بر اساس گزارش NordPass، به طور متوسط سالانه ۸۰۰هزار جرم سایبری رخ می‌دهد و روزانه ۳۰هزار وب سایت در سراسر جهان در معرض خطر حملات هکری قرار می‌گیرند. هر ۳۹ ثانیه یک حمله هکری صورت می‌گیرد و برخی از این حملات منجر به سرقت داده‌ها، آلودگی بدافزاری و از دست دادن اطلاعات محرمانه می‌شود. این بدان معناست که روزانه بیش از ۲۳۲۸ حمله سایبری در اینترنت رخ می‌دهد. همچنین روزانه بیش از ۵۶۰هزار بدافزار تولید می‌شود.

دست رد «رمزهای عبور» امن به سینه هکرها

پسورد پیچیده انتخاب کنید تا دردام هکرها نیفتید

میترا جلیلی
روزنامه‌نگار

این روزها ما بسیاری از داده‌های خود را به اینترنت سپرده‌ایم و با ایجاد حساب کاربری برای انجام امور روزمره ازجمله پرداخت قبوض، گشت وگذار در سایت‌های مختلف، حضور در شبکه‌های اجتماعی آنلاین و خرید آنلاین، عملاً حریم شخصی‌مان در اینترنت در معرض حمله هکرها و مجرمان سایبری قرار گرفته است. در این میان، پسوردها یا رمزهای عبور که از آنها با عنوان گذرواژه هم یاد می‌شود، محافظان اصلی حریم خصوصی، داده‌های شخصی و امور مالی ما هستند به شرطی که به امنیت آنها توجه ویژه داشته باشیم و از رمزهای عبور ساده و قابل حدس زدن استفاده نکنیم.

خسارت ۸ تریلیون دلاری حملات سایبری

حمله‌های سایبری روندی روبه رشد دارند و انتظار می‌رود تعداد هک‌ها در سال ۲۰۲۳ افزایش یابد. محققان حوزه فناوری معتقدند هکرها رمزهای عبور ضعیف را بهشتی برای خود می‌دانند چراکه ضعف‌های امنیتی این گذرواژه‌ها، بهترین راه نفوذ آنها محسوب می‌شود و بخش عمده حمله‌های هکری هم ازطریق همین رمزهای عبور ناامن صورت می‌گیرد.

حمله‌های سایبری، زیان‌های اقتصادی زیادی به شرکت‌ها و مؤسسات تحمیل می‌کنند و نشت داده‌های شخصی، گاه می‌تواند اطلاعات بانکی و داده‌های خصوصی افراد همچون عکس و فیلم آنها را لو بدهد و دردسرساز شود. در تازه‌ترین گزارش مجله سایبرسکیوریتی، پیش‌بینی شده که میزان خسارت حمله‌های سایبری در جهان تا پایان سال ۲۰۲۳ به ۸/۱۵ تریلیون دلار می‌رسد و این رقم تا سال ۲۰۲۵ به ۱۰/۵تریلیون دلار خواهد رسید درحالی که می‌توان با انتخاب یک رمزعبور مناسب، مانع بخش زیادی از این خسارت‌ها شد.

یک روز جهانی برای رمز عبور

امنیت گذرواژه‌ها آنقدر اهمیت دارد که «اینتل»، از کمپانی‌های مطرح دنیای فناوری در سال ۲۰۱۳ پیشنهاد داد در تقویم مناسبت‌های جهانی، یک روز به نام روز جهانی «رمزعبور» نامگذاری شود تا مردم برای افزایش ضریب امنیت گذرواژه‌های خود تشویق شوند و کمتر در دام هکرها بیفتند. درنهایت مقرر شد نخستین پنجشنبه ماه مه هر سال به عنوان روز جهانی رمزعبور شناخته شود. امسال هم به مناسبت روز جهانی رمزعبور، محققان و فعالان حوزه سایبری، راهکارهایی به مردم ارائه دادند تا بتوانند از حریم شخصی خود محافظت کنند و کمتر قربانی حمله‌های سایبری شوند.

این رمزهای عبور محبوب، اما خطرناک

محققان حوزه سایبری، امسال هم در روز جهانی رمزعبور، اطلاعات و آماری درباره دنیای گذرواژه‌ها ارائه داده‌اند که دانستن آنها خالی از لطف نیست. امسال شرکت مدیریت پسورد NordPass در تازه‌ترین گزارش خود آورده است با وجود اطلاع رسانی‌های گسترده، مردم عادات غلط خود در تعیین رمزهای عبور را ترک نکرده‌اند و همچنان از پسوردهای ضعیف برای محافظت از حساب‌های کاربری خود استفاده می‌کنند. در این گزارش که فهرستی از رمزهای عبور پرکاربرد در ایالات متحده و ۲۹ کشور دیگر مورد مطالعه قرار گرفته، مشخص شد همچنان «۱۲۳۴۵۶» محبوب‌ترین رمزعبور در جهان است و پس از آن، گذرواژه های «password» و «۱۲۳۴۵۶۷۸۹» قرار گرفته اند؛ گذرواژه‌هایی که بسرعت قابل حدس زدن هستند و اطلاعات کاربر در معرض خطر حمله هکری قرار دارد.

> حمله‌های سایبری روندی روبه رشد دارند و انتظار می‌رود تعداد هک‌ها در سال ۲۰۲۳ افزایش یابد. محققان حوزه فناوری معتقدند هکرها رمزهای عبور ضعیف را بهشتی برای خود می‌دانند چراکه ضعف‌های امنیتی این گذرواژه‌ها، بهترین راه نفوذ آنها محسوب می‌شود و بخش عمده حمله‌های هکری هم ازطریق همین رمزهای عبور ناامن صورت می‌گیرد

هر ۳۹ثانیه یک هک

بر اساس گزارشNordPass، به طور متوسط سالانه ۸۰۰هزار جرم سایبری رخ می‌دهد و روزانه ۳۰هزار وب سایت در سراسر جهان در معرض خطر حملات هکری قرار می‌گیرند. هر ۳۹ ثانیه یک حمله هکری صورت می‌گیرد و برخی از این حملات منجر به سرقت داده‌ها، آلودگی بدافزاری و از دست دادن اطلاعات محرمانه می‌شود.این بدان معناست که روزانه بیش از ۲۳۲۸ حمله سایبری در اینترنت رخ می‌دهد. همچنین روزانه بیش از ۵۶۰هزار بدافزار تولید می‌شود. ایجاد بدافزار جدید در چند سال گذشته به طور پیوسته در حال افزایش بوده است و پیش‌بینی می‌شود در سال ۲۰۲۳ حدود ۳۳ میلیارد حساب کاربری نقض شود.

حملات سایبری از کجا می‌آیند؟

اگرچه حملات سایبری از سراسر جهان انجام می‌شود، ولی یافته‌های این شرکت نشان می‌دهد روسیه، رومانی، امریکا، چین، برزیل و کره جنوبی کشورهایی هستند که بیشترین تعداد مهاجمان سایبری را دارند.

شکستن رمز عبور در کسری از ثانیه

شرکت NordPass بیش از ۳ ترابایت داده را با کمک محققان مستقل ارزیابی کرد تا میزان امنیت ۲۰۰رمزعبور پرطرفدار را در ۳۰ کشور مختلف مشخص کند. نتیجه این تحقیقات نشان داد ۸۳درصد از رایج‌ترین رمزهای عبور جهان ازجمله «۱۲۳۴۵۶»، «password»، «abc۱۲۳»، «qwerty» و«۱۱۱۱۱» در کمتر از یک ثانیه شکسته می‌شوند. این گزارش همچنین نشان می‌دهد که در امریکا رمز عبور password بیش از سایر گذرواژه‌ها مورد توجه هکرها قرار داشته درحالی که در آلمان، مجرمان سایبری رمز عبور«۱۲۳۴۵۶» و در روسیه، پسورد qwerty»» را بیش از همه هک کرده‌اند.

از تیم‌های فوتبال تا الگوهای عددی

در این گزارش گذرواژه‌ها بر اساس کشورها هم مورد تجزیه و تحلیل قرار گرفته‌اند و مشخص شد کلمه «سلام»(به زبان کشورهای مختلف)، یک رمزعبور محبوب در سراسر جهان است. در کشورهای دوستدار فوتبال یعنی هر دو کشور ایتالیا و اسپانیا، بیشتر کاربران نام تیم‌های فوتبال برجسته خود را در حداقل یکی از ۱۰ رمزعبور خود دارند. کاربران آلمانی و اسپانیایی برای ایجاد گذرواژه‌های خود به اعداد علاقه دارند ولی کاربران روس بیشتر از سایر کشورها الگوهای صفحه کلید مانند@ و $ را برای رمزهای عبور انتخاب می‌کنند.

چگونه گذرواژه امن بسازیم؟

محققان حوزه فناوری برای ایجاد گذرواژه‌های امن به کاربران توصیه می‌کنند از رمزهای عبور با بیشتر از ۸ کاراکتر استفاده کنند و هرچه این گذرواژه طولانی‌تر باشد بهتر است. - کارشناسان معتقدند رمزعبور حداقل ۱۶کاراکتری، بهترین گذرواژه است به شرطی که در آن اعداد، حروف بزرگ، کوچک و کاراکترهای خاص به کار رفته باشد. ولی هرگز رمز عبورتان به گونه‌ای نباشد که با یک حرف بزرگ شروع شده و به یک عدد ختم شود چرا که بسیاری کاربران از این الگو استفاده می‌کنند و راه را برای هکرها هموارتر می‌کند.

- از سال تولد، کد ملی یا محل تولد خود یا افراد مشهور برای ساخت گذرواژه استفاده نکنید. نام شهرها، عنوان آهنگ‌ها و نقل قول‌های معروف هم ایده خوبی برای ساخت یک رمز مناسب و امن نیست. هیچ کلمه‌ای از آدرس ایمیل خود را به عنوان بخشی از رمز عبورتان وارد نکنید و از گذرواژه‌های آسیب‌پذیری که به راحتی حدس زده می‌شوند، اجتناب کنید. با یک جست‌وجوی ساده در موتور جست‌وجوی گوگل می‌توانید گذرواژه‌های رایج مورد استفاده را که به راحتی توسط هکرها شکسته می‌شوند شناسایی کنید و هرگز آنها را به کار نبرید.
- درست است که به خاطر سپردن گذرواژه‌های متعدد چندان ساده نیست و کسی به این کار علاقه‌ای ندارد ولی برای امنیت بیشتر بهتر است از یک گذرواژه برای چندین حساب کاربری استفاده نکنید. می‌توانید از سیستم‌های مدیریت رمزعبور مانند Dashlane و Locker کمک بگیرید.
- استفاده از یک آنتی ویروس مناسب ازجمله Norton، Malwarebytes و Bitdefenderهم می‌تواند سد محکمی مقابل هکرها ایجاد کند. البته به روزرسانی این آنتی ویروس‌ها و سیستم‌های مدیریت گذرواژه هم موضوع مهمی است که کاربران باید به آن توجه داشته باشند وگرنه باز هم در معرض حمله مهاجمان سایبری قرار می‌گیرند.
- استفاده از روش‌های احراز هویت چند عاملی2FA هم یک راهکار مناسب برای مقابله با حملات هکری است.همیشه، همیشه از 2FA استفاده کنید. به این ترتیب حتی اگر رمز عبور شما به خطر بیفتد، باز هم لایه دوم حفاظتی از حساب کاربری شما حفاظت می‌کند.
- بهتر است از سیستم‌های 2FA که یک کد را به گوشی هوشمند شما ارسال می‌کنند، خودداری کنید چراکه کلاهبرداری‌هایی که درقالب آن، یک مجرم سایبری شماره تلفن شما را تصاحب می‌کند، در حال افزایش است و اگر مجرم شماره تلفن شما را در اختیار بگیرد، پیامک 2FA شما را دریافت خواهد کرد و می‌تواند به راحتی به حساب کاربریتان دسترسی پیدا کند.

30

شرکت NordPass بیش از ۳ ترابایت داده را با کمک محققان مستقل ارزیابی کرد تا میزان امنیت ۲۰۰رمزعبور پرطرفدار را در ۳۰ کشور مختلف مشخص کند. نتیجه این تحقیقات نشان داد ۸۳درصد از رایج‌ترین رمزهای عبور جهان ازجمله «۱۲۳۴۵۶»، «password»، «abc۱۲۳»، «qwerty» و«۱۱۱۱۱» در کمتر از یک ثانیه شکسته می‌شوند.