Ouch! ژوئیه 2023

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

ایمن سازی حساب های مالی شما

مقدمه

حسابها و اکانتهای مالی شما هدف اصلی مجرمان سایبری است. شما پول دارید، و آنها هر کاری میکنند تا آن را سرقت کنند. منظور ما از حساب‌های مالی، نه تنها حساب‌های چک یا پس‌انداز، بلکه حساب‌های سرمایه‌گذاری، بازنشستگی و پرداخت آنلاین مانند PayPal شما است. خوشبختانه، با چند قدم ساده و اساسی می توانید از خودتان محافظت کنید.

آنها چگونه حمله میکنند؟

بانکها مقدار زیادی پول برای ایمن سازی سیستمهای خود سرمایه گذاری میکنند، که هک کردن آنها را برای یک مجرم سایبری بسیار دشوار می سازد. به همین دلیل است که به جای آن مجرمان سایبری، شما و حسابهای شما را هدف قرار میدهند. آنها میدانند که شما تیم امنیتی شخصی ندارید تا از شما محافظت کند، بنابراین هک کردن شما بسیار آسانتر از یک بانک است. در اینجا دو روش متداول وجود دارد که آنها به وسیله آن شما را هدف قرار داده و سعی می کنند پول شما را بدزدند:

رمزهای عبور: هر کدام از حسابهای مالی شما توسط یک رمز عبور محافظت میشود. اگر یک مجرم سایبری بتواند هر یک از آن رمزهای عبور را حدس زده یا به خطر بیاندازد، می تواند به جای شما وارد سیستم شده و سپس پول شما را به حساب های بانکی تحت کنترل خود منتقل کند. راه های بسیار زیادی هستند که مهاجمان سایبری برای به دست آوردن رمزهای عبور شما امتحان میکنند. یکی از رایجترین روش‌ها، آلوده کردن رایانه شما به بدافزار میباشد. هنگامی که رایانه شما آلوده شد، آنها می توانند نام کاربری و رمز عبور شما را هنگامی که به وبسایت بانک خود متصل میشوید به دست آورند. یکی از روشهای رایج دیگر ارسال ایمیلهای فیشینگ است که وانمود میکند از بانک شما ارسال شده است. هنگامی که روی پیوند موجود در ایمیل کلیک می کنید، تصور میکنید که وارد وب سایت بانک خود شده اید، اما در حقیقت، وارد یک وب سایت جعلی که مجرمان آن را کنترل می کنند شده اید. این اتفاق به آن‌ها اجازه می‌دهد یک بار دیگر نام کاربری و رمز عبور شما را بدست آورده، و سپس بتوانند از آن برای ورود به سیستم به جای شما استفاده کنند.

درخواست: مجرمان سایبری میتوانند به سادگی رمز عبورتان را از شما درخواست کرده و یا از شما بخواهند برای آنها پول را انتقال دهید. اینگونه حملات مهندسی اجتماعی اغلب با برقراری تماس تلفنی با شما شروع می شوند. مجرمان سایبری می دانند که به محض اینکه شما را وادار به صحبت کنند، با استفاده از احساسات برای آنها بسیار ساده تر خواهد بود تا شما را به اشتباه بیاندازند. به همین دلیل است که شما ایمیل‌های فیشینگ، پیغامهای صوتی و پنجره‌های بازشو مرورگرهای (pop-ups) بیشتری میبینید که در شما یک حس فوریت ایجاد کرده و به شما میگویند که میبایست با یک شماره تلفن تماس بگیرید تا مشکل خاصی را حل کنید و یا از یک فرصت شگفت انگیز قبل از اینکه زمان آن تمام شود بهره ببرید . هنگامی که با شماره تلفن فوق تماس می گیرید، مجرمان فشار احساسی فراوانی ایجاد می کنند تا به آنها اجازه دسترسی به حسابهای خود را داده یا پول خود را برای آنها به یک حساب متفاوت انتقال دهید. به عنوان مثال، آنها ممکن است به شما بگویند که از بخش پشتیبانی فنی یا خود دولت هستند و ادعا می کنند که رایانه شما آلوده شده است و اگر همین الان اقدام نکنید، تمام پول خود را از دست خواهید داد.

از خود محافظت کنید

خوشبختانه، ایمن سازی حساب های بانکی شما ساده تر از آن چیزی است که فکر می کنید. در اینجا سه مورد ساده ذکر میکنیم تا از خودتان محافظت کنید.

1. **ذهن مشکوک داشته باشید**: اول و مهمتر از هر چیز، بهترین ابزار دفاعی شما، خودتان هستید. اگر ایمیل، پیام متنی، پست صوتی یا پنجره بازشو در مرورگری دریافت می کنید که عجیب یا مشکوک به نظر می رسد، ممکن است یک حمله باشد. هر چه احساس اضطرار بیشتر بوده، و هر چه بیشتر تحت فشار قرار بگیرید تا فوری اقدامی انجام دهید، احتمال حمله بیشتر میباشد.

2. **از رمزهای عبور قوی/احراز هویت چند عاملی استفاده کنید**: از هر یک از ایمیلهای مرتبط با حساب های مالی و شخصی خود با یک رمز عبور طولانی و منحصر به فرد محافظت کنید. نمی توانید تمام رمزهای عبور منحصر به فرد خود را به خاطر بسپارید؟ استفاده از یک برنامه مدیریت رمز عبور برای یادآوری و نگهداری ایمن همه آنها را برای خودتان در نظر بگیرید. بهترین راه برای محافظت از هر یک از حساب های مالی شما، فعال کردن ویژگی خاصی به نام احرازهویت چند عاملی (MFA) برای هر یک از حسابها است.

3. **زیرنظر داشتن**: در نهایت، همه حسابهای مالی خودتان را زیر نظر داشته باشید. می‌توانید هشدارهای خودکاری تنظیم کنید تا هر زمان که پول به حساب‌های شما منتقل شده یا از آن خارج می‌شود، برای شما ایمیل یا پیامک ارسال کند. به این ترتیب می توانید به سرعت هر تراکنش غیرمجاز یا مشکوکی را شناسایی نمائید. هر چه سریعتر بتوانید مشکلی را تشخیص داده و آن را به بانک خود گزارش دهید، احتمال بیشتری وجود دارد که بتوانید پول خود را برگردانید.

سردبیر مهمان

لین دوم، مدیر اجرایی زنان در امنیت سایبری (WiCyS) است. لین از تجربه‌اش در بخش آموزش امنیت سایبری گرفته تا مشارکت فعال در برنامه‌ها و سازمان‌های غیرانتفاعی با بودجه کمک مالی، از اهمیت تنوع بخشیدن به نیروی کار امنیت سایبری حمایت کرده و آن را گسترش می‌دهد.
توئیتر: @lynn_dohm. لینکدین: https://www.linkedin.com/in/lynndohm.

منابع

محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
حملات فیشینگ فریبکارانه تر میشوند: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers/
احراز هویت چند عاملی: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو