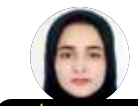
بر اساس تحقیقات انجام شده، مردم از پسوردهای ساده استفاده می‌کنند تا راحت‌تر در ذهن‌شان بماند؛ چیزهایی مانند اعداد، اسامی، نام غذاها و حتی الفاظ رکیک! به طور مثال پسورد ۱۲۳۴۵ سال گذشته، رتبه اول را در میان پسوردهای پرتکرار به دست آورده بود

با توجه به اینکه افراد ممکن است دارای چندین حساب بانکی باشند به خاطر سپردن این رمزها سخت‌تر نیز خواهد شد. برای این مورد می‌توانید از نرم‌افزارهای مدیریت رمز استفاده کنید.

کلیک پسوردهای پرطرفدار را بررسی می‌کند

انتخاب‌های خطرناک برای رمزعبور



معصومه‌سعادت
خبرنگار

بسیاری از ما ترجیح می‌دهیم به جای بیرون رفتن از خانه، بسیاری از کارهای بانکی و خرید خود را از طریق اینترنت انجام دهیم. این روزها جرایم سایبری افزایش یافته و گاهی شاهد نقض داده‌ها و سرقت هویت افراد هستیم. بسیاری از مجرمان سایبری می‌توانند از رمزهای عبور برای خرید یا از طریق دوربین‌های امنیتی متصل به وای‌فای به منظور اقدامات خرابکارانه و جاسوسی استفاده کنند. به همین دلیل، این موضوع ما را بر آن داشت به علل هک‌شدن اطلاعات این اشخاص بپردازیم. یکی از علل مهم این قضیه، استفاده از رمزهای عبور ساده است که بسیاری از افراد به آن کم توجه هستند.

در حالی که سال‌هاست سازمان‌های انتظامی و امنیتی درباره پیشرفته شدن حملات هکرها علیه دولت‌ها و شهروندان هشدار می‌دهند، اما هنوز هم بسیاری از مردم به استفاده از پسوردهای ناامن اصرار دارند. بر اساس تحقیقات انجام شده، مردم از پسوردهای ساده استفاده می‌کنند تا راحت‌تر در ذهن‌شان بماند؛ چیزهایی مانند، اعداد، اسامی، نام غذاها و حتی الفاظ رکیک! به طور مثال پسورد ۱۲۳۴۵ سال گذشته، رتبه اول را میان پسوردهای پرتکرار به دست آورده بود و امسال با بیش از ۱۸۸ هزار رای از سوی کاربران در نظرسنجی NordPass در رتبه هشتم فهرست قرار گرفت. از دیگر اعداد پراستفاده به عنوان رمز عبور باید به ۱۱۱۱۱۱ و ۱۲۳۱۲۳ اشاره کنیم که از رده‌های هفدهم و هجدهم پارسال به رتبه‌های ششم و هفتم امسال صعود کرده‌اند.

نحوه ایجاد رمزهای عبور امن

بهترین روش‌ها برای ایجاد رمزهای عبور امن عبارتند از:

- یک رمز عبور غیرقابل نفوذ باید ۱۶ کاراکتر یا بیشتر باشد.
- رمز عبور باید ترکیبی از حروف، اعداد و کاراکترها باشد.
- رمز عبور نباید با هیچ حساب دیگری به اشتراک گذاشته شود.
- رمز عبور نباید شامل اطلاعات شخصی کاربر مانند آدرس یا شماره تلفن باشد.
- رمز عبور نباید حاوی حروف یا اعداد متوالی باشد.
- رمز عبور نباید همان کلمه password یا حرف و شماره تکرار شده باشد.

به خاطر سپردن رمزهای عبور با بیش از هشت کاراکتر برای بسیاری از افراد کاری دشوار است و با توجه به این‌که افراد ممکن است دارای چند حساب بانکی باشند، به خاطر سپردن این رمزها سخت‌تر نیز خواهد شد. برای این مورد می‌توانید از نرم‌افزارهای مدیریت رمز استفاده کنید.

نرم‌افزار مدیریت رمز در اصل یک اتاق دیجیتال رمزنگاری شده است که اطلاعات نام کاربری و رمز عبور شما را برای دسترسی به برنامه‌ها و حساب‌ها در دستگاه تلفن‌همراه، وب‌سایت‌ها و سایر سرویس‌های شما ذخیره می‌کند.

در حالی که سال‌هاست سازمان‌های انتظامی و امنیتی درباره پیشرفته شدن حملات هکرها علیه دولت‌ها و شهروندان هشدار می‌دهند، اما هنوز هم بسیاری از مردم به استفاده از پسوردهای ناامن اصرار دارند

چند نمونه از بهترین ابزارهای مدیریت رمز عبور

۱- LastPass: از بین همه ابزارهایی که وجود دارد ما ابزار LastPass را به عنوان یکی از بهترین‌ها یافتیم. این ابزار دارای مجموعه‌ای غنی از امکانات رایگان است که به بیشتر کاربران اجازه می‌دهد بدون نیاز به پرداخت هیچ‌گونه هزینه‌ای به هر آنچه نیاز دارند، دسترسی داشته باشند. این ابزار در بیشتر مرورگرها و تقریبا تمام دستگاه‌های هوشمند قابل دسترس است و همچنین امکانات به اشتراک‌گذاری را در نسخه پولی خود ارائه می‌کند.

مزایا: آسانی در استفاده، امکانات عالی در نسخه رایگان، احراز هویت چندعاملی

معایب: برنامه‌های دسکتاپ قدیمی است. نمی‌توان برخی از داده‌های شخصی را به صورت خودکار پر کرد. در سال ۲۰۱۵ وب‌سایت آن هک شد.

LastPass یک مدیر رمز مبتنی بر مرورگر است که دارای افزونه‌هایی برای اپرا، سافاری، فایرفاکس، کروم، اج (Edge) و همچنین برای اندروید، آی‌اواس و ویندوزفون است. از استاندارد رمزنگاری AES 256-bit استفاده می‌کند و همچنین دارای احراز هویت چندعاملی (MFA) است که به کاربران اجازه می‌دهد با استفاده از تلفن هوشمند یا اثر انگشت به حساب خود دسترسی داشته باشند.

۲- Dashlane: این برنامه را می‌توان به عنوان یکی از بهترین ابزار با امکانات امنیتی انتخاب کرد، زیرا در این ابزار اسکن وب تاریک را برای نشت داده‌ها، شبکه خصوصی مجازی امن (VPN) و گزینه تغییر رمز عبور را ارائه می‌کند.

مزایا: همگام‌سازی بین دستگاه‌ها، دارای VPN داخلی و نظارت بر وب تاریک

معایب: محدودیت ۵۰ رمز عبور در نسخه رایگان، برنامه محدود به استفاده در یک دستگاه است. فضای ذخیره‌سازی ابری محدود است.

نسخه رایگان Dashlane محدود به ۵۰ رمز عبور و یک استفاده فقط در یک دستگاه است و از احراز هویت دو مرحله‌ای و قابلیت به اشتراک‌گذاری در حداکثر پنج حساب را پشتیبانی می‌کند. Dashlane دارای برنامه‌هایی برای اندروید، مک، ویندوز، آی‌اواس و همچنین دسترسی به سیستم‌های عامل مبتنی بر لینوکس و کروم‌بوک از طریق افزونه‌های مرورگر است. یکی از ویژگی‌های جالب توجه در ابزار Dashlane که تعداد کمی از ابزارهای مشابه ارائه می‌کنند، این است که امکان تغییر رمز عبور و جایگزینی آن با صدها رمز عبور دیگر تنها با یک کلیک امکان‌پذیر است.

۳- LogMeOnce: ابزار LogMeOnce را می‌توان به عنوان بهترین ابزار با قابلیت پشتیبانی از چند پلتفرم دانست، زیرا به کاربران اجازه می‌دهد به گذرواژه‌های خود دسترسی داشته باشند و تقریبا در هر مرورگر، رایانه یا تلفن‌همراه با تصویر، اثر انگشت یا PIN می‌توان وارد سیستم شد.

مزایا: پشتیبانی از خاصیت چند پلتفرمی، ذخیره‌سازی رمزگذاری شده، قابلیت شخصی‌سازی

معایب: می‌تواند برای کاربران جدید خسته‌کننده باشد. افزونه‌ها می‌توانند گران شوند.

LogMeOnce یک طرح تبلیغاتی رایگان ارائه می‌کند که شامل رمز عبور و دستگاه‌های نامحدود است، دارای احراز هویت دو مرحله‌ای و یک مگابیت فایل رمزنگاری شده است. LogMeOnce دارای لیست چشمگیری از بیش از ۵۰ ویژگی است که بسیاری از آنها در این پلتفرم منحصر به فرد هستند و امکان سفارشی‌سازی را فراهم می‌آورند. کاربران می‌توانند یک داشبورد قابل تنظیم، ورود عکس و موارد دیگر را به صورت رایگان دریافت کنند.

۴- Bitwarden: ما می‌توانیم ابزار Bitwarden را به عنوان یکی از بهترین ابزارهای رایگان انتخاب کنیم زیرا با این‌که امکانات یکسانی را نسبت به سایر ابزارهای مشابه ارائه می‌کند، با ارائه پشتیبانی از دستگاه‌های نامحدود و قابلیت به اشتراک‌گذاری، حتی می‌تواند برنامه LastPass را نیز شکست دهد.

مزایا: رمزهای عبور نامحدود و همگام‌سازی در نسخه رایگان، تولیدکننده رمزهای ایمن

معایب: دارای برخی مشکلات در افزونه مرورگر اج، پشتیبانی محدود از آی‌اواس، اشتراک‌گذاری امن با هزینه است.

برنامه رایگان Bitwarden شامل همگام‌سازی بین دستگاه‌ها، ذخیره‌سازی امن، احراز هویت دومرحله‌ای و گزینه ذخیره رمزهای عبور به صورت آفلاین به جای استفاده از فضای ذخیره‌سازی ابری است. نسخه پولی این ابزار شامل یک گیگابایت فضای ذخیره‌سازی فایل رمزنگاری شده، گزینه‌های اضافی برای احراز هویت، ایجاد رمز عبور و پشتیبانی پیشرفته است. کد Bitwarden به عنوان یک پلتفرم منبع‌باز به صورت رایگان برای بازرسی، آزمایش و تغییر در دسترس همه قرار دارد.