ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

رمز عبارت گونه

مقدمه

سردبیر مهمان

Guy Bruneau مشاور ارشد امنیت اطلاعات در شرکت IPSS است. او همچنین مربی SANS و یکی از کارکنان بخش ISC در موسسه SANSاست. او دارای مدرک SANS GSE است و دوره افسر سایبری SANS را به پایان رسانده است. می توانید او را در توییتر **@GuyBruneau** و یا در آدرس **handlers.sans.org/gbruneau** دنبال کنید.

رمز عبور چیزی است که شما تقریبا هر روز از آن استفاده میکنید. از دسترسی به ایمیل و بانکداری آنلاین تا خرید اینترنتی کالا و یا دسترسی به گوشی های هوشمندتان. در عین حال رمز عبور یکی از نقاط ضعف شما نیز هست، اگر کسی رمز عبور شما را بدست آورد، می تواند هویت شما را سرقت، پول شما را انتقال و یا به اطلاعات شخصی شما دسترسی پیدا کند. رمز عبور قوی برای حفاظت از خود ضروری است. در این خبرنامه، خواهید آموخت که چگونه با استفاده از یک نوع رمز عبور که رمز عبارت گونه نامیده میشود، رمز عبوری قوی ایجاد کنید که در عین حال بتوانید به آسانی آنرا به خاطر بسپارید.

رمز عبارت گونه

چالشی که همه ما با آن روبرو هستیم این است که هکرهای سایبری روشهای پیچیده ای برای حدس زدن و یافتن رمز عبور توسعه داده اند، و هر روز هم ماهر تر میشوند. این به این معنی است که اگر رمزهای عبور ضعیف که حدس زدن آنها آسان است انتخاب کنید، هکرها می توانند رمزهای عبور شما را به راحتی بدست آوردند. یک گام مهم برای حفاظت از خود استفاده از رمز عبوری قوی است. هر چه رمز شما کاراکترهای بیشتری داشته باشد، قوی تر و حدس آن برای هکر سخت تر است. اما، به خاطر سپردن رمز عبور پیچیده و طولانی مشکل است. بنابراین توصیه میکنیم از رمزهای عبارت گونه استفاده کنید. اینها عبارات یا جملات ساده ای هستند که به آسانی قابل به خاطر سپردن هستند، اما به دست آوردن یا حدس زدن آنها سخت است. در اینجا مثالی میزنیم.

Where is king Julian?

دلیلی که این رمز عبارت گونه را خیلی قوی میکند، نه تنها طول 21 حرفی آن است، بلکه از حروف بزرگ و علایم نقطه گذاری نیز استفاده میشود (به یاد داشته باشید، فاصله و علامت سوال از علائم هستند). شما می توانید رمز عبارت گونه را حتی قوی تر کنید اگر حروف را با اعداد و یا علایم جایگزین کنید، مثلا جایگزین کردن حرف a با نماد @ و یا حرفo با عدد صفر. اگر وب سایت یا برنامه ای تعداد کاراکترهای عددی که در رمز میتوانید بکار ببرید را محدود میکند، حداکثر تعداد کاراکترهای مجاز را استفاده کنید.

رمز عبارت گونه

استفاده از رمزهای عبارت گونه بصورت امن

همچنین باید دقت کنید که چگونه از رمزهای عبارت گونه استفاده میکنید. استفاده از یک رمز عبارت گونه کمکی نخواهد کرد اگر خرابکارها بتوانند به راحتی آن را سرقت و یا کپی کنند.

استفاده از رمز عبارت گونه یکی از موثر ترین اقداماتی است که شما می توانید برای محافظت از هویت و اطلاعات خود بردارید.

۱. حتما از رمزهای عبور مختلف برای هر حساب و یا دستگاه خود استفاده کنید. به عنوان مثال، هرگز از همان رمز عبوری که برای کار و یا حساب بانکی خود استفاده میکنید، برای حساب های شخصی خود، مانند فیس بوک، یوتیوب و یا توییتر استفاده نکنید. به این ترتیب، اگر یکی از حساب های شما هک شد، حساب های دیگر هنوز در امان هستند. اگر رمزهای عبور زیادی برای بخاطر سپردن دارید (که بسیار معمول است)، به فکر استفاده از یک برنامه مدیریت رمز عبور باشید. این برنامه ای است که تمام رمزهای عبور شما را بطور امن ذخیره میکند. به این ترتیب تنها رمز عبوری که شما لازم است به یاد داشته باشید، رمز عبور ورود به رایانه و این برنامه مدیریت رمز عبور می باشد.

۲. هرگز رمز عبور خود یا تکنیکی که برای ایجاد یا انتخاب آنها به کار میبرید را با کسی در میان نگذارید، از جمله همکاران خود. به یاد داشته باشید، رمز عبور یک راز است. اگر کس دیگری می داند، آن عبارت دیگر امن نیست. اگر شما تصادفا رمز خود را با شخص دیگری به اشتراک گذاشتید، و یا فکر میکنید که عبارت عبور شما ممکن است به خطر افتاده باشد و یا به سرقت رفته باشد، لازم است تا آن را بلافاصله تغییر دهید.

۳. درست مانند رمز عبور کلمه ای، از انتخاب رمزهای عبارت گونه متداول و آنهایی که به آسانی قابل حدس زدن هستند بپرهیزید. به عنوان مثال، عبارت «Four score and seven years ago» یک رمز عبارت گونه خوبی نیست از آن جهت که شناخته شده است.

۴. از رایانه های عمومی مانند رایانه های داخل هتل ها و یا کتابخانه ها برای ورود به حساب کاری یا بانک استفاده نکنید. از آنجا که هر کسی می تواند از این رایانه ها استفاده کند، ممکن است این رایانه ها با برنامه های مخرب که تمام کلید های تایپ شده را ثبت میکند آلوده شده باشد. تنها با استفاده از رایانه و یا دستگاه های تلفن همراه قابل اعتماد به حساب محل کار خود و یا حساب های بانکی وارد شوید.

۵. مراقب وب سایتهایی باشید که از شما میخواهند به سوالات شخصی پاسخ دهید. این سوال ها موقعی مورد استفاده قرار میگیرند که شما رمز عبور خود را فراموش کرده باشید و نیاز به بازنشانی آن هستید. مشکل این است که پاسخ به این پرسش ها اغلب می تواند در اینترنت، و یا حتی در صفحه فیس بوک شما یافت. حتما اگر شما به سوالات شخصی پاسخ میدهید، تنها جوابهایی را انتخاب کنید که در دسترس عموم نیست و یا اطلاعات ساختگی استفاده کنید. نرم افزارهای مدیریت رمز عبور می تواند در این انتخاب و ذخیره این پاسخها به شما کمک کنند.

رمز عبارت گونه

۶. بسیاری از حساب های آنلاین خدماتی به نام احراز هویت دو عاملی یا دو مرحله ای ارائه میکنند. در این حالت شما نیاز به بیش از فقط رمز عبور برای ورود هستید، مثلا رمز عبور به گوشی های هوشمند شما فرستاده میشود. این گزینه بسیار امن تر از رمز عبارت گونه تنها است. در صورت امکان، همیشه از این روشهای قوی تر احراز هویت استفاده کنید.

۷. دستگاه های موبایل، اغلب نیاز به PIN برای محافظت از دسترسی به آنها است. به یاد داشته باشید PIN چیزی بیش از رمز عبور نیست. هرچه PIN طولانی تر باشد، امن تر است. بسیاری از دستگاه های تلفن همراه به شما اجازه تغییر شماره PIN به رمز عبارت گونه واقعی را میدهند.

۸. در نهایت، اگر شما دیگر از حسابی استفاده نمیکنید، حتما آن را ببندید، حذف و 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: http://www.securingthehuman.org

یادداشت مترجم

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

منابع

تایید هویت دو مرحله:	http://www.securingthehuman.org/ouch/2013#august2013
نرم افزار مدیریت رمز عبور:	http://www.securingthehuman.org/ouch/2013#october2013
مهندسی اجتماعی:	http://www.securingthehuman.org/ouch/2014#november2014
اصطلاحات متداول امنیت اطلاعات:	http://www.securingthehuman.org/resources/security-terms

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