حفاظت رایانه

توصیه های حفاظتی در استفاده از رایانه ها:

۱- هرگز از رایانه خود به ویژه در محل کار، بدون رمز عبور (پسورد) استفاده نکنید.
همیشه برای رایانه خود رمز عبور تعیین کرده و آن را طوری تنظیم نمائید که در صورت عدم استفاده از آن به مدت (حداکثر) پنج دقیقه از شما اسم عبور درخواست نماید. این کار مانعی برای دسترسی دیگران به رایانه شما خواهد بود و تا حدودی امنیت سیستم شما را افزایش می‌دهد.

۲- هرگز از رمز عبور ساده و مشخص استفاده نکنید.
سعی کنید رمز عبورهای سیستم خود را پیچیده و غیرقابل پیش بینی انتخاب کنید. انتخاب رمز عبور با کارکترهای زیاد، با حروف و اعداد، حروف کوچک و بزرگ و یا انتخاب آن به زبان دیگر، می‌تواند امنیت سیستم شما را افزایش دهد.

۳- هرگز اطلاعات محرمانه خود را در فایل‌های آشکار و سهل الوصول قرار ندهید.
فایل‌های محرمانه خود را می‌توانید به‌صورت پنهان و در زیر مجموعه فایل‌های سیستمی یا زیر مجموعه سایر برنامه‌های نصبی سیستم قرار دهید تا به‌راحتی در اختیار افراد بیگانه قرار نگیرد. در غیر این صورت، احتمال دسترسی راحت به این‌گونه فایل‌های همواره متصور است.

۴- هرگز از کامپیوتری که دارای اطلاعات محرمانه و با اطلاعات خصوصی است، برای متصل شدن به اینترنت استفاده نکنید.
همیشه در هنگام متصل شدن به اینترنت خطر سرقت اطلاعات، تخریب اطلاعات به‌صورت جدی وجود داشته و در صورت بی تفاوتی به این مطلب خطرات جبران ناپذیری سیستم و اطلاعات شما را تهدید می‌کند.

۵- هرگز کامپیوتر خود را که حاوی اطلاعات محرمانه یا خصوصی است، جهت تعمیر به افراد متفرقه و ناشناس ندهید.
حتماً نسبت به تعمیرکار کامپیوتر خود اطمینان حاصل نموده و سعی کنید شخصاً هنگام تعمیر حضور داشته باشید.

۶- هرگز قطعات آسیب دیده سیستم کامپیوتر خود را (مانند: هارد، فلاپی، سی دی و ...) دور نیاندازید.
حتما این‌گونه لوازم از کار افتاده را منهدم کرده و امکان بهره برداری مجدد را از آن‌ها بگیرید. اغلب کامپیوترهای مستعمل و از رده خارج شده دارای اطلاعات ارزشمندی است که در هنگام تعویض یا فروش بر اثر سهل انگاری در سیستم‌ها باقی مانده است. هم‌چنین امکان بازیافت اطلاعات از حافظه‌های پاک شده سیستم وجود داشته و صرف پاک کردن یا فرمت کردن سیستم نمی‌توان از پاک شدن صد در صد آن‌ها اطمینان داشت. بنابراین بعضی از افراد تصور می‌کنند با پاک کردن هاردهای مستعمل تمام اطلاعات آن‌ها از بین رفته و می‌توانند آن‌ها را دور ریخته یا به فروش برسانند.

۷- هرگز به تماس‌های تلفنی از طریق اینترنت اعتماد نداشته باشید.
امروز اغلب تلفن‌های خارج از کشور توسط تماس‌های تلفنی اینترنتی صورت می‌گیرد که کارت‌های خدماتی آن‌ها در همه جا قابل دسترس می‌باشد. از آن‌جا که شرکت‌های خدمات اینترنت (آی- اس- پی) و کشورهای سرویس دهنده (بک بن) توانایی استراق سمع تمامی مکالمات تلفنی را دارند. استفاده از این ارتباطات نیز ناامن و غیرمطمئن می‌باشد.

۸- هرگز از مشخصات اصلی خود در محیط اینترنت استفاده نکنید.
در هنگام حضور افراد در خارج از کشور یکی از راه‌های به‌دست آوردن اطلاعات از آن‌ها، مراجعه به فضای اینترنت می‌باشد. در صورتی که مشخصات شما در یک سایت یا ایمیل یا .... مشاهده گردد. اطلاعات با ارزشی نسبت به شما می‌تواند به‌دست آید.

۹- هرگز از کامپیوتر مخصوص اینترنت برای کارهای متفرقه استفاده ننمائید.
در نظر دشته باشید که مودم، پرینتر، اسکنر و بعضی از اجزای داخلی کامپیوتر «آی- پی» پذیر بوده و می‌تواند اطلاعات خود را به آدرس برنامه ریزی شده از طریق اینترنت ارسال کنند. بنابراین ممکن است نامه‌ای که تایپ کرده و پرینت گرفته‌اید و حتی از کامپیوتر خود را که پاک کرده‌اید، بعد از آن‌که به اینترنت متصل می‌شوید، به آدرس برنامه ریزی شده ارسال گشته بدون آن‌که شما از آن مطلع گردید.

۱۰- هرگز نسبت به محافظت و نگهداری نسخه ذخیره اطلاعات backup بی تفاوت نباشید.
معمولاً به‌خاطر محافظت از اطلاعات و پیش‌گیری از تخریب آن‌ها اقدام به تهیه نسخه‌های ذخیره می‌نمایند. حفاظت و نگهداری این نسخه‌ها حتی از اطلاعاتی که در سیستم‌ها نگهداری می‌شوند با اهمیت‌تر می‌باشد. زیرا این اطلاعات به‌صورت آماده و بدون دردسر می‌باشند. سهل انگاری در نگهداری از این نسخه‌های ذخیره بعضاً معضلات جبران ناپذیری در بر خواهد داشت.

11 هرگز در مواقع غیرضروری سیستم خود را به شبکه اینترنت متصل ننمائید.
اغلب در ارتباطات لیزلاین و شبکه‌ای، ارتباط اینترنتی به‌صورت پیوسته و شبانه روزی است. اما با توجه به تهدیداتی که از این طریق برای سیستم شما متصور است، در مواقعی که نیازی به ارتباط با اینترنت ندارید، آن را قطع نمائید تا از گزند هکرها و جاسوسان اینترنتی و عوامل بیگانه در امان باشید. هکرها توانائی فعال‌سازی میکروفن و دوربین (وب کم) شما را بدون توافق با شما را دارند. لذا با توجه به متصل بودن بی‌مورد و طولانی مدت سیستم شما به اینترنت این‌گونه خطرات همواره متصور است.

12-هرگز نسبت به تهیه نسخه ذخیره از اطلاعات درون رایانه خود مسامحه نکنید.
رایانه‌ها ابزار قابل اطمینانی نیستند و همواره احتمال صدمه دیدن آن‌ها متصور است لذا همیشه سعی کنید از اطلاعات داخل سیستم خود یک نسخه ذخیره داشته باشید تا در صورت بروز هرگونه اختلالی اطلاعات شما در اختیارتان باشد.

13- هرگز به موارد شناخته نشده در اینترنت پاسخ ندهید.
ایمیل‌های ناشناخته یکی از موارد بوده که هرگز نباید آن‌ها را گشود، زیرا در مواردی با گشودن ایمیل یا یک تصویر اینترنتی تروجانی از این طریق وارد سیستم شما گشته و مراحل کار جاسوسی و نفوذ به سیستم شما را آغاز می‌نماید یا پنجره‌هایی که در خلال کار با اینترنت به‌صورت ناخواسته ظاهر گشته یا درخواست‌های اشتراک در سایت، شما را ترغیب به دادن نام کاربر و نام عبور می‌نماید که از این طریق اطلاعات مربوط به رمز عبور شما را در اختیار گرفته و از آن بهره برداری کنند.

اجازه ندهید فرد دیگری از حساب کاربری شما استفاده کند
حساب کاربری شما نشان دهنده تمام منابعی است که فقط شما مجاز به دسترسی به آن هستید. اگر به شخص دیگری اجازه دهید که به حساب کاربری شما دسترسی پیدا کند، هر کاری که او انجام می دهد، مسئولیت آن بر عهده شما خواهد بود.

از درایوهای شبکه برای فایل های حساس یا مهم استفاده کنید
تمام پرونده هایی حاوی اطلاعات حساس یا مهم، تا زمانی که مورد نیاز هستند،باید در یک درایو شبکه ذخیره شوند. هر کسی که به کامپیوتر دسترسی فیزیکی داشته باشد، می تواند یک یا چند راه دسترسی به فایل های ذخیره شده در درایو های محلی کامپیوتر پیدا کند. درایو های کامپیوتری معمولا با حروفی مانند " " :Fنامگذاری می شوند.

زمانی که قصد دارید میز کار خود را برای مدت کوتاهی ترک کنید، کامپیوتر خود را در حالت قفل شده قرار دهید
حتی اگر از قوی ترین رمز عبور دنیا هم استفاده کنید، کافیست چند دقیقه به دور از میز کار خود باشید و کامپیوتر خود را در حالت قفل نشده قرار دهید تا سیستم شما هک بشود. زمان ترک میز کار خود در ویندوز کلیدهای Ctrl-Alt-Delرا هم زمان فشار داده و قفل ایستگاه کاری را انتخاب کنید. همچنین هنگامی که در محل کار هستید سعی کنید کامپیوتر خود را طوری قرار دهید که صفحه نمایش شما توسط بازدیدکنندگان معمولی مشاهده نشود.

از رمز عبور قوی استفاده کنید و آن را مخفی نگه دارید

هنگامی که قصد ترک محل کار را دارید کامپیوتر خود را خاموش نمایید

هر شب وقتی قصد دارید محل کار خود را ترک کنید، کامپیوتر خود را خاموش نمایید. کامپیوتری که خاموش باشد نمی توان آن را با حملات سایبری آلوده کرد.

از رمزگذاری برای مشاهده و تبادل اطلاعات حساس استفاده کنید

برای مشاهده وب سایت های حاوی اطلاعات حساس همیشه باید از رمزگذاری استفاده کنید. اگر آدرس وب با https شروع شود، می توانید بگویید این وب سایت از رمزگذاری استفاده می کند. اگر شما یک وب سایت ایجاد کرده اید که داده های حساس را جمع آوری می کند، باید مطمئن شوید که سایت در هنگام ارسال داده های کاربران از رمزگذاری استفاده می کند و داده ها، هنگامی که ارسال می شوند، به صورت ایمن ذخیره می شوند. اگر شما قصد انتقال داده های حساس از طریق ایمیل را دارید، باید اطلاعات را از طریق یک فایل پیوست که با رمز عبور محافظت شده است، ارسال کنید.

نرم افزار های تایید نشده را نصب نکنید
هر نرم افزاری که به صورت رایگان در فضای اینترنت وجود دارد را نصب نکنید. این برنامه ها اغلب خطر های امنیتی بزرگی را برای کاربران در پی خواهند داشت. سعی کنید از برنامه هایی که توسط مراکز معتبر تایید شده اند استفاده کنید.

قبل از باز کردن پیوست های ایمیل فکر کنید
از باز کردن ایمیل هایی که حاوی پیوست های مشکوک هستند خودداری نمایید، حتی اگر از طرف کسی ارسال شده باشد که شما او را می شناسید. قبل از باز کردن پیوست با آن شخص تماس بگیرید و اطمینان حاصل کنید که بسته ارسالی معتبر می باشد.

از یک برنامه آنتی ویروس در کامپیوتر خود استفاده کنید
سعی کنید برای محافظت از کامپیوتر خود از یک نرم افزار آنتی ویروس قدرتمند استفاده نمایید.
نرم‌افزار های آنتی‌ویروس سه وظیفهٔ عمده را انجام می‌دهند: ۱. بازرسی یا کشف ۲. تعیین هویت یا شناسایی ۳. آلودگی‌زدایی یا پاکسازی

هنگام استفاده از مرورگر اینترنت اکسپلورر احتیاط کنید
مرورگر وب اینترنت اکسپلورر که همراه با ویندوز مایکروسافت عرضه شد، تقریبا هر ماه یک مشکل امنیتی جدید دارد. توصیه می شود به جای آن از موزیلا فایرفاکس یا گوگل کروم استفاده نمایید و از اینترنت اکسپلورر فقط هنگام مراجعه به وب سایت هایی که به آن نیاز دارند استفاده کنید.

آفلاین باشید.
ممکن است که بدون آب و غذا چند روز یا حتی چند هفته هم زنده بمانیم اما بدون اینترنت، یک روز هم دوام نخواهیم آورد! شاید کمی این قضیه را دراماتیک جلوه داده باشیم اما واقعاً برای بیشتر افراد این موضوع صدق می کند. زیاد در این باره شنیده ایم که ممکن است روزی مجبور شویم کارهایمان را آفلاین انجام دهیم، پس چه خوب است که از هم اکنون به جدایی از فضای مجازی عادت کرده و مدت زمان حضورمان را در اینترنت، به حد نیاز کاهش دهیم. ممکن است در ابتدا انجام این کار برای شما دور از ذهن به نظر برسد اما بهتر است بدانید که شانس هک کردن شما توسط هکرها در زمانی که به اینترنت متصل باشید، ۲۴/۷ برابر خواهد شد.

امنیت فیزیکی را هم در نظر بگیرید.

با وجود تمامی حوادث امنیت سایبری و حفاظت از امنیت دیجیتالی، فراموش نکنیم که امنیت فیزیکی دستگاه های دیجیتالی مان به اندازه امنیت سایبری آنها دارای اهمیت است. لپ تاپ ها و تبلت ها با توجه به وزن کم و اندازه کوچک شان، بیشتر در معرض خطر سرقت قرار دارند. بنابراین هنگامی که در مکان های عمومی چنین تجهیزاتی را حمل کرده یا از آنها استفاده می کنید، بیشتر مراقب باشید. وارد شدن فشار فیزیکی زیاد به این دستگاه ها نیز می تواند یکی از مشکلاتی باشد که می توان با رعایت دستورالعمل های اولیه ایمنی، از آنها جلوگیری کرد.

پشتیبان گیری، پشتیبان گیری و باز هم پشتیبان گیری

این نکته باید در رأس تمامی فعالیت های شما قرار گیرد. به دنبال افزایش حملات سایبری در سال های اخیر، پشتیبان گیری از اطلاعات به طور منظم، مهم ترین اقدامی است که همه ما باید آن را انجام دهیم؛ مگر این که اطلاعات مان برایمان مهم نباشد. پس داشتن نسخه پشتیبان از اطلاعات مهم می تواند مانعی جدی برای جلوگیری از، از دست رفتن اطلاعات باشد.

گذر واژه ها را جایی یادداشت نکرده ودر رایانه خود ذخیره ننمایید

وی‌پی‌ان VPN

برای اینکه هویت شما در فضای آنلاین از دید مجرمان سایبری پنهان شده و قادر به نظارت بر رفتارهای شما نباشند، حتماً باید از یک وی‌پی‌ان معتبر و قابل اعتماد استفاده کنید. وی‌پی‌ان یا شبکه خصوصی مجازی، داده‌هایی را که از طریق اینترنت ارسال و دریافت می‌کنید، رمزنگاری می‌کند. لازم به ذکر است استفاده از وی‌پی‌ان برای کارمندان دورکاری که خواهان برقراری ارتباطات امن با محیط کارشان هستند، بسیار مفید و ضروری است.
یکی از روش‌های آسان برای تهیه یک سرویس وی‌پی‌ان، خرید بسته‌های امنیتی کامل است که معمولاً شامل نرم افزار ضدویروس، فایروال، ابزار ضدهرزنامه و یک وی‌پی‌ان هستند.

مهندسی اجتماعی
Social Engineering

مهندسی اجتماعی Social Engineering

یک روش **مجرمانه** است که در آن تلاش می‌شود تا به طور غیرمستقیم و با استفاده از تاثیرگذاری بر روی عواطف، روان‌شناسی و رفتار افراد، اطلاعات محرمانه را به دست آورد، دسترسی به سیستم‌ها و منابع محدود را کسب کند یا فعالیت‌های غیرقانونی را انجام دهد. در واقع، مهندسی اجتماعی به معنای بهره‌برداری از ضعف‌ها و نقاط ضعف روانی و اجتماعی افراد به منظور دستیابی به اهداف خود است. روش‌های مهندسی اجتماعی شامل تکنیک‌ها و فنون متنوعی است که استفاده از آن‌ها می‌تواند شامل تهدیدات دروغین، مراحل تست نفوذ (penetration testing)یا هرگونه فعالیت مجرمانه‌ای باشد که به منظور دسترسی به شبکه‌های سازمانی انجام می‌شود. این روش‌ها می‌توانند شامل تقلید هویت، تکنیک‌های مهندسی اجتماعی، استفاده از تکنیک‌های جعلی و تلاش برای متقاعد کردن افراد به ارائه اطلاعات محرمانه، کلمات عبور یا دسترسی به سیستم‌ها باشند. اهداف مهندسی اجتماعی می‌تواند شامل دستیابی به اطلاعات حساس، سرقت هویت، دسترسی غیرمجاز به سیستم‌ها و شبکه‌ها، به دست آوردن رمزهای عبور، انجام تقلب مالی یا بهره‌برداری از اعتماد و هویت افراد باشد.

برای مقابله با مهندسی اجتماعی، آگاهی و آموزش افراد درباره روش‌ها و تکنیک‌های مهندسی اجتماعی بسیار مهم است. همچنین، اعمال سیاست‌ها و فرآیندهای امنیتی، استفاده از سیستم‌های شناسایی و پیشگیری از تهدیدات امنیتی نیز می‌تواند مؤثر باشد.

مهندسی اجتماعی از کجا شروع شد؟

مهندسی اجتماعی به عنوان یک روش برای تاثیرگذاری بر رفتار افراد و دستیابی به اطلاعات محرمانه، ریشه تاریخی دارد و تاریخچه آن به قبل از ظهور رایانه‌ها می‌رسد. در واقع، این روش بر اساس بهره‌برداری از ضعف‌ها و نقاط ضعف انسانی به منظور دستیابی به اهداف مدنظر افراد مورد استفاده قرار می‌گرفتند.

به عنوان مثال، مهندسی اجتماعی در قرن نوزدهم و قرن بیستم، در حوزه امنیت فیزیکی به کار گرفته می‌شد. افراد با استفاده از ترفندها و تکنیک‌های روان‌شناختی، سعی می‌کردند به ساختمان‌ها نفوذ کنند که به طور عادی دسترسی به آن‌ها امکان‌پذیر نبو.د. در این موارد، مهندسی اجتماعی به معنای تاثیرگذاری بر روی افراد از طریق نشان داده خود به عنوان یک فرد مهم، دروغ‌گویی یا تزویر هویت برای عبور از سیستم‌های امنیتی بود.

با پیشرفت فناوری و گسترش رایانه‌ها و اینترنت، مهندسی اجتماعی به طور گسترده‌تر در فضای سایبری نیز به کار گرفته شد. هکرها و نفوذگران با استفاده از روش‌های مهندسی اجتماعی، سعی می‌کنند از طریق فریب و تقلب افراد، اطلاعات حساس را بدست آورند، به سیستم‌ها و شبکه‌های کامپیوتری نفوذ کنند و فعالیت‌های مخرب انجام دهند.

به همین دلیل، مهندسی اجتماعی امروزه به عنوان یک تهدید جدی در حوزه امنیت سایبری شناخته می‌شود و تقریبا در هر صنعت و سازمانی که از فناوری استفاده می‌کند، رخدادهای مربوط به مهندسی اجتماعی ممکن است رخ دهد.

مهندسی اجتماعی در زیرمجموعه چه علمی قرار می‌گیرد؟

مهندسی اجتماعی در واقع یک زیرشاخه از علوم اجتماعی محسوب می‌شود. این حوزه علمی در تلاش است تا با استفاده از دانش اجتماعی، روانشناسی اجتماعی و تحلیل رفتار انسانی، به درک عملکرد اجتماعی افراد و گروه‌ها بپردازد. هدف اصلی مهندسی اجتماعی، درک و تحلیل رفتار اجتماعی افراد و بهره‌گیری از آن در طراحی سیستم‌ها، فرآیندها و راهبردهایی است که بتواند رفتار و تصمیم‌گیری افراد را تحت تأثیر قرار دهد.
با توجه به ماهیت ترکیبی علوم اجتماعی، روانشناسی و فناوری اطلاعات، مهندسی اجتماعی پیوندی بین علوم انسانی و فناوری محسوب می‌شود. این علم به طور گسترده در حوزه‌های امنیت اطلاعات، امنیت سایبری، مدیریت ریسک، طراحی رابط کاربری و همچنین در سازمان‌ها و سیستم‌های اجتماعی کاربرد دارد.

تکنیک های مهندسی اجتماعی چگونه می‌توانند در حملات تست نفوذ مورد استفاده قرار بگیرند؟

روش‌های مهندسی اجتماعی در حملات تست نفوذ به عنوان یک ابزار مؤثر برای نفوذ به سیستم‌ها و شبکه‌ها استفاده می‌شوند. این روش‌ها به طور خلاصه بر اساس تقلب و تاثیرگذاری بر رفتار انسانی، تلاش می‌کنند تا اطلاعات حساس را به دست آورده و دسترسی غیرمجاز به منابع را فراهم کنند. در زیر تعدادی از روش‌های مهندسی اجتماعی که در حملات تست نفوذ مورد استفاده قرار می‌گیرند را بررسی می‌کنیم:

فریب و فریبکاری (:(Phishingدر این روش، حمله‌کننده با استفاده از ایمیل‌ها، پیامک‌ها یا صفحات وب جعلی، سعی می‌کند به طور مشابه با یک سازمان یا خدمات معروف، افراد را فریب دهد و اطلاعات حساس مانند نام کاربری و رمز عبور را دریافت کند.

سوء استفاده تلفنی (:(Vishingدر این روش، حمله‌کننده با تماس تلفنی با قربانی، تلاش می‌کند خود را یکی از کارمندان سازمان نشان دهد که از یک تلفن معتبر تماس گرفته و نیازمند اطلاعات است.

روش دوست یا دشمن مشترک Friend or Foeدر این روش، حمله‌کننده با تعامل و برقراری رابطه با افراد درون یک سازمان یا شبکه، سعی می‌کند اعتماد و همکاری آن‌ها را جلب کند و سپس درخواست‌های خود را برای دسترسی به منابع محدود یا اطلاعات حساس از آن‌ها مطرح کند.

جعل هویت Impersonationدر این روش، حمله‌کننده به نمایندگی از یک شخصیت یا سازمان مورد اعتماد، سعی می‌کند افراد را فریب دهد و اطلاعات حساس را به دست آورد. به طور مثال، با استفاده از ساخت یک اکانت ایمیل جعلی منتصب به مدیر عامل یک سازمان سعی می‌کند از کارمندان بخش مالی اطلاعاتی در ارتباط با میزان فروش یا شماره حساب‌ها به دست آورد.

جمع‌آوری اطلاعات Information Gathering در این روش، حمله‌کننده با استفاده از منابع عمومی و اطلاعات در دسترس، اطلاعاتی درباره هدف خود (مانند شرکت، سازمان یاشخص) جمع‌آوری می‌کند. این داده‌ها می‌توانند شامل اطلاعات افراد، ساختار سازمانی، نقاط ضعف امنیتی و غیره باشند. این اطلاعات به حمله‌کننده کمک می‌کنند تا در مراحل بعدی حمله بهتر برنامه‌ریزی کند.

مهندسی اجتماعی در حملات تست نفوذ به عنوان یک روش مؤثر برای به دست آوردن دسترسی غیرمجاز و اطلاعات حساس استفاده می‌شود. با توجه به اینکه مهندسی اجتماعی بر روی عوامل انسانی تمرکز دارد و ضعف‌ها و آسیب‌پذیری‌های انسانی را بهره‌برداری می‌کند، آگاهی و آموزش افراد درباره روش‌های مهندسی اجتماعی و رفتارهای مورد توجه در برابر آنها می‌تواند بهبود قابل توجهی در امنیت سازمان‌ها و سیستم‌ها به همراه داشته باشد.

اساس کار مهندسان اجتماعی چیست؟

مهندسی اجتماعی فرایندی است که در آن حمله‌کنندگان سعی می‌کنند به طور غیرمجاز به اطلاعات حساس و محرمانه دسترسی پیدا کنند یا افراد را به اقداماتی ناخواسته تحریک کنند. این روش، بر خلاف روش‌های سنتی نفوذ به سیستم‌ها که معمولا از طریق شکاف‌ها و ضعف‌های فنی بهره می‌برند، بر روی انسان و عوامل اجتماعی تمرکز دارد.
مهندسان اجتماعی با استفاده از تکنیک‌ها و روش‌های مختلف، سعی در فریب و تحت فشار قرار دادن افراد دارند تا به اطلاعات محرمانه دسترسی پیدا کنند یا اقداماتی را انجام دهند که به ضرر فرد یا سازمان مورد نظر است. این تکنیک‌ها ممکن است شامل موارد زیر باشند:

فریب: مهندسان اجتماعی اغلب با استفاده از شخصیت‌پردازی و تیترهای جذاب، سعی می‌کنند فرد را به اعمالی نادرست تشویق کنند. به طور مثال، با ارسال ایمیل‌های جعلی از نام یک سازمان معتبر، درخواست ارائه اطلاعات حساب بانکی یا رمز عبور را می‌کنند.

تهدید و فشار: مهندسان اجتماعی ممکن است از تهدید، ترس و فشار برای متقاعد کردن فرد به انجام اقدامات خاص استفاده کنند. به طور مثال، با تهدید انتشار اطلاعات شخصی، فرد را مجبور به ارائه اطلاعات حساس می‌کنند.

ایجاد اعتماد غیرمجاز: مهندسان اجتماعی ممکن است با شناختن جزئیاتی از فرد یا سازمان، اعتماد او را جلب کنند و در نتیجه به اطلاعات محرمانه دسترسی پیدا کنند. به طور مثال، با استفاده از تماس تلفنی در نقش یک کارمند داخلی سازمان، اعتماد فرد را جلب کرده و اطلاعات محرمانه را دریافت می‌کنند.

جمع‌آوری اطلاعات:

مهندسان اجتماعی ممکن است از روش‌های جمع‌آوری اطلاعات متنوع مانند تحقیقات آنلاین، مطالعه پروفایل‌های شبکه‌های اجتماعی، بررسی زباله‌ها و مستندات موجود برای دستیابی به اهداف خود از ترکیب مهارت‌های فنی و دانش روانشناختی استفاده می‌کنند. آن‌ها معمولا تحقیقات جامعی درباره هدف خود انجام می‌دهند، از جمله مطالعه رفتارها، عادات، ترجیحات و الگوهای رفتاری فرد یا سازمانی که قصد دستیابی به آن را دارند. سپس، با استفاده از اطلاعات به دست آمده، تکنیک‌های اجتماعی و روانشناختی را به کار می‌برند تا فرد را متقاعد کنند تا اقدامات مورد نظر را انجام دهد یا اطلاعات حساس را فاش کند.
اهداف مهندسان اجتماعی می‌تواند متنوع باشد، از جمله دسترسی غیرمجاز به سیستم‌ها و شبکه‌های کامپیوتری، سرقت هویت، دستیابی به اطلاعات مالی یا حساس، و یا تحت تأثیر قرار دادن افراد برای کسب منافع شخصی یا سیاسی.
از آنجایی که مهندسی اجتماعی بر روی عوامل انسانی تمرکز دارد و در بسیاری از موارد با استفاده از فریب و تلاش برای ایجاد اعتماد غیرمجاز عمل می‌کند، آگاهی و آموزش درباره تهدیدات امنیتی و تکنیک‌های مهندسی اجتماعی می‌تواند به شناسایی و پیشگیری از این نوع حملات کمک کند.

فرایند حمله مهندسان اجتماعی چگونه است؟

فرایند حمله مهندسان اجتماعی ممکن است به شکل زیر انجام شود:

جمع‌آوری اطلاعات: مهندسان اجتماعی در ابتدا اطلاعات لازم را درباره فرد یا سازمان هدف جمع‌آوری می‌کنند. این موضوع شامل مطالعه پروفایل‌های شبکه‌های اجتماعی، تحقیقات آنلاین، بررسی زباله‌ها و مستندات، مصاحبه با افراد مرتبط و کسب اطلاعات روان‌شناختی است. هدف این مرحله، به دست آوردن اطلاعاتی است که در مراحل بعدی برای فریب و تحت فشار قرار دادن فرد مورد نظر مورد استفاده قرار می‌گیرد.

برقراری رابطه: مهندسان اجتماعی برای برقراری ارتباط با فرد هدف از روش‌های مختلفی استفاده می‌کنند. این روش‌ها شامل تماس تلفنی، ارسال ایمیل، ارسال پیامک یا استفاده از رسانه‌های اجتماعی است. آن‌ها معمولا با استفاده از تیترها و جملات جذاب، تلاش می‌کنند اعتماد فرد را جلب کنند و در راستای اهداف خود حرکت کنند.

فشار و ترغیب: مهندسان اجتماعی برای به دست آوردن اطلاعات حساس یا تحریک فرد به اقدامات ناخواسته از تهدید و فشار استفاده می‌کنند. آن‌ها ممکن است با تهدید انتشار اطلاعات شخصی، فرد را مجبور به ارائه اطلاعات محرمانه کنند یا تلاش کنند تا با ایجاد ترس و نگرانی، فرد را به اقدامات مورد نظر تحریک کنند.

بهره‌برداری از ضعف‌ها و اشتباهات: مهندسان اجتماعی ممکن است با بررسی ضعف‌ها و اشتباهات در رفتار و روند کاری فرد یا سازمان، از آن‌ها بهره ببرند. آن‌ها می‌توانند با استفاده از این ضعف‌ها و اشتباهات، اطلاعات محرمانه را سرقت کنند یا اقدامات خاصی را انجام دهند.
استفاده از تکنیک‌های روانشناختی: مهندسان اجتماعی از تکنیک‌های روانشناختی برای متقاعد کردن فرد به انجام اقدامات خاص استفاده می‌کنند. این تکنیک‌ها شامل استفاده از ترس، دعوت به مهمانی‌ها، پیشنهادهای مالی و غیره است.
استفاده از فناوری: مهندسان اجتماعی در برخی موارد ممکن است از تکنیک‌های فنی و فناوری برای حمله استفاده کنند. این موضوع شامل ارسال ایمیل‌های فیشینگ ((Phishing، ایجاد صفحات وب تقلبی، استفاده از برنامه‌های مخرب (مانند نرم‌افزارهای جاسوسی یا بدافزارها) و سایر روش‌های مشابه است.

دسترسی به هدف: پس از به دست آوردن اطلاعات مورد نیاز یا محرک کافی، مهندسان اجتماعی سعی می‌کنند به هدف نفوذ کنند. این موضوع می‌تواند شامل دسترسی به سیستم‌های کامپیوتری، حساب‌های آنلاین، شبکه‌های اجتماعی یا سایر منابع مرتبط باشد.

استفاده و غربالگری اطلاعات: پس از دسترسی به هدف، مهندسان اجتماعی از اطلاعات به دست آمده بهره‌برداری می‌کنند. آن‌ها ممکن است اطلاعات محرمانه را دزدیده و استفاده کنند، اطلاعات را تغییر دهند یا آن‌ها را برای اهداف خود غربالگری کنند.
نکته مهمی که باید به آن توجه کنید این است که حملات مهندسی اجتماعی بسیار پیچیده و متنوع هستند و روش‌هایی که در بالا ذکر شده، تنها چند مثال از آن‌ها هستند. همچنین، آگاهی و محافظت از اطلاعات شخصی و آموزش درباره روش‌های مهندسی اجتماعی می‌تواند به شما کمک کند تا از خودتان در برابر این نوع حملات محافظت کنید.

انواع تکنیک های مهندسی اجتماعی

روش‌های مهندسی اجتماعی متنوع هستند و به توانایی مهندسان اجتماعی در فریب و تحت فشار قرار دادن افراد و سازمان‌ها بستگی دارد. در زیر به برخی از روش‌های مهندسی اجتماعی پرکاربرد اشاره می‌کنم:

فیشینگ (Phishing): در این روش، مهندسان اجتماعی با ارسال ایمیل‌ها، پیامک‌ها یا پیام‌های ناخواسته با هدف جلب توجه فرد، اطلاعات شخصی و حساس از جمله رمز عبور، اطلاعات بانکی یا اطلاعات کاربری را جمع‌آوری می‌کنند. این ایمیل‌ها معمولا به ظاهر شکل رسمی دارند و از طرف سازمان‌ها یا خدمات آنلاین برای قربانی ارسال می‌شوند و فرد را به مشارکت تشویق می‌کنند.

مهندسی اجتماعی (Social Engineering): در این روش، مهندسان اجتماعی از رویکردهای اجتماعی برای تحت فشار قرار دادن افراد استفاده می‌کنند. آن‌ها ممکن است با تلاش برای ایجاد اعتماد، دوستی یا رابطه حرفه‌ای با فرد هدف، اطلاعات محرمانه را دریافت کنند یا اقدامات خاصی را از فرد تحریک کنند.

تماس تلفنی Vishing در این روش، مهندسان اجتماعی با تماس تلفنی با هدف، تلاش می‌کنند او را متقاعد کنند که اطلاعات شخصی، مالی یا حساب کاربری خود را ارائه دهد. آن‌ها ممکن است به عنوان نمایندگان بانک، شرکت‌های خدمات مالی یا سازمان‌های دولتی خود را معرفی کنند.

تروجان اجتماعی Social Trojan در این روش، مهندسان اجتماعی با استفاده از برنامه‌ها و فایل‌های مخرب، فرد را تشویق می‌کنند تا آن‌ها را دانلود و نصب کند. این برنامه‌ها معمولا به عنوان نرم‌افزارهای مفید یا مورد نیاز به نظر می‌رسند، اما در واقع، اطلاعات شخصی را جمع‌آوری و برای هکرها ارسال می‌کنند.

تهدید و فشار: مهندسان اجتماعی ممکن است با تهدید انتشار اطلاعات شخصی یا حرفه‌ای مهم شوند یا با ایجاد فشار و ترس، افراد را مجبور به انجام اقدامات خاصی کنند. این موضوع می‌تواند شامل تهدید به افشای اطلاعات حساس، تهدید به آسیب رساندن به شخص یا همکارانش، یا تهدید به خرابکاری سیستم‌ها و شبکه‌های مورد استفاده فرد هدف باشد.

روش‌های مقابله با مهندسی اجتماعی

برای مقابله با مهندسی اجتماعی، روش‌ها و اقدامات زیر می‌توانند مفید باشند:

آموزش و آگاهی: آموزش کارکنان و کاربران درباره روش‌های مهندسی اجتماعی، شناسایی نشانه‌ها و رفتارهای مشکوک می‌تواند بسیار مؤثر باشد. افراد باید در مورد حملات مهندسی اجتماعی آگاه شوند و در صورت شک و تردید، به تیم امنیت سازمان گزارش دهند.

استفاده از فناوری: پیاده‌سازی فناوری‌های امنیتی مانند فیلترینگ ایمیل، عدم ورود به سایت‌های جعلی و استفاده از راهکارهای رمزنگاری و دسترسی محدود می‌تواند در کاهش اثرات مهندسی اجتماعی مؤثر باشد.

ارتقاء سیاست‌ها و راهکارهای امنیتی: سازمان‌ها باید سیاست‌ها و راهکارهای امنیتی قوی را پیاده‌سازی کنند. این موضوع شامل استفاده از پسوردهای قوی و تغییر دوره‌ای آن‌ها، اعتبارسنجی دو عاملی (۲FA)، مدیریت دسترسی، رمزنگاری اطلاعات حساس و مانیتورینگ فعالیت‌های ناشناس است.

ارزیابی امنیتی و آزمون نفوذ: انجام بررسی‌های امنیتی منظم و آزمون نفوذ در سازمان می‌تواند به شناسایی ضعف‌ها و نقاط ضعف امنیتی کمک کند. با شناسایی نقاط ضعف موجود در سیستم‌ها و فرآیندهای امنیتی، می‌توان اقدام به تقویت این نقاط نمود و از آسیب‌پذیری‌ها در برابر حملات مهندسی اجتماعی پیشگیری کرد.

افزایش آگاهی در مورد اطلاعات عمومی: سازمان‌ها و افراد باید اطلاعات عمومی درباره خود را محدود نگه دارند. اطلاعاتی مانند اطلاعات تماس، جزئیات شغلی، وضعیت اجتماعی و غیره می‌توانند توسط حمله‌کنندگان برای پیاده‌سازی فرایندهای مهندسی اجتماعی مورد استفاده قرار گیرند

ارتباط مستقیم و اعتمادسازی: در صورت بروز شک و تردید درباره هویت یک کاربر، مهم است که ارتباط مستقیم با شخص مورد نظر زیرنظر قرار بگیرد. برای اطمینان حاصل کردن از اعتبار هویت یک فرد، می‌توانید از روش‌های اعتمادسازی مانند تماس تلفنی مستقیم، استفاده از آدرس ایمیل رسمی و موارد مشابه استفاده کنید.

مراقبت از اطلاعات شخصی: بهتر است از اشتراک گذاری اطلاعات شخصی در شبکه‌های اجتماعی و سایر پلتفرم‌های آنلاین پرهیز کنید. اطلاعات شخصی مانند تاریخ تولد، شغل، محل زندگی و اطلاعات مالی می‌توانند توسط حمله‌کنندگان به منظور مهندسی اجتماعی به کار گرفته شوند.

آگاهی از روش‌های حمله: با شناخت روش‌های مهندسی اجتماعی رایج مانند پیامک جذاب، پیام‌های ایمیل جعلی، تماس‌های تلفنی تقلبی و غیره، می‌توانید از خود در برابر این نوع حملات محافظت کنید. همچنین، به روز بودن در مورد مهم‌ترین روش‌های حمله و الگوهای جدید اهمیت دارد.

تحلیل و بررسی حملات گذشته: بررسی حملات مهندسی اجتماعی گذشته و شناسایی الگوها و موارد مشابه می‌تواند به شما کمک کند تا از تکنیک‌های استفاده شده توسط حمله‌کنندگان آگاه شوید و اقدامات پیشگیرانه مناسب را اتخاذ کنید.

استفاده از نرم‌افزارهای امنیتی: استفاده از نرم‌افزارهای ضد ویروس، فایروال و آنتی‌اسپم می‌تواند به شما در تشخیص و جلوگیری از حملات مهندسی اجتماعی کمک کند.

مهم‌ترین نکته این است که در مقابله با مهندسی اجتماعی باید همواره مطلع و آگاه باشید، برنامه‌های امنیتی قوی را پیاده‌سازی کنید و با هوشیاری و دقت بیشتری تعاملات آنلاین و آفلاین را انجام دهید.

مراقب پیشنهادهای وسوسه انگیز باشید.
اگر پیشنهادی بیش از حد فریبنده به نظر می رسد ، قبل از پذیرفتن آن خوب فکر کنید. جستجو در مورد موضوع می تواند به شما کمک کند تا به سرعت تشخیص دهید که با یک پیشنهاد قانونی روبرو هستید یا یک دام.

حملات مهندسی اجتماعی اشکال مختلفی دارد و می توانند در هر جایی که با تعاملات انسانی دخیل است انجام شود. در ادامه پنج شکل متداول از حملات مهندسی اجتماعی دیجیتال آورده شده است.

طعمه گذاری Baiting

حملات طعمه گذاری همانطور که از نام آن نیز پیداست ، از یک وعده دروغین برای تحریک طمع یا کنجکاوی قربانی استفاده می کنند. آنها کاربران را به دامی سوق می دهند که اطلاعات شخصی آنها را دزدیده یا سیستم های آنها را به بدافزار آلوده می کند.
رایج ترین شکل طعمه گذاری از رسانه های فیزیکی برای پراکنده کردن بدافزار استفاده می کند. به عنوان مثال ، مهاجمان طعمه را به صورت درایوهای فلش آلوده به بدافزار در مناطق قابل توجهی که قربانیان بالقوه مطمئناً آنها را می بینند قرار می دهند. طعمه ظاهری معتبر دارد ، مانند برچسبی که آن را به عنوان لیست حقوق و دستمزد شرکت نشان می دهد.
قربانیان از روی کنجکاوی طعمه را برمی دارند و آن را وارد رایانه محل کار یا خانه می کنند و در نتیجه بدافزار خودکار روی سیستم نصب می شود.
کلاهبرداری طعمه گذاری لزوماً نباید در دنیای فیزیکی انجام شوند. انواع آنلاین طعمه گذاری شامل تبلیغات فریبنده ای است که منجر به ایجاد سایت های مخرب می شود یا کاربران را به بارگیری یک برنامه آلوده به بدافزار ترغیب می کند.

حملات مهندسی اجتماعی

ترس افزار Scareware

ترس افزار شامل بمباران قربانیان با هشدارهای دروغین و تهدیدات ساختگی است. در واقع کاربران را فریب می دهند که سیستمشان به بدافزار آلوده است ، و باعث می شود نرم افزاری نصب کنند که هیچ منفعتی (به جز برای مجرم) ندارد یا خود یک بدافزار است. از ترس افزار به عنوان نرم افزار فریب ، نرم افزار اسکنر سرکش و کلاهبرداری نیز یاد می شود.

نرم افزار تبلیغاتی Adware

بدافزاری است که مرورگر شما را مجبور می کند به سمت تبلیغات وب هدایت شود ، که اغلب خود به دنبال دانلود بیشتر نرم افزارهای مخرب هستند. همانطور که نیویورک تایمز متذکر می شود ، نرم افزارهای تبلیغاتی مزاحم اغلب به برنامه های "رایگان" وسوسه انگیز مانند بازی ها یا افزونه های مرورگر منتقل می شوند.

یک مثال متداول برای ترسناک بودن ، بنرهای پنجره ای با ظاهر قانونی است که هنگام مرور وب در مرورگر شما ظاهر می شوند و متن هایی از جمله "کامپیوتر شما ممکن است به برنامه های جاسوسی مضر آلوده شود" را نشان می دهد. این برنامه یا نصب این ابزار (که اغلب به بدافزار آلوده است) را برای شما پیشنهاد می کند ، یا شما را به یک سایت مخرب هدایت می کند که رایانه شما آلوده می شود.

یک مثال متداول برای ترسناک بودن ، بنرهای پنجره ای با ظاهر قانونی است که هنگام مرور وب در مرورگر شما ظاهر می شوند و متن هایی از جمله "کامپیوتر شما ممکن است به برنامه های جاسوسی مضر آلوده شود" را نشان می دهد. این برنامه یا نصب این ابزار (که اغلب به بدافزار آلوده است) را برای شما پیشنهاد می کند ، یا شما را به یک سایت مخرب هدایت می کند که رایانه شما آلوده می شود.

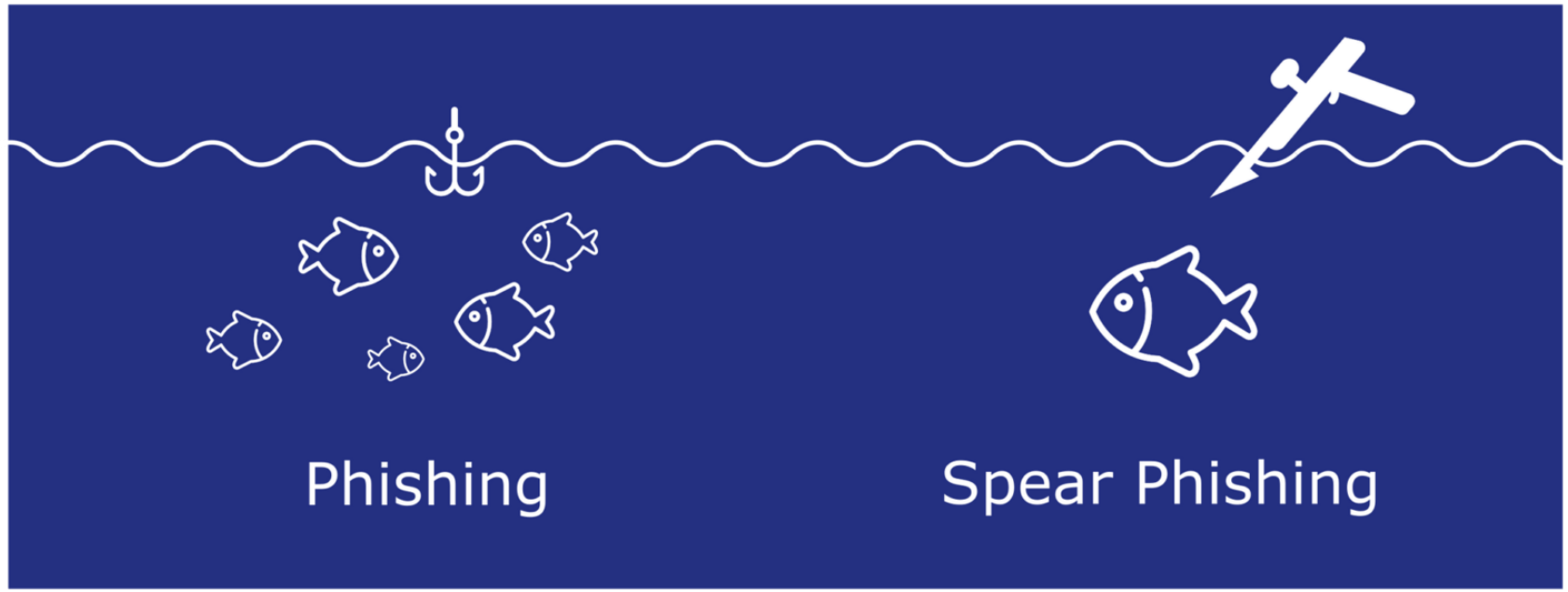
ترس افزار همچنین از طریق ایمیل اسپم توزیع می‌شود که هشدارهای جعلی را تایید می‌کند، و یا پیشنهاداتی برای کاربران برای خرید خدمات بی‌ارزش و مضر ارائه می‌دهد.

بهانه سازی Pretexting

در اینجا یک مهاجم اطلاعات را از طریق یک سری دروغ های هوشمندانه بدست می‌آورد. این کلاهبرداری اغلب توسط مجرمی شروع می‌شود که وانمود می‌کند به اطلاعات حساس یک قربانی نیاز دارد تا یک کار مهم و ضروری را انجام دهد.
مهاجم معمولاً با اعتماد به نفس در مقابل قربانی خود با جعل هویت از همکاران ، پلیس ، مقامات بانکی و مالیاتی یا سایر اشخاصی که دارای قدرت شناخت درست هستند ، شروع می کند. بهانه گیر سوالاتی را مطرح می کند که ظاهراً برای تأیید هویت قربانی لازم است ، و از طریق آنها اطلاعات شخصی مهم را جمع آوری می کند.
انواع اطلاعات و سوابق مربوطه با استفاده از این کلاهبرداری مانند شماره های تأمین اجتماعی ، آدرس های شخصی و شماره تلفن ها ، سوابق تلفن ، تاریخ تعطیلات کارکنان ، سوابق بانکی و حتی اطلاعات امنیتی مربوط به گیاه فیزیکی جمع آوری می شود.

فیشینگ Phishing

کلاهبرداری فیشینگ به عنوان یکی از محبوب ترین انواع حمله های مهندسی اجتماعی، عبارتند از برنامه های ایمیل و پیام کوتاه با هدف ایجاد احساس اضطرار ، کنجکاوی یا ترس در قربانیان است. سپس آنها را ترغیب کرده تا اطلاعات حساس را فاش کنند ، روی پیوندها به وب سایتهای مخرب کلیک کنند یا پیوستهایی را که حاوی بدافزار هستند باز کنند.
به عنوان مثال ایمیلی برای کاربران یک سرویس آنلاین ارسال شده است که به آنها در مورد نقض خط مشی هشدار می دهد که نیاز به اقدام فوری از طرف آنها مانند تغییر گذرواژه دارد. این شامل لینک به یک وب سایت غیرقانونی است که تقریباً از نظر ظاهری با نسخه قانونی آن تقریباً یکسان است و باعث می شود کاربر اعتبار فعلی و رمز ورود جدید خود را وارد کند. پس از ارسال فرم ، اطلاعات برای مهاجم ارسال می شود.
با توجه به اینکه پیامهای یکسان یا تقریباً یکسان در کمپین های فیشینگ برای همه کاربران ارسال می شود ، شناسایی و مسدود کردن آنها برای سرورهای نامه ای که به سیستم عامل های اشتراک تهدید دسترسی دارند بسیار آسان تر است.


Phishing
Spear Phishing

فیشینگ نیزه ای Spear phishing

فیشینگ نیزه ای یک نسخه هدفمندتر از حمله فیشینگ است که به موجب آن مهاجم، افراد یا شرکت های خاصی را انتخاب می کند. آنها سپس پیام های خود را بر اساس ویژگی ها ، موقعیت های شغلی و ارتباطات متعلق به قربانیان خود تنظیم می کنند تا حمله آنها کمتر مشهود شود. فیشینگ نیزه ای به تلاش بیشتری از سوی مجرم احتیاج دارد و ممکن است هفته ها و یا ماه ها طول بکشد تا متوقف شود. اگر با مهارت انجام شوند ، تشخیص آنها بسیار دشوارتر و میزان موفقیت آن ها بالاتر است.
یک سناریوی فیشینگ نیزه ای ممکن است شامل یک مهاجم باشد که به عنوان مشاور ITسازمان، یک ایمیل برای یک یا چند کارمند ارسال می‌کند. این نامه دقیقا همان طور که مشاور به طور معمول انجام می‌دهد، نوشته شده و امضا شده‌است، در نتیجه دریافت کنندگان را طوری فریب می‌دهد که فکر می‌کنند این یک پیام معتبر است. این پیام باعث می‌شود که گیرنده رمز عبور خود را تغییر داده و آن‌ها را با یک لینک هدایت کند که آن‌ها را به صفحه مخربی که در آن مهاجم اعتبار آن‌ها را ثبت می‌کند، هدایت می‌کند.