیک های آن

فرآورده‌های خبری و تولیدات پژوهشی در بخش های زیر قابل دسترس است:

ـ وب سایت خبرگزاری صداوسیما (سرویس پژوهش) http://www.iribnews.ir

پژوهشگر: یاسر بهشتی

فـهرسـت مـطالـب

عنـــــوان **صفحـــــه**

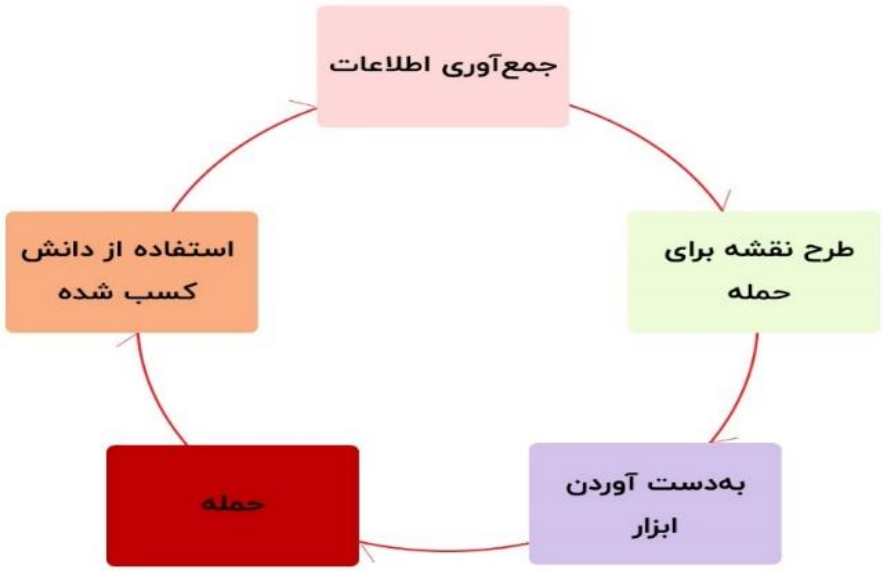
۱- مبتنی بر انسان ۵
۲- مبتنی بر کامپیوتر ۵
تکنیک های حمله مهندسی اجتماعی ۶
طعمه **(Baiting)** ۶
ترسناک **(Scareware)** ۶
بهانه **(Pretexting)** ۶
فیشینگ **(Phishing)** ۷
فیشینگ نیزه **(Spear phishing)** ۷
روش **Quid Pro Quo** ۷
حمله **Pretexting** ۷
حمله **Piggybacking** ۸
پیامدهای گسترده حملات مهندسی اجتماعی حتی در حوزه سیاست ۸
مقابله با حملات مهندسی اجتماعی ۸
جمع بندی ۱۰
کلام آخر ۱۱
منبع ۱۱

مقدمه:

- حملات مهندسی اجتماعی همواره در صدر لیست حملات سایبری قرار داشته و اطلاعات محرمانه سرقت شده با استفاده از این حملات، نقطه شروع مرسومی برای خرابکاران سایبری محسوب می شوند.
- با فراگیر شدن اینترنت و استفاده از آن برای کنترل حساب‌های بانکی و نقل انتقال پول، دزدی ها نیز مجازی شده است. هکرها علاوه بر استفاده از روش‌های قدیمی هک به روش‌های جدید که مبتنی بر مهندسی اجتماعی هستند روی آورده اند. آن‌ها با استفاده از تکنیک‌های روانشناسی بر روی ذهن قربانیان خود کار می‌کنند تا اطلاعات مورد نظرشان را به دست بیاورند.
- این روزها مهندسی اجتماعی یک روش بسیار معمول است که توسط هکرها برای عبور از حصار امنیتی کاربران استفاده می‌شود. روش کار هکرها در این روش به این صورت است که کاربران را فریب می‌دهند تا آن‌ها به دست خودشان اطلاعات مهم و حساس را افشا کنند.
- روش مهندسی اجتماعی از آن جهت برای هکرها حائز اهمیت است که اطلاعاتی جهت حمله به قربانی را در اختیار آن‌ها قرار می‌دهد به این معنی که هکرها برای فریب دادن کاربران از راه‌های معمولی مانند استفاده از ایمیل یا تلفن استفاده می‌کنند.
- آنها در روش مهندسی اجتماعی به جای اینکه حفره‌های امنیتی قربانی را پیدا کنند، کاربران را به مکان‌هایی که می‌خواهند هدایت می‌کنند. برای مثال از طریق یک تماس تلفنی و با استفاده تمایلات و گرایش‌های آن فرد و جلب اعتماد او، اطلاعات مورد نیاز خود را کسب می‌کنند.
- هک با استفاده از مهندسی اجتماعی علاوه بر کاربران خانگی، برای شرکت‌ها نیز بسیار خطرناک است. حتی برای شرکت‌هایی که از فایروال یا حتی سیستم‌های احراز هویت استفاده می‌کنند. زیرا هکرها با این روش حصارهای امنیتی را مورد هجوم قرار نمی‌دهند، بلکه آن را دور می‌زنند.
- مهم‌ترین اقدام برای جلوگیری از چنین حملاتی، آشنا شدن با روش‌های گوناگون هک و دزدی اطلاعات است تا در هنگام برخورد با چنین حملاتی از آمادگی لازم برخوردار بوده و از ارائه اطلاعات حساس و مهم جلوگیری شود.

تعریف:

مهندسی اجتماعی[1] اصطلاحی است که اولین‌بار در حوزه علوم اجتماعی ظاهر شد و به نوعی مداخله مستقیم دانشمندان در علوم انسانی بود.[2]



چرخه حمله مهندسی اجتماعی

مهندسی اجتماعی یک متد غیر فنی نفوذ به یک سیستم یا یک شبکه است. این کار در واقع فریب دادن کاربران یک سیستم و متقاعد کردن آنها به انجام کارهای پرفایده برای هکر است. مانند گرفتن اطلاعاتی از آنها که بتوان در شکستن یا دور زدن مکانیزم امنیتی استفاده کرد. درک مفهوم مهندسی اجتماعی مهم است زیرا می توان با استفاده از آن به عنصر انسانی یک سیستم حمله کرد و معیارهای فنی امنیتی را دور زد . این متد را می‌توان در جمع آوری اطلاعات، قبل یا حین یک حمله استفاده کرد.

یک مهندس اجتماعی معمولا از تلفن یا اینترنت برای فریب مردم به منظور آشکارسازی اطلاعات حساس استفاده می‌کند یا با گرفتن آنها بر ضد قوانین امنیتی سازمان استفاده می کند. با استفاده از این شیوه مهندسین اجتماعی به جای نفوذ به حفره‌های امنیتی کامپیوتر، از گرایش طبیعی یک شخص بهره می‌گیرند تا شخص به سخنانشان اعتماد کنند. خطرناک‌ترین بخش مهندسی اجتماعی این است که شرکت‌ها با پروسه های تشخیص هویت، فایروال‌ها، شبکه‌های خصوصی مجازی[3] و نرم افزارهای مانیتور شبکه هنوز هم خیلی به روی حملات باز و آسیب پذیر هستند، چون مهندسی

---

[1] social engineering.

[2] ۲. اصطلاح «مهندسی اجتماعی» نخستین بار توسط Van Marken در سال ۱۸۹۴ ابداع شد و هدف آن ترویج این ایده بود که برای مقابله با مشکلات انسانی، وجود افراد حرفه‌ای ضرورت دارد. درست همان‌طور که نمی‌توانید بدون آموزش مهارت‌های لازم مشکلات فنی را حل کنید، مسایل و مشکلات اجتماعی را هم بدون داشتن مهارت‌های لازم نمی‌توانید حل کنید.

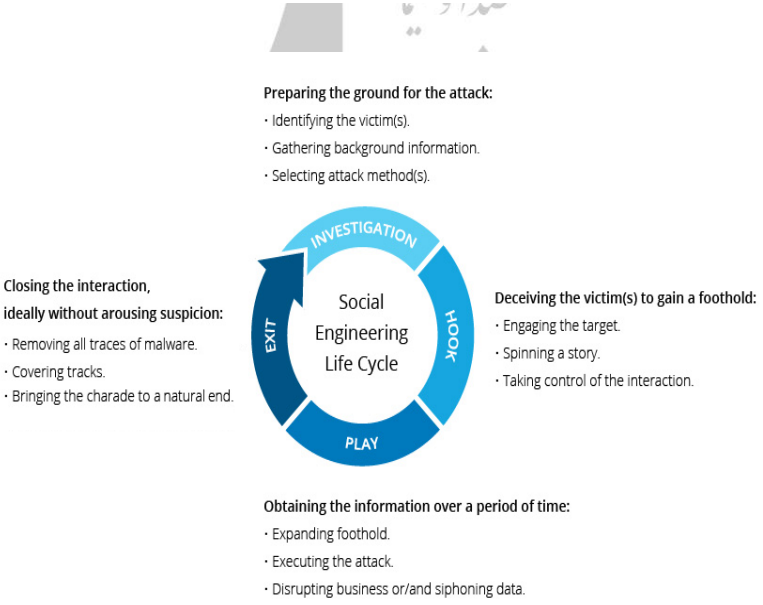
[3] VPNs.

اجتماعی به طور مستقیم به معیارهای امنیتی حمله نمی‌کند. به جای آن یک حمله مهندسی اجتماعی معیارهای امنیتی را دورزده و به دنبال عناصر انسانی یک سازمان می‌رود .

در واقع مهندسی اجتماعی عبارت است از بدست آوردن اطلاعات حساس یا امتیاز دسترسی ناشایست توسط یک شخص بیگانه بر اساس بنای نامناسب اعتماد در روابط. هدف یک مهندس اجتماعی فریب دادن شخصی به منظور فراهم کردن اطلاعات ارزشمند یا دسترسی به آن اطلاعات است.

همگان موافقند که کاربران پیوند ضعیفی در امنیت هستند. این اصل چیزی است که عملکرد مهندسی اجتماعی را ممکن می‌سازد؛ در هر نوع حمله در حوزه فناوری اطلاعات که بتوان آن را جزو حملات مهندسی اجتماعی دانست باید از انواع عملیات روانی مانند اقناع و ... استفاده شود تا کاربران را متقاعد به ارتکاب اشتباه‌های امنیتی کند و این همان **هنر دستکاری و سوء استفاده است.** توانایی یکی شدن با افراد معمولا به عنوان بخشی از هنر سواستفاده است. بدین ترتیب کاربران معمولا ضعیف‌ترین پیوند زنجیره امنیت هستند. مهندسی اجتماعی بر اساس خصوصیت‌های طبیعی بشر همچون آرزوی مفید بودن، تمایل به اعتماد به مردم و ترس از دچار مشکل شدن شکار می‌کند.

حملات مهندسی اجتماعی در یک یا چند مرحله اتفاق می افتد. یک نفوذگر ابتدا برای قربانی در نظر گرفته شده برای جمع‌آوری اطلاعات لازم، از جمله نقاط احتمالی ورود و پروتکل های امنیتی ضعیف، برای انجام حمله، تحقیق می‌کند. سپس مهاجم برای جلب اعتماد قربانی و ایجاد انگیزه برای اقدامات بعدی که باعث نقض اقدامات امنیتی می شود مانند افشای اطلاعات حساس یا دسترسی به منابع مهم تلاش می کند.



آنچه مهندسی اجتماعی را خطرناک می‌کند این است که به جای آسیب پذیری در نرم افزار و سیستم عامل ها به خطای انسانی می‌پردازد. اشتباهات انجام شده توسط کاربران مشروع بسیار کمتر قابل پیش بینی است و باعث می‌شود تا شناسایی و خنثی‌سازی آن از یک نفوذ مبتنی بر بدافزار سخت تر شود.

این عمل نه تنها در بعد فردی برای هر کاربر محتمل است بلکه در سطح سازمانی نیز انجام می‌شود. یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد. مثلا وانمود نماید که یک کارمند جدید است، یک تعمیرکار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید. یک مهاجم ، با طرح سؤالات متعدد و برقراری یک ارتباط منطقی بین آنان، می‌تواند به بخش‌هائی از اطلاعات مورد نیاز

خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا کند. در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نشود، وی ممکن است با شخص دیگری از همان سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول، توانمندی خود را افزایش دهد.

انواع حملات مهندسی اجتماعی:

۱- مبتنی بر انسان

در حالت مبتنی بر انسان، هکر از طریق ارتباط با شخص اطلاعات مورد نیاز خود را به دست می آورد که تکنیک‌های این قسم را می‌توان به دسته بندی‌های زیر تقسیم کرد :

- **وانمود کردن به‌عنوان یک کاربر مهم** همچون یکی از قوای اجرایی یا مدیران سطح بالا و نیازمند دستیاری فوری به دسترسی به یکی از کامپیوترها یا فایل ها
- **تقلید صدای یک کارمند یا یک کاربر مورد تایید**
- **استفاده از سوم شخص**
- **تماس پشتیانی فنی**
- **مشاهده پسورد از روی دست**[۱]
- **استفاده از زباله دان**[۲]

۲- مبتنی بر کامپیوتر

مهندسی اجتماعی متکی به کامپیوتر نیز، به داشتن نرم افزار کامپیوتر که تلاش کند اطلاعات هدف را بازیابی کند، اشاره دارد. این حمله‌ها می‌تواند شامل موارد زیر باشد:

- **پیوست های ایمیل**[۳]
- **وبسایت های جعلی**[۴]
- **پنجره های پاپ آپ**[۵]

---

۱. Shoulder surfing
۲. **Dumpster diving**
۳. Email attachments
۴. Fake websites
۵. Pop-up windows

- **حمله از داخل**[1] (اســتخدام شــدن به عنوان یکی از کارمندان یا پیداکردن یک کارمند ناراضــی برای کمک در حمله)

تکنیک های حمله مهندسی اجتماعی

حملات مهندسی اجتماعی به اشکال مختلفی رخ می دهد و می تواند در هر جایی که تعامل انسان در آن دخیل باشد ، انجام شود.

طعمه (Baiting)

همان‌طور که از نام آن پیداســت، حملات طعمه زدن از یک قول دروغین برای ترســاندن، طمع یا کنجکاوی یک قربانی استفاده می‌کنند. آنها کاربران را به دام انداخته و اطلاعات شخصی آنها را سرقت می‌کنند.

جدیدترین شکل طعمه استفاده از رسانه های فیزیکی برای پراکندگی بدافزارها است. به عنوان مثال، مهاجمین طعمه ها را (معمولاً فلش مموری های آلوده به بدافزار) در مناطقی آشــکار که قربانیان احتمالی حتماً آنها را مشــاهده می کنند (جلوی شرکت، آسانسور، پارکینگ یک شرکت و ...)، ترک می‌کنند. قربانیان طعمه را از حس کنجکاوی برداشته و آن را درون یک کامپیوتر کار یا خانه قرار می‌دهند و در نتیجه نصب بدافزار خودکار روی سیستم انجام می‌شود.

ترسناک (Scareware)

شامل قربانیانی است که با هشدارهای دروغین و تهدیدهای ساختگی دست به انجام کارهای اجباری می‌کنند. کاربران فریب خورده اند و فکر می کنند سیستم آنها به بدافزار آلوده شده است و از آنها خواسته می شود نرم افزاری را نصب کنند که هیچ فایده واقعی ندارد و یا دراصل خود بدافزار است.

بهانه (Pretexting)

در اینجا یک مهاجم از طریق یک سری از دروغ های هوشمندانه دست به دست هم می‌دهد. کلاهبرداری غالباً توسط متخلف آغاز می‌شود و وانمود می‌کند که به اطلاعات حساس یک قربانی احتیاج دارد تا بتواند یک کار مهم را انجام دهد.

مهاجم معمولاً با جعل اعتماد به قربانی خود با جعل هواداری از همکاران، پلیس، بلنک و مقامات مالیاتی یا ســایر افراد دارای صلاحیت شناخت شروع می کند سپس سؤالاتی را مطرح می‌کند که ظاهراً برای تأیید هویت قربانی لازم است، و از طریق آنها داده های شخصی مهم را جمع می‌کند. انواع اطلاعات و سوابق مربوطه با استفاده از این کلاهبرداری مانند شماره های تأمین اجتماعی، آدرس های شخصی و شماره تلفن‌ها ، سوابق تلفنی، تاریخ تعطیلات کارکنان ، سوابق بانکی و حتی اطلاعات امنیتی جمع‌آوری می‌شود.

[1] .Insider Attacks

فیشینگ (Phishing)

یکی از محبوب ترین انواع حمله مهندسی اجتماعی، کلاهبرداری فیشینگ است که از طریق کمپین های ایمیل و پیام متنی با هدف ایجاد احساس فوریت، کنجکاوی یا ترس در قربانیان هستند. سپس آنها را به آشکار ساختن اطلاعات حساس، کلیک روی پیوندها به وب سایت‌های مخرب یا باز کردن پیوست های حاوی بدافزار سوق می‌دهد.

به عنوان مثال ایمیلی است که برای کاربران یک سرویس آنلاین ارسال شده است و به آنها هشدار می دهد که نقض خط مشی نیاز به اقدام فوری از طرف آنها، مانند تغییر رمز عبور، شماره کارت اعتباری و رمز اینترنتی آن و ... دارد. این شامل پیوندی به یک وب سایت نامشروع است (از لحاظ ظاهری تقریباً با نسخه قانونی آن یکسان است) باعث می‌شود کاربر ناشناس به وارد کردن اعتبار فعلی و رمزعبور جدید خود شود. پس از ارسال فرم، اطلاعات به مهاجم ارسال می‌شود.

فیشینگ نیزه (Spear phishing)

این یک نسخه هدفمند تر از کلاهبرداری فیشینگ است که به موجب آن فرد مهاجمی افراد یا بنگاه‌های خاص را انتخاب می‌کند. آنها سپس پیام‌های خود را بر اساس ویژگی‌ها ، موقعیت‌های شغلی و مخاطبین متعلق به قربانیان خود متناسب می‌کنند تا حمله آنها آشکارتر شود. این تکنیک نیاز به تلاش بیشتری از طرف نفوذگر دارد و ممکن است هفته ها و ماه ها طول بکشد.

بعنوان مثال یک سناریو ممکن است یک مهاجمی باشد که در جعل هویت مشاور یک سازمان، یک ایمیل به یک یا چند کارمند ارسال می‌کند. این متن دقیقاً مطابق آنچه معمولاً مشاور انجام می دهد، امضا شده است و بدین ترتیب گیرندگان فکر می‌کنند که این یک پیام معتبر است. این پیام گیرندگان را ترغیب می کند که رمز عبور خود را تغییر دهند و پیوندی را برای آنها فراهم می‌کند که آنها را به صفحه مخرب هدایت می کند که در آن زمان مهاجم اعتبارنامه های خود را ضبط می کند.

روش Quid Pro Quo

این نوع حمله نیز مانند طعمه گذاری است. هکر در ازای خدماتی که به کاربر ارائه می‌دهد از او تقاضای اطلاعات شخصی یا اطلاعات ورود حساب کاربری‌اش را دارد. مثلا هکری به شما تلفن کرده و خود را کارمند شرکت کاریابی معرفی می‌کند و برای پیدا کردن شغل برای شما اطلاعات شخصی‌تان شامل شماره منزل، شماره تلفن همراه، آدرس منزل و ... را می‌گیرد.

حمله Pretexting

این نوع حمله مهندسی اجتماعی هم مشابه فیشینگ است. در آن هکر تلاش می‌کند خودش را شخص دیگری معرفی کند، تا بتواند به اطلاعات حساس و شخصی کاربر دسترسی پیدا کند. در برخی موارد هکر مجبور است یک هویت جدید بسازد. هکر سعی می‌کند با دروغگویی و فریب بسیار، خود را شخص دیگری معرفی کرده، و با ایجاد اعتماد بین خودش و قربانی، اطلاعات وی را به‌دست بیاورد.

حمله Piggybacking

در آن، فرد غیر مجاز به صورت فیزیکی به دنبال فرد مجاز به یک سیستم یا منطقه با دسترسی محدود شده وارد می‌شود. مثلا مجرم به کارمند موسسه یا شرکت تلفن میزند و از او می‌خواهد درب را برایش باز کند، زیرا فراموش کرده است که کارت ورود خود را همراهش بیاورد.

کارشناسان امنیتی برای حصول اطمینان از امنیت سایبری شرکت‌ها و سازمان‌ها باید مطمئن شوند که تمامی کارمندان از انواع حملات مهندسی اجتماعی آگاهی کامل دارند. این نوع از آگاهی فقط شامل کارمندان سازمان‌ها وشرکت‌ها نیست. هر شخصی که با اینترنت سروکار دارد لازم است با انواع حملات سایبری از جمله مهندسی اجتماعی آشنایی داشته و آنها را بشناسد.

پیامدهای گسترده حملات مهندسی اجتماعی حتی در حوزه سیاست

مفهوم «مهندسی اجتماعی» در حوزه سیاست نیز کاربرد دارد. در سیاست، از این عبارت گاهی برای انتشار خبرها و اطلاعات غلط نیز استفاده می کنند. البته این مفهوم چیزی فراتر از ارسال یک ایمیل فیشینگ یا فیشینگ تلفنی (ویشینگ) بوده و بیشتر مرتبط با این مطلب است که عملکرد سیاستمداران به چه صورت است، چگونه اطلاعات را منتشر می‌کنند و مردم چه تفسیری از آن اطلاعات خواهند داشت.

مقابله با حملات مهندسی اجتماعی

در بسیاری از حملات مهندسی اجتماعی مهاجم مستقیم به سراغ قربانی رفته و به صورت شفاهی یا کتبی با وی گفتگو می‌کند تا او را فریب داده و اطلاعات لازم را از وی دریافت نماید. اکثر راهکارهای دفاعی در برابر حملات مهندسی اجتماعی بر همین موضوع تاکید داشته و به افراد گوشزد می‌نمایند تا در هنگام ارتباط با دیگران به چه موضوعاتی توجه داشته باشند تا خطر مواجهه با حملات مهندسی اجتماعی کاهش یابد.

اصلی‌ترین روش‌های دفاعی عبارت است از:

۱. آموزش

اولین و مهم‌ترین اصل در مقابله با مهندسی اجتماعی، آگاهی تک‌تک افراد و فرهنگ‌سازی مناسب است. افراد آگاه به سادگی می‌توانند حملات مهندسی اجتماعی را خنثی کنند. فرهنگ‌سازی در برابر حملات مهندسی اجتماعی می‌تواند در سطوح مختلفی انجام شود؛ از سطوح بسیار ساده و ابتدایی نظیر آموزش‌های والدین به فرزندان، تا سطوح بسیار پیشرفته در سازمان‌های اطلاعاتی و امنیتی.

مسئله اصلی، افزایش سطح آگاهی افراد و آمادگی ذهنی آن‌ها در این موارد است:

۱-۱ آگاهی از وجود خطر: افراد باید این نکته را در ذهن داشته باشند که در هر ارتباط با افراد بیرونی ممکن است در معرض حملات مهندسی اجتماعی باشند. توجه به همین نکته ساده باعث افزایش هوشیاری افراد شده و سبب می‌شود تا اطلاعات شخصی و داخلی که دیگران نیازی به آگاهی از آن‌ها ندارند را به سادگی فاش نسازند.

۱-۲ شناخت اطلاعات حساس: فرهنگ‌سازی و آگاهی‌رسانی به افراد باید به گونه‌ای باشد تا طبقه‌بندی اطلاعات را به آن‌ها بیاموزد. در این صورت، افراد می‌توانند میان اطلاعات حساسی که باید در داخل مجموعه (خانواده، گروه، سازمان و غیره) باقی بماند و اطلاعات معمولی که می‌توان آن‌ها را فاش کرد تمایز قائل شوند. این آموزش‌ها باید توسط افراد خبره

و یا بر اساس دستورالعمل‌های علمی انجام شود؛ چرا که اصلی‌ترین جنبه این آموزش، شناخت صحیح اطلاعات حساس است که نیازمند بررسی‌های علمی و داشتن تجربه است.

۳-۱ حصول اطمینان از صداقت افراد: آخرین نکته‌ای که در مبحث آموزش باید مورد توجه قرار گیرد، آموزش این نکته به افراد است که نباید به سادگی به حرف دیگران اعتماد کرد و باید بدون تعارف و اضطراب، ابتدا از صداقت طرف مقابل (چه در قالب مکالمه شفاهی و چه به صورت رایانامه، پیامک و پیام‌های چندرسانه‌ای) اطمینان حاصل کرد. همین فعالیت ساده، می‌تواند بسیاری از حملات مهندسی اجتماعی را خنثی کند. برای مثال، تحقیقات نشان می‌دهد که متداول‌ترین روش‌ها برای حمله مهندسی اجتماعی به کارمندان یک سازمان، تماس با آن‌ها و معرفی خود به عنوان «کارمند جدید» یا «مسئول جمع‌آوری آمار» از سوی خود سازمان است. اگر هر کارمند در صورت مواجهه با چنین افرادی و پیش از دادن اطلاعات، با یک تماس ساده با مدیر ارشد خود، صداقت حرف فرد مقابل را بررسی کند، اکثر حملات مهندسی اجتماعی به شکست خواهد انجامید.

