ماهنامه آگاهی از امنیت اطلاعات برای شما

سه روش اصلی کلاهبرداری در شبکه های اجتماعی

مقدمه

با اینکه شبکه های اجتماعی روشی فوق العاده برای برقراری ارتباط، اشتراک گذاری اطلاعات و تفریح با دیگران را برای ما فراهم میکند اما در عین حال راهی کم هزینه برای مجرمان سایبری است تا میلیونها نفر را فریب داده و از آنها سوء استفاده کنند. قربانی سه کلاهبرداری رایج در رسانه های اجتماعی نشوید.

کلاهبرداری با روش سرمایه گذاری

آیا تاکنون مطلبی در مورد یک فرصت خاص برای سرمایه گذاری که در آن به شما وعده داده شده باشد در مدتی بسیار اندک، با ریسکی بسیار کم و یا در ظاهر بدون هیچگونه خطری سرمایه شما چندین برابر خواهد شد، دیده اید؟ واقعیت این است که این وعده ها در حقیقت نوعی کلاهبرداری تحت عنوان سرمایه گذاری می باشند. کلاهبردارها به سادگی پس از اینکه به حساب آنها پولی پرداخت میکنید، آن را میدزدند. این مدل از کلاهبرداری ها اغلب با تبلیغات و داستانهایی از موفقیت مشتریان قبلی برای ترغیب شما به سرمایه گذاری همراه است، اما آنها فقط توصیفاتی غیر واقعی برای جلب اعتماد بیشتر شما میباشند. اغلب این کلاهبرداری ها سرمایه گذاری در زمینه ی رمزارزها (crypto-currencies) یا املاک است و کلاهبردارها اغلب پرداخت از طریق ارزهای دیجیتال و یا سایر روشهای پرداختی غیراستاندارد را درخواست میکنند. اگر از نظر شما یک سرمایه گذاری بیش از اندازه خوب است که واقعی باشد، پس به احتمال زیاد واقعی نیست. به خاطر داشته باشید، چیزی به نام سرمایه گذاری تضمین شده، با بازدهی بالا وجود ندارد. پول خودتان را فقط در منابع قابل اعتماد و شناخته شده سرمایه گذاری کنید، نه توسط افرادی غریبه که به صورت آنلاین با آنها آشنا شده اید.

کلاهبرداری های احساسی

کلاهبرداری احساسی روشی است که در آن مجرمان فردی را که تنها و آسیب پذیر است شناسایی کرده و با او رابطه آنلاین برقرار میکنند. مجرمان از هر روش و ترفندی برای جلب اعتماد قربانیان خود استفاده میکنند، مثلا با قربانی عکسهای تقلبی رد و بدل کرده و یا هدایایی برای او میفرستند، سپس داستانی غم انگیز تعریف میکنند که در آن نیاز به پرداخت پول مثلا برای صورتحساب بیمارستان و یا هزینه سفر برای دیدار حضوری قربانی خود دارند. برای ممانعت از ملاقات حضوری، این مجرمان ممکن است بگویند که در یک صنعت یا جایگاهی کار میکنند که مانع از این کار آنها میشود، مانند صنعت ساخت و ساز، صنایع دارویی بین المللی و یا ارتش. آنها اغلب برای دریافت سریع پول نقد و ناشناس ماندن هویتشان درخواست انتقال الکترونیکی وجه یا کارت هدیه میکنند. این نوع از کلاهبرداری ها نه تنها در رسانه های اجتماعی، بلکه در برنامه های دوستیابی آنلاین نیز رواج دارد. مراقب افرادی که به صورت آنلاین ملاقات میکنید باشید، کارها را به آرامی جلو برده (عجله نکنید)، و هرگز برای کسی که تنها به صورت آنلاین با او ارتباط برقرار کرده اید پولی ارسال نکنید.

علاوه بر این، اگر فکر میکنید که فردی را میشناسید که در مقابل چنین حمله ای آسیب پذیر بوده، یا در یک رابطه آنلاینی میباشد که این هشدارها را به همراه دارد، به او پیشنهاد کمک دهید. بعضی وقتها برای کسی که در یک رابطه عاطفی غرق شده است، توضیح اینکه وضعیت چقدر خطرناک است، بسیار سخت و دشوار می باشد.

کلاهبرداری های خرید اینترنتی

کلاهبرداریهای خرید اینترنتی زمانی اتفاق می افتد که شما کالایی را به صورت آنلاین با قیمتی فوق العاده پائین یا مبلغی باورنکردنی خریداری کرده اید اما هرگز به دستتان نمیرسد. تبلیغات وسوسه انگیز در رسانه های اجتماعی با قیمتهایی باورنکردنی، حاوی لینکهایی هستند تا شما را به سایتهایی که به نظر قانونی بوده و مارکهایی معروف را به فروش میرسانند هدایت کنند، اما اغلب این سایتها جعلی هستند. مراقب وب سایت هایی که اطلاعات تماس نداشته و یا فرمهای تماس خراب و مشکل دار دارند، یا از آدرسهای ایمیل شخصی استفاده میکنند، باشید. نام فروشگاه اینترنتی یا آدرس وبسایت آن را در یک موتور جستجو وارد کنید تا ببینید دیگران در مورد آن چه گفته اند. به دنبال اصطلاحاتی مانند "فریب"، "کلاهبرداری"، "دیگر هرگز" و "جعلی" باشید. نسبت به تبلیغات آنلاین یا معاملاتی که به نظرتان به شکل غیر قابل باوری خوب هستند، به شدت محتاط باشید. خرید کالا با هزینه ی بالاتر از سایت هایی که قابل اعتماد هستند و شما و یا دوستانتان قبلا از آن استفاده کرده اید، بسیار امن تر میباشند.

خبر خوشحال کننده این است که : بهترین دفاع خود شما هستید. کنترل اوضاع در دستان شما است. فقط در برابر کلاهبرداری هایی مانند این موارد هوشیار بوده تا با خیال راحت و به صورت ایمن از رسانه های اجتماعی بهترین استفاده را ببرید.

سردبیر مهمان

Chris Elgee (@chriselgee) یک کارشناس تست نفوذ و طراح چالش برای @CounterHackSec است و فرمانده ای در گارد ملی ارتش و مربی خبره SANS میباشد. او از یادگیری جزئیات فنی سخت، ایجاد درک سازمانی بیشتر و به اشتراک گذاری این اطلاعات با دانش آموزان و مشتریان لذت می برد.

منابع

دفتر بازرگانی بهین شده شناسایی کلاهبرداری ها: https://www.bbb.org/ScamTracker

حملات مهندسی اجتماعی: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
خرید آنلاین ایمن: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
حملات تماس تلفنی و کلاهبرداری - Vishing: https://www.sans.org/newsletters/ouch/vishing :

ترجمه شده برای عموم توسط: هومن خجاو، مجید هدایتی