اوچ! نوامبر 2024

اجازه ندهید مجرمان سایبری پس اندازهای شما را سرقت کنند: حساب های مالی خود را قفل کنید!

یک کلاهبرداری نرم و یک حساب بانکی خالی

امیلی یک سه شنبه معمولی و شلوغی داشت. قهوه صبحگاهی خودش را برداشت، نگاهی به تلفنش انداخت و متوجه پیامکی از بانکش شد: "تو این معامله را انجام دادی؟ با آره یا نه جواب بده." امیلی اخم کرد. او آن روز چیزی خرید نکرده بود. شاید فقط یک نقص فنی بود.

او پاسخ داد "نه" و در عرض چند دقیقه، یک تماس گرفته شد. پشت خط زنی بود که ادعا می کرد از بخش کلاهبرداری بانکش است و با لحنی آرام و حرفه ای صحبت می کرد. "ما فعالیت غیرعادی در حساب شما شناسایی کرده ایم. برای ایمن کردن آن، باید برخی جزئیات را بررسی کنیم." امیلی که هنوز غرق خواب بود، پاسخ داد. تماس‌گیرنده امیلی را طی یک سری مراحل راهنمایی کرد، رمز عبور بانکی آنلاین او را درخواست نمود و حتی او را راهنمایی کرد تا یک اعلان را روی تلفنش تأیید کند. آن زن به او اطمینان داد که: "این کار دسترسی هکرها را مسدود می کند." امیلی او را همراهی کرد و متوجه نشد که در تله افتاده است.

چند ساعت بعد، تلفن امیلی دوباره زنگ زد. این بار یک اعلان بود: 5,000 دلار از حساب پس انداز او برداشت شده بود. او وحشت زده به برنامه بانکش وارد شد، اما خیلی دیر شده بود. برنامه رمز عبور او را قبول نمی کرد. حساب کاربری او قفل شده بود. سپس او دید که برداشت دیگری اتفاق افتاده است، سپس یکی دیگر

امیلی در یک لحظه، متوجه شد. تماس "بخش کلاهبرداری" یک فریب کاری بود، یک حمله کاملا سازماندهی شده توسط یک مجرم سایبری که اکنون کنترل کامل حساب او را در اختیار داشت. امیلی به

سرعت با بانک خود تماس گرفت و امیدوار بود بتواند حساب بانکی خود را به موقع نجات دهد.

چرا باید از حساب های مالی خود محافظت کنید؟

حساب‌های مالی آنلاین ما - حساب‌های چک، پس‌انداز، و سرمایه‌گذاری - چیزی بیش از پول به همراه دارند. آنها نشان دهنده سالها کار سخت، برنامه های آینده و ثبات مالی ما هستند. مجرمان سایبری دائماً به دنبال فرصتهایی برای دسترسی به پول شما هستند و یک اشتباه ساده می تواند منجر به زیان مالی قابل توجهی شود. اگر فکر می کنید یک رمز عبور ساده می تواند این مجرمان را دور نگه دارد، مجدد فکر کنید.

مجرمان سایبری امروزی باهوش، آب زیر کاه و خستگی ناپذیر هستند. بسیار مهم است که در تامین امنیت حساب های مالی خود فعال باشید. این مورد نه تنها به جلوگیری از دسترسی غیرمجاز کمک می کند، بلکه با دانستن اینکه پولی که به سختی کسب کردید ایمن است، آرامش خاطر شما را نیز فراهم می نماید.

پنج قدم برای بستن راه نفوذ مجرمان سایبری

1. **همین حالا احراز هویت چند عاملی (MFA) را روشن کنید:** احراز هویت چند عاملی با الزام شما به تأیید هویت خود از طریق دو یا چند روش - چیزی که می دانید (رمز عبور)، چیزی که دارید (تلفن هوشمند یا رمز سخت افزاری) یا چیزی که هستید (اثر انگشت یا تشخیص چهره) به حساب های آنلاین شما یک لایه امنیتی اضافه می کند. حتی اگر یک مجرم سایبری به رمز عبور شما دسترسی پیدا کند، باز هم برای دسترسی به حساب شما به عامل دوم نیاز دارد. همیشه در هر کجا که در امکانش وجود دارد، MFA را انتخاب کنید، به ویژه برای حساب های مالی خود.

2. **از رمزهای عبور قوی و منحصر به فرد استفاده کنید:** برای هر حساب رمزهای عبور قوی و منحصر به فرد ایجاد کنید. هرچه رمز عبور شما طولانی تر بوده و کاراکترهای بیشتری داشته باشد، بهتر است. یک راهکار این است که از یک

عبارت عبور استفاده کنید، که رمز عبوری است که از چندین کلمه تشکیل شده است. حافظه خیلی قوی ای ندارید؟ مشکلی نیست. از یک برنامه مدیریت رمز عبور استفاده کنید تا به شما در ایجاد و پیگیری همه آن رمزهای عبور طولانی و منحصر به فرد کمک کند.

3. **کلاهبرداری ها دائمی هستند - در دام آنها نیفتید:** یکی از ساده ترین راه ها برای دسترسی مهاجمان سایبری به حساب های شما این است که از شما بپرسند. آنها ایمیلها، پیام های متنی یا حتی تماس های تلفنی ایجاد می کنند که به ظاهر یا به گوش شما جوری برسد که از بانک یا موسسه مالی شما میباشد. همیشه قبل از کلیک بر روی پیوندها، دانلود پیوست ها یا پاسخ دادن به پیامها یا تماس‌های تلفنی، منبع آنها را تأیید کنید. هر چه احساس فوریت بیشتر باشد، احتمال حمله ایمیل، پیام یا تماس تلفنی بیشتر می شود. بهترین راه برای محافظت از خودتان این است که با تایپ کردن آدرس در مرورگر خود مستقیماً به وب سایت رسمی بانک خود بروید یا با استفاده از یک شماره تلفن مورد اعتماد با بانک یا مؤسسه مالی خود تماس بگیرید.

4. **در نظارت بر حساب های خود وسواس داشته باشید:** بررسی مکرر حساب های مالی خود را برای هرگونه تراکنش غیرعادی جزو عادت قرار دهید. حتی بهتر از آن، بیشتر موسسات مالی هشدارهای خودکار را برای برداشت‌های بزرگ یا فعالیت‌های مشکوک ارائه می‌دهند. تنظیم هشدارهای خودکار می‌تواند به شما کمک کند تا تراکنش‌های جعلی را زودتر شناسایی کرده و برای به حداقل رساندن آسیبهای آن سریعتر اقدام کنید. اگر چیزی درست به نظر نمی رسد، منتظر نمانید - فورا اقدام کنید.

5. دستگاه های خود را محکم قفل کنید: تلفن، لپ تاپ و تبلت شما مانند خزانه ای برای دنیای مالی شما هستند. با قفل قوی صفحه نمایش و آخرین به روز رسانی های نرم افزاری، آنها را ایمن نگه دارید، ما توصیه می‌کنیم به روز رسانی خودکار را فعال کنید.

ویرایشگر مهمان

الیزابت راسنیک، استادیار مرکز امنیت سایبری در دانشگاه فلوریدای غربی، با تجربه در برنامه نویسی و خدمت در تیم واکنش به حوادث است. او به عنوان معاون ارشد WiCyS فلوریدا و دارای مدرک دکترا در فناوری اطلاعات است.

منابع

سه راه اصلی که مهاجمان سایبری شما را هدف قرار می دهند:
https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you
محرک های احساسی - چگونه مهاجمان سایبری شما را فریب می دهند:
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you

ترجمه شده برای انجمن توسط: مجید هدایتی، هومن خجاو