۲. آگاهی کامل از اطلاعات انتشار یافته

موضوع دیگر، آگاهی افراد در زمان‌های دیگر، به خصوص در زمان انجام فعالیت‌های روزمره و شخصی است. مهاجمانی که با اهداف جدی اقدام به حمله مهندسی اجتماعی می‌کنند، معمولا از قبل افرادی را هدف‌گیری کرده و اقدام به جمع‌آوری اطلاعات در مورد آن‌ها می‌نمایند. در چنین موقعیت‌هایی است که حتی رفتارهای روزمره افراد می‌تولند به عنوان ابزاری برای جلب اعتماد و یا تعیین فرصت مناسب حمله توسط مهاجمین مورد استفاده قرار گیرد. لذا باید آگاهی داشته باشیم که در صحبت‌های روزمره خود با دیگران و یا در شبکه‌های اجتماعی، چه اطلاعاتی را از خودمان (نه از گروه، سازمان یا غیره) منتشر می‌کنیم و به بیانی دیگر، چه اندازه به افراد ناآشنا اجازه می‌دهیم تا ما را بشناسند.

۳. شناختن اطلاعات و داشته‌های خود

شناسایی داشته‌ها و اطلاعات حساس، معمولا به عنوان یکی از فعالیت‌های پایه امنیتی در هر سازمانی انجام می‌شود؛ خواه در سطح کوچک (مثل اطلاعات حساب مالی یک خانواده) و خواه در سطوح پیشرفته (مثل اطلاعات محرمانه و سری یک سازمان اطلاعاتی و نظامی). اما باید توجه داشت که تنها اطلاعات حساس نیست که نیاز به مراقبت و پنهان‌بودن از دیدهای بیرونی دارند؛ چرا که گاهی اوقات با وجود آنکه از اطلاعات اصلی و حساس مراقبت می‌شود، اطلاعات دیگری که به صورت مستقیم حائز اهمیت نبوده و به چشم نمی‌آیند، مورد استفاده مهاجمین مهندسی اجتماعی قرار می‌گیرند.

۴. تدوین سیاست‌های امنیتی

در نهایت، باید توجه داشت که این تلاش‌ها به صورت مدیریت‌شده و سیستماتیک صورت گرفته و در نهایت، سیاست‌های مدونی برای رفتار امن افراد تهیه شده و آگاهی‌رسانی به آن‌ها نیز بر اساس همین سیاست‌های صورت گیرد. تنها در این صورت است که می‌توان اطمینان داشت تلاش‌ها ثمربخش هستند. نکته‌ای که در این خصوص حائز اهمیت است، پای‌بندی افراد به پیروی از سیاست‌ها و دستورالعمل‌ها است. حتی اگر امنیت رایانه‌ای را در دیگر بخش‌ها بتوان با سامانه‌های کنترل دسترسی، دیوار آتش و از این دست ابزارها فراهم کرد، در حوزه مهندسی اجتماعی بدون پای‌بندی افراد و التزام آن‌ها به سیاست‌های امنیتی به هیچ عنوان امکان‌پذیر نیست

جمع بندی:

دقیقاً به این دلیل که حملات مهندسی اجتماعی متکی بر اعتماد مردم هستند، محافظت در برابر آنها فقط با استفاده از ابزارهای فنی ممکن نیست. مفهوم مهندسی اجتماعی هم دقیقاً همین است. یعنی فریب دادن برای کمک به هکرها جهت دور زدن سازوکارهای محافظتی موجود.

با گسترش ترفندهای مهندسی اجتماعی که به عنوان عاملی برای برانگیختن وسوسه انسانی شناخته می‌شوند، پیدا کردن علت ریشه‌ای این حملات می‌تواند مانعی برای به دام افتادن افراد توسط نفوذگران باشد. محققان امنیت سایبری معمولاً استفاده از راهکارهای آموزشی اثربخش کارمندان توسط سازمان‌ها و افزایش مهارت های شخصی را جهت شناسایی و مقابله با حملات مهندسی اجتماعی از جمله عوامل بازدارنده چنین حملاتی می دانند.

مهاجمان سایبری می‌توانند از طریق اوسینت[1] یا منبع هوش آزاد، هر اطلاعاتی را که می‌خواهند در مورد افراد اطلاعات به دست آورند، آنها را ثبت و پالایش کرده و در نهایت نیز گزارش کاملی را از آن فرد داشته باشند. این اطلاعات که با جمع آوری داده های به اشتراک گذاشته شده خود کاربران در شبکه های اجتماعی و وب‌سایت‌های مختلف گردآوری می‌شوند می توانند تمام آنچه که یک مهاجم می‌خواهد را در اختیار وی قرار دهند. بنابراین افراد به نوعی به ارزیابی و تشخیص مخاطره از طریق اوسینت نیاز داشته و می‌بایست آموزش‌هایی را در خصوص آنچه که با دیگران به اشتراک می گذارند ببینند.

با توجه به آنچه که گفته شد، حملات مهندسی نه تنها در طول سال های اخیر کاهش نیافته اند بلکه با بهره گیری از راهکارهای فناورانه، پیچیده تر نیز شده‌اند. از این رو، تمامی افراد باید آموزش های لازم را در خصوص نحوه مقابله با این حملات دیده تا احتمال این مخاطره را تا کمترین حد ممکن کاهش دهند.

قاعدتاً افراد بر اساس آموزش هایی که دیده اند و هوش اجتماعی شان، عکس‌العمل‌های متفاوتی را در برابر حمله مهندسی از خود نشان خواهند داد. البته این را نیز می‌دانیم که افراد مسن‌تر و نسل‌های پیشین نسبت به مخاطرات اورژانسی، مثل مواردی نظیر «باید این کار را انجام بدی یا همین الان اخراج می‌شی» واکنش شدیدتری دارند. در حالی که افراد جوان‌تر، بیشتر مستعد انجام اقدام های احساسی و پاداش گونه هستند؛ برای مثال، «برای دریافت شارژ رایگان ایرانسل بر روی این لینک کلیک کنید» یا «برای دریافت یک سفر رایگان روی این قسمت کلیک کنید» یا مواردی از این قبیل می تواند برای بعضی از اشخاص، وسوسه کننده بوده و آنها را دچار حملات مهندسی اجتماعی کند. بنابراین با توجه به نسلی که با آن سروکار داریم، روش‌های متفاوتی باید اتخاذ شود.

کلام آخر:

باید متذکر شد که یکی از پایه‌های اصلی حمله مهندسی اجتماعی، جمع آوری اطلاعات است. بنابراین مراقب اطلاعاتی که در اینترنت به اشتراک می‌گذارید باشید. اطلاعات منتشر شده توسط خودتان ممکن است علیه شما استفاده شود. یکی دیگر از پایه‌های مهندسی اجتماعی، جلب اعتماد است. هرگز به اشخاصی که در دنیای دیجیتال با آنها گفتگو می‌کنید، ولی آنها را رودررو ندیده‌اید و نمی‌شناسید اعتماد نکنید.

یکی از بهترین کارهایی که یک سازمان می‌تواند به منظور مقابله با حملات مهندسی اجتماعی کارکنانش انجام دهد، ایجاد فرهنگ گزارش‌دهی حوادث است. چرا که اغلب زمان‌ها افراد وقتی کاری را «اشتباه» انجام می‌دهند، از بیان آن احساس شرمساری می‌کنند. آنها ممکن است بر روی یک لینک مخرب کلیک کرده، اطلاعات سازمانی را لو داده و در اختیار افراد غیرمجاز قرار دهند یا موجب ایجاد یک رخنه اطلاعاتی در شبکه‌های اجتماعی و پیام رسان های ارتباطی

---

[1] OSINT.

شـــوند. به همین دلیل نســـبت به بیان آن اندکی خجالت زده و معذب خواهند شـــد. بنابراین اولین گام، ترویج فرهنگ گزارش‌دهی رخدادها در سـازمان اسـت. دومین گام هم برگزاری آموزش‌های مناسـب در جهت ایجاد هوشـیاری و افزایش دانش بصورت مستمر وشخصی است.