وای! | سپتامبر 2019

کلاه برداری از شما از طریق رسانه های اجتماعی

مقدمه

بسیاری از ما حملات ایمیل فیشینگ، در محل کار یا در خانه را دریافت کرده ایم. ایمیلهایی که به نظر عادی می رسند، مانند ایمیل از طرف بانک، رئیس خود و یا فروشگاه اینترنتی مورد علاقه. با این حال، اینها واقعاً آنچه ادعا میکنند نیستند و سعی در ترغیب یا فریب شما دارند به انجام اقدامی که نباید انجام دهید، مانند باز کردن پیوست ایمیل آلوده، یا اعلام کردن گذرواژه یا انتقال پول. چالش این است که هر چه ما در تشخیص و متوقف کردن این حملات ایمیل باهوش تر می شویم، مجرمان سایبری راه های دیگر ارتباط و کلاهبرداری با افراد را پیدا میکنند.

تلاش برای کلاه برداری یا فریب دادن شما می تواند تقریباً به هر شکلی از ارتباطاق که استفاده می کنید اتفاق بیفتد، از Skype، WhatsApp و Slack گرفته تا توییتر، فیس بوک، اسنپ چت، اینستاگرام یا حتی بازی های رایانه ای. برقراری ارتباط از طریق این برنامه ها یا کانال ها می تواند غیر رسمی یا قابل اعتماد تر به نظر برسد، به همین دلیل است که مهاجمان برای فریب دیگران از آنها استفاده می کنند. علاوه بر این، با فن آوری های امروزی، هر مهاجمی در هر نقطه از جهان بسیار آسان میتواند وانمود کند که هر کسی یا هر چیزی که می خواهد باشد. یادآوری این نکته حائز اهمیت است که هرگونه ارتباطی که با شما برقرار میشود ممکن است آنگونه که تصور میکنید نباشد و طرف مقابل آنهایی نباشند که ادعا میکنند.

چند نکته مهم که باید بخاطر بسپارید

در اینجا شایع ترین سرنخ هایی که به شما در تشخیص حملات سایبری کمک میکند ذکر میشود.

فوریت: در مورد پیامی که از شما «اقدام فوری» میخواهد و اگر عجله نکنید اتفاق بدی می افتد، مانند «تهدید به بستن حساب» یا فرستادن شما به زندان احتیاط کنید. مهاجم می خواهد که این دستپاچگی شما باعث اشتباه و کمتر فکر کردن شما شود.

فشار: فشار بر شما برای دور زدن یا نادیده گرفتن قوانین، سیاست ها یا رویه های کاری.

کنجکاوی: یک حس کنجکاوی شدید یا چیزی که خیلی رویایی است. نه، شما بلیط بخت آزمایی میلیونی برنده نشده اید!

اطلاعات حساس: درخواست اطلاعات بسیار حساس مانند شماره کارت اعتباری یا گذرواژه یا هرگونه اطلاعاتی که به راحتی به اشتراک نمی گذارید.

پیام های رسمی: پیام ادعا میکند که از یک سازمان رسمی ارسال شده است، اما گرامر و نگارش ضعیفی دارد. بیشتر سازمان های دولتی از رسانه های اجتماعی برای ارتباطات رسمی به طور مستقیم با شما استفاده نمی کنند. اگر مطمئن نیستید که پیام واقعی است، با سازمان مربوطه تماس بگیرید اما از یک شماره تلفن مطمئن مانند شماره ای که روی وب سایت آنها ذکر شده استفاده کنید.

جعل هویت: شما از یك دوست یا همکار خود پیام دریافت می کنید، اما لحن یا متن پیام غیرعادی است. اگر مشکوک هستید، برای تأیید از طریق تلفن با فرستنده پیام تماس بگیرید. ساخت پیام از طرف افرادی که می شناسید برای یک مهاجم سایبری آسان است. در بعضی موارد آنها می توانند حساب کاربری دوست شما هک کنند، سپس وانمود کنند که دوست شما هستند و به شما پیام بدهند. بسیار مواظب پیام های متنی، توییتر و سایر قالب های پیام کوتاه باشید، چون تشخیص شخصیت فرستنده دشوارتر است.

شما بهترین دفاع در برابر کلاه برداری، فریب و حملات مانند اینها هستید. اگر پیامی عجیب و یا مشکوک به نظر می رسد، خیلی ساده آن را نادیده بگیرید یا حذف کنید یا اگر از شخصی است که شما شخصاً می شناسید، با شخص مورد نظر تماس تلفنی بگیرید تا تأیید کند که آیا واقعاً آن را ارسال کرده یا خیر.

سردبیر مهمان

دکتر جسیکا بارکر (@drjessicabarker) یک پیشرو در موضوعات انسانی امنیت سایبری است. او یکی از مدیرعامل های شرکت سیگنتا است، جایی که با اشتیاق سعی در بهبود آگاهی دادن، تغییر رفتار کاربر ها و فرهنگ سازی در زمینه امنیت سایبری در سراسر جهان را دارد. او رئیس انجمن ClubCISO و یک سخنران شناخته شده است.

منابع

مهندسی اجتماعی: https://www.sans.org/u/Uz6

کلاه برداری با تماس تلفنی: https://www.sans.org/u/Uzb

حملات فیشینگ را متوقف کنید: https://www.sans.org/u/Uzg

کلاه برداری های هدفمند: https://www.sans.org/u/Uzl