ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- مقدمه
- رمز عبور
- تایید دو مرحله ای

تایید دو مرحله ای

مقدمه

فرایند اثبات اینکه شما چه کسی هستید (تایید هویت نامیده می شود) کلید مصونیت اطلاعات شماست. تایید هویت قوی موجب می شود فقط شما بتوانید به اطلاعاتتان، از قبیل ایمیل، عکسهایتان، و حساب بانکی تان دسترسی داشته باشید. سه راه مختلف برای تایید اینکه شما چه کسی هستید وجود دارد؛ چیزی که شما می دانید- مثل رمز عبور، چیزی که شما دارید- مثل گواهینامه رانندگی، چیزی که شما هستید- مثل اثر انگشتتان. هر کدام از این روش ها مزایا و معایبی دارند. متداول ترین روش رمز عبور است، چیزی که شما می دانید. در این شماره قصد داریم به شما بیاموزیم که چگونه خود را با روش تایید دو مرحله ای مصون کنید، چیزی بسیار مطمئن تر از رمز عبور تنها و خیلی ساده برای استفاده. برای فهم بهتر روش تایید دو مرحله ای، باید اول با رمز عبور شروع کنیم.

سردبیر مهمان

Keith Palmgren بیش از ۳۰ سال در زمینه امنیت اطلاعات کار کرده است. او مدرس مورد تایید SANS و نویسنده دوره پنج روزه درس مقدمه ای بر امنیت اطلاعات یعنی SANS SEC301 می باشد Keith بجز تدریس روی مشاوره و نوشتن پروژه تمرکز دارد. او را در توییتر به آدرس **@kplmgren** دنبال کنید.

رمز عبور

کلمات عبور بر اساس چیزی که شما می دانید اثبات می کنند که شما چه کسی هستید. خطر رمز عبور اینست که آنها تك نقطه شکست هستند. اگر کسی بتواند حدس بزند یا پسورد تان را بدست آورد، آنها می توانند که وانمود کنند شما هستند و به همه اطلاعاق از شما دسترسی پیدا کنند که با آن رمز عبور امن شده بود. بهمین دلیل شما مراحل محافظت از رمز عبور را می آموزید، مراحلی مثل رمز عبور قوی که یعنی رمز عبوری که حدس زدنش برای دیگران سخت باشد، انتخاب کلمات عبور متفاوت برای هر حساب یا اینکه هرگز رمز عبورتان را در اختیار کسی نگذارید. در حالیکه این نصایح هنوز هم تاکید می شوند، رمز های عبور بیش از فایده شان دوام آورده اند، آنها دیگر در این عصر جدید موثر نیستند. با آخرین تکنولوژی ها حمله کنندگان سایبری براحتی رمز های عبور را پیدا می کنند. ما به راه حل آسان برای استفاده و امن تر برای تصدیق قوی نیاز داریم. خوشبختانه گزینه متداولی موجود است، که تایید دو مرحله ای نامیده می شود.

تایید دو مرحله ای

تایید دو مرحله ای (گاهی تصدیق دو عاملی یا 2FA نامیده می شود) راه حلی بسیار امن تر داشتن فقط یك رمز عبور است. در این روش نه از یك بلکه از دو شیوه برای تصدیق خودتان استفاده می کنید. مثل استفاده از دستگاه خود پرداز بانك. وقتی پول از ماشین خودپرداز می گیرید،

تایید دو مرحله ای

در حقیقت از یکی از انواع تایید دو مرحله ای استفاده می کنید. برای دسترسی به پولتان به دو چیز احتیاج دارید، کارت ATM (چیزی که شما دارید) و عدد PIN (چیزی که شما می دانید). اگر کارت ATM را گم کنید پولتان هنوز محفوظ است. کسی که کارت شما را پیدا می کند نمی تواند از حساب شما برداشت کند چون عدد PIN شما را نمی داند(مگر اینکه عدد PIN را روی کارت نوشته باشید که اصلا کار درستی نیست) همینطور اگر کسی کارت را داشته باشد و PIN را نداند هم نمی تواند پولی برداشت کند. به همین دلیل تایید دو مرحله ای بسیار امن تر است چون دو لایه امنیت داریم.

در هر کجا تایید دو مرحله ای امکان دارد استفاده کنید، چون یکی از قوی ترین گامهایی است که می توانید برای حفاظت از اطلاعاتتان بردارید.

کاربرد تایید دو مرحله ای

تایید دو مرحله ای چیزیست که شما شخصا برای هرکدام از حسابهایتان راه اندازی می کنید. خوشبختانه بسیاری از خدمات آنلاین آن را ارائه می دهند. یکی از پیشگامان در ارائه خدمات تایید دو مرحله ای گوگل است. حسابهای گوگل یکی از اهداف اصلی حمله کنندگان سایبری است چون گوگل انواع مختلف خدمات آنلاین رایگان را به میلیونها نفر اطراف دنیا ارائه می دهد. چون گوگل می بایست «سیستم تصدیق» قوی تری تهیه کند یکی از اولین سازمان هایی بود که تایید هویت دو مرحله ای را برای بیشتر خدمات آنلاینش به اجرا در آورد. اگر شما بفهمید چگونه سیستم تایید دو مرحله ای گوگل کار می کند، خواهید فهمید که تایید هویت دو مرحله ای سایت های دیگر مثل Twitter, Facebook, Apple, Instagram و بسیاری از بانکها چگونه کار می کند.

نخست، شما تایید هویت دو مرحله ای را در حساب گوگلتان فعال می کنید و شماره موبایلتان را آنجا ثبت نام می کنید. وقتی اینکار انجام شد، تایید دو مرحله ای به این طریق کار می کند. به حسابتان «لاگین» می کنید مثل همیشه با نام کاربری و رمز عبور. این اولین مرحله از ۲ عامل است-چیزی که شما می دانید. سپس گوگل پیامی حاوی کد منحصر بفردی به تلفن شما می فرستد، بطور خاص زنجیره ای از ٦ رقم. دقیقا مثل رمز عبور، شما این ٦ رقم را در وبسایت وارد می کنید. این دومینِ عامل است. سپس با موفقیت به حسابتان «لاگین » کنید. شما باید هم پسوردتان را بدانید هم موبایلتان را داشته باشید تا کد منحصر بفرد را دریافت کنید. حتی اگر حمله کننده رمز عبور شما را بداند، به حساب گوگل شما دسترسی نخواهد داشت مگر اینکه تلفن شما را هم داشته باشد. برای اطمینان از اینکه حساب شما کاملا امن است، هر باری که «لاگین» می کنید گوگل به شما کد منحصر بفرد جدیدی می فرستد.

گزینه دیگری برای تایید دو مرحله ای با گوگل و بسیاری از سایت های دیگر وجود دارد. بجای دریافت کد منحصر بفرد با پیامك ، شما می توانید اپلیکیشن تصدیق هویت روی تلفن هوشمندتان نصب کنید. این اپلیکیشن کد منحصر بفرد در هر بار که می خواهید واردحسابتان شوید تولید

تایید دو مرحله ای

می کند. مزیت استفاده از اپلیکیشن اینست که احتیاج نخواهید داشت به سرویس تلفن متصل باشید تا کد منحصربفرد را دریافت کنید، تلفنتان آنرا برایتان تولید می کند. بعلاوه چون کد در موبایلتان بطور داخلی تولید شده و به شما فرستاده نشده، قابل رهگیری نیست.

به یاد داشته باشید، تایید دو مرحله ای بطور پیش فرض فعال نیست، باید آنرا خودتان فعال کنید.

اگرچه تایید دو مرحله ای ممکن است خیلی «وقت گیر» به نظر بیاید ما به شما پیشنهاد می کنیم حتما هر گاه امکان پذیر است استفاده کنید، مخصوصا برای خدمات حساسی مثل ایمیل، بانکداری اینترنتی یا ذخیره پرونده ها بطور آنلاین. تایید دو مرحله ای برای حفاظت از اطلاعات شما پا را از فقط رمز عبور ساده فراتر می گذارد.

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: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

رمز عبور:	http://www.securingthehuman.org/ouch/2015#april2015
سایت هایی که تایید دو مرحله ای را پشتیبانی می کنند:	https://twofactorauth.org
توقف| تفکر| ارتباط:	http://stopthinkconnect.org/2stepsahead
تایید دو مرحله ای گوگل:	http://www.google.com/landing/2step/
نکته روز SANS:	http://www.sans.org/tip_of_the_day.php

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی