ZENDEGI-SALAM
ضمیمه روزنامه خراسان
یک‌شنبه ● ۱۲ تیر ۱۴۰۱
۳ ذی الحجه ۱۴۴۳ ● ۳ جولای ۲۰۲۲
شماره ۲۰۹۷۶
۲۱۹۶

رویین‌تن در برابر هکرها

بسیاری می‌گویند من که اطلاعات خاصی ندارم یا شخصیت مهمی نیستم اما هکرها به هیچ فردی رحم نمی‌کنند از اشتباهات و ویژگی‌های ساخت یک گذرواژه و راه‌های بالا بردن ایمنی‌اش گفتیم

نجات شکوندی | روزنامه‌نگار

پرونده

روزی نیست که به اهمیت امنیت رمز عبور اضافه نشود اما متأسفانه همچنان «۱۲۳۴۵۶» متداول‌ترین رمز عبور در سراسر جهان است. امروزه ما تقریباً برای هر کار آنلاینی که انجام می‌دهیم از رمز عبور استفاده می‌کنیم، چه ورود به حساب‌های ایمیل و حساب‌های بانکی باشد، چه سایت‌های رسانه‌های اجتماعی، حساب‌های خرید، انجمن‌های آنلاین و... به راستی که انتهای این فهرست مشخص نیست. با وجود بسیاری از سایت‌های محافظت شده با رمز عبور، به خاطر سپردن رمزهای عبور جداگانه برای هر حساب دشوار است بنابراین ما تمایل داریم از رمز عبور یکسان یا حداقل مشابه برای سایت‌های مختلف استفاده کنیم تا به نوعی زندگی را کمی آسان‌تر کنیم! اغلب اوقات، این رمزهای عبور امنیت بسیار ضعیفی دارند و حاوی نام اعضای خانواده، نام مستعار، تاریخ تولد و سایر اطلاعاتی هستند که به راحتی قابل شناسایی‌اند. متاسفانه بسیاری می‌گویند من که اطلاعات خاصی ندارم یا شخصیت مهمی در عرصه سیاست یا مثلا نظامی نیستم اما هکرها به هیچ کس رحم نمی‌کنند و بسیاری از اطلاعات شما را که حتی فکر می‌کنید اهمیت ندارند، می‌دزدند و در اختیار باقی افراد قرار می‌دهند و به نوعی راه را برای هدف سوء استفاده واقع شدن‌تان باز می‌کنند. این رویکرد برای ایمنی رمز عبور بسیار خطرناک است و بسیاری از افراد را در معرض هک قرار می‌دهد. هکرها طیف وسیعی از ابزارها را در اختیار دارند اما ساده‌ترین و رایج‌ترین روش برای دسترسی به یک حساب کاربری حدس زدن رمزهای عبور است. در پرونده امروز زندگی سلام، به سراغ دنیای امنیت رمزها و روش‌های آن رفته‌ایم تا بتوانیم بهتر از امنیت اطلاعات‌مان حفاظت کنیم.

اشتباه اول، رمز عبور یکسان

گذرواژه‌ها سنگ بنای دفاع سایبری شما هستند اما مدیریت موثر و ایمن آن‌ها می‌تواند یک چالش واقعی باشد. از طرفی هم هکرها از نرم‌افزارهای تخصصی استفاده می‌کنند که به آن‌ها امکان می‌دهد هزاران ترکیب نام کاربری و رمز عبور احتمالی را در هر ثانیه آزمایش کنند که نشان‌دهنده نیروی بی‌رحمانه‌ای است که آن‌ها برای حمله استفاده می‌کنند. در یکی از آمارهای جهانی آمده است که ۶۰ درصد افراد از یک نام کاربری و رمز عبور برای همه حساب‌های خود استفاده می‌کنند، بنابراین اگر هکرها بتوانند به یک حساب دسترسی پیدا کنند، می‌توانند به بقیه هم نفوذ کنند. به محض این که هکرها به این اطلاعات شخصی دسترسی پیدا کنند، می‌توانند از آن برای ارتکاب کلاهبرداری هویت، فروش به اشخاص ثالث مجرم یا به سادگی برای پاک‌سازی حساب‌های بانکی استفاده کنند به طوری که حتی توانایی ردیابی آن‌ها هم مشکل باشد. اما ایجاد یک رمز عبور قوی برای محافظت از هویت آنلاین ما و اطمینان از این که هدف آسانی برای هکرها نیستیم، بسیار مهم است.

آناتومی یک رمز عبور قوی

بعد از آشنا شدن نسبی با شیوه‌های هک، می‌توانیم رمزهای عبور قوی ایجاد کنیم که بیشترین امنیت را داشته باشد؛ اگرچه راه مقابله با کلاهبرداری فیشینگ این است که به لینک غیرمجاز وارد نشویم اما در صورتی که رمز عبور شما از سه قانون مهم پیروی کند، تقریبا غیرقابل شکستن است. اولین نکته پرهیز از بدیهیاتی مانند استفاده از اعداد یا حروف متوالی است. پس بهتر است گذرواژه‌های منحصربه‌فردی ایجاد کنید که شامل هیچ اطلاعات شخصی مانند نام یا تاریخ تولد شما نشود. طولانی کردن، مهم‌ترین عامل تقویت امنیت رمز عبور است. چیزی کمتر از ۱۵ کاراکتر انتخاب نکنید، در صورت امکان حتی بیشتر و البته هرچه بیشتر از حروف (ترکیبی از حروف بزرگ و کوچک)، اعداد و نمادها استفاده کنید، رمز عبور شما قوی‌تر و شکستن آن سخت‌تر می‌شود. از مسیرهای به یاد ماندنی صفحه کلید (مانند qwerty)، استفاده نکنید. روشی به عنوان «روش بروس اشنایر» وجود دارد که در آن شما به یک جمله تصادفی ولی آشنا در ذهن‌تان فکر و با استفاده از یک قانون آن را به یک رمز عبور تبدیل می‌کنید. برای مثال، جمله‌ای را در نظر بگیرید و سعی کنید یکی در میان حروف آن را بزرگ و کوچک بنویسید. برای هر فرد دیگری، شکاندن این رمز سخت است اما برای شما کاملاً منطقی است. اطمینان حاصل کنید جمله‌ای را که انتخاب می‌کنید تا حد امکان شخصی و غیرقابل حدس زدن باشد. روش دیگر گنجاندن سه کلمه تصادفی، ترکیبی از حروف بزرگ و کوچک، اعداد (۳۷۵۶) و نمادها (!#$%) است.

سایت‌های ناامن بلای جان رمز عبورها

وب‌سایت‌های امنیتی رمز عبور کاربران خود را «هش» می‌کنند و حتی اگر داده‌ها خارج شوند، رمزهای عبور واقعی رمزگذاری می‌شوند. به زبان ساده، هشینگ با استفاده از یک تابع ریاضی مقداری را به مقدار دیگر تبدیل می‌کند. به طور روزانه، بیشتر کاربران در خصوص گذرواژه‌های خود از فرایند هشینگ استفاده می‌کنند. به عنوان مثال، زمانی که می‌خواهید یک آدرس ایمیل و رمز عبور برای خود ایجاد کنید، سایت ارائه‌دهنده ایمیل احتمالاً گذرواژه شما را به همان صورت ذخیره نمی‌کند. در عوض رمز عبور شما را از طریق یک الگوریتم هشینگ اجرا و سپس هش رمز عبور شما را ذخیره می‌کند. هر بار که می‌خواهید به ایمیل‌تان وارد شوید، آن سایت رمز عبوری را که وارد می‌کنید به هش تبدیل می‌کند و آن را با هشی که ذخیره کرده است مقایسه می‌کند و تنها در صورتی که این دو هش با هم تطابق داشته باشند، شما مجاز به دسترسی به ایمیلتان هستید. اما گاهی پیش می‌آید که وب‌سایت‌های دیگر زحمت این مرحله را نمی‌کشند. قبل از راه‌اندازی حساب‌ها، ایجاد گذرواژه و سپردن اطلاعات حساس به وب‌سایت، لحظه‌ای را به ارزیابی سایت اختصاص دهید. آیا https در نوار آدرس وجود دارد که اتصال ایمن را تضمین کند؟ آیا این احساس را دارید که مطابق با جدیدترین استانداردهای امنیتی روز است؟ اگر نه، درباره به اشتراک گذاشتن هر گونه اطلاعات شخصی در آن فکر کنید.

امان از هکرها و ترفندهای‌شان!

این افراد اما مثل ما منفعل نیستند و هر بار با روشی جدیدتر، رمز عبور ما را به چالش فرا می‌خوانند. در این بخش، چند ترفند معروف دنیای هکرها را بررسی می‌کنیم.

۱ خرید از دارک وب| مجرمان سایبری چندین تاکتیک هک رمز عبور را در اختیار دارند اما ساده‌ترین آن‌ها خرید رمزهای عبور خود از وب تاریک (Darkweb) است. در این میان پول زیادی هم در گردش است. پس اگر سال‌هاست از یک رمز عبور استفاده می‌کنید، به احتمال زیاد به خطر افتاده و در این سایت، منتشر شده است. اما اگر عاقلانه تصمیم گرفته‌اید و هر ماه رمزهای خود را تغییر داده‌اید، هکرها مجبور به استفاده از دیگر راه‌ها برای شکاندن آن هستند.

۲ حمله بی‌رحمانه| در این نوع حمله، مهاجم سعی می‌کند، هر ترکیبی را حدس بزند تا زمانی که به ترکیب رمز شما برسد. برای مثال مهاجم، نرم‌افزار را خودکار می‌کند تا هرچه بیشتر ترکیب‌های موجود را در سریع‌ترین زمان ممکن امتحان کند.

۳ حمله به دیکشنری| یک نوع دیگر از حمله هم وجود دارد به اسم حمله به دیکشنری. این الگو دقیقاً همان چیزی است که از اسمش به نظر می‌رسد و در آن هکر با یک فرهنگ لغت به شما حمله می‌کند و در فهرستی از پیش تنظیم‌شده از کلمات، فرهنگ لغت را امتحان می‌کند. پس اگر کلمه عبور شما واقعاً یک کلمه معمولی است، تنها در صورتی از حمله فرهنگ لغت جان سالم به در خواهید برد که کلمه شما بسیار نامتعارف باشد یا از چند عبارت تشکیل شده باشد.

۴ فیشینگ| نفرت‌انگیزترین تاکتیک «فیشینگ» است و زمانی است که مجرمان سایبری سعی می‌کنند از طریق مهندسی اجتماعی شما را فریب دهند، ارعاب کنند یا به شما فشار بیاورند تا ناخواسته آن چه را که می‌خواهند انجام دهید. یک ایمیل یا پیام فیشینگ ممکن است به شما بگوید (به اشتباه) مشکلی در حساب کارت اعتباری شما وجود دارد. شما را هدایت می‌کند تا روی پیوندی کلیک کنید که شما را به یک وب سایت ساختگی می‌برد که شبیه شرکت کارت اعتباری شماست. کلاهبرداران منتظرند تا شما فقط اطلاعات کارت و رمز خود را وارد کنید. هکرهای فیشینگ حتی می‌توانند شما را از طریق تماس‌های تلفنی به دام بیندازند. پس در خصوص هر گونه تماس یا پیامی که ادعا می‌کند مربوط به حساب کارت اعتباری شماست، احساس خطر کنید.

رابطه ویژگی‌های رمز عبور و سرعت هک‌شدنش

گزارشی از شرکت امنیت سایبری CNBC Hive Systems در ۲۰۲۲ نشان می‌دهد که یک هکر معمولی چقدر طول می‌کشد تا رمز عبور مورد استفاده شما را کشف کند. به عنوان مثال، تنها استفاده از اعداد ممکن است به یک هکر اجازه دهد تا بلافاصله (کمتر از یک ثانیه) رمز عبور ۴ تا ۱۱ کاراکتری شما را شناسایی کند. از آن طرف هم، یک رمز عبور ۱۸ کاراکتری با استفاده از ترکیبی از اعداد، حروف بزرگ و کوچک و نمادها ۴۳۸ تریلیون سال طول می‌کشد تا توسط یک هکر کشف شود.

ترکیب نماد، اعداد، حروف کوچک و بزرگ	ترکیب اعداد، حروف کوچک و بزرگ	حروف کوچک و بزرگ	حروف کوچک	فقط عدد	تعداد کاراکترها
فورا	فورا	فورا	فورا	فورا	۴
فورا	فورا	فورا	فورا	فورا	۵
فورا	فورا	فورا	فورا	فورا	۶
۳۱ ثانیه	۷ ثانیه	۲ ثانیه	فورا	فورا	۷
۳۹ دقیقه	۷ دقیقه	۲ دقیقه	فورا	فورا	۸
۲ روز	۷ ساعت	۱ ساعت	۱۰ ثانیه	فورا	۹
۵ ماه	۳ هفته	۳ روز	۴ دقیقه	فورا	۱۰
۳۴ سال	۳ سال	۵ ماه	۲ ساعت	فورا	۱۱
۳ هزار سال	۲۰۰ سال	۲۴ سال	۲ روز	۲ ثانیه	۱۲
۲۰۲ هزار سال	۱۲ هزار سال	۱۰۰۰ سال	۲ ماه	۱۹ ثانیه	۱۳
۱۶ میلیون سال	۷۵۰ هزار سال	۶۴ هزار سال	۴ سال	۳ دقیقه	۱۴
۱۶ میلیارد سال	۴۶ میلیون سال	۳ میلیون سال	۱۰۰ سال	۳۲ دقیقه	۱۵
۹۲ میلیارد سال	۳ میلیارد سال	۱۷۳ میلیون سال	۳ هزار سال	۵ ساعت	۱۶
۷ تریلیون سال	۱۷۹ میلیارد سال	۹ میلیارد سال	۶۹ هزار سال	۲ روز	۱۷
۴۳۸ تریلیون سال	۱۱ تریلیون سال	۴۶۷ میلیارد سال	۲ میلیون سال	۳ هفته	۱۸

روش‌هایی برای بالابردن امنیت رمز عبورها

بالابردن امنیت فقط مختص به انتخاب گذرواژه با شیوه‌های گفته‌شده نیست. راهکارهایی وجود دارد که می‌تواند به حفظ بیشتر امنیت رمزهایمان کمک کند. از جمله:

استفاده از احراز هویت چند عاملی

احراز هویت چند عاملی یک لایه حفاظتی اضافی است که در صورت لو رفتن جزئیات حساب شما اولین لایه محافظتی شما می‌شود. این‌ها به استاندارد جدیدی برای بالابردن امنیت موثر تبدیل شده‌اند. حال شما می‌توانید در تمامی حساب‌های ایمیل و شبکه‌های اجتماعی با استفاده از این فرایند امنیت را بالا ببرید. بعضی از این حساب‌ها علاوه بر رمز عبور به چیزی مانند بیومتریک (اثر انگشت، اسکن چشم و غیره) یا یک نشانه فیزیکی نیاز دارند. به این ترتیب، به همان اندازه که رمز عبور شما ساده یا پیچیده باشد، شکاندن آن توسط هکر تنها نیمی از حل معماست البته توجه داشته باشید که بعد از هک معروف سایت «Reddit» در سال ۲۰۱۸ آن‌هم از طریق رهگیری پیامک، استفاده از پیامک به عنوان دومین عامل احراز هویت توصیه نمی‌شود.

استفاده از برنامه‌های گوشی هوشمند

یکی از بهترین روش‌ها استفاده از یک اپلیکیشن تخصصی برای گوشی هوشمندتان است. برای مثال اپلیکیشن «Google's Authenticator» موجود برای آیفون و اندروید یا «Authy» دو نمونه رایگان در این زمینه هستند. این برنامه هر بار یک رمز یک بار مصرف ایجاد می‌کند که شما آن را به عنوان عامل اضافی در طول فرایند ورود خود وارد می‌کنید. این رمزها (پین) به صورت خودکار هر ۳۰ ثانیه تغییر می‌کند و می‌تواند برای حساب‌هایی که ابراز هویت چند عاملی دارند، عالی باشد.

استفاده از سوالات دشوار

در بعضی از حساب‌های فضای مجازی سوالی مطرح می‌شود که شما می‌توانید با پاسخ دادن به آن یک مرحله دیگر به امنیت رمز خود بیفزایید. یعنی هنگامی که هکر چندبار تلاش می‌کند تا رمز عبور شما را هک کند، سیستم متوجه می‌شود و برای اطمینان از او یک سوال به خصوص با جواب منحصر به فرد شما را می‌پرسد. پس هنگام انتخاب سؤالات امنیتی موقع ایجاد یک حساب کاربری، گزینه‌هایی را انتخاب کنید که فقط شما پاسخ آن‌ها را می‌دانید. بسیاری از سوالات در کانال‌های اجتماعی با یک جست و جوی ساده پاسخ‌های آسانی دارند، پس مراقب باشید و با دقت انتخاب کنید.

پرونده

جایگزین‌های خوب برای کیسه‌های پلاستیکی

هر ایرانی روزانه ۳ کیسه پلاستیکی استفاده می‌کند؛ در روز جهانی بدون کیسه پلاستیکی از اهمیت توجه به این موضوع و آشنایی با چند جایگزین برای استفاده در موقعیت‌های مختلف گفتیم

#نه_به_کیسه_های_پلاستیکی

مهسا کسنوی | روزنامه‌نگار

هر ساله روز سوم جولای (مصادف با ۱۲ تیر) به عنوان روز جهانی بدون کیسه پلاستیکی (Plastic Bag Free Day) گرامی داشته می‌شود. همچنین بازه زمانی ۱۲ تا ۲۱ تیر (۳ تا ۱۲ جولای) را به عنوان دهه بدون کیسه پلاستیکی در نظر می‌گیرند. هدف از این نام‌گذاری، بررسی تاثیرات استفاده از کیسه‌های پلاستیکی بر طبیعت و اهمیت جایگزینی این کیسه‌ها با گزینه‌های دیگری است که قابلیت تجزیه‌پذیری دارند. به همین بهانه و در پرونده امروز زندگی سلام درباره عواقب استفاده از این کیسه‌های پلاستیکی و جایگزین‌هایش می‌گوییم.

هر ایرانی، ۳ کیسه پلاستیکی در روز

براساس تحقیقات انجام شده تنها در ایران سالانه بیش از سه میلیون تن پلاستیک تولید می‌شود. هر ایرانی روزانه به‌طور میانگین سه کیسه پلاستیکی استفاده می‌کند که متوسط عمر استفاده از هر کیسه، تنها ۱۲ دقیقه است. برای از بین بردن هر کدام از این کیسه‌ها در طبیعت، بین یک تا ۳۰۰ سال زمان نیاز است. هنگامی که کیسه‌های پلاستیکی به عنوان زباله دور ریخته می‌شوند، به علت ماندگاری بیش از ۳۰۰ سال در محیط، باعث آلودگی محیط زیست می‌شوند. این کیسه‌ها به همراه باد جابه‌جا و وارد رودخانه‌ها و کانال‌های آب می‌شوند، در نتیجه موجب گرفتگی آبراهه‌ها شده و در بسیاری موارد به علت ساکن ماندن آب، زادولد انواع حشرات افزایش می‌یابد. کیسه‌های پلاستیکی در صورت ورود به محیط زیست دریایی، وارد زنجیره غذایی جانوران دریایی می‌شوند و سالانه هزاران گونه از جانوران آبزی و پرندگان دریایی به اشتباه بر اثر خوردن این کیسه‌ها و خفگی ناشی از آن، می‌میرند.

جایگزین‌های کیسه‌های پلاستیکی

یکی از بهترین راه‌ها برای گرامی‌داشت این روز این است که در خریدهای روزمره خودمان از کیسه‌های پلاستیکی استفاده نکنیم و از اطرافیان خود بخواهیم از فروشنده کیسه پلاستیکی نخواهند؛ اما برای کیسه‌های پلاستیکی چه جایگزینی در موقعیت‌های مختلف وجود دارد؟

✓ کیسه پارچه‌ای برای نانوایی

پیشنهاد ما این است که از کیسه پارچه‌ای برای رفتن به نانوایی و قرار دادن نان در آن استفاده کنید. انجام این کار باعث می‌شود تا نان‌های شما تازه بمانند و میزان استفاده از کیسه‌های پلاستیکی را به طرز چشمگیری کاهش دهید.

✓ استفاده از کیف برای خریدهای دم‌دستی

شما می‌توانید یک کیف کوچک و دستی، همیشه به همراه داشته باشید تا محصولاتی را که اقدام به خرید آن‌ها می‌کنید، در این کیف قرار دهید. این روش برای استفاده روزانه یا خریدهای دم‌دستی مناسب به نظر می‌رسد.

✓ کیسه تجزیه‌پذیر برای استفاده روزانه

یکی از انواع کیسه‌هایی که در سال‌های اخیر تولید شده، کیسه‌های تجزیه‌پذیر هستند. در واقع این دسته از محصولات به سرعت در طبیعت تجزیه می‌شوند و قابلیت بازگشت سریع به محیط زیست را دارند. شما می‌توانید از این کیسه‌ها در موارد ضروری و برای مصرف روزانه استفاده کنید.

✓ ظرف‌های چند بار مصرف برای فریز کردن مواد غذایی

شاید بپرسید برای فریز کردن مواد غذایی به جای کیسه پلاستیکی از چه چیزی استفاده کنیم؟ ظرف‌های پلاستیکی که قابلیت شست‌وشو دارند، انتخاب مناسبی هستند. این ظروف را می‌توانید چندین سال استفاده کنید و بعد از هر بار مصرف آن را بشویید و بدین صورت به اندازه چند سال در مصرف کیسه پلاستیکی صرفه‌جویی کنید.

✓ کیسه پلاستیکی چندبار مصرف

به عنوان آخرین پیشنهاد و برای بیشتر موقعیت‌ها، از کیسه‌های پلاستیکی چند بار مصرف استفاده کنید و با این کار حجم مصرف کیسه‌های پلاستیکی را به طرز چشمگیری کاهش دهید. این کیسه‌ها هم برای استفاده روزانه بهترین انتخاب هستند.