وای! آوریل 2017

SafeNet Network & Security Services
شبکه امن اندیشه فردا

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

گذرعبارات

مقدمه

سردبیر مهمان

خانم My-Ngoc Nguyen (با تلفظ Me-Nop Wynn) مدرس رسمیSANS و مدیر و مشاور راهکار های امن در حوزه IT است. وی با بیش از 14 سال تجربه، دارای مدارک تخصصی بالا در توسعه، رشد و مدیریت برنامه های امنیت سایبری برای صنایع مختلف میباشد. آدرس توییتر وی **@MenopN** و در لینکدین My-Ngoc «Menop» Nguyen

گذرواژه ها تقریبا هر روز برای دسترسی به ایمیل، بانکداری آنلاین، خرید کالا و حتی دسترسی به موبایل توسط همه مورد استفاده قرار میگیرد. در عین حال گذرواژه یکی از مهمترین نقاط ضعف شما به حساب می آید. اگر کسی به گذرواژه شما دسترسی داشته باشد و یا بتواند آن را حدس بزند، میتواند به حساب شما دسترسی پیدا کرده و پول شما را جابجا کند، ایمیل شما را بخواند و یا هویت شما را به سرقت ببرد. به همین دلیل است که گذرواژه های قوی از ضروریات حفاظت از خود محسوب میشود. اما، معمولا وارد کردن گذر واژه ها و به خاطر سپردن آن سخت است و عموما برای افراد گیج کننده است. در این مقاله یاد خواهید گرفت که چگونه گذر واژه های قوی درست کنید که به راحتی قابل حفظ کردن بوده و به سادگی نوشته میشوند - که اصطلاحا به آنها گذرعبارات(passphrases) گفته میشود.

گذرعبارات

چالشی که همه ما با آن روبرو هستیم این است که هکرهای سایبری روشهای پیچیده و موثر، برای یافتن و حدس زدن اتوماتیک (brute force) گذرواژه ها را توسعه داده اند. این به این معنی است که اگر گذرواژه های شما ضعیف و قابل حدس زدن باشند، هکرها میتوانند به راحتی آنها را بدست بیاورند. یک قدم مهم برای حفاظت از خود، استفاده از گذرواژه های قوی است. معمولا این کار با درست کردن گذرواژه های پیچیده انجام می شد ولی به خاطر سپردن این گذرواژه ها کاری سخت و پیچیده بوده و وارد کردن آن نیز دشوار است. هرچقدر گذرعبارات شما حروف بیشتری داشته باشد قوی تر است. از مزایای استفاده از گذرعبارت این است که به راحتی قابل حفظ کردن و تایپ کردن هستند و هک کردن آنها نیز دشوارتر است. گذرعبارات Sustain-Easily-Imprison و Time for tea at 1:23دو مثال متفاوت از این دست هستند.

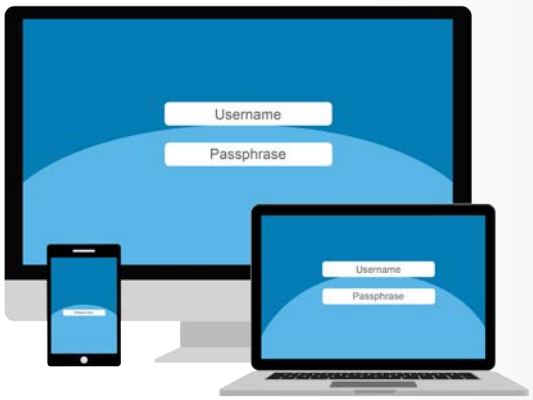
چیزی که استفاده از گذرعبارات را خیلی قوی میکند علاوه بر طول آنها، استفاده از حروف بزرگ انگلیسی و علائم است (به فاصله و نقطه گذاری و علائم در دو مثال بالا دقت کنید). در ضمن این گذرواژه ها هم به راحتی قابل حفظ کردن و تایپ کردن هستند. شما میتوانید گذرعبارات خود را با جایگزینی حروف با اعداد یا علائم قوی تر هم بکنید، بعنوان مثال میتوانید حرف a را با @ و یا حرف o را با عدد

گذرعبارات

صفر جایگزین کنید. در صورتیکه وب سایت یا برنامه ای در استفاده از تعداد کاراکترهای قابل استفاده در گذرواژه محدودیت ایجاد میکند، حداکثر کاراکتر های مجاز را استفاده کنید.

استفاده امن از گذرعبارات

در نحوه استفاده از گذرعبارات هم میبایست دقت کنید. اگر هکری بتواند به سادگی گذرعبارت را بدزدد و یا کپی کند، استفاده از آن به شما کمکی نخواهد کرد.



استفاده از گذرعبارات روش آسان تری برای ایجاد و به خاطر سپردن گذرواژه های قوی است.

۱. برای هر حساب و یا هر دستگاه خود گذرعبارت متفاوتی ایجاد و از آن استفاده کنید. بعنوان مثال هرگز از گذرعبارت یکسان برای حساب کاری و حساب بانکی خود استفاده نکنید، برای حسابهای شخصی خود نظیر فیس بوک، یوتیوب و یا توییتر استفاده نکنید. در این صورت اگر یکی از حسابهای شما هک شد، حسابهای دیگر شما همچنان امن خواهند بود. اگر گذرعبارات زیادی دارید که مجبور به حفظ کردن آنها هستید (که بسیار معمول است)، به فکر استفاده از یک برنامه مدیریت گذرواژه باشید. مدیریت گذرواژه برنامه ای است که تمام گذرعبارات شما را بطور امن ذخیره میکند. به این ترتیب تنها گذرعبارتی که نیاز است به خاطر بسپارید، گذرعبارت ورود به رایانه و برنامه مذکور است.

۲. هرگز گذرعبارات خود و یا روش ایجاد آنها را با هیچ کس از جمله همکاران و یا سرپرست خود در میان نگذارید. به خاطر داشته باشید که گذرعبارت یک راز است، اگر شخص دیگری آن را بداند آن گذرعبارت دیگر امن نیست. اگر بطور اتفاق گذرعبارت خود را با شخص دیگری به اشتراک گذاشتید و یا فکر میکنید که گذرعبارت شما ممکن است به سرقت رفته باشد، بلافاصله آن را تغییر دهید. تنها یک استثنا برای اشتراک گذاشتن گذرعبارات شخصی شما وجود دارد و آن هم در صورت اضطرار با عضوی از خانواده که بسیار قابل اعتماد است.

۳. از رایانه های عمومی مانند رایانه هتل ها و یا کافی نت ها برای ورود به حساب کاربری خود استفاده نکنید.از آنجاییکه هر کسی میتواند از این رایانه ها استفاده کند، ممکن است آلوده بوده و تمام کلیدهای زده شده شما را ثبت کند. برای وارد شدن به حساب کاربری خود تنها از رایانه های قابل اعتماد و یا تلفن همراه خود استفاده کنید.

۴. مراقب وب سایت هایی که از شما میخواهند به سوالات شخصی پاسخ دهید، باشید. این سوالها زمانی مورد استفاده قرار میگیرند که شما گذرواژه خود را فراموش کرده باشید و نیاز به بازیابی آن دارید. مشکل این است که پاسخ مربوط به اغلب این پرسش ها را میتوان در اینترنت و یا حتی در صفحه فیس بوک شما یافت. حتما اگر به سوالات شخصی پاسخ میدهید، تنها جوابهایی را استفاده کنید که در دسترس

گذرعبارات

عموم نیست و یا از اطلاعات ساختگی استفاده کنید. گزینه دیگر استفاده از نرم افزار مدیریت گذرواژه است، بسیاری از آنها امکان ذخیره سازی امن اطلاعات اضافی را هم به شما می دهند.

۵. بسیاری از حسابهای آنلاین خدماتی به نام احراز هویت دوعاملی ارائه میدهند در این حالت شما نیاز به بیش از فقط یک گذرواژه برای عبور هستید، مثلا کد عبور که به گوشی هوشمند شما ارسال میشود. این گزینه بسیار امن تر از گذرعبارت تنها است. در صورت امکان، همیشه از این روشهای قوی تر برای احراز هویت استفاده کنید.

۶. برای حفاظت از دسترسی به دستگاه های موبایل، اغلب نیاز به وارد کردن PIN است. به خاطر داشته باشید که چیزی بیش از گذرواژه نیست.هرچه PIN طولانی تر باشد، امن تر است.بسیاری از دستگاه های تلفن همراه به شما اجازه تغییر شماره PIN به یک گذرعبارت واقعی و یا استفاده از بیومتریک نظیر اثر انگشت را میدهند

۷. اگر از حساب کاربری دارید که دیگر استفاده نمیکنید، حتما آن را ببندید، یا حذف یا غیر فعال کنید.

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

مدیریت گذرواژه:	https://securingthehuman.sans.org/ouch/2015#october2015
احراز هویت دو عاملی:	https://securingthehuman.sans.org/ouch/2015#september2015
ورود خود را قفل کنید:	https://lockdownyourlogin.com
SANS SEC301 - دوره 5 روزه اصول امنیت سایبری:	https://sans.org/sec301

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