Ouch! جولای 2022

حملات فیشینگ فریبنده تر میشوند

حملات فیشینگ به شایع ترین روشی که مهاجمین سایبری برای هدف قراردادن افراد در منزل و محل کار استفاده میکنند، تبدیل شده است. به صورت سنتی حملات فیشینگ، ایمیلهایی هستند که مهاجمین سایبری برای فریب شما به انجام کاری که نباید انجام دهید ارسال میکنند، مانند باز کردن ضمیمه های آلوده در ایمیل، کلیک روی یک لینک مخرب، یا به اشتراک گذاشتن رمزعبورتان. در شرایطی که امروز هنوز حملات فیشینگ سنتی ادامه دارد، مهاجمین سایبری زیادی نیز حملات فیشینگ با ایمیلهای پیشرفته تری میسازند که بیشترسفارشی سازی شده است و شناسایی آنها سخت تر میباشد. آنها همچنین از فناوریهایی مانند پیامهای متنی، رسانه های اجتماعی، یا حتی تماسهای تلفنی برای تعامل و فریب شما بهره میبرند. در اینجا آخرین ترفندها و نحوه تشخیص آنها را ذکر میکنیم.

مهاجمین سایبری در حال انجام تحقیقات خود هستند.

قبلا شناسایی ایمیل‌های فیشینگ آسان‌تر بود، زیرا آنها پیام‌هایی عمومی و کلی بودند که برای میلیون‌ها نفر به صورت تصادفی ارسال می‌شدند. مهاجمین سایبری هیچ ایده ای از اینکه چه کسانی قربانی آنها خواهند شد نداشتند، آنها فقط میدانستند هر چه ایمیل بیشتری ارسال کنند احتمال فریب خوردن افراد بیشتری میباشد. ما اغلب میتوانستیم این حملات را با گشتن به دنبال جملات مشکوک در ابتدای آنها مانند"مشتری عزیز"، وجود غلط املایی و یا پیغامی که برای حقیقی بودن خیلی خوب جلوه میکرد شناسایی کنیم، همانند این ایمیل که یک پرنسس نیجریه ای به شما میلیونها دلار پیشنهاد میدهد.

مهاجمین سایبری امروزی بسیار پیچیده تر هستند. امروزه آنها در مورد قربانیان مورد نظر خود برای ایجاد یک حمله سفارشی تر تحقیق می کنند. به جای اینکه ایمیلهای فیشینگ را برای پنج میلیون نفر ارسال کنند، یا تظاهر به ارسال ایمیلهای عمومی از طرف شرکتها کنند، ممکن است آنها فقط برای پنج نفر ایمیل ارسال کرده و جوری حمله را طراحی کنند که به نظر از سمت کسی که میشناسیم ارسال شده باشد. مهاجمان سایبری با روشهای زیر کارشان را انجام میدهند:

- در پروفایل لینکدین، چیزهایی را که در شبکه اجتماعی پست میکنیم، و یا با استفاده از اطلاعاتی که به صورت عمومی و یا در دارک وب موجود است درباره ی ما تحقیق میکنند.
- پیامهایی میسازند که به نظر از سمت مدیریت، همکاران، یا فروشندگانی که میشناسید و با آنها کار کرده اید ارسال شده است.
- بررسی میکنند که به چه چیزهایی علاقه دارید و پیغامهایی برای شما ارسال میکنند که در آن تظاهر میکنند فردی با علایق مشترک با شما هستند.
- بررسی میکنند که آیا شما به کنفرانس تازه ای رفته اید یا فقط از یک سفر برگشته اید و سپس ایمیلی میسازند که به سفرهای شما رجوع میکند.

مهاجمان سایبری به صورت فعالانه در حال استفاده از روشهای دیگر برای ارسال پیغامهای مشابه هستند، مانند ارسال پیغام متنی و یا حتی تماس مستقیم تلفنی با شما.

چگونه این حملات فیشینگ پیشرفته تر را شناسایی کنیم

به دلیل اینکه مهاجمان سایبری وقت گذاشته و در مورد قربانیان مورد نظر خود تحقیق می کنند، شناسایی این حملات می تواند دشوارتر باشد. خبر خوب این است که اگر بدانید به دنبال چه چیزی هستید، هنوز هم می توانید آنها را شناسایی کنید. قبل از اقدام در مورد یک پیغام مشکوک، سوالهای زیر را از خودتان بپرسید:

1. آیا پیام احساس فوریت شدیدی ایجاد می کند؟ آیا برای دور زدن سیاست های امنیتی سازمان خود تحت فشار قرار گرفته اید؟ آیا شما را در وضعیتی قرار میدهند تا در اثر تعجیل زیاد عمل اشتباهی را انجام دهید؟ هرچه فشار و احساس فوریت شدیدتر باشد، احتمال حمله بیشتر خواهد بود.
2. آیا ایمیل یا پیغام با عقل جور در می آید ؟ آیا مدیر عامل شرکت شما با فوریت به شما پیامک داده و از شما کمک میخواهد؟ آیا واقعا سرپرست شما نیاز دارد که با عجله بیرون رفته و کارت های هدیه بخرید؟ چرا بانک شما، یا شرکت کارت اعتباری تان باید از شما اطلاعات شخصی تان را بخواهد در صورتیکه میبایست از قبل آنها را در مورد شما داشته باشد؟ اگر پیغام به نظر عجیب یا نابجا رسید، احتمال دارد یک حمله باشد.
3. آیا شما یک ایمیل مربوط به کار از طرف یک همکار معتمد و یا شاید سرپرستتان دریافت کرده اید، اما این ایمیل از یک آدرس ایمیل شخصی مانند @gmail.com استفاده کرده است؟
4. آیا یک ایمیل یا پیغام از طرف کسی که میشناسید دریافت کرده اید، اما عبارات، لحن صدا و یا امضای داخل پیغام اشتباه و غیر عادی است؟

اگر یک پیام عجیب یا مشکوک به نظر می رسد، ممکن است یک حمله باشد. اگر می‌خواهید تأیید کنید که ایمیل یا یک پیام قانونی است، یکی از گزینه‌ها این است که با فرد یا سازمانی که پیام را برای شما ارسال کرده است، با یک شماره تلفن مطمئن تماس بگیرید.

شخص شما تا حد زیادی بهترین دفاع از خودتان خواهید بود. از عقل سلیم استفاده کنید.

سردبیر مهمان

فیل هافمن یک مشاور فناوری اطلاعات نیمه بازنشسته با 40 سال تجربه است، تمرکز او بر زیرساخت و امنیت است. او یک مشارکت‌کننده و ویراستار بلند مدت برای !OUCH، و علاقه مند به فناوری، دوچرخه‌سواری و عکاسی است.

منابع

حملات مهندسی اجتماعی: https://www.sans.org/newsletters/ouch/social-engineering-attacks
سه کلاهبرداری اصلی: https://www.sans.org/newsletters/ouch/top-three-social-media-scams
حملات پیام رسانی: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
حملات تماس تلفنی: https://www.sans.org/newsletters/ouch/vishing
بررسی منابع آنلاین عمومی: https://www.sans.org/security-awareness-training/resources/search-yourself-online

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو