SANS SECURITY AWARENESS

وای! | ژولای 2018

OUCH!

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

کلاهبرداری از طریق تماس تلفنی

مقدمه

شما احتمالا فکر می کنید مجرمان اینترنتی مغزهای متفکری هستند که پشت کامپیوتر نشسته اند و حملات و حقه های پیچیده ای را از طریق اینترنت طراحی و پیاده میکنند. در حالی که بسیاری از مجرمان اینترنتی امروزه با استفاده از فن آوری هایی مانند ایمیل یا پیامک های فوری، یا تلفن برای فریب قربانیان خود استفاده می کنند. استفاده از تلفن دو مزیت بزرگ دارد. اول اینکه، بر خلاف ایمیل تکنولوژی های امن سازی کمتری وجود دارد که بتوان بر تماس های تلفنی نظارت کرد و قادر به شناسایی و جلوگیری از جرم شد. دوم، برای بزهکاران انتقال احساسات از طریق تلفن بسیار آسان تر است که این احتمال فریب قربانیان را زیاد میکند. حالا ببینیم چگونه میتوان این حقه ها را شناسایی و از آنها جلوگیری کرد.

گونه فریبهای تلفنی کار می کنند؟

اول، باید بدانیم که هدف این اعمال چیست. آنها معمولا دنبال پول، اطلاعات و یا دسترسی به کامپیوتر شما (یا هر سه) هستند. آنها این کار را با فریب شما به انجام آنچه که آنها می خواهند انجام می دهند. آدمهای بزهکار با مردم در سراسر جهان تماس می گیرند و شرایطی را برای فرد ایجاد می کنند که بسیار اضطراری بنظر می آید. آنها می خواهند ذهن شما را با نگران کردن مشغول کنند تا شما نتوانید به وضوح فکر کنید، و سپس شما را دستپاچه کرده تا اشتباه کنید. برخی از رایج ترین نمونه ها عبارتند از:

تماس گیرنده ادعا میکند که از اداره مالیات تماس میگیرد و شما مالیات را بدرستی پرداخت نکرده اید. سپس میگویند که اگر مالیات را بلافاصله پرداخت نکنید به زندان خواهید رفت و شما را تحت فشار قرار میدهند تا مالیات را روی خط از طریق کارت اعتباری پرداخت کنید. این کلاهبرداری است. خیی از ادارات دولتی از جمله اداره مالیات هرگز تلفنی تماس نمیگیرید و همه مکاتبات از طریق نامه رسمی است.

تماس گیرنده وانمود میکند که از بخش پشتبانی فنی شرکت مایکروسافت تماس میگیرد و توضیح میدهد که کامپیوتر شما به ویروس آلوده شده است. سپس شما را قانع میکنند که کامپیوتر شما آلوده شده است و شما را تحت فشار و اضطرار قرار میدهند که نرم افزار آنها را خریده و دانلود کنید یا اینکه به آنها اجازه دسترسی از راه دور به کامپیوترتان بدهید. شرکت مایکروسافت هرگز به خانه شما تلفن نمیزند!

شما یک پیام ماشینی دریافت میکنید که حساب بانکی شما بسته شده است و باید به شماره ای زنگ بزنید تا حساب شما دوباره فعال شود. وقتی که تماس میگیرد به پاسخگوی ماشینی وصل میشوید که از شما میخواهد خود را معرفی کنید و تعدادی سوالهای خصوصی از شما میپرسد. اینها واقعا از بانک شما نیستند و فقط قصد سرقت اطلاعات و هویت شما و سوء استفاده از آنها را دارند.

چگونه از خود حفاظت کنید؟

بزرگترین حافظ شما در مقابل این نوع کلاه برداریها خود شما هستید.

هر زمان هر کس با شما تماس گرفت و ایجاد حس اضطرار در شما ایجاد کرد، و شما را تحت فشار قرار داد که کاری برایشان انجام دهید، شدیدا مشکوک باشید. اگر تماس تلفنی در ابتدا به نظر عادی میرسد ولی کم کم عجیب به نظر میرسد، دیگر ادامه ندهید و «نه» بگویید.

اگر به این باور رسیدید که تماسی کلاهبرداری است سریع قطع کنید. اگر شک کردید یا خواستید مطمئن شوید که تماس کلاهبرداری بود یا نه، به وبسایت آن سازمان یا شرکت (مثلا بانک) بروید و شماره تلفن پشتیبانی آن سازمان یا اداره را پیدا کرده و با آنها مستقیم تماس بگیرید. اینطوری میدانید که دارید با آن سازمان حقیقی صحبت میکنید.

هرگز به نمایشگر شماره تلفن و شماره ای که روی صفحه تلفن دیده میشود اعتماد نکنید. بزهکاران معمولا کاری میکنند که شماره های مجاز شرکت یا سازمانی (مثلا اداره مالیات) بر روی تلفن شما نمایش داده شود.

هرگز به هیچ تماس گیرنده ای اجازه دسترسی و در اختیار گرفتن کامپیوتر خود را ندهید. یا اینکه شما را فریب دهند که نرم افزاری را دانلود و نصب کنید. بزهکاران اینگونه کامپیوتر شما را آلوده میکنند.

اگر تماس از طرف شخصی است که شما شخصا نمیشناسید، بگذارید تماس به روی پیامگیر برود. بعدا میتوانید بررسی کنید که چه کسی بود و چه کار با شما داشته است. در بعضی تلفنها میتوانید روی وضعیت "do not disturbe" بگذارید که تماسهای ناشناس بطور خودکار به پیامگیر وصل میشوند.

کلاهبرداری های تلفنی در حال افزایش هستند. شما بهترین حافظ خود در مقابل این نوع جرائم هستید.

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

سردبیر مهمان

جن فاکس در زمینه آگاهی سازی از امنیت اطلاعات و آشنایی با مهندسی اجتماعی و ارزیابی ریسک به عنوان مشاور ارشد امنیت اطلاعات در شرکت All Covered خدمات ارائه می کند. جن را میتوانید در توییتر به آدرس @j_fox پیدا کنید.

منابع

اطلاعات بیشتر در خصوص هویت، حریم خصوصی و امنیت اطلاعات: https://www.consumer.ftc.gov/topics/privacy-identity-online-security

گزارش کلاهبرداری تلفنی (در آمریکا): https://www.ftccomplaintassistant.gov/#crnt

مهندسی اجتماعی (فریب افراد): https://www.sans.org/u/Fi5

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click , Cheryl Conley | ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی