حملات پیام‌های متنی: حماسه‌ای عجیب

مارک از پیام متنی، اعلان تحویل بسته از آمازون گیج شده بود - "تلاش برای تحویل گرفتن بسته را از دست داده اید! اکنون برای برنامه ریزی مجدد روی پیوند کلیک کنید وگرنه بسته شما بازگردانده خواهد شد." مارک به یاد نمی آورد که اخیراً چیزی آنلاین سفارش داده باشد، اما صادقانه بگویم، او چیزهای زیادی را آنلاین سفارش میداد که به راحتی فراموش می شدند. او که نمی‌خواست هیچ بسته‌ای را از دست بدهد، روی پیوند کلیک کرده و صفحه‌ای بارگذاری شد که اطلاعات تماس او را «برای اطمینان از زمان‌بندی مناسب» درخواست می‌کرد. این پیام کمی عجیب به نظر می رسید، اما مارک فکر کرد بهتر است اینکار راانجام دهد تا پشیمان نشود. او مشخصات آدرس منزل خود را وارد کرده و سپس از او اطلاعات بیشتری از جمله اطلاعات کارت اعتباری خود خواسته است. او با اعتماد به شرکت، تمام خواسته هایش را برای اطمینان از تحویل وارد میکند. سپس با پیغام بسته او باید به زودی تحویل داده شود در صفحه مواجه میشود. سپس، در عرض پانزده دقیقه، مارک یک تماس تلفنی از شرکت کارت اعتباری خود دریافت کرد و به او اطلاع داد که کارت او برای پرداخت هزینه های آنلاین متعدد در سراسر جهان استفاده شده است. مارک خشکش زد زیرا متوجه شد که هیچ بسته ای وجود ندارد و این پیامک کلاهبرداری بوده است تا او را فریب داده، اطلاعات او از جمله کارت اعتباری اش را سرقت کنند.

حملات پیام رسانی (Smishing) چیست؟

حملات پیام‌رسانی که Smishing (ترکیبی از کلمات SMS و Phishing) نیز نامیده می‌شوند، زمانی اتفاق می‌افتند که مهاجمان سایبری از SMS، پیام کوتاه یا فناوری‌های پیام‌رسانی مشابه استفاده می‌کنند تا شما را فریب دهند تا کاری را انجام داده که نباید انجام دهید، مانند واگذاری اطلاعات کارت اعتباری یا رمز عبور حساب بانکی یا نصب یک برنامه موبایل جعلی. درست مانند حملات فیشینگ ایمیل، مجرمان سایبری اغلب با احساسات شما مانند ایجاد حس فوریت یا کنجکاوی بازی می کنند. با این حال، چیزی که حملات پیام‌رسانی را بسیار خطرناک می‌کند این است که اطلاعات بسیار کمتر و سرنخ‌های کمتری در یک متن نسبت به ایمیل وجود دارد، که تشخیص اشتباه بودن آن را برای شما سخت‌تر می‌کند.

گاهی اوقات مجرمان سایبری حتی تماس های تلفنی را با حملات پیام رسانی ترکیب می کنند. به عنوان مثال، ممکن است یک پیام متنی اضطراری از بانک خود دریافت کنید که از شما می پرسد آیا اجازه پرداختی غیرعادی را داده اید یا خیر. این پیام از شما می‌خواهد برای تایید پرداخت، با جواب بله یا خیر پاسخ دهید. اگر شما پاسخ دهید، اکنون مجرم سایبری می داند که مایل به تعامل هستید و با شما تماس می گیرد و وانمود میکند که از بخش پیشگیری از کلاهبرداری بانک تماس گرفته است. سپس آنها می توانند سعی کنند اطلاعات مالی و کارت اعتباری شما یا حتی ورود به سیستم و رمز عبور حساب بانکی شما را با شما مطرح کرده و بفهمند.

مشاهده و توقف حملات Smishing

در اینجا برخی از رایج ترین سرنخ های حمله پیام رسانی آورده شده است:

- ضرورت: هر پیامی که احساس فوریت فوق العاده ای ایجاد می کند، زمانی که شخصی می خواهد عجله کند یا شما را تحت فشار قرار دهد تا اقدامی انجام دهید، مثلاً ادعا کند حساب های شما بسته می شود یا شما به زندان می روید.
- طمع: آیا پیام بیش از حد باور خوب به نظر میرسد؟ نه، شما واقعاً یک آیفون جدید به صورت رایگان برنده نشده اید.
- حس کنجکاوی: اگر پیامی دریافت کردید که شبیه یک «شماره اشتباه» است، یا کسی که نمی‌شناسید فقط «سلام» می‌گوید، به آن پاسخ ندهید یا سعی نکنید با فرستنده تماس بگیرید. فقط آن را حذف کنید. اینها تلاش مجرمان سایبری برای شروع گفتگو با شما هستند، مانند کلاهبرداری های عاشقانه.
- اطلاعات:آیا این پیام شما را به وب‌سایت‌هایی می‌برد که اطلاعات شخصی، کارت اعتباری، رمز عبور یا سایر اطلاعات حساسی را که نباید به آنها دسترسی داشته باشند، می‌خواهد؟
- مبلغ پرداختی: به درخواست‌های پرداخت غیرعادی مانند ارسال پول از طریق Western Union یا بیت‌کوین بسیار مشکوک باشید.

اگر پیامکی از یک سازمان رسمی دریافت کردید که فکر می کنید ممکن است قانونی باشد، مستقیماً با سازمان تماس بگیرید. با این حال، از شماره تلفن موجود در پیام استفاده نکنید، به جای آن از یک شماره تلفن قابل اعتماد استفاده کنید. به عنوان مثال، اگر از بانک خود پیامکی دریافت کردید که می گوید مشکلی در حساب یا کارت اعتباری شما وجود دارد، با مراجعه به وب سایت بانک خود یک شماره تلفن قابل اعتماد دریافت کنید، شماره تلفن را در صورتحساب یا از پشت بانک خود بیابید. یا کارت اعتباری، سپس با استفاده از آن شماره تماس بگیرید. همچنین به یاد داشته باشید که اکثر سازمان‌های دولتی، مانند سازمان‌های مالیاتی یا مجری قانون، هرگز از طریق پیامک با شما ارتباط برقرار نمیکنند، بلکه فقط از طریق پست قدیمی با شما تماس خواهند گرفت.

وقتی صحبت از حملات پیام رسانی می شود، بهترین دفاع خود شما هستید.

سردبیر مهمان

Destiny Plaza یک مهندس امنیت سایبری در موسسه مهندسی نرم افزار دانشگاه کارنگی ملون است. او دوست دارد با سخنرانی برای طیف وسیعی از مخاطبان، از مبتدی تا حرفه ای امنیت سایبری، الهام بگیرد. او دارای مدرک CISSP، لیسانس در علوم کامپیوتر و کارشناسی ارشد در سیستم های اطلاعات مدیریت است.

منابع

پیام‌رسانی بایدها و نبایدها: https://www.sans.org/newsletters/ouch/messaging-dos-and-donts
جلوی حملات تماس تلفنی فریبکارانه را بگیرید: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو