کلاهبرداری های خیریه و بلاهای طبیعی

مجرمان سایبری می‌دانند که یکی از بهترین راه‌ها برای تعجیل مردم به اشتباه کردن، ایجاد یک حس اضطرار است. و یکی از ساده‌ترین راه‌ها برای ایجاد این حس فوریت، سوء استفاده از یک موقعیت بحرانی است. به همین دلیل است که مجرمان سایبری عاشق زمانی هستند که یک رویداد آسیب زا با تأثیر جهانی رخ می دهد. چیزی که بیشتر ما به عنوان یک تراژدی در نظر می گیریم، مجرمان سایبری به دید یک فرصت به آن نگاه میکنند، مانند وقوع یک جنگ، یک فاجعه طبیعی بزرگ مانند انفجار یک آتشفشان و البته شیوع بیماریهای عفونی مانند COVID-19 هنگامی که رسانه های اجتماعی و پوشش خبری زیادی در مورد یک رویداد خاص وجود دارد، مجرمان سایبری می دانند که زمان حمله فرا رسیده است.

آنها از این فرصت برای ایجاد ایمیل های فیشینگ یا کلاهبرداری به موقع در مورد این رویداد استفاده می کنند و سپس آن ایمیل فیشینگ را ارسال یا کلاهبرداری خود را برای میلیون ها نفر در سراسر جهان راه اندازی میکنند. به عنوان مثال، در طول یک بلای طبیعی، ممکن است آنها وانمود کنند که یک موسسه خیریه هستند و درخواست کمکهای اهدایی برای نجات کودکان نیازمند کنند. مجرمان سایبری می توانند اغلب ظرف چند ساعت پس از بروز یک بحران یا فاجعه وارد عمل شوند، زیرا آنها تمام زیرساخت های فنی را مهیا کرده و از قبل آماده هستند. چگونه می توانیم از خود در مقابل یک بحران یا فاجعه بزرگ محافظت کرده و مورد سوء استفاده مجرمان سایبری قرار نگیریم؟

چگونه میتوان این کلاهبرداری ها را شناسایی و در برابر آنها دفاع کرد

کلید اجتناب از این کلاهبرداری ها این است که به هر کسی که به سراغ شما می آید، مشکوک باشید. به عنوان مثال، به یک ایمیل ضروری که ادعا می کند از یک موسسه خیریه است و به شدت نیاز به کمک مالی دارد، اعتماد نکنید، حتی اگر به نظر از سمت یک نام معتبر که میشناسید و اعتماد دارید ارسال شده باشد. به یک تماس تلفنی که ادعا می کند از یک بانک غذایی محلی است و شما را برای کمک مالی تحت فشار قرار می دهد، اعتماد نکنید. هرچه احساس فوریت بیشتر باشد، احتمال اینکه درخواست فوق یک حمله باشد بیشتر است. در ذیل به برخی از معمول ترین سرنخ های بروز یک حمله خیریه ای اشاره میکنیم:

- به هر موسسه خیریه ای که نیاز به کمک مالی از طریق ارز دیجیتال، حواله ارزی، واریز پول یا کارت های هدیه دارد، بسیار مشکوک باشید.
- مجرمان سایبری می توانند شناسه (caller ID) تلفن خود را تغییر دهند تا تلفن شان جوری به نظر برسد که مثلا از کد منطقه ای شما و یا از یک نام مورد اعتماد است. این روزها نمی توان به شناسه تماس گیرنده (Caller ID) اعتماد کرد.
- برخی از مجرمان سایبری از نام ها و آرم (لوگو) هایی استفاده می کنند که از لحاظ شنیداری و دیداری به نظر یک موسسه خیریه واقعی برسد. این یکی از دلایلی است که قبل از اهداء کمک، میبایست تحقیق کرد.
- مجرمان سایبری اغلب ادعاهای مبهم و احساسی زیادی در مورد آنچه که با پول شما انجام خواهند داد مطرح می کنند، اما هیچ گونه جزئیاتی در مورد اینکه چگونه کمک مالی شما استفاده خواهد شد، ارائه نخواهند کرد.
- درخواست کمک در سایت‌های سرمایه گذاری جمعی مانند GoFundMe یا سایت‌های رسانه‌های اجتماعی مانند TikTok را مشروع فرض نکنید، به ویژه در پی وقوع یک بحران یا تراژدی.
- برخی از مجرمان سایبری ممکن است سعی کنند با تشکر از شما برای کمکی که در گذشته به آنها انجام داده اید شما را فریب داده تا به آنها کمک کنید، اگرچه در واقعیت، شما هیچوقت به آنها کمکی اهدا نکرده اید.
- در پاسخ به هرگونه درخواست ناخواسته ای، اطلاعات شخصی یا مالی خود را ارائه نکنید.

چگونه با حفظ امنیت، تفاوت ایجاد کنیم

برای کمک در مواقع ضروری یا کمک به افراد آسیب دیده در یک فاجعه، فقط به سازمان های شناخته شده و مورد اعتماد کمک مالی نمائید. شما ارتباطات را شروع می کنید و تصمیم می گیرید که با چه کسی این ارتباط را برقرار نمائید، مثلاً از چه وب سایت هایی بازدید کرده یا با چه سازمان هایی تماس بگیرید. وقتی می‌خواهید به یک موسسه خیریه کمک کنید، نام آن را در کنار کلماتی مانند «شکایت»، «بررسی»، «رده‌بندی» یا «کلاهبرداری» جستجو کنید. مطمئن نیستید به کدام موسسه خیریه میتوانید اعتماد کنید؟ با تحقیق بر روی وب سایت های دولتی که به آن اعتماد دارید، یا شاید لینکهایی که توسط یک سازمان خبری معروف و بسیار قابل اعتماد ارائه شده است، شروع کنید. کمک مالی در مواقع نیاز راهی فوق العاده برای ایجاد تفاوت است، فقط مطمئن شوید که به یک سازمان های قانونی و معتبر کمک می کنید.

سردبیر مهمان

دکتر جسیکا بارکر یک پیشرو و برنده جایزه در بخش جنبه های انسانی امنیت است. او یکی از مدیران اجرایی Cygenta و یک نویسنده پرفروش است. جسیکا در هیئت مشاوره ای SANS Security Awareness Summit است.

منابع

FTC کلاهبرداری خیریه: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
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
راهنمای خیریه: https://www.charitynavigator.org

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو