SANS SECURITY AWARENESS
SafeNet Network & Security Services
شبکه امن اندیشه فردا

وای! دسامبر 2017

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- رمزعبور
- احراز هویت دوعاملی چیست
- و چگونه کار میکند

صفحه ورود خود را قفل کنید

مقدمه

قسمت مهم حفاظت از اطلاعاتی مثل ایمیل، رسانه های اجتماعی یا حسابهای آنلاین بانکی شما، فرایندی است بنام احراز هویت که اثبات میکند کسی که میخواهد وارد حساب آنلاین شود، چه کسی هست. ممکن است ندانید ولی سه روش مختلف برای اثبات اینکه شما چه کسی هستید وجود دارد: چیزی که شما میدانید - مثل رمز عبور، چیزی که دارید - مثل گواهینامه رانندگی، و آنچه شما هستید (مشخصات زیست شناسی شما) بخشی از شما - مثل اثر انگشت. هر یک از این روش ها دارای مزایا و معایبی است. معمول ترین روش احراز هویت، استفاده از رمزعبور است، چیزی که شما میدانید. متاسفانه استفاده از فقط رمز عبور به عنوان تنها راه اثبات هویت، روز به روز نا امن تر میشود. در این خبرنامه به شما خواهیم آموخت تا چگونه با استفاده از روشهایی که احراز هویت دو عاملی نامیده میشوند، از خود محافظت کرده و صفحه ورود خود را قفل کنید .

سردبیر مهمان

تیفانی اسکوینیک(Tiffany Schoenike) با شناسه (**@staysafeonline**) مدیر تبلیغات و فرهنگ سازی در موسسه اتحاد ملی امنیت سایبری (National Cyber Security Alliance) میباشد. در سال 2016 خانم اسکوینیک به منظور توسعه و اجرای کمپینی با عنوان صفحه ورود خود را قفل کن که بخشی از برنامه ((STOP. THINK. CONNECT است با کاخ سفید، دولت و صنایع همکاری میکرد.

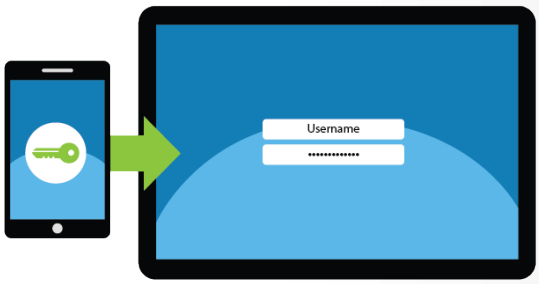
رمزهای عبور دیگر به تنهایی کافی نیستند

رمزهای عبور نوعی احراز هویت کاربر بر مبنای آنچه که شما میدانید است. در صورتیکه کسی رمز عبور شما بدست بیاورد و یا آن را حدس بزند، خواهد توانست خود را جای شما معرفی کرده و به تمامی اطلاعات شما دسترسی پیدا کند. یکی از مهمترین دلایل هک شدن اکانت ها استفاده از رمز های عبوری است که قابل حدس هستند. به همین دلیل است که شما توصیه میشود که از گذرواژه های عبارتگونه (رمز عبوری که از کنار هم گذاشتن چند کلمه ساخته میشوند) استفاده کنید که حدس زدن آن برای دیگران سخت است، همچنین برای هر یک از حسابهای کاربری خود رمزهای عبور متفاوت داشته باشید و رمزعبور خود را با دیگران به اشتراک نگذارید. علیرغم توجه به پیشنهادات فوق باز هم رمزهای عبور شما موثر نیستند. خوشبختانه راهکار سریع و ساده ای برای کنترل و محافظت از اطلاعات شخصی شما وجود دارد و آن استفاده از احراز هویت دوعاملی است.

صفحه ورود خود را قفل کنید

احراز هویت دو عاملی چیست؟

احراز هویت دو عاملی (گاها تایید دو عاملی و یا احراز هویت چند عاملی و یا 2FA نیز نامیده میشود) بسیار قوی تر از استفاده از رمزعبور به تنهایی است. این راه حل با فراهم کردن دو روش ثابت میکند شما همان شخصی هستید که اعلام میکنید. برای مثال میتوان به استفاده از کارت بانکی در ATM اشاره کرد. زمانیکه شما از دستگاه ATM پول دریافت میکنید، در واقع از مکانیزم احراز هویت دو عاملی استفاده کرده اید. برای دریافت پول نقد شما دو چیز لازم دارید، کارت بانکی خود (چیزی که دارید) و رمز کارت بانکی (چیزی که میدانید). اگر کارت بانکی شما گم و یا دزدیده شود کسی بدون داشتن رمز کارت شما قادر به برداشت پول از حساب شما نخواهد بود. سارقین برای دریافت پول از حساب شما میبایست هم رمز شما را داشته باشد و هم کارت بانکی شما را. احراز هویت دو عاملی نیز از همین مفاهیم استفاده میکند.



اگر امکان استفاده از احراز هویت دو عاملی هست، صفحات ورود خود را اینگونه قفل کنید، این کار یکی از قویترین گام ها برای حفاظت از خودتان در محیط های آنلاین خواهد بود.

چگونه کار میکند؟

احراز هویت دوعاملی در بسیاری از سایت ها، ایمیل ها، شبکه های اجتماعی و بانکهای بزرگ استفاده میشود. علاوه بر این بسیاری از این سایتها دستورالعمل های ساده و گام به گام را برای راه اندازی احراز هویت دو عاملی را ارائه میدهند (برای اطلاعات بیشتر به بخش منابع در پایان این خبرنامه مراجعه کنید). زمانیکه این قابلیت را فعال میکنید انتظار دارید عملکرد آن به این شکل باشد. ابتدا، به حساب خود با استفاده از نام کاربری و رمز عبور که از قبل داشتید، وارد میشوید. این مرحله بخش اول از دو عاملی است که برای ورود نیاز دارید - چیزی که میدانید. سپس یک کد منحصر به فرد را که غالبا بصورت پیام کوتاه به تلفن هوشمند شما ارسال میشود را دریافت خواهید کرد. در آخر این کد را بر روی صفحه ورودی وارد میکنید. این بخش نیز عامل دوم از این احراز هویت است - شما میبایست تلفن خود را برای دریافت این کد در دسترس داشته باشید. به این ترتیب حساب کاربری شما بطور کامل قفل شده است. حتی اگر مجرمان سایبری رمز عبور شما را بدست بیاورند نخواهند توانست به حساب کاربری شما وارد شوند مگر اینکه موبایل شما را هم داشته باشند.

بجای دریافت کد خاص از طریق پیام کوتاه، میتوانید برنامه مخصوص احراز هویت را بر روی تلفن هوشمند خود نصب کنید. این برنامه موبایل هر زمان که بخواهید به حساب کاربری خود وارد شوید برای شما کد منحصر به فرد تولید میکند. مزیت استفاده از برنامه موبایل

صفحه ورود خود را قفل کنید

امنیت بالاتر آن نسبت به ارسال کد از طریق پیامک است. علاوه بر این استفاده از برنامه موبایل به این دلیل که نیازی به ارتباط با شرکت های ارائه دهنده سرویس تلفن همراه ندارد، راحت تر نیز هست. این برنامه دائما در حال تولید کد های منحصر بفرد جدید است تا برای ورود به حساب کاربری استفاده شود.

درحالیکه به نظر میرسد استفاده از احراز هویت دوعاملی کار شما را بیشتر خواهد کرد ولی در حد بالایی باعث افزایش امنیت اطلاعات شخصی شما نیز خواهد شد. منتظر نباشید تا حساب شما هک شود و بعد به فکر امن کردن آن بیافتید. با فعال کردن احراز هویت دو عاملی صفحه ورود خود را برای حساب های بانکی، ایمیل و رسانه های اجتماعی امن کنید و از اینکه امنیت بالاتری بدست اوردید لذت ببرید.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

گذرواژه عبارتگونه: https://securingthehuman.sans.org/ouch/2017#april2017

سایت هایی که از احراز هویت هویت دوعاملی پشتیبانی میکنند: https://twofactorauth.org

توقف|تفکر|اتصال: https://www.lockdownyourlogin.org

تایید دو عاملی گوگل: http://www.google.com/landing/2step/

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی