مهندسی اجتماعی و راهکارهای مقابله

تهیه شده توسط مدیریت فناوری اطلاعات دانشگاه بوعلی سینا

تیرماه ۱۴۰۳

فهرست مطالب

سخنی با همکاران

حملات مهندسی اجتماعی یکی از بزرگترین تهدیدات امنیتی برای کارکنان دانشگاه و اعضای هیات علمی هستند. این حملات می توانند به سرقت اطلاعات محرمانه، دسترسی غیرمجاز به سیستم ها و حتی فریب کارکنان برای انجام اقدامات مخرب منجر شوند. با توجه به حساسیت اطلاعات و دسترسی های موجود در محیط های دانشگاهی، آموزش کارکنان در زمینه شناسایی و مقابله با این حملات بسیار مهم است. کارکنان باید با تکنیک های مهندسی اجتماعی آشنا شوند و بتوانند به سرعت آنها را تشخیص داده و واکنش مناسب نشان دهند. این آموزش ها می تواند شامل موارد مختلفی از جمله شناسایی تلاش های فیشینگ، مدیریت رمزهای عبور ایمن و آگاهی از سایر حملات احتمالی باشد.

اجرای پروژه سیستم مدیریت امنیت اطلاعات (ISMS) در سال گذشته در سطح دانشگاه نشان داد که متاسفانه در زمینه آگاهی از حملات مهندسی اجتماعی و راهکارهای مقابله با آن، بلوغ کافی وجود ندارد و این مساله، ضرورت آشنایی با این نوع حملات در دانشگاه بوعلی سینا را بیش از پیش مشخص می کند. بر همین اساس، از همکاران، کارکنان و اعضای محترم هیات علمی خواهشمند است، جزوه حاضر را که توسط مدیریت فناوری اطلاعات تهیه و تدوین گردیده است را مطالعه کرده و پس از آن در محیط دانشگاه رعایت فرمایند. امید است که انشاءالله با آگاهی رسانی های بیشتر زمینه امن سازی دانشگاه بوعلی سینا را فراهم آوریم.

۱ مقدمه

در زمینه امنیت اطلاعات، مهندسی اجتماعی عبارت است از «دست‌کاری روان‌شناختی»[۱] (اغوای) افراد برای انجام اقدامات مورد نظر یا افشای اطلاعات. این مفهوم با تعریف مهندسی اجتماعی در علوم اجتماعی که به افشای اطلاعات محرمانه مربوط نمی‌شود، متفاوت است. به دیگر سخن، مهندسی اجتماعی ترفندهایی برای جمع‌آوری اطلاعات، تقلب یا دسترسی به سیستم است که با یک کلاه‌برداری سنتی متفاوت است زیرا اغلب یکی از چندین مرحله موجود در یک طرح کلاه‌برداری پیچیده‌تر است. در مهندسی اجتماعی معمولاً بدون اینکه فرد درکی از آنچه در حال رخ دادن است داشته باشد به نوعی متقاعد شده و یا فریب می‌خورد که اطلاعاتی را افشا کند. این کار ممکن است با استفاده و یا بدون استفاده از فناوری رخ دهد.

مهندسی اجتماعی، تاکتیکی بسیار رایج در حملات امروزی است و مشتریان و کاربران تجاری در معرض این حملات هستند؛ بنا بر مطالعه‌ای[۲] که در سال ۲۰۱۳ توسط TNS Global و شرکت امنیت ایمیل هالون انجام شد، ۳۰ درصد از کاربران آمریکایی مشتاقانه ایمیل‌های مخرب را باز می‌کنند؛ حتی زمانی که می‌دانند که لینک مخرب است. اگرچه این نکته عجیب به نظر می‌رسد، اما روندها و الگوهای روان‌شناختی ثابت‌شده‌ای وجود دارد که این واقعیت را توجیه می‌کند. همچنین مطالعات و نمونه‌های بیشتری نیز این موضوع را نشان داده‌اند که در اینجا به برخی از آمارهای جالب توجه از یکی از این مطالعات[۳] اشاره می‌کنیم:

- ۹۴ درصد بدافزارها از طریق ایمیل منتشر می‌شوند.
- حملات فیشینگ بیش از ۸۰ درصد از حوادث امنیتی گزارش‌شده را تشکیل می‌دهند.
- در هر دقیقه ۱۷۷۰۰ دلار به دلیل حملات فیشینگ از دست می‌رود.

اگرچه کاربران دائماً طعمه این موضوع می‌شوند، آنچه بسیاری از مطالعات نشان می‌دهند این است که همین افراد در محل کار نیز به همان اندازه آسیب‌پذیر هستند. این روند نگران‌کننده‌ای است که گروه‌های امنیتی برای رسیدگی به آن کوشش می‌ورزند و آزمون‌های نفوذ مهندسی اجتماعی نشان می‌دهند که سازمان‌ها باید زمان بیشتری را برای آموزش آگاهی‌های امنیتی اختصاص دهند.

امروزه مهاجمان، روش‌های خود را برای مهندسی اجتماعی پیشرفته‌تر کرده‌اند؛ به این صورت که با به دست آوردن اطلاعات دقیق از هدف خود از منابع مختلف مانند شبکه‌های اجتماعی، پیام‌هایی به طور خاص برای هدف ارسال می‌کنند که موجب فریب ایشان می‌گردد. مثلاً ایمیلی ارسال می‌کنند که فرد مورد نظر را با نام کامل خطاب می‌کند و حاوی اطلاعاتی است که دریافت‌کننده را به این باور می‌رساند که ارسال‌کننده از هویت وی اطلاع دارد.

---

[۱] Psychological manipulation

[۲] http://www.csoonline.com/article/2133877/social-engineering/social-engineering--study-finds-americans-willingly-open-malicious-emails.html

[۳] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-andstatistics.html

۲ روانشناسی مهندسی اجتماعی

در این بخش، برخی از اصول روانشناسی کلیدی را که برای شناخت و پیشگیری از مهندسی اجتماعی باید در نظر داشت، پوشش داده می‌شود. اگر چه مطالب این بخش به صورت عمیق به روانشناسی متقاعدسازی و اغوای افراد نمی‌پردازد، اما به درک نکات کلیدی این حوزه کمک می‌کند.

۲-۱ اصول متقاعدسازی از نظر دکتر رابرت چالدینی

بسیاری معتقدند که دکتر رابرت چالدینی[۱]، روانشناس آمریکایی، پدر تحقیقات در حوزه متقاعدسازی انسانی است که مستقیماً با فعالیت‌های درگیر در مهندسی اجتماعی مرتبط است. دکتر چالدینی انواع مختلفی از رفتارهای انسانی را مورد مطالعه قرار داد، اما بر ویژگی‌های طبیعت انسان که بیشتر مستعد دست‌کاری و اغوا بود، تمرکز کرد. ایشان در کتاب خود به نام «تأثیر: روانشناسی متقاعدسازی»[۲] اصول عمده‌ای را بیان می‌کند که اساس بسیاری از نحوه تأثیرگذاری ما بر افراد را تشکیل می‌دهند. این اصول در مورد همه انواع متقاعدسازی صدق می‌کند، از فروشنده‌ای که می‌داند چگونه قرارداد موفقی داشته باشد تا کارمندی که در حال مذاکره برای افزایش حقوق است و یا یک مهندس اجتماعی که تلاش می‌کند شما را وادار کند روی یک پیوند کلیک کنید یا اطلاعات شخصی خود را از طریق تلفن را افشا کنید.

در ادامه این بخش، کار دکتر چالدینی را از دیدگاه یک مهندس اجتماعی حرفه‌ای مورد بحث قرار می‌دهیم. او شش اصل را ارائه کرده است که با الگوهای رفتاری انسانی مرتبط با متقاعدسازی مرتبط است. چه چیزی باعث می‌شود افراد به آن توجه کنند؟ چگونه می‌توان آنها را متقاعد کرد که اطلاعات خود را در اختیار یک مهندس اجتماعی قرار دهند؟ مهندسان اجتماعی چگونه باید رفتار کنند و کمپین‌های آنها باید شامل چه ویژگی‌های ایده‌آلی باشند تا حساسیت به مهندسی اجتماعی را به حداکثر برسانند؟

۲-۱-۱ اصل نخست: معاوضه

اولین اصل که «معاوضه» نام دارد به طور خلاصه به این معنی است که مردم وقتی کاری برای آنها انجام می‌دهند احساس بدهکاری می‌کنند و اغلب اطلاعاتی را ارائه می‌دهند یا فعالیت‌های نمادینی را برای پرداخت «بدهی» انجام می‌دهند. نکات ظریف زیادی در این اصل وجود دارد. اولاً، تنها ارائه چیز خوبی به کسی، حتی اگر در نهایت آن را نیز دریافت نکند، می‌تواند برای ایجاد احساس بدهکار شدن کافی باشد. دوم، آنچه که مهندسی اجتماعی درخواست می‌کند باید متناسب با آنچه داده شده یا ارائه شده باشد؛ شما نمی‌توانید پیشنهاد دهید که در را برای کسی نگه دارید و سپس انتظار داشته باشید که شماره حساب بانکی خود را به شما بدهد. با این حال، می‌توانید انتظار داشته باشید که در ازای آن (در برخی موارد) یا چیزی مشابه، درب دوم را برای شما نگه دارند. این تکنیک همیشه توسط مهندسان اجتماعی و مجرمان به طور یکسان استفاده می‌شود. یکی از معروف‌ترین نمونه‌های این اصل در عمل، کمپین کلاسیک هرزنامه[۳] معروف به «شاهزاده نیجریه» است؛ به این معنی که ایمیلی دریافت می‌شود که ادعا می‌کند از طرف فرد ثروتمندی است که در موقعیت ناخوشایندی قرار گرفته است و باید مقدار زیادی پول را به سرعت از حسابش خارج کند. این شخص به کمک گیرنده نیاز دارد که باید مشخصات بانکی را برای انتقال پول به آن ارائه دهد که مبلغ یا درصدی از پول در ازای این جابجایی به او تعلق می‌گیرد. آنها درخواست کمک می‌کنند، اما دادن پول به شما باعث می‌شود که شما خود را مدیون آنها تصور کنید. البته، هیچ پولی در کار نیست - این فقط یک کلاه‌برداری برای دریافت جزئیات

---

[۱] Robert Cialdini

[۲] Influence: The Psychology of Persuasion

[۳] Spam

حساب بانکی است. مثال‌های ظریف‌تری که در تمرین‌های مهندسی اجتماعی وجود دارند عبارت‌اند از جلب توجه به نفس[1] شخص یا دادن یک هدیه یا نشانه کوچک. مثال اول ممکن است به شکل یک ایمیل سفارشی باشد که می‌پرسد آیا فرد علاقه‌مند به سخنرانی در یک کنفرانس یا شرکت در یک رویداد معتبر هست. برای اطلاع از آن، گیرنده باید روی یک پیوند کلیک کند یا یک پیوست را باز کنند. مورد دوم ممکن است در یک نمایشگاه تجاری اتفاق بیفتد به این صورت که فروشنده یک درایو USB رایگان را به شما می‌دهد اما قبل از ارائه آن، آدرس ایمیل و اطلاعات تماس شما را برای پیگیری می‌خواهد. یک مثال عالی در این زمینه، آزمایشی است که در سال ۲۰۰۴ در بریتانیا انجام شد که در طی آن، محققان تکه‌ای شکلات را به مسافرانی که رمز عبور خود را می‌دادند، پیشنهاد دادند و بیش از ۷۰٪ این کار را انجام دادند.

۲-۱-۲ اصل دوم: اثبات اجتماعی

اصل دوم، «اثبات اجتماعی» به این موضوع مربوط می‌شود که چطور انسان‌ها وقتی نمی‌دانند چگونه رفتار کنند یا واکنش نشان دهند، به دنبال اطمینان هستند. بیشتر مردم مانند دیگران رفتار می‌کنند؛ اگر بخشی از یک گروه همتا باشند به ویژه زمانی که رفتار رهبران یا کسانی که در موقعیت‌های قدرت یا صاحب اختیار هستند را ببینند، این رفتارها را تقلید می‌کنند.

برای مثال، ایمیل‌هایی که کاربر را برای انجام دادن کاری (مثلاً کلیک کردن روی لینک یا باز کردن یک فایل) فریب می‌دهند، می‌توانند به‌گونه‌ای جعل شوند که به نظر برسد از طرف کسی در گروه همتایان هدف یا گروه دیگری مرتبط با او باشد و همین امر می‌تواند احتمال موفقیت حمله را افزایش دهد. اگر سایر افراد در گروه همتایان یا یک گروه مرتبط همگی از یک برنامه یا فناوری خاص استفاده کنند، حمله‌ای هدفمند که از «فشار همتایان» برای استفاده از همان فناوری یا برنامه (شاید با یک لینک به برنامه در ایمیل) استفاده می‌کند، ممکن است موفق‌تر باشد. همچنین مهاجم می‌تواند از هنجارهای گروهی مانند سیگار کشیدن در بیرون یا رفتن به یک کافی‌شاپ خاص در نزدیکی برای هدف قرار دادن و به خطر انداختن قربانی استفاده نماید.

این روش نیازمند شخصی‌سازی است، به این معنی که نفوذگر باید کمی تحقیق کند. برای ایجاد تکنیک‌های فشار قانع‌کننده از طریق همکاران، دوستان و سایر نزدیکان، نفوذگران باید در مورد آنها و رفتارهایشان اطلاعات کسب کنند.

۲-۱-۳ اصل سوم: تعهد و ثبات

اصل سوم چالدینی، تعهد و ثبات است. اگر کسی به طور شفاهی یا کتبی با انجام کاری موافقت کند، به احتمال زیاد آن را انجام خواهد داد. این کار الزاماً نباید یک‌باره اتفاق بیفتد - موافقت‌های کوچک و تدریجی برای انجام کارها در نهایت می‌تواند منجر به درخواست مهاجم برای تعهد بزرگ‌تری شود که ممکن است در آینده اتفاق بیفتد. به طور معمول، درخواست تعهد بزرگ بلافاصله ممکن است باعث سوءظن شود، بنابراین مهاجمان محتاط ابتدا تعهد کوچکی (کلیک کردن روی یک لینک) را درخواست می‌کنند و به سمت تعهد بزرگ‌تر (ارائه دادن اطلاعات حساس) حرکت می‌نمایند. ثبات فقط یک ویژگی انسانی است. ما تمایل داریم الگوها و عادت‌ها را در زندگی روزمره دنبال کنیم؛ هر روز در صورت امکان در یک مکان پارک می‌کنیم، در همان رستوران‌ها غذا می‌خوریم و در زمان‌های مشخصی ایمیل خود را بررسی می‌کنیم. مهاجمان می‌توانند این الگوها را یاد بگیرند و از آنها سوءاستفاده کنند. کِوین میتنیک[2] به خاطر این سبک حمله مشهور بود. او به طور مرتب با افراد تماس می‌گرفت (ایجاد ثبات) و سپس به تدریج درخواست لطف‌های کوچکی می‌کرد. در نهایت، او به آنچه از آنها می‌خواست می‌رسید.

[1] Ego

[2] Kevin Mitnick

۲-۱-۴ اصل چهارم: علاقه‌مندی

این اصل چالدینی به نسبت ساده است – مردم تمایل دارند به افرادی که از نظر ظاهری برایشان جذابیت دارند یا کسانی که از برخی جهات به آنها شباهت دارند، علاقه‌مند شوند. برای استفاده از این اصل، نفوذگران سایبری نیاز دارند تا رابطه‌ای دوستانه با هدف برقرار کنند. این یکی از مؤثرترین تکنیک‌ها برای مهندسی اجتماعی موفق است و نکته کلیدی آن این است که کاری کنید افراد شما را دوست داشته باشند. برای این کار، مهاجم در مورد علایق و سرگرمی‌های هدف خود تحقیق می‌کند و آنها را به زبان خودشان بازگو می‌کند. این کار نیاز به تمرین دارد. همچنین می‌توان از افراد تعریف کرد، البته باید توجه داشت که این کار ظرافت‌های خاصی دارد، زیرا تعریف بیش از حد باعث می‌شود که هدف به فرد مهاجم مشکوک شود یا حرف‌هایش را نادیده بگیرد. هرچند ممکن است کلیشه‌ای به نظر برسد، اما گاهی اوقات کلید اینکه افراد شما را دوست داشته باشند این است که تا حد ممکن شبیه آنها باشید. شباهت ممکن است به معنای لباس پوشیدن به سبک خاص، رفتار به شیوه‌ای معین یا استفاده از نوع خاصی از زبان باشد.

۲-۱-۵ اصل پنجم: اقتدار

اصل پنجم چالدینی، اصل اقتدار است. به‌کارگیری این اصل برای نفوذگران سایبری نیازمند ظرافت بیشتری است. اعمال آشکار اقتدار در بسیاری از فرهنگ‌های غربی می‌تواند نتیجه عکس داشته باشد. برای مثال، تماس با هدف و گفتن این جمله که «سلام، من رئیسِ رئیسِ رئیس شما هستم، حالا رمز عبور این کاربر را به من بده!» به طور کامل با شکست مواجه خواهد شد. با این حال، روش‌های زیادی برای استفاده ظریف از اصل اقتدار وجود دارد. به عنوان مثال، لباس پوشیدن مرتب یا رانندگی با یک ماشین لوکس ممکن است به راحتی روی افراد تأثیر بگذارد و آنها را به این باور برساند که شما فرد مهمی هستید. این کار در برخی موارد می‌تواند به راحتی مهاجم را از سد منشی یا نگهبانان عبور دهد.

در تماس‌های تلفنی و ایمیل‌ها، زبانی که مهاجم استفاده می‌کند و نحوه ارائه سناریوی مورد نظر، ممکن است بر روی هدف تأثیر بگذارد. یک رویکرد ظریف‌تر ممکن است کارساز باشد. در واقع، برخی از موفق‌ترین تلاش‌های مهندسی اجتماعی، مواردی هستند که به طور غیرمستقیم به اقتدار اشاره می‌کنند. برای مثال، «رئیسم قبل از پایان روز به X نیاز دارد... آیا می‌توانید کمک کنید؟» در این مورد، اشاره به شخصیت‌های با اقتدار که ضرب‌الاجل تعیین می‌کنند، ممکن است بر روی هدف تأثیر بگذارد – چه کسی یک رئیسِ سلطه‌گر را که در مدت کوتاهی خواستار چیزهایی است، درک نمی‌کند؟

۲-۱-۶ اصل ششم: کمیابی

اصل کمیابی چالدینی درک ساده‌ای دارد، اما اجرای آن در مهندسی اجتماعی دشوارتر است. همه ما چیزهایی را می‌خواهیم که دیگران دارند و ما نداریم. با کمی زیرکی می‌توان به راحتی از این موضوع سوءاستفاده کرد. برای مثال، ایمیلی که یک «پیشنهاد با زمان محدود» یا «محصولات اپل قبل از انتشار رسمی» را ارائه می‌دهد، می‌تواند توجه قابل توجهی را جلب کند، حتی اگر به نظرمان این موضوع سطحی و غیرقابل باور باشد.

موضوعی دیگر مرتبط با کمیابی، فشار زمان است. گاهی اوقات، برای انجام یک کار خاص در یک بازه زمانی کوتاه، مهاجم، هدف را ترغیب کرده یا تحت فشار قرار می‌دهد. بسته به سناریو، از پاداش یا تنبیه ممکن است برای ترغیب اهداف به انجام عمل مورد نظر استفاده کند.

۲-۲ پنج اصل کلیدی مهندسی اجتماعی از دیدگاه کریس هدناگی

کریس هَدناگی[۱]، مهندس اجتماعی و متخصص تست نفوذ فیزیکی مشهور جهان، کتابی با عنوان «مهندسی اجتماعی: هنر هک کردن انسان»[۲] نوشته است. هدناگی در کتاب خود، پنج اصل کلیدی نفوذ و ترغیب را شرح می‌دهد که همسو با اصول کلاسیک چالدینی هستند. این اصول که مهاجمان سایبری از آنها برای مهندسی اجتماعی استفاده می‌کنند عبارت‌اند از:

- **تعیین اهداف مشخص:** هنگام تلاش برای مهندسی اجتماعی یک فرد، حتماً برنامه‌ای داشته باشید. برای مثال، صرفاً در محل هدف حاضر نشوید و به شانس تکیه نکنید. بدانید که برنامه شما این است که وارد یک ناحیه خاص شوید، به دنبال کارمندان در ورودی مشخصی حرکت کنید و غیره.
- **ایجاد ارتباط دوستانه:** برقراری ارتباط دوستانه با افراد، کلید به دست آوردن خواسته‌های شماست که همیشه یک هدف در مهندسی اجتماعی است. در ادامه این نوشتار بیشتر در این مورد صحبت خواهد شد.
- **مراقب محیط اطراف خود باشید:** به ویژه در مهندسی اجتماعی حضوری، لازم است به دقت به افراد، رفتارها، شرایط خاص محل و غیره توجه کنید. برای مثال، شناسایی کافی را روی یک مکان فیزیکی انجام داده‌اید و می‌دانید که می‌خواهید چه کسی را تعقیب کنید. فرض کنید زمانی که در حال اقدام هستید، ناگهان دو ماشین پلیس به طور کاملاً اتفاقی درست جلوی در ورودی متوقف می‌شوند؛ در این حالت، بهتر است صبر کنید یا رویکرد دیگری را امتحان کنید تا لو نروید.
- **انعطاف‌پذیر باشید:** هرگز فقط یک رویکرد نداشته باشید! مهندسین اجتماعی موفق می‌دانند که انعطاف‌پذیری با افراد و شرایط متغیر، کلید دستیابی به اهداف است.
- **با خودتان (احساسات) ارتباط برقرار کنید:** اگرچه این مورد کمی مبهم به نظر می‌رسد، اما در واقع یک اصل بسیار ساده است. همه افراد، از جمله مهندسان اجتماعی، متفاوت هستند. تمایلات و عادات خود را بشناسید و در طول تعاملات آنها را در نظر بگیرید. برای مثال، اگر شخصیت بیش‌فعالی دارید، اما قصد ورود به یک محیط اداری بسیار آرام و بدون استرس را دارید، باید قبل از ورود تلاش کنید تا آرام شوید و خونسرد به نظر برسید.

[۱] Chris Hadnagy

[۲] Social Engineering: The Art of Human Hacking

۳ انواع حملات مهندسی اجتماعی

همان طور که پیش‌تر توضیح داده شد، حملات مهندسی اجتماعی از طریق فریب و سوءاستفاده از روانشناسی انسان برای وادار کردن قربانیان به انجام اقداماتی که به نفع مهاجم است، انجام می‌شوند. این اقدامات می‌تواند شامل لو دادن اطلاعات شخصی، نصب بدافزار یا انجام سایر اقداماتی باشد که به مهاجم اجازه می‌دهد به سیستم‌ها یا شبکه‌های شما دسترسی پیدا کند.

این حملات بسیار متنوع و پیچیده هستند و می‌توانند اشکال مختلفی به خود بگیرند. در این بخش، به برخی از رایج‌ترین انواع حملات مهندسی اجتماعی و نحوه عملکرد آنها می‌پردازیم.

۳-۱ فیشینگ[۱]

فیشینگ رایج‌ترین نوع حمله مهندسی اجتماعی است. در این نوع حمله، مهاجم سعی می‌کند با ارسال ایمیل، پیام کوتاه یا پیامی از طریق رسانه‌های اجتماعی که به نظر می‌رسد از منبعی معتبر مانند بانک یا وب‌سایت مورد علاقه هدف ارسال شده است، وی را فریب دهد. ایمیل یا پیام جعلی معمولاً حاوی لینکی است که دریافت‌کننده را به وب‌سایتی تقلبی هدایت می‌کند که شبیه به وب‌سایت واقعی است. هنگامی که دریافت‌کننده روی لینک کلیک می‌کند و اطلاعات شخصی خود را در وب‌سایت تقلبی وارد می‌کند، مهاجم می‌تواند به این اطلاعات دسترسی پیدا کرده و از آن برای اهداف مخرب مانند سرقت هویت یا کلاه‌برداری مالی استفاده کند. نمونه‌ای از ایمیل فیشینگ در شکل ۱ نشان داده شده است. مثال مورد استفاده در این شکل، مسئله‌ای در خصوص سرویس‌های ویژه گوگل مطرح می‌کند در حالی که از سوی یک آدرس عادی جیمیل ارسال شده است که نشان می‌دهد که از طرف کاربری عادی است و نه گوگل.

---------- Forwarded message ----------
From: **account iran** <kerioserver42@gmail.com>
Date: 2013/4/22
Subject: فرصت محدود برای استفاده از سرویس ویژه گوگل
To:

برای رهایی از فیلتر و چک کردن گروپ های خود در جیمیل کافی است از طریق سرور های جدید گوگل که ویژه کشور هایی مثل ایران که در تحریم است راه اندازی شده است به منظور ارایه سرویس و افزایش امار بازدید کنندگان.

تنها کافی است از طریق لینک زیر وارد جیمیل و گروپ های خود شوید.پس از ورود ظرف مدت 24ساعت کد فعال سازی توسط سرورهای گوگل برای شما ارسال میشود.و اکانت شما برای استفاده از این سرویس جیمیل اماده میشود.

*لطفا توجه فرمایید از public نمودن سرور ها ما به منظور ایجاد نشدن ترافیک سنگین خودداری نمایید.

در صورت بلوک گردیدن سرورها سریعا مسیر جدید برای شما ایمیل میشود.

برای ورود بر روی لینک زیر کلیک نمایید:

account.google.com

برای گروپ ها بر روی لینک زیر کلیک نمایید:

group.google.com

idehalTech

شکل ۱: نمونه از یک ایمیل فیشینگ

[۱] Phishing

۳-۲ شکار نهنگ[۱]

شکار نهنگ (والینگ) نوعی حمله فیشینگ است که به طور خاص مدیران ارشد و سایر افراد مهم را هدف قرار می‌دهد. مهاجمان برای انجام این نوع حمله، تحقیقات بیشتری در مورد قربانی خود انجام می‌دهند تا ایمیل‌ها یا پیام‌های شخصی‌سازی شده‌ای را ارسال کنند که به احتمال زیاد مورد توجه قربانی قرار می‌گیرند. به عنوان مثال، مهاجم ممکن است ایمیلی ارسال کند که به نظر می‌رسد از مدیرعامل شرکت شما ارسال شده است و از شما می‌خواهد که اطلاعات مالی حساسی را به اشتراک بگذارید.

۳-۳ چیزی در ازای چیزی[۲]

در این نوع حمله، مهاجم با وعده ارائه یک سرویس مطلوب (مانند پشتیبانی فنی جعلی) از قربانی درخواست اطلاعات حساس می‌کند. به عنوان مثال، مهاجم ممکن است با تماس تلفنی ادعا کند که از بخش فناوری اطلاعات سازمان شما است و برای حل مشکلی جعلی به اطلاعات ورود به سیستم شما نیاز دارد.

۳-۴ بهانه‌تراشی[۳]

این نوع حمله شامل ساختن سناریوهای باورپذیر یا «بهانه‌هایی» است که به احتمال زیاد قربانیان را متقاعد می‌کند تا داده‌های ارزشمند و حساس را به اشتراک بگذارند. نمونه‌هایی از این بهانه‌ها شامل کلاه‌برداری‌های عاشقانه یا «کشتار خوک»[۴] (کسب وجوه از طریق فریب و سوءاستفاده عاطفی) می‌شود. در کلاه‌برداری کشتار خوک، کلاه‌بردار با قربانی رابطه‌ای عاطفی برقرار می‌کند و به مرور زمان اعتماد او را جلب می‌کند. هنگامی که کلاه‌بردار احساس کرد که قربانی به اندازه کافی به او وابسته شده است، از او پول یا اطلاعات شخصی درخواست می‌کند. این درخواست‌ها می‌تواند به صورت وام، هدیه یا سرمایه‌گذاری باشد.

۳-۵ فیشینگ پیامکی[۵]

این نوع حمله مهندسی اجتماعی به طور خاص از طریق پیام‌های SMS انجام می‌شود. در این حمله، کلاه‌برداران سعی می‌کنند کاربر را فریب دهند تا روی لینکی کلیک کند که او را به یک وب‌سایت مخرب هدایت می‌کند و بدافزار و محتوای مخرب را دانلود می‌کند. نمونه‌ای از این نوع فیشینگ در شکل ۲ و همچنین شکل ۳ آمده است. با توجه به آدرس فرستنده، اطلاعاتی که در متن پیام به آنها اشاره کرده و یا مواردی که از قلم انداخته است و نیز لحن پیام و لینکی که در آن نهاده شده است و مواردی دیگر می‌توان جعلی بودن این گونه پیام‌ها را تشخیص داد که در بخش‌های بعدی توضیح داده می‌شوند.

---

[۱] Whaling

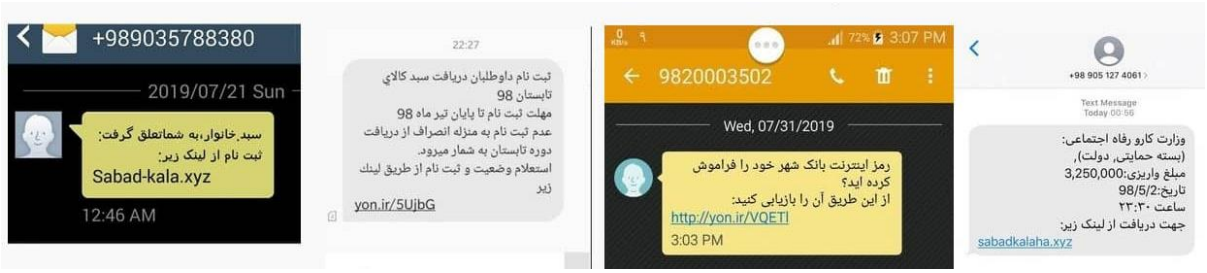
[۲] Quid pro quo

[۳] Pretexting

[۴] Pig butchering scam

[۵] SMS-phishing (Smishing)

شکل ۲: نمونه از یک فیشینگ پیامکی



شکل ۳: نمونه پیامک‌های جعلی با لینک‌های تقلبی

۳-۶ فیشینگ صوتی[۱]

در این نوع حمله از تماس‌های تلفنی برای فریب قربانیان و وادار کردن آنها به ارائه اطلاعات حساس استفاده می‌شود. مهاجم ممکن است وانمود کند که از بانک یا یک سازمان دولتی تماس می‌گیرد و با ایجاد حس فوریت یا اضطرار، قربانی را فریب دهد تا اطلاعات شخصی مانند شماره‌حساب یا رمز عبور خود را فاش کند.

یک نمونه از این نوع فیشینگ، حمله انجام شده به بیماران بیمارستان‌های نبراسکا است. در گزارش‌ها آمده است که کلاه‌بردارانی با ادعای نماینده بودن از بیمارستان‌های ایالتی با آنها تماس می‌گیرند. این اتفاقات پس از حمله باج افزار[۲] به شرکت Change Healthcare (زیرمجموعه Optum) در تاریخ ۲۹ فوریه ۲۰۲۴ رخ داده که باعث خارج شدن این شرکت از دسترس شده است.

[۱] Voice phishing (Vishing)

[۲] باج‌افزار (Ransomware) نوعی بدافزار است که تمامی اطلاعات روی دستگاه را با رمزگذاری از دسترس کاربر خارج کرده و در ازای ارائه کلید رمزگشایی، تقاضای باج می‌کند.

انجمن بیمارستان‌های نبراسکا در تاریخ ۴ مارس ۲۰۲۴ با انتشار اطلاعیه‌ای عمومی در لینکدین اعلام کرد: «کلاه‌برداران به بیماران اطلاع می‌دهند که در صورت ارائه شماره کارت اعتباری، مستحق بازپرداخت کامل هستند.»

۳-۷ ترس‌افزار[۱]

ترس‌افزار نوعی بدافزار است که با استفاده از مهندسی اجتماعی، احساس ترس، اضطراب یا تهدید را در کاربر ایجاد می‌کند تا او را به انجام اقداماتی خاص، خرید نرم‌افزارهای ناخواسته یا فاش کردن اطلاعات شخصی وادار کند. این نوع بدافزار از طریق روش‌های مختلفی مانند باز کردن پیوست‌های آلوده، کلیک بر روی لینک‌های فریبنده یا دانلود نرم‌افزارهای جعلی وارد سیستم قربانی می‌شود. پس از نفوذ، با نمایش پیام‌های هشدار جعلی، پاپ‌آپ‌های آزاردهنده و تصاویر گرافیکی ترسناک بر روی صفحه‌نمایش، سعی می‌کند به کاربر القا کند که سیستم او به شدت آلوده شده و در معرض خطر قریب‌الوقوع قرار دارد. ترس‌افزار با بزرگنمایی خطرات و القای حس فوریت، کاربر را به انجام اقداماتی خاص مانند خرید نرم‌افزارهای ضد بدافزار جعلی، تماس با پشتیبانی فنی دروغین یا ورود به وب‌سایت‌های آلوده ترغیب می‌کند. در نهایت، هدف اصلی ترس‌افزار، سرقت اطلاعات شخصی و محرمانه کاربر مانند اطلاعات بانکی، رمز عبور و اطلاعات تماس است. این اطلاعات می‌توانند برای کلاه‌برداری مالی، سرقت هویت و سایر مقاصد مجرمانه مورد سوءاستفاده قرار گیرند.

۳-۸ حمله آبشخور[۲]

حمله آبشخور نوعی حمله مهندسی اجتماعی است که در آن مهاجمان با هدف فریب افراد و سرقت اطلاعات یا دسترسی به سیستم‌ها از منابعی که حدس می‌زنند مورد اعتماد قربانیان است سوءاستفاده می‌کنند. این منابع می‌توانند شامل وب‌سایت‌ها، برنامه‌ها یا حتی افراد باشند.

در این حمله، مهاجمان ابتدا طعمه‌های خود را شناسایی می‌کنند. این افراد می‌توانند شامل کارمندان یک شرکت، مشتریان یک بانک یا حتی کاربران یک شبکه اجتماعی باشند. سپس طعمه‌ای جعلی ایجاد می‌کنند که شبیه به منبع مورد اعتماد قربانیان است. این طعمه می‌تواند شامل یک وب‌سایت جعلی؛ برای نمونه، وب‌سایتی که کارمندان بیشتر از آن استفاده می‌کنند و به آن اعتماد دارند، یک برنامه آلوده یا حتی یک ایمیل فیشینگ باشد. مهاجمان، طعمه جعلی را به گونه‌ای طراحی می‌کنند که قربانیان را به کلیک کردن روی آن یا دانلود آن تشویق می‌کند. هنگامی که قربانیان با طعمه جعلی تعامل دارند، اطلاعات شخصی یا دسترسی به سیستم‌های آنها به خطر می‌افتد.

برای مثال، فرض کنید مهاجمان می‌خواهند اطلاعات شخصی کارمندان یک شرکت را سرقت کنند. آنها می‌توانند با انجام مراحل زیر این کار را انجام دهند:

۱. شناسایی طعمه: مهاجمان ابتدا وب‌سایت شرکت را شناسایی می‌کنند و آدرس ایمیل کارمندان را از طریق روش‌های مختلف مانند جستجوی آنلاین یا هک کردن پایگاه داده شرکت به دست می‌آورند.
۲. ایجاد طعمه: مهاجمان سپس یک وب‌سایت جعلی شبیه به نمونه اصلی شرکت ایجاد می‌کنند. این وب‌سایت جعلی ممکن است حاوی یک فرم ورود به سیستم باشد که از کارمندان برای وارد کردن اطلاعات شخصی خود مانند نام کاربری و رمز عبورشان درخواست می‌کند.
۳. فریب قربانی: مهاجمان یک ایمیل فیشینگ که شامل لینکی به وب‌سایت جعلی است را به کارمندان شرکت ارسال می‌کنند که در آن از آنها خواسته می‌شود برای مشاهده اطلاعیه مهمی به وب‌سایت شرکت مراجعه کنند.

---

[۱] Scareware

[۲] Waterholing

۴. سرقت اطلاعات: هنگامی که کارمندان روی لینک کلیک می‌کنند و به وب‌سایت جعلی هدایت می‌شوند، اطلاعات شخصی خود را در فرم ورود به سیستم وارد می‌کنند. مهاجمان می‌توانند از این اطلاعات برای سرقت هویت، دسترسی به حساب‌های بانکی یا سایر اقدامات مجرمانه استفاده کنند.

۹-۳ تله گذاری[۱]

تله گذاری نوعی حمله مهندسی اجتماعی است که از انگیزه یا پیشنهادی جذاب برای فریب قربانی به انجام یک اقدام ناامن استفاده می‌کند. به عنوان مثال، مهاجم ممکن است یک حافظه USB آلوده را در مکانی عمومی رها کند و منتظر بماند تا کسی آن را پیدا کند و نصب کند. هنگامی که قربانی حافظه USB را به کامپیوتر خود متصل می‌کند، بدافزار موجود در آن می‌تواند کامپیوتر او را آلوده کند. یک نمونه پیچیده از این نوع حمله توسط گروه هکری Lazarus کره شمالی بود. مهاجمان با ایجاد پروفایل‌های جعلی، ارسال ایمیل‌های هدفمند با پیوست‌های آلوده، اطلاعات حساس را از شرکت‌های دفاعی و دولتی سرقت می‌کردند. نمونه از این حمله به این صورت است:

قربانی: شما چه چیزی برای ارائه دارید؟

مهاجم: ما می‌توانیم شغل رؤیایی خود را که می‌خواهید به شما ارائه دهیم.

قربانی: پیشنهاد شما چه چیزی دارد که آن را متمایز می‌کند؟

مهاجم: شاید حقوق خیلی بیشتری دریافت کنید.

قربانی: چه شغلی را پیشنهاد می‌کنید؟

مهاجم: مدیر عملیات قانونی در MUT Aero Engines.
(شرح شغل به زبان آلمانی)

قربانی: آن را برایتان به انگلیسی ترجمه می‌کنم.
آدرس ایمیلتان چیست؟

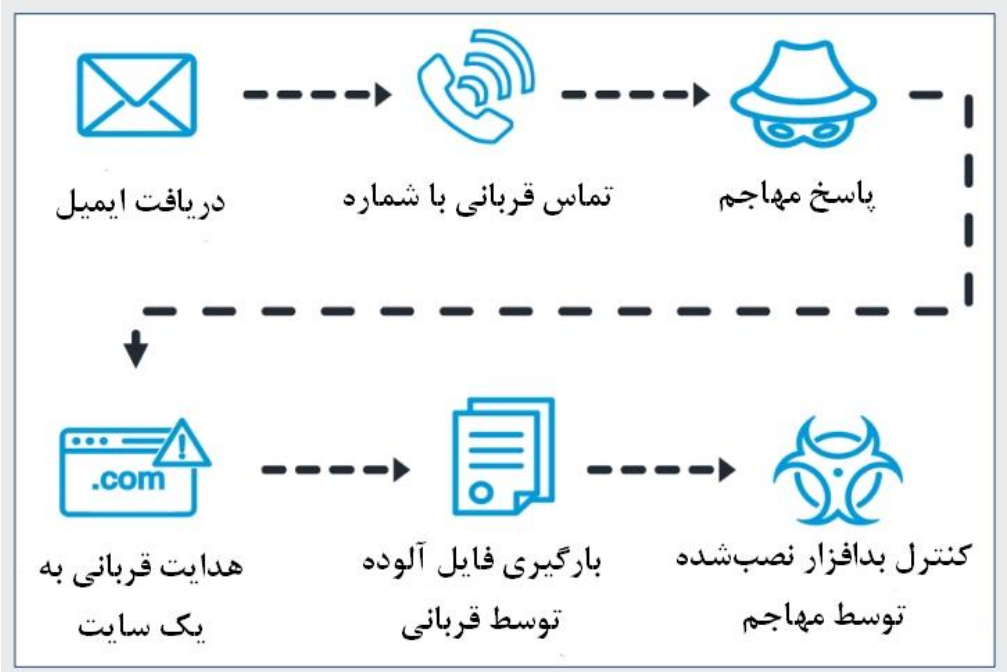
مهاجم: (آدرس ایمیل)

۱۰-۳ حملات تلفن محور[۲]

گونه دیگر حملات مهندسی اجتماعی، حملات تلفن محور (TOAD) نوع جدیدی از فریب آنلاین هستند که در آن، مجرمان سایبری با برقراری تماس تلفنی با افراد، سعی در سرقت اطلاعات شخصی یا نصب بدافزار بر روی سیستم آنها دارند. این روش، ممکن است طعمه را از طریق ایمیل فریب دهد و سپس او را به تماس با یک مرکز تماس تقلبی که توسط مجرمان سایبری اداره می‌شود، هدایت کند. نحوه عملکرد حملات TOAD همان طور که در شکل ۴ نشان داده شده است به این شرح است:

[۱] Baiting

[۲] Telephone-Oriented Attack Delivery (TOAD)

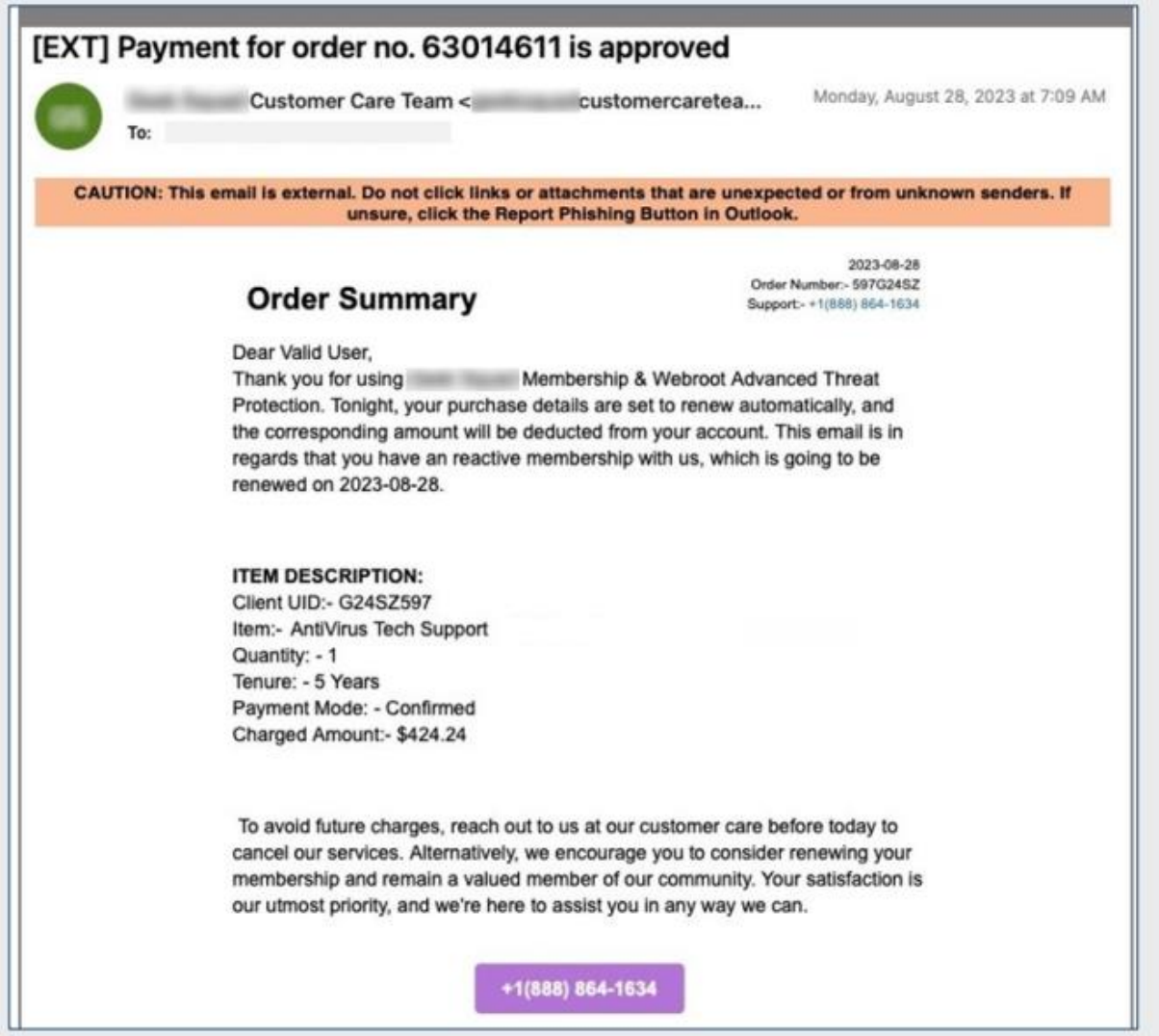


شکل ۴) نمای کلی زنجیره یک حمله معمول TOAD برای نصب بدافزار در سیستم قربانی

- مجرمان سایبری، ایمیلی جعلی ارسال می‌کنند که به نظر می‌رسد از یک شرکت یا سازمان معتبر مانند بانک، شرکت مخابراتی یا ارائه‌دهنده خدمات اینترنتی است. این ایمیل حاوی اطلاعاتی مبنی بر وجود مشکلی در حساب کاربری یا صورتحساب فرد است و او را به تماس با یک شماره تلفن خاص برای حل مشکل تشویق می‌کند. مجرمان سایبری برای فریبندگی بیشتر، اغلب از موضوعاتی مرتبط با اشتراک نرم‌افزارهای امنیتی و یا حساب‌های آنلاین مانند نورتون، پی‌پل یا مک‌آفی سوءاستفاده می‌کنند. آنها در ایمیل خود با ذکر جزئیاتی جعلی از صورت‌حساب، این‌گونه القا می‌کنند که قربانی باید برای لغو اشتراک با یک شماره تلفن خاص تماس بگیرد.
- تماس با مرکز تماس جعلی: هنگامی که فرد با شماره تلفن تماس می‌گیرد، به جای یک اپراتور واقعی، با یک مجرم سایبری آموزش‌دیده که وانمود می‌کند نماینده شرکت یا سازمان مورد نظر است، صحبت می‌کند.
- فریب و سرقت اطلاعات: مجرم سایبری با استفاده از تکنیک‌های مهندسی اجتماعی، سعی می‌کند تا از قربانی اطلاعات شخصی مانند نام کاربری، رمز عبور، شماره کارت اعتباری یا اطلاعات بانکی را به دست آورد.
- نصب بدافزار: در برخی موارد، مجرم سایبری ممکن است قربانی را متقاعد کند تا یک فایل یا برنامه را بر روی سیستم خود دانلود و نصب کند. این فایل‌ها معمولاً بدافزارهایی هستند که می‌توانند اطلاعات شخصی را سرقت کنند، کنترل سیستم را به دست بگیرند یا برای اهداف مخرب دیگر مورد استفاده قرار گیرند.

مجرمان سایبری دائماً در حال یافتن روش‌های جدیدی برای فریب دادن افراد و ارتکاب حملات TOAD هستند. در دسامبر ۲۰۲۳، نوع جدیدی از حملات TOAD با عنوان «BazaCall» مشاهده شد که در آن مجرمان از فرم‌های گوگل[۱] برای دور زدن دروازه‌های امنیتی ایمیل استفاده می‌کردند. این امر نشان می‌دهد که برای مقابله با این تهدیدات در حال تکامل، باید دائماً هوشیار بود و اقدامات پیشگیرانه خود را به‌روز نگه داشت. نمونه‌ای از ایمیل استفاده‌شده توسط مهاجمان در این حمله در شکل ۵ نشان داده شده است.

[۱] Google Forms


[EXT] Payment for order no. 63014611 is approved

Customer Care Team <customercaretea... Monday, August 28, 2023 at 7:09 AM

To:

CAUTION: This email is external. Do not click links or attachments that are unexpected or from unknown senders. If unsure, click the Report Phishing Button in Outlook.

2023-08-28
Order Number:- 597G24SZ
Support:- +1(888) 864-1634

Order Summary

Dear Valid User,
Thank you for using Membership & Webroot Advanced Threat Protection. Tonight, your purchase details are set to renew automatically, and the corresponding amount will be deducted from your account. This email is in regards that you have an reactive membership with us, which is going to be renewed on 2023-08-28.

ITEM DESCRIPTION:
Client UID:- G24SZ597
Item:- AntiVirus Tech Support
Quantity: - 1
Tenure: - 5 Years
Payment Mode: - Confirmed
Charged Amount:- $424.24

To avoid future charges, reach out to us at our customer care before today to cancel our services. Alternatively, we encourage you to consider renewing your membership and remain a valued member of our community. Your satisfaction is our utmost priority, and we're here to assist you in any way we can.

+1(888) 864-1634

شکل ۵) نمونه از ایمیل مورد استفاده در حمله TOAD رخ داده آگوست ۲۰۲۳

۳-۱۱ فریب تلفنی هدفمند[۱]

فریب تلفنی هدفمند، نوع خاصی از فریب هدفمند است و تفاوت آن با سایر انواع مشابه، این است که از طریق تماس تلفنی یا دیگر شکل‌های ارتباط صوتی، کاربر را برای اعطای دسترسی به سیستم‌ها فریب می‌دهد. فریب تلفنی هدفمند اغلب با تکنیک‌های مهندسی اجتماعی همراه است، مانند جا زدن به عنوان یک منبع قابل اعتماد (مثل جعل هویت)؛ مهاجم خود را به عنوان فردی شناخته‌شده، مانند کارمند بخش IT یا یک مقام ارشد جا می‌زند. همچنین ایجاد حس فوریت یا هشدار نیز دیگر روش مهاجمان است به این صورت مهاجم با القای حس فوریت یا هشدار، قربانی را تحت فشار قرار می‌دهد تا بدون دقت کافی، درخواست او را تأیید کند.

در برخی موارد، ممکن است فریب تلفنی هدفمند با تولید درخواست تأیید هویت چندعاملی (MFA) ترکیب شود. در این سناریو، مهاجم پس از فریب دادن قربانی برای اعطای دسترسی اولیه، ممکن است درخواستی جعلی برای تأیید هویت چندعاملی به قربانی ارسال کند. با تأیید این درخواست، قربانی ناخواسته اجازه دسترسی کامل به سیستم‌ها را به مهاجم می‌دهد.

[۱] Spear Phishing Voice

۳-۱۲ جعل تماس تلفنی

حملات جعل تماس تلفنی به مهاجمان سایبری این امکان را می‌دهد تا هویت تماس‌گیرنده را پنهان کنند و وانمود کنند که از شماره‌ای معتبر، مانند یک شماره محلی یا یک کسب‌وکار شناخته‌شده، تماس می‌گیرند. این ترفند آنها را قادر می‌سازد تا قربانیان را فریب دهند و اطلاعات شخصی یا دسترسی به سیستم‌ها را به دست آورند. در اینجا روش‌هایی که مهاجمان برای جعل تماس تلفنی استفاده می‌کنند، آورده شده است:

- **استفاده از پروتکل صدای روی بستر اینترنت (VoIP):** VoIP امکان برقراری تماس‌های تلفنی از طریق اینترنت را فراهم می‌کند. مهاجمان می‌توانند از سرویس‌های VoIP برای برقراری تماس تلفنی جعلی استفاده کنند و در عین حال، شماره دلخواه خود را برای گیرنده نمایش دهند.
- **سرویس‌های جعل:** ارائه‌دهندگان غیرقانونی، سرویس‌هایی را ارائه می‌دهند که به مهاجمان اجازه می‌دهد تا شماره تماس خود را هنگام برقراری تماس تلفنی پنهان یا جعل کنند. این سرویس‌ها اغلب برای اهداف غیرقانونی مانند کلاه‌برداری و فریب تلفنی هدفمند مورد استفاده قرار می‌گیرد.
- **جعبه نارنجی (Orange Boxing):** جعبه نارنجی، روشی قدیمی‌تر برای جعل تماس تلفنی است که شامل سخت‌افزار تخصصی برای برقراری تماس تلفنی جعلی و دست‌کاری اطلاعات نمایش داده شده شماره تماس‌گیرنده است.
- **سوءاستفاده از تعویض سیم‌کارت (SIM Swapping):** سوءاستفاده از تعویض سیم‌کارت روشی است که در آن مهاجم تلاش می‌کند شماره تلفن همراه قربانی را به سرقت ببرد. این اتفاق زمانی رخ می‌دهد که یک مجرم بتواند شرکت ارائه‌دهنده خدمات تلفن همراه را فریب دهد تا شماره قربانی را به سیم‌کارت خودش منتقل کند.

۳-۱۳ دور زدن روش‌های احراز هویت چندعاملی

در دنیای امروز که حملات سایبری رو به افزایش است، استفاده از روش‌های احراز هویت چندعاملی (MFA) برای محافظت از حساب‌های آنلاین، امری ضروری است. با این حال، هیچ روشی بی‌نقص نیست و هکرها همواره در تلاش برای دور زدن این تدابیر امنیتی هستند. در این بخش، به برخی از روش‌های رایج که مهاجمان برای دور زدن MFA استفاده می‌کنند، می‌پردازیم:

- **سوءاستفاده از تعویض سیم‌کارت (SIM Swapping)** که در بخش پیشین توضیح داده شد.
- **حمله مهاجم میانی (Adversary-in-the-middle - AITM)**[1]: در این نوع حمله، مهاجم بین قربانی و وب‌سایتی که می‌خواهد به آن وارد شود، قرار می‌گیرد و ترافیک داده‌های او را رهگیری و دست‌کاری می‌کند. مهاجم می‌تواند با این روش، کدهای تأیید MFA که به صورت آنلاین ارسال می‌شوند را جاسوسی کند و به حساب‌های قربانی دسترسی یابد.
- **بمباران اعلان‌های MFA (MFA Prompt Bombing):** در این روش، مهاجم تعداد زیادی اعلان MFA را به دستگاه قربانی ارسال می‌کند تا او را گیج و خسته کند. در نهایت، ممکن است در اثر بی‌توجهی، قربانی یکی از این اعلان‌ها را تأیید کند و به مهاجم اجازه ورود به حساب خود را بدهد.
- **سرقت توکن:** توکن‌های MFA کدهای منحصر به فردی هستند که برای تأیید هویت استفاده می‌شوند. مهاجمان می‌توانند با روش‌های مختلفی مانند بدافزار، فیشینگ یا مهندسی اجتماعی، این توکن‌ها را سرقت کرده و به حساب‌های افراد دسترسی یابند.

[1] این حمله، همچنین به نام حمله مرد میانی (Man-In-The-Middle) یا MITM نیز شناخته می‌شود.

- **فیشینگ صوتی و پیامکی:** این دو گونه از فیشینگ نیز روش‌هایی هستند که در آنها مهاجم با تماس تلفنی یا پیامک‌های جعلی که ظاهری معتبر دارند، قربانی را فریب می‌دهند تا اطلاعات شخصی خود، از جمله رمز عبور و کدهای تأیید MFA را به اشتراک بگذارد.

۳-۱۴ دامنه‌های متقلبانه

تکنیک‌های دامنه متقلبانه (Typosquatting) که در بخش‌های پیشین نیز به آن اشاره‌ای شد شامل ثبت عمدی نام‌های دامنه با غلط‌های املایی وب‌سایت‌های شناخته‌شده برای فریب بازدیدکنندگان ناآگاه و هدایت آنها به وب‌سایت‌های جعلی است که اغلب اهداف مخربی مانند کلاه‌برداری را دنبال می‌کنند. برخی از روش‌های رایج دامنه متقلبانه عبارت‌اند از:

- حذف نقطه بعد از www: (مثال: wwwaa.com)
- حذف یک حرف: (مثال: apple.om)
- جا به جا کردن دو حرف: (مثال: faecbook.com)
- دوبله کردن حروف: (مثال: twiiter.com)
- استفاده از حروف شبیه به هم: (مثال: google.com با یک حرف آی «i» انگلیسی بزرگ به جای حرف اِل کوچک «l»)
- فشار دادن کلید اشتباه: (مثال: costko.com)

مهاجمان با استفاده از این تکنیک‌ها، دامنه‌هایی را ثبت می‌کنند که بازدیدکنندگان به اشتباه فکر می‌کنند وب‌سایت واقعی را تایپ کرده‌اند. با هدایت قربانیان به وب‌سایت‌های جعلی، مهاجمان می‌توانند برای مقاصد مخرب مانند سرقت اطلاعات شخصی، نصب بدافزار یا هدایت به صفحات فیشینگ اقدام کنند.

۳-۱۵ آدرس‌های اینترنتی جعلی

باید توجه داشت که آدرس‌های اینترنتی که به نام URL[۱] شناخته می‌شوند همواره امن نبوده و برخی از آنها توسط مجرمین سایبری ایجاد شده‌اند. لینک‌های مخرب در ایمیل‌ها، پیام‌های متنی، پست‌های رسانه‌های اجتماعی، پنجره‌های بازشو (پاپ‌آپ) و موارد دیگر پنهان شده‌اند. کاری که کلاه‌برداران انجام می‌دهند این است که این لینک‌ها را ایجاد و توزیع می‌کنند و سعی در این دارند که کاربران را فریب داده وبه کلیک کردم روی آن‌ها سوق دهند. هنگامی کاربر این گونه وب‌سایت‌های را باز می‌کند ممکن است در معرض نرم‌افزارهای مخرب، ویروس‌ها و سایر محتوای خطرناک قرار بگیرد.

لینک‌های خطرناک شما را به وب‌سایت‌های خطرناک هدایت می‌کنند و داده‌ها، رایانه و شبکه شما را در معرض خطر قرار می‌دهند. تشخیص یک URL امن از یک URL مخرب ممکن است دشوار باشد، اما علائم هشداردهنده‌ای وجود دارد که می‌توان به آن‌ها توجه کرد.

۱. انتهای دامنه مهم‌ترین بخش برای بررسی است. بخش دامنه یک URL می‌تواند به شما در مورد منبع لینک، بینشی بدهد. دامنه را می‌توان بعد از پروتکل (احتمالاً http://) پیدا کرد؛ در برخی از لینک‌های طولانی‌تر، دامنه قبل از اولین «/» تمام می‌شود. برای مثال، در لینک «https://google.com/maps»، دامنه «google.com» است. اگرچه که به نظر ساده می‌رسد اما واقعیت این است که کلاه‌برداران، دامنه‌ها را دست‌کاری می‌کنند تا آنها را شبیه چیزی جلوه دهند که نیستند. جهت روشن شدن موضوع و اینکه چگونه مجرمان سایبری از این مسئله سوءاستفاده می‌کنند به این مثال توجه کنید: در آدرس «http://google.com.cust_login.ie»، دامنه «cust_login.ie» است، نه

[۱] Uniform Resource Locator (URL)

«google.com» و نیز در «http://accounts_login.cz/google.com»، دامنه «accounts_login.cz» است، و نه «google.com». حال آنکه در نگاه اول ممکن است اینطور به نظر برسد با آدرس وب‌سایت گوگل مواجه هستیم. به همین دلیل است که مهم است فاصله بین «http://» و اولین «/» را بررسی کنید و مراقب جعل‌های صورت گرفته در این بخش باشید.

۲. وجود خط تیره و نمادها در لینک‌های مخرب رایج هستند. وب‌سایت‌های معتبر اغلب خط تیره یا نماد در نام دامنه خود ندارند. همانطور که در مثال‌های ذکر شده در بخش پیشین اشاره شد، کلاه‌برداران از این عناصر همراه با برندهای شناخته‌شده برای فریب کاربر استفاده می‌کنند. برای مثال، «www.google.com» با «www.google-search.com» متفاوت است.

۳. مراقب دامنه‌هایی که کاملاً عددی هستند باشید. گاهی اوقات با دامنه‌ای روبرو می‌شوید که فقط به صورت یک آدرس IP نمایش داده می‌شود (مثلاً http://101.10.1.101). در چنین لینک‌هایی، معمولا نمیتوان مالک واقعی دامنه را اعتبارسنجی کرد. بنابراین تنها در صورتی روی چنین لینک‌هایی کلیک کنید که دقیقا آدرس IP آن را میدانید و با آن آشنا هستید.

۴. در خصوص آدرس‌های کوتاه شده، می‌توان اینگونه آنها را تعبیر کرده که گویی آدرس‌هایی هستند که استتار کرده‌اند. با محدودیت کاراکتر در برخی از پلتفرم‌های رسانه‌های اجتماعی، دیدن URLهای کوتاه شده رایج است. اما این آدرس‌ها همچنین در پیام‌های متنی، ایمیل‌ها و سایر رسانه‌ها نیز یافت می‌شوند. سرویس‌هایی مانند TinyURL، Bitly یا نمونه‌های ایرانی مثل b2n.ir آدرس‌های طولانی‌تر را دریافت کرده و آنها را به یک URL با کاراکترهای کمتر تبدیل می‌کنند. در این گونه موارد، واقعیت این است که آدرس کوتاه شده، ماسکی برای همان آدرس اولیه است. دراین موارد نیز باید مراقب باشید؛ مانند دامنه‌های آدرس IP، نمی‌توانید از منابع واقعی اینگونه لینک‌ها مطمئن باشید. برای مثال آدرس‌های https://t.ly/9gd99 و https://shorturl.at/45Mtc هر دو نمونه‌های کوتاه شده این آدرس هستند: https://www.du.edu/it/services/security/5-url-warning-signs.

۵. کلاه‌برداران می‌توانند آدرس‌های خطرناک را در داخل لینک‌ها، متن، لوگوها و تصاویر به ظاهر معتبر جاسازی کنند. اما نکته اینجاست که با قرار دادن نشانگر ماوس روی این لینک‌ها، می‌توان مشاهده کرد که چه واقعا به کجا لینک دارد. هنگام نگه داشتن ماوس، آدرسی را که روی صفحه شما ظاهر می‌شود با آدرسی که قابل مشاهده است مقایسه کنید. اگر تفاوت قابل توجهی وجود داشته باشد یا برخی از علائم هشداردهنده را در URL پنهان مشاهده کنید، از آن لینک (و ایمیل، وب‌سایت یا تبلیغی که حاوی آن است) خودداری کنید. مثلا ممکن است عکسی در ایمیل باشد که وقتی ماوس را روی آن نگه میدارید ادرسی را مشاهده کنید که احتمالا به وب‌سایتی غیرمرتبط یا مخرب هدایت می‌شود و یا ممکن است در ایمیل آدرسی به صورت www.google.com وجود داشته باشد اما وقتی ماوس را روی آن می‌برید آدرسی دیگر مثلا www.google-search.com پدیدار می‌شود.

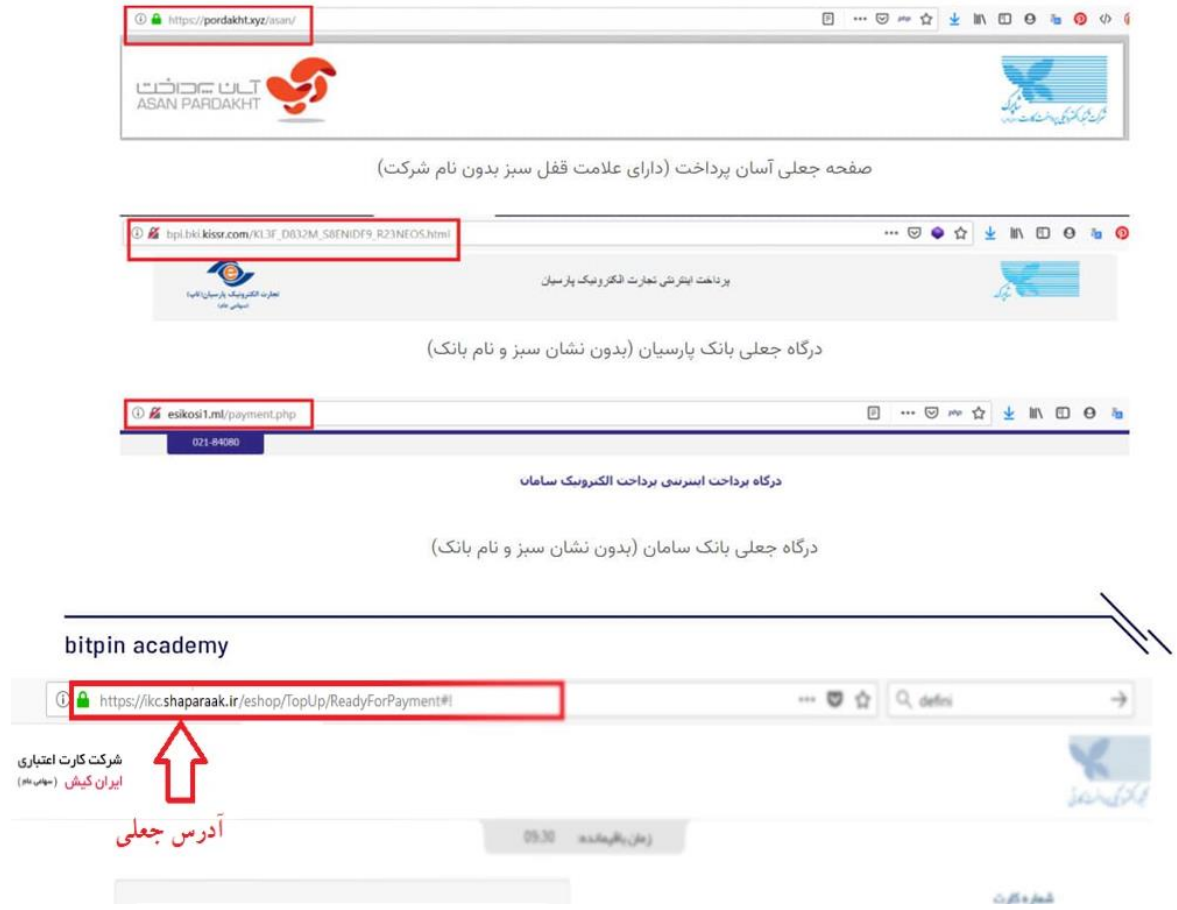
۳-۱۶ درگاه‌های پرداخت جعلی: فیشینگ در دنیای پرداخت آنلاین

درگاه‌های پرداخت آنلاین، بسترهای امنی برای انجام تراکنش‌های الکترونیکی هستند که به کسب‌وکارها و مشتریان امکان می‌دهند تا به صورت غیرحضوری و با آسودگی خاطر، مبادلات مالی خود را انجام دهند. با این حال، متأسفانه، این بستر امن نیز می‌تواند مورد سوءاستفاده مجرمان سایبری قرار گرفته و به ابزاری برای کلاه‌برداری و فیشینگ تبدیل شود.

درگاه‌های پرداخت جعلی، وب‌سایت‌هایی هستند که ظاهری شبیه به درگاه‌های واقعی دارند و توسط مجرمان سایبری برای فریب کاربران و سرقت اطلاعات بانکی آنها طراحی شده‌اند. این درگاه‌ها معمولاً از طریق روش‌های مختلفی مانند ایمیل‌های فیشینگ، تبلیغات فریبنده در شبکه‌های اجتماعی و یا صفحات جعلی در وب‌سایت‌های معتبر، به کاربران معرفی می‌شوند.

همچنین آدرس این درگاه‌ها معمولاً با استفاده از تکنیک‌های دامنه متقلبانه به آدرس اصلی شبیه بوده و یا به گونه‌ای فریب‌دهنده است که اعتماد کاربر را جلب کند. مهم‌ترین نکات آدرس‌های جعلی درگاه‌های پرداخت عبارت‌اند از:

۱. آدرس‌های با پسوندهای غیر از com. یا ir. که از موارد معمول هستند ممکن است که جعلی بوده و باید با دقت بیشتری آنها را بررسی نمود. مثلاً پسوند xyz. یکی از موارد مشکوک و متداول است.
۲. درگاه پرداخت در ایران همگی زیردامنه‌ای از آدرس shaparak.ir هستند مانند موارد زیر:
   - آسان پرداخت پرشین https://asan.shaparak.ir
   - به پرداخت ملت https://bpm.shaparak.ir
   - تجارت الکترونیک پارسیان https://pec.shaparak.ir
   - تجارت الکترونیک پارسیان https://pecco.shaparak.ir
   - پرداخت الکترونیک سامان https://sep.shaparak.ir
   - پرداخت الکترونیک پاسارگاد https://pep.shaparak.ir
   - پرداخت نوین آرین https://pna.shaparak.ir
   - پرداخت الکترونیک سداد https://sadad.shaparak.ir
   - کارت اعتباری ایران کیش https://ikc.shaparak.ir
   - فن آوا کارت https://fanava.shaparak.ir
   - مبنا کارت آریا https://mabna.shaparak.ir
   - الکترونیک کارت دماوند https://ecd.shaparak.ir
   - سایان کارت https://sayan.shaparak.ir
۳. آدرس‌هایی شبیه به آدرس درگاه شاپرک اصلی مانند shaqarak.ir یا shaparak.xyz یا shaperak.ir ممکن است در نگاه اول بسیار شبیه به آدرس اصلی به نظر برسد و هر فردی را گمراه کند. نمونه‌ای از آدرس‌های مورد استفاده مهاجمان در شکل ۶ نشان داده شده است.



شکل ۶: نمونه‌ای از چند آدرس جعلی درگاه پرداخت

نحوه عملکرد درگاه‌های پرداخت جعلی به این صورت است:

۱. مجرمان سایبری با ارسال ایمیل، پیامک یا تبلیغات فریبنده، کاربران را به کلیک بر روی لینک‌های موجود در این پیام‌ها ترغیب می‌کنند.
۲. با کلیک بر روی لینک، کاربر به یک وب‌سایت جعلی که ظاهری شبیه به درگاه پرداخت واقعی یک فروشگاه یا بانک دارد، هدایت می‌شود.
۳. در این وب‌سایت جعلی، از کاربر خواسته می‌شود تا اطلاعات کارت بانکی خود مانند شماره کارت، رمز عبور و CVV2 را وارد کند.
۴. پس از سرقت اطلاعات بانکی، مجرمان سایبری می‌توانند از آنها برای برداشت غیرمجاز از حساب بانکی کاربر، انجام تراکنش‌های غیرقانونی و یا فروش اطلاعات به افراد دیگر استفاده کنند.

راه‌های تشخیص درگاه‌های پرداخت جعلی نیز شامل موارد زیر است:

- بررسی آدرس وب‌سایت: آدرس وب‌سایت‌های درگاه‌های پرداخت جعلی معمولاً دارای غلط املایی یا حروف اضافی هستند و یا ویژگی‌های بیان شده در بخش پیشین را ندارد.
- عدم وجود گواهی‌نامه SSL: وب‌سایت‌های معتبر دارای گواهی‌نامه SSL هستند که با علامت قفل (معمولاً به رنگ سبز) در نوار آدرس مرورگر نشان داده می‌شود. البته تنها وجود این گواهینامه دلیل بر صحت وب‌سایت نیست چرا که وب‌سایت جعلی نیز می‌تواند SSL داشته باشد و لذا باید دیگر موارد را نیز بررسی نمود. کاری که این گواهینامه انجام

می‌دهد به طور مختصر عبارت است تصدیق هویت وب‌سایت و رمزگذاری ترافیک میان شما و وب‌سایت. تصدیق هویت به این معناست که شخص ثالثی، به جای سرور اصلی وب‌سایت مورد نظرخود را جا نزده است. البته توجه داشته باشید که ممکن است مهاجم تکنیک دامنه متقلبانه استفاده کرده و آدرسی شبیه به واقعی را ارائه می‌کند! همچنین رمزگذاری باعث می‌شود که مهاجم نتواند با حمله AITM (یا همان MITM) ترافیک را در بیان راه شنود و دست‌کاری کند.

- عدم تطابق با اطلاعات فروشگاه: اطلاعات درج شده در درگاه پرداخت جعلی، مانند نام فروشگاه و شماره تماس، ممکن است با اطلاعات واقعی فروشگاه مطابقت نداشته باشد.

۴ نقش هوش مصنوعی در مهندسی اجتماعی

در دنیای امروز، حملات سایبری به طور فزاینده‌ای پیچیده‌تر و خطرناک‌تر می‌شوند. هوش مصنوعی (AI) به عنوان یک ابزار قدرتمند، در حال حاضر توسط مجرمان سایبری برای ارتقای کارایی و اثربخشی روش‌های حمله خود مورد استفاده قرار می‌گیرد. یکی از نمونه‌های بارز این امر، افزایش چشمگیر حملات فیشینگ صوتی (Vishing) پس از راه‌اندازی ChatGPT در نوامبر ۲۰۲۲ است.

تحقیقات نشان می‌دهد که از زمان راه‌اندازی ChatGPT، حملات فیشینگ صوتی، فیشینگ پیامکی (Smishing) و فیشینگ ایمیلی (Phishing) به طرز شگفت‌انگیزی به میزان ۱۲۶۵ درصد افزایش یافته است. این افزایش قابل‌توجه، نشان‌دهنده سوءاستفاده گسترده مجرمان سایبری از ChatGPT برای فریب قربانیان و سرقت اطلاعات شخصی و مالی آنها است.

مطالعه شرکت Enea نشان می‌دهد که ۷۶ درصد از سازمان‌ها از حفاظت کافی در برابر کلاه‌برداری‌های صوتی و پیامکی برخوردار نیستند. این موضوع، سازمان‌ها را به شدت در برابر حملات فیشینگ صوتی مبتنی بر هوش مصنوعی که توسط ChatGPT و ابزارهای مشابه آن انجام می‌شوند، آسیب‌پذیر می‌کند.

پیشرفت‌های تکنولوژی و هوش مصنوعی، ورود به حوزه جرائم سایبری را برای مجرمین آسان‌تر کرده و پیچیدگی حملات را افزایش داده است. ابزارهای هوش مصنوعی مانند ChatGPT به مجرمان سایبری امکان می‌دهند تا به طور خودکار محتوای متقاعدکننده و هدفمند تولید کنند که فریب دادن قربانیان را آسان‌تر می‌کند.

پیش‌بینی می‌شود که ابزارهای هوش مصنوعی تولیدکننده محتوا مانند ChatGPT در آینده نقش مهمی در ایجاد حملات سایبری مؤثرتر، به ویژه در زمینه مهندسی اجتماعی، ایفا کنند. این موضوع، ضرورت افزایش آگاهی و اتخاذ تدابیر امنیتی قوی‌تر توسط سازمان‌ها و افراد را برای مقابله با این تهدید رو به رشد، بیش از پیش آشکار می‌کند.

۴-۱ کلاه‌برداری با تماس‌های تصویری جعل‌شده با هوش مصنوعی (Deepfake)

فناوری هوش مصنوعی (AI) در حال نفوذ به بسیاری از جنبه‌های زندگی روزمره ما است، اما متأسفانه، مجرمین سایبری نیز از این فناوری قدرتمند برای اهداف مخرب خود استفاده می‌کنند. یکی از نمونه‌های نگران‌کننده این سوءاستفاده، ظهور کلاه‌برداری با تماس‌های تصویری جعل‌شده با هوش مصنوعی (Deepfake) است.

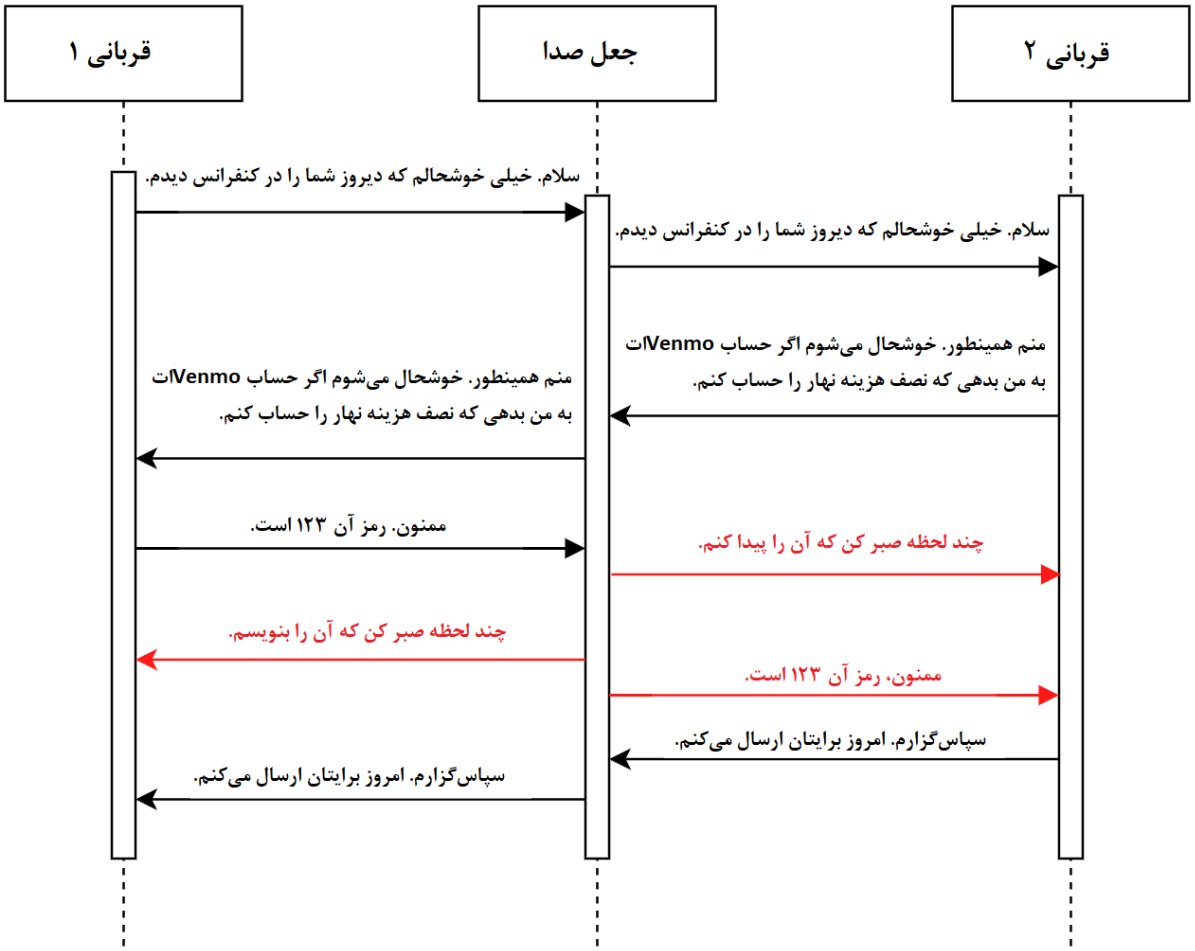
در اوایل سال ۲۰۲۴، طبق گزارش CNN، کلاه‌برداران با استفاده از فناوری Deepfake و جعل چهره مدیر مالی ارشد یک شرکت چندملیتی در یک تماس تصویری، توانستند یک کارمند را فریب دهند که بیش از ۲۵ میلیون دلار برای آنها ارسال کند. این کلاه‌برداری با یک ایمیل فیشینگ آغاز شد که در ابتدا تا حدی مشکوک به نظر می‌رسید، اما تماس تصویری Deepfake باعث تقویت اعتبار مجرمین سایبری شد و کارمند بخش مالی را متقاعد کرد تا پول را به حسابی در خارج از کشور منتقل کند.

به احتمال زیاد، این کلاه‌برداری توسط سازمان‌های جنایتکار حرفه‌ای و سازمان‌یافته‌ای با چندین عضو که نقش‌های مختلفی را در طول دوره کلاه‌برداری بر عهده داشتند، انجام شده است. این پرونده نشان می‌دهد که مجرمین سایبری با استفاده از فناوری‌های پیشرفته مانند Deepfake، قادر به انجام حملات فریبنده و پیچیده‌ای هستند.

۴-۲ سوءاستفاده از مدل‌های زبانی بزرگ (LLM) برای مهندسی اجتماعی

در کنار پیشرفت‌های خیره‌کننده هوش مصنوعی (AI)، شاهد ظهور تهدیدات جدیدی در حوزه امنیت سایبری هستیم. یکی از این تهدیدات، سوءاستفاده از «مدل‌های زبانی بزرگ»[۱] برای مهندسی اجتماعی است. مدل‌های زبانی بزرگ سامانه‌های هوش مصنوعی پیشرفته‌ای هستند که می‌توانند متن را با دقتی بالا تولید و درک کنند. متأسفانه، مجرمین سایبری از این قابلیت‌ها برای فریب دادن قربانیان به منظور سرقت اطلاعات شخصی یا مالی آنها سوءاستفاده می‌کنند.

در فوریه ۲۰۲۴، تحقیقات منتشر شده توسط IBM نشان داد که چگونه می‌توان از هوش مصنوعی برای ایجاد اختلال در مکالمات صوتی زنده استفاده کرد. این روش با استفاده از مدل‌های زبانی بزرگ برای درک مکالمه و دست‌کاری خروجی صدا بدون اطلاع شرکت‌کنندگان، امکان ربودن مکالمات زنده را فراهم می‌کند. اجرای چنین حمله‌ای مستلزم نصب بدافزار روی تلفن‌های قربانیان یا نفوذ به سرویس‌های VoIP (Voice over IP) است. نحوه انجام این نوع حمله در شکل ۷ نشان داده شده است.



شکل ۷: نحوه انجام جعل صدا با استفاده از هوش مصنوعی

متداول‌ترین و معروف‌ترین ابزارهای مبتنی بر مدل‌های زبانی بزرگ که امروزه توسط مهاجمان استفاده می‌شود عبارت‌اند از:

- WormGPT: این ابزار در سال ۲۰۲۱ راه‌اندازی شده و به طور گسترده‌ای در حملات فیشینگ با ایمیل‌های تجاری (BEC) مورد استفاده قرار گرفته است و توانایی نوشتن ایمیل‌های فیشینگ بسیار متقاعدکننده را دارد.

[۱] Large Language Models (LLM)

- FraudGPT: از جولای ۲۰۲۳ فعال است و می‌تواند طیف وسیعی از محتوا از جمله صفحات فیشینگ، ایمیل‌های فیشینگ و پیامک‌های فیشینگ را ایجاد کند.
- WolfGPT: از جولای ۲۰۲۳ فعال است و عمدتاً بر پشتیبانی از توسعه کد تمرکز دارد، اما ممکن است برای حملات فیشینگ پیشرفته نیز مورد استفاده قرار گیرد.

۵ مقابله با حملات مهندسی اجتماعی

حملات مهندسی اجتماعی، مقابله به خصوصی را می‌طلبند؛ چرا که این نوع از حمله عمداً برای سوءاستفاده از ویژگی‌های طبیعی انسان، مانند کنجکاوی، احترام به اقتدار و تمایل به کمک به دوستان، طراحی شده است. با این حال، راهکارهایی وجود دارد که به شناسایی حملات مهندسی اجتماعی کمک می‌کند. در ادامه، نکاتی در خصوص پیشگیری از این حملات توضیح داده شده است. در این خصوص باید توجه داشت که هیچ کدام از این نکات به تنهایی و به قطعیت، جعلی یا یا واقعی بودن یک پیام یا تماس را نشان نمی‌دهد و همواره باید با در نظر گرفتن همه آنها تصمیم‌گیری نمود.

۵-۱ بررسی منبع

در صورت دریافت یک پیام از ایمیل، پیامک یا هر روش دیگری، چند لحظه‌ای برای بررسی منشأ پیام دریافتی توقف کرده و به هیچ وجه بلافاصله به آن اعتماد نکنید. مثلاً یک فلش‌مموری ناشناس روی میز کارتان پیدا کرده‌اید یا تماس تلفنی ناگهانی‌ای به شما می‌گوید ۵ میلیارد تومان ارث برده‌اید و یا اگر ایمیلی از مدیرعاملتان دریافت کرده‌اید که درخواست اطلاعاتی درباره تک‌تک کارمندان دارد. همه این موارد مشکوک به نظر می‌رسند و باید با آنها با احتیاط رفتار شود.

بررسی منبع پیام، کار دشواری نیست. برای مثال، در مورد ایمیل، به سربرگ ایمیل نگاه کنید و آن را با ایمیل‌های معتبر از همان فرستنده مقایسه کنید. علاوه بر آن، ببینید لینک‌ها به کجا هدایت می‌شوند – هایپرلینک‌های جعلی با نگه‌داشتن مکان‌نما روی آنها به سادگی قابل شناسایی هستند (البته روی لینک کلیک نکنید!). به املا و دستور زبان توجه کنید؛ شرکت‌های معتبر، تیم‌هایی از افراد متخصص در زمینه برقراری ارتباط با مشتریان دارند، بنابراین ایمیلی با اشتباهات فاحش، احتمالاً جعلی است.

در صورت تردید، به وب‌سایت رسمی مراجعه کرده و با یک نماینده رسمی تماس بگیرید. آنها می‌توانند تأیید کنند که ایمیل یا پیام دریافتی معتبر است یا جعلی.

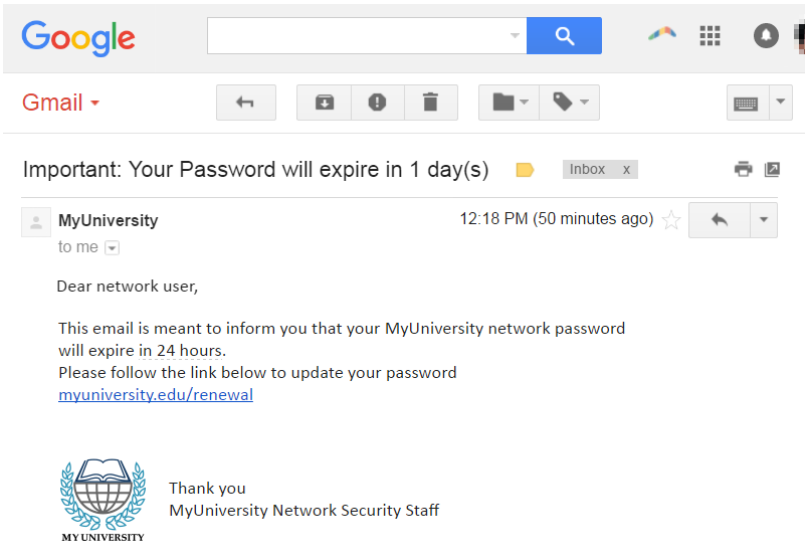
۵-۲ بررسی اطلاعات فرستنده

آیا فرستنده پیام، اطلاعاتی را که انتظار دارید در اختیار داشته باشد، در اختیار دارد؟ به عنوان مثال، اگر بانکی با شما تماس می‌گیرد، باید تمامی اطلاعات شما را در اختیار داشته باشد و پیش از اعمال هرگونه تغییر در حساب، سؤال‌های امنیتی را از شما بپرسد. چنانچه این اتفاق رخ نداد، احتمال جعلی بودن ایمیل یا تماس و یا پیام بسیار بالا است و باید نسبت به آن احتیاط کنید.

همچنین نسبت به تماس‌ها، ایمیل‌ها و ملاقات‌های ناخواسته که درخواست اطلاعات شخصی یا سازمانی را دارند، مشکوک باشید. در صورت تماس فردی ناشناس که مدعی عضویت در یک سازمان معتبر است، با آن سازمان تماس گرفته و هویت وی را تأیید کنید. علاوه بر آن هرگز اطلاعات شخصی یا سازمانی مانند ساختار شبکه را بدون اطمینان از مجوز فرد متقاضی، فاش نکنید.

۵-۳ شکستن حلقه عجله

حملات مهندسی اجتماعی اغلب بر حس فوریت تکیه دارند. مهاجمان امیدوارند قربانیان بدون تفکر زیاد، با آنها همکاری کنند. بنابراین، صرف اندکی زمان برای تأمل می‌تواند مانع این حملات شده و ماهیت جعلی آنها را آشکار سازد. به عنوان مثال ممکن است ایمیلی دریافت کنید که به نظر از یک نهاد قانونی مانند واحد فناوری اطلاعات سازمان شما باشد و با ابراز اینکه رمز عبور حساب کاربری شما به زودی منقضی می‌شود درخواست کند که روی لینک مربوطه کلیک کرده و هرچه سریع‌تر رمز را تغییر دهید. مثالی از این نوع پیام در شکل ۸ نشان داده شده است.



شکل ۸: نمونه از القای حس فوریت در پیام‌های فیشینگ

در چنین شرایطی علاوه بر توجه نکاتی که در دیگر بخش‌ها آمده است می‌توان به‌جای ارائه اطلاعات از طریق تلفن یا کلیک روی لینک، با شماره رسمی سازمان تماس گرفت و یا از طریق وب‌سایت رسمی آنها اقدام نمود. برای بررسی اعتبار منبع، از روش‌های ارتباطی دیگری نیز می‌توان بهره برد. برای مثال، اگر ایمیلی از دوست خود مبنی بر درخواست حواله پول دریافت کردید، با شماره موبایل او تماس بگیرید تا صحت موضوع را تأیید نمایید.

همچنین هنگامی که در مکالمه‌ای احساس فوریت می‌کنید، به‌خصوص احتیاط کنید؛ این روش متداول بازیگران مخرب برای جلوگیری از تفکر عمیق قربانیان است. اگر احساس فشار می‌کنید، کل فرآیند را کُند کنید. اعلام کنید که برای به دست آوردن اطلاعات، مشورت با مدیر خود یا نداشتن جزئیات در حال حاضر به زمان نیاز دارید؛ هر روشی برای کند کردن روند و فرصت دادن به خود برای تفکر. در بیشتر مواقع، مهندسان اجتماعی با درک از دست رفتن عنصر غافلگیری، پافشاری نمی‌کنند.

۵-۴ درخواست شناسایی

یکی از ساده‌ترین حملات مهندسی اجتماعی، دور زدن حراست برای ورود به ساختمان با حمل جعبه یا پوشه بزرگی از پرونده است؛ به این ترتیب، فردی خیرخواه درِ ورودی را برای او نگه می‌دارد. فریب این ترفند را نخورید و همیشه سند شناسایی معتبر را درخواست کنید.

این رویکرد در موارد دیگر نیز کاربرد دارد. هنگام دریافت تماس یا درخواست اطلاعات، باید به طور معمول نام و شماره فرد تماس‌گیرنده را جویا شوید و بپرسید «به چه کسی گزارش می‌دهید؟». پیش از ارائه هرگونه اطلاعات خصوصی یا شخصی، با بررسی چارت سازمانی یا دفترچه تلفن سازمان، صحت و اعتبار فرد را تأیید کنید. چنانچه فرد درخواست‌کننده اطلاعات را نمی‌شناسید و همچنان برای ارائه اطلاعات تردید دارید، به او اطلاع دهید که باید با فرد دیگری مشورت کنید و بعداً پاسخ او را بدهید.

۵-۵ استفاده از فیلتر هرزنامه قدرتمند

اگر برنامه ایمیل شما به اندازه کافی ایمیل‌های ناخواسته را فیلتر یا علامت‌گذاری نمی‌کند، ممکن است نیاز به تغییر تنظیمات آن داشته باشید. فیلترهای هرزنامه قدرتمند از انواع مختلف اطلاعات برای تشخیص ایمیل‌های مشکوک استفاده می‌کنند. این

فیلترها ممکن است فایل‌ها یا لینک‌های مشکوک را شناسایی کنند، فهرستی سیاه از آدرس‌های IP یا شناسه‌های فرستنده مشکوک داشته باشند و یا محتوای پیام‌ها را برای تشخیص جعلی بودن آنها تجزیه و تحلیل نمایند.

۵-۶ بررسی واقع‌بینانه بودن

برخی حملات مهندسی اجتماعی با فریب قربانی برای واکنش بدون تحلیل و بررسی، انجام می‌شوند. صرف زمان برای ارزیابی واقع‌بینانه موقعیت می‌تواند به شناسایی بسیاری از حملات کمک کند. برای مثال:

- اگر دوست شما واقعاً در جایی گیر افتاده باشد و راه فراری نداشته باشد، آیا برای شما ایمیل می‌فرستد یا با شما تماس تلفنی می‌گیرد یا پیامک می‌فرستد؟
- آیا احتمال دارد شاهزاده نیجریه‌ای یک میلیون دلار در وصیت‌نامه‌اش برای شما به جا گذاشته باشد؟
- آیا بانک با شما تماس می‌گیرد و درخواست جزئیات حسابتان را می‌کند؟ در واقع، بسیاری از بانک‌ها زمان ارسال ایمیل یا برقراری تماس تلفنی با مشتریان خود را یادداشت می‌کنند. بنابراین در صورت تردید، حتماً بررسی مجدد انجام دهید.

۵-۷ واکنش سریع و گزارش‌دهی

در صورتی که گمان می‌کنید هدف حمله مهندسی اجتماعی واقع شده‌اید، در صورت افشای اطلاعات حساس، فوراً موضوع را به مسئولان ذی‌ربط در سازمان خود اطلاع دهید. همچنین اگر به سرقت اطلاعات مالی مشکوک هستید، با مؤسسه مالی خود تماس گرفته و حساب‌های مربوطه را مسدود کنید. تراکنش‌های بانکی خود را به‌طور دقیق رصد کنید و فقط از درگاه‌های بانکی معتبر برای پرداخت‌های آنلاین استفاده کنید. و در نهایت گزارشی از نوع حمله را تهیه و به مراجع قانونی ذی‌ربط ارائه دهید.

۵-۸ امن سازی دستگاه‌ها برای مقابله با مهندسی اجتماعی

افزون بر شناسایی حملات و افزایش آگاهی، امن سازی دستگاه‌ها نیز اهمیت ویژه‌ای دارد. بدین ترتیب، حتی در صورت موفقیت یک حمله مهندسی اجتماعی، دامنه خسارت آن به همان حمله محدود می‌شود. اصول اولیه این امر، فارغ از نوع دستگاه (چه تلفن هوشمند، چه شبکه خانگی ساده و چه سیستم سازمانی بزرگ) یکسان است:

۱. **به‌روزرسانی مداوم نرم‌افزارهای ضد بدافزار و ضدویروس:** این اقدام می‌تواند از نصب بدافزارهایی که از طریق ایمیل‌های فریب آمیز وارد سیستم می‌شوند، جلوگیری کند.
۲. **به‌روزرسانی مرتب نرم‌افزارها و سیستم‌عامل‌ها، به‌ویژه وصله‌های امنیتی:** اجرای این اقدام ضروری است. نرم‌افزارها و سیستم‌عامل‌ها همواره در معرض آسیب‌پذیری‌هایی هستند که توسط هکرها کشف و مورد سوءاستفاده قرار می‌گیرند. به‌روزرسانی‌های امنیتی، حفره‌های امنیتی شناخته‌شده را رفع کرده و از نفوذ هکرها به سیستم جلوگیری می‌کنند.
۳. **اجتناب از اجرای دستگاه در حالت Root یا Administrator:** در صورت عدم اجرای گوشی‌های هوشمند با دسترسی روت (Root) و یا اجرای شبکه و رایانه شخصی در حالت مدیر (Administrator) حتی در صورت موفقیت حمله مهندسی اجتماعی و به دست آوردن رمز عبور کاربریِ حساب «کاربر» توسط مهاجم، امکان بازپیکربندی سیستم یا نصب نرم‌افزار بر روی آن برای وی وجود نخواهد داشت.
۴. **عدم استفاده از رمز عبور یکسان برای حساب‌های کاربری مختلف:** در صورتی که حمله مهندسی اجتماعی منجر به سرقت رمز عبور حساب کاربری شبکه اجتماعی شما شود، نباید به مهاجم امکان دسترسی به سایر حساب‌های کاربریتان را نیز بدهید.

۵. **بهره‌گیری از تأیید دو مرحله‌ای برای حساب‌های کاربری حساس:** در این روش، صرفاً داشتن رمز عبور برای دسترسی به حساب کاربری کافی نیست و ممکن است نیاز به تأیید هویت از طریق تشخیص صدا، استفاده از ابزار امنیتی، اثر انگشت یا کدهای تأیید پیام کوتاه باشد.
۶. **تغییر فوری رمز عبور در صورت افشا:** چنانچه رمز عبور حسابی را در اختیار فردی ناشناس قرار داده‌اید و احتمال مهندسی اجتماعی می‌دهید، بلافاصله رمز عبور آن حساب را تغییر دهید.
۷. **با مطالعه مستمر منابع معتبر،** خود را در برابر خطرات جدید امنیت سایبری آگاه سازید. بدین ترتیب، با شناخت روش‌های نوظهور حمله، احتمال قربانی شدنتان به میزان قابل توجهی کاهش می‌یابد.

۹-۵ مدیریت ردپای دیجیتال برای مقابله با مهندسی اجتماعی

یکی دیگر از جنبه‌های حائز اهمیت در مقابله با حملات مهندسی اجتماعی، مدیریت ردپای دیجیتال است. به اشتراک گذاشتن بیش از حد اطلاعات شخصی در فضای آنلاین، به‌ویژه از طریق شبکه‌های اجتماعی، می‌تواند به سود مهاجمان عمل کند. برای مثال، در حساب‌های کاربری خود از «نام بازیگر محبوب شما» به‌عنوان یکی از سؤالات امنیتی احتمالی استفاده شده باشد. آیا این اطلاعات را در شبکه‌های اجتماعی به اشتراک نگذاشته‌اید؟ در صورتی که چنین است، ممکن است در معرض خطر باشید! افزون بر این، برخی حملات مهندسی اجتماعی با بررسی رویدادهای اخیر که در شبکه‌های اجتماعی به اشتراک گذاشته‌اید، سعی در کسب اطلاعات درباره شما می‌کنند.

توصیه می‌شود تنظیمات شبکه‌های اجتماعی خود را بر روی «فقط دوستان» به جای «همه» قرار دهید و در مورد اطلاعاتی که به اشتراک می‌گذارید، محتاط باشید. لزومی به دچار شدن به پارانویا در این زمینه نیست، اما احتیاط همواره ضروری است.

به سایر جنبه‌های زندگی آنلاین خود که به اشتراک می‌گذارید نیز بیندیشید. برای نمونه، اگر رزومه آنلاین دارید، بهتر است آدرس، شماره تلفن و تاریخ تولد خود را از آن حذف کنید. همه این اطلاعات برای هر کسی که قصد انجام حمله مهندسی اجتماعی را دارد، مفید است. در حالی که برخی حملات مهندسی اجتماعی عمیقاً با قربانی درگیر نمی‌شوند، برخی دیگر با وسواس، برنامه‌ریزی می‌شوند. با به حداقل رساندن اطلاعات در دسترس مجرمان، زمینه کمتری برای سوءاستفاده آنها فراهم می‌آورید.

مهندسی اجتماعی به این دلیل بسیار خطرناک است که از موقعیت‌های کاملاً عادی سوءاستفاده کرده و آنها را برای اهداف مخرب به کار می‌گیرد. بااین‌حال، با آگاهی کامل از نحوه عملکرد این حملات و اتخاذ تدابیر احتیاطی اولیه، احتمال قربانی شدن به میزان قابل توجهی کاهش می‌یابد

۶ نمونه‌های مشهور حمله مهندسی اجتماعی در دنیا

در این بخش، چند نمونه از حمله‌های مهندسی اجتماعی مشهور در دنیا را توضیح می‌دهیم که به درک بهتر مفهوم این حمله و چگونگی بهره‌برداری مهاجمان سایبری از آن و نیز اثراتی که می‌تواند بر جای بگذارد کمک می‌کند.

در سال ۲۰۱۱، RSA، یک شرکت پیشرو در امنیت سایبری، از طریق حمله هوشمندانه‌ای توسط مهندسی اجتماعی مورد نفوذ قرار گرفت. مهاجمان، ایمیل‌هایی را که به عنوان ارتباطات قانونی شرکت عنوان می‌شد به کارکنان ارسال می‌کردند. این ایمیل‌ها حاوی پیوست‌های مخرب، به‌ویژه صفحات گسترده مایکروسافت اکسل (.xls) بودند که از تاکتیک‌های مهندسی اجتماعی برای فریب گیرنده استفاده می‌کردند تا آنها را باز کند. هنگامی که کارمندی، پیوست مورد نظر را باز می‌کرد، یک «آسیب‌پذیری روز صفر»[۱] در Adobe Flash مورد سوءاستفاده قرار می‌گرفت و بدافزاری را روی سیستم او نصب می‌کرد که به مهاجمان اجازه نفوذ به شبکه RSA را می‌داد. مهاجمان سپس توانستند با نفوذ به شبکه این شرکت، اعتبارنامه‌ها را سرقت کند و به سیستم‌های حساس‌تر، دسترسی پیدا کنند. این حمله، اثربخشی مهندسی اجتماعی را حتی در برابر شرکت‌های امنیت سایبری و اهمیت آموزش مداوم هوشیاری و آگاهی برای کارکنان را بیش از پیش نمایان نمود.

یک مثال دیگر، نقض عظیم داده‌های یاهو است که بیش از ۵۰۰ میلیون حساب کاربری را تحت تأثیر قرار داد، این حمله که به طور رسمی در سال ۲۰۱۶ فاش شد اما گمان می‌رود در سال ۲۰۱۴ آغاز شده باشد، ناشی از یک حمله مهندسی اجتماعی ماهرانه بود. در جریان این حمله بزرگ حتی FBI نیز برای تحقیقات بیشتر و کمک به یاهو وارد کار شد. در طول تحقیقات، مشخص شد که اپراتورهای دولتی روسیه تعدادی حساب خاص یاهو را هدف قرار داده و چندین هکر بسیار ماهر را برای نفوذ و یافتن اطلاعات حساب استخدام کرده‌اند. این مهاجمان ورود اولیه را از طریق ایمیل‌های «فیشینگ نیزه‌ای»[۲] هدفمند که برای مدیران سطح بالای یاهو ارسال می‌شد، به دست آوردند و سپس از سیستم‌های مدیریت به سایر بخش‌های شبکه یاهو (یک تاکتیک رایج و آشنا) منتقل شدند. «درهای پشتی»[۳] برای دسترسی مکرر فعال شدند و جزئیات بیشتری که ظاهر شد نشان می‌دهد که احتمالاً میلیاردها حساب تحت تأثیر قرار گرفته‌اند.

لازم به ذکر است که فیشینگ نیزه‌ای، گونه‌ای از فیشینگ است که به طور خاص شخص یا گروه خاصی از افراد را هدف قرار می‌دهد. برخلاف ایمیل‌های فیشینگ معمولی که از رویکرد پراکنده‌ای برای مخاطبان زیادی استفاده می‌کنند، ایمیل‌های فیشینگ نیزه‌ای به‌دقت ساخته شده‌اند تا برای قربانی انتخاب‌شده مرتبط و قابل باور به نظر برسند.

در مثالی دیگر، چندین حساب توییتر در جولای ۲۰۲۰ شروع به ارسال درخواست‌های بسیار غیرعادی برای اهدای بیت کوین کردند، از جمله جف بزوس، بیل گیتس، باراک اوباما، جو بایدن و بسیاری دیگر. توییتر به سرعت حساب‌های مورد بحث را مسدود کرد، اما تحقیقات نشان داد که بیش از صد حساب مهم به خطر افتاده است و ظاهراً داده‌های شخصی برخی از حساب‌ها به دست مهاجمان افتاده است. توییتر در همان ابتدا اذعان کرد که درگیر یک حمله مهندسی اجتماعی هدفمند علیه کارمندانش شده است و مراحل بعدی تحقیقات نشان داد که مهاجمان به طور خاص کارمندان جدید و کم‌تجربه را با بهانه‌های تلفنی هدف قرار داده‌اند و از آنها درخواست برای وارد کردن اعتبارنامه می‌کردند. پس از آن که کارمندان اعتبارنامه را وارد کردند به وب‌سایتی جعلی هدایت شدند و یک درخواست احراز هویت چندعاملی مبتنی بر تلفن نیز به کارمندان رسید که برخی از آنها این را نیز

---

[۱] آسیب‌پذیری روز صفر، یک نقص امنیتی است که قبل از اینکه توسعه‌دهندگان از آن آگاه شوند، توسط هکرها کشف می‌شود.

[۲] Spear phishing

[۳] Backdoor

وارد کردند و به این ترتیب، مهاجمان اجازه دسترسی یافتند. سیستم‌های این کارمندان، داده‌ها و اطلاعات کافی را برای هدف قرار دادن موفقیت‌آمیز کارمندان رده‌بالا با موفقیت و تسلط بر ابزارهای مدیریت حساب توییتر برای مهاجمان فراهم نمود.

صنعت بهداشت و درمان نیز به دلیل حجم بالای اطلاعات حساس بیماران، به طور فزاینده‌ای به هدفی جذاب برای مجرمان سایبری تبدیل شده است. علاوه بر این، صنعت مالی نیز به دلیل وجود اطلاعات مالی حساس مانند اطلاعات حساب بانکی و کارت اعتباری، مورد هدف قرار می‌گیرد. در سال ۲۰۲۳، شاهد افزایش نگران‌کننده‌ای در حملات فیشینگ به صنعت بهداشت و درمان بوده‌ایم. به طور میانگین، هر روز نزدیک به دو مورد نقض داده با حجم بیش از ۵۰۰ رکورد گزارش شده است. این آمار نشان می‌دهد که هکرها به طور فعال به دنبال سوءاستفاده از نقاط ضعف امنیتی در این بخش هستند و حجم عظیمی از اطلاعات حساس بیماران در معرض خطر قرار دارد.

مجرمان سایبری دائماً در حال یافتن روش‌های جدیدی برای دور زدن تدابیر امنیتی موجود هستند. در سال ۲۰۲۴، شاهد افزایش استفاده از تاکتیک‌هایی مانند فیشینگ صوتی، فیشینگ پیامکی، جعل هویت و فیشینگ مبتنی بر کد QR بوده‌ایم. این تاکتیک‌ها می‌توانند کاربران را فریب دهند تا اطلاعات شخصی خود را فاش کنند یا بدافزار را بر روی دستگاه‌های خود نصب کنند، حتی اگر با «دروازه‌های امنیتی ایمیل»[۱] محافظت شده باشند.

حملات فیشینگ نه تنها می‌توانند منجر به سرقت اطلاعات شخصی و مالی شوند، بلکه کاملاً ممکن است که به آسیب به شهرت و اعتبار سازمان‌های مورد حمله نیز منجر شوند. در سال ۲۰۲۳، اداره حقوق مدنی ایالات متحده[۲] (OCR) اولین توافق‌نامه خود را به دنبال تحقیق در مورد حمله فیشینگ به یک گروه پزشکی اعلام کرد. این امر نشان می‌دهد که مقامات دولتی در حال افزایش نظارت بر این نوع حملات سایبری و اعمال مجازات‌های شدید برای متخلفان هستند.

در اواخر سه ماهه سوم سال ۲۰۲۳، مهاجمان با انگیزه مالی، حملات مهندسی اجتماعی پیچیده‌ای را علیه کارکنان میزهای راهنمای فناوری اطلاعات (IT Help Desk) در سازمان‌های بهداشتی انجام دادند. این حملات با هدف نهایی انجام کلاه‌برداری با تغییر مسیر پرداخت‌ها، از طریق تماس تلفنی با شماره‌های محلیِ سازمان‌های هدف صورت گرفت. مهاجم با ادعای خرابی تلفن همراه و عدم امکان دریافت توکن‌های تأیید هویت چندعاملی (MFA)، کارکنان میز راهنما را متقاعد می‌کرد تا دستگاه جدیدی را برای دسترسی به منابع سازمانی در اختیار آنها قرار دهند. پس از دسترسی، مهاجم بر اطلاعات ورود به وب‌سایت‌های پرداخت‌کنندگان تمرکز می‌کرد و با تغییر فرم‌های مربوط به سیستم انتقال وجوه خودکار (ACH) در حساب‌های پرداخت‌کنندگان، وجه‌های قانونی را به حساب‌های بانکی تحت کنترل خود در آمریکا منتقل می‌کرد و سپس این وجه‌ها را به حساب‌های خارج از کشور انتقال می‌داد. در طول این کمپین مخرب مهندسی اجتماعی، مهاجم همچنین دامنه‌ای با یک حرف متفاوت از نام دامنه سازمان هدف ثبت کرد. این تکنیک به عنوان دامنه متقلبانه یا Typosquatting شناخته می‌شود. دامنه‌های متقلبانه شامل ثبت عمدی دامنه‌هایی با نام‌های غلط وب‌سایت‌های معروف برای فریب بازدیدکنندگان ناآگاه به وب‌سایت‌های جایگزین، و اغلب برای اهداف مخرب، مانند کلاه‌برداری است.

[۱] Secure Email Gateway (SEG)، ابزاری است که ایمیل‌های آلوده را شناسایی کرده و آنها را پیش از رسیدن به صندوق ورودی مقصد، مسدود می‌کند

[۲] Office for Civil Rights (OCR)

منابع و مآخذ

۱. حملات مهندسی اجتماعی علیه بخش مراقبت‌های بهداشتی و بهداشت عمومی[۱]، *وزارت بهداشت و خدمات انسانی ایالات متحده*، ۱۱ آپریل ۲۰۲۴.

۲. مهندسی اجتماعی برای مهندسان امنیت (SANS SEC 467)، *موسسه SANS*، ۲۰۲۱.

۳. روش‌های جلوگیری از حملات مهندسی اجتماعی[۲]، *موسسه امنیت سایبری کسپرسکی*، ۲۲ می ۲۰۲۴.

۴. تمرین‌های تیم قرمز و شبیه‌سازی حملات دشمن (SANS SEC 564)، *انتشارات ناقوس*، میثم ناظمی، زمستان ۱۴۰۰.

۵. چگونه می‌توان از معتبر بودن صفحه پرداخت مطمئن شد؟[۳]، *ایبِنا، شبکه خبری اقتصاد و بانک ایران*، ۸ اسفند ۱۳۹۶.

۶. آشنایی با حملات فیشینگ، نحوه شناسایی آنها و چند مثال واقعی[۴]، *آکادمی بیت‌پین*، ۶ تیر ۱۴۰۲.

۷. پنج علامت هشداردهنده درباره آدرس‌های اینترنتی که باید مراقب آنها بود[۵]، *مرکز فناوری اطلاعات دانشگاه دنور*، ۲۰۱۵.

[۱] https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf

[۲] https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

[۳] https://www.ibena.ir/000LWB

[۴] https://bitpin.ir/academy/phishing-attack/

[۵] https://www.du.edu/it/services/security/5-url-warning-signs