وای! ژ ا آوریل 2020

SANS SECURITY AWARENESS

ماهنامه آگاهی از امنیت اطلاعات برای شما

مدیریت رمز عبور

مقدمه

یکی از مهمترین اقداماتی که می توانید برای محافظت از خود انجام دهید استفاده از یک رمزعبور منحصر به فرد و قوی برای هر یک از حسابها و برنامه های خود است. متأسفانه، به خاطر سپردن کلمه عبورهای مختلف تقریباً غیرممکن است. علاوه بر این، میدانیم که وارد کردن مداوم رمزهای عبور در سایتهای مختلف، تولید رمز های جدید، پیگیری جواب های مربوط به سوالات امنیتی، و بسیاری از عوامل دیگر کاری زمان بر است. با این حال، راه حلی وجود دارد که زندگی شما را ساده تر و به مراتب ایمن تر خواهد کرد و آن استفاده از برنامه های مدیریت رمزعبور است.

برنامه های مدیریت رمزعبور چگونه کار میکنند

برنامه های مدیریت رمزعبور با ذخیره کردن کلمه عبور شما در یک پایگاه داده کار می کنند که بعضا به آن قفل (Vault) می گویند. برنامه مدیریت پسورد محتویات پایگاه داده (Vault) را رمزگزاری کرده و با یک رمزعبور اصلی که فقط شما آن را میدانید از آن محافظت میکند. زمانیکه به رمزهای عبور خود نیاز دارید، مانند ورود به حساب بانکی آنلاین یا ایمیل، به سادگی می توانید رمز ورود اصلی خود را در برنامه مدیریت رمز عبور وارد کنید تا قفل را باز کند. برنامه مدیریت رمزعبور به طور خودکار رمز عبور صحیح را بازیابی کرده و بصورت امن شما را به وب سایت وارد می کند. دیگر لازم نخواهد بود تا رمزهای عبور خود را به خاطر بسپارید یا به صورت دستی وارد حساب های خود شوید.

علاوه بر این ، بیشتر برنامه های مدیریت رمزعبور امکان همگام سازی خودکار در چندین دستگاه را نیز شامل می شوند. به این ترتیب ، وقتی یک گذرواژه را در لپ تاپ خود به روز می کنید ، آن تغییرات با تمام دستگاه های دیگر شما همگام می شوند. در خاتمه، بیشتر برنامه های مدیریت رمز عبور وقتی می خواهید یک حساب آنلاین جدید ایجاد کنید یا رمز ورود یک حساب موجود را به روز کنید، آن تغییرات را تشخیص داده و به طور خودکار پایگاه داده(Vault) را برای شما به روز می کنند.

بسیار مهم است که رمز عبور اصلی که برای محافظت از برنامه مدیریت رمز عبور استفاده می کنید طولانی و منحصر به فرد باشد. در واقع، توصیه ما این است که رمزعبور اصلی خود را به یک عبارت تبدیل کنید - یک رمز عبور طولانی که از چندین کلمه یا عبارات تشکیل شده است. اگر برنامه مدیریت رمز عبور شما از تأیید صحت دو مرحله ای پشتیبانی می کند، از آن برای رمز عبور اصلی خود نیز استفاده کنید. در آخر ، حتماً عبارت عبور اصلی خود را بخاطر بسپارید. اگر آن را فراموش کنید، نمی توانید به هیچ یک از رمزهای عبور دیگر خود دسترسی پیدا کنید.

انتخاب برنامه مدیریت رمزعبور

روشهای بسیاری برای انتخاب برنامه مدیریت رمزعبور وجود دارد در بخش منابع آدرسی ارائه شده که به بررسی برنامه مدیریت رمز عبور می پردازد. در ضمن، برای پیدا کردن بهترین برنامه، موارد زیر را در خاطر داشته باشید:

برنامه مدیریت رمز عبور باید ساده باشد. اگر کار کردن با یک برنامه پیچیده بود، برنامه دیگری را بیابید که متناسب با سبک و تخصص شما باشد.

برنامه مدیریت رمز عبور باید روی تمام دستگاه های مورد نیاز برای استفاده از رمزهای عبور کار کند. همچنین باید بتواند کلمات عبور شما را به آسانی با تمام دستگاه های دیگر متعلق به شما همگام سازی کند.

تنها ار برنامه های مدیریت پسوردی که قابل اطمینان و شناخته شده هستند استفاده کنید. استفاده از محصولاتی که مدت زمان زیادی از تولید آنها نمیگذرد و یا نظرات کمتری نسبت به آنها داده شده پرهیز کنید. مجرمان سایبری می توانند با ارائه برنامه های مدیریت رمز عبور جعلی اطلاعات شما را به سرقت ببرند. همچنین، به فروشنده هایی که تبلیغ می کنند که راه حل رمزگذاری خود را توسعه داده اند و در برنامه مدیریت پسورد استفاده میکنند بسیار مشکوک باشید.

از استفاده ار برنامه های مدیریت رمزعبوری که ادعا می کنند می توانند رمز عبور اصلی شما را بازیابی کنند، خودداری کنید. این بدان معنی است که آنها رمزعبور اصلی شما را می دانند، که شما را در معرض خطر زیادی قرار می دهد.

از هر راهکاری که استفاده میکنید، اطمینان حاصل کنید که فروشنده دائما برنامه مدیریت رمز عبور را به روز رسانی و وصله میکند، و به ویژه مطمئن باشید که همیشه از جدیدترین نسخه استفاده می کنید.

برنامه مدیریت رمز عبور باید به شما امکان ذخیره داده های حساس دیگر، مانند پاسخ به سؤالات امنیتی، اطلاعات کارت اعتباری و شماره مکرر پرواز را به شما بدهد.

توجه کنید که عبارت اصلی خود را در یک پاکت بسته قرار داده و آن را در یک کابین قفل شده، گاوصندوق یا صندوق امن نگه دارید.

برنامه مدیریت گذرواژه راهی عالی برای ذخیره ایمن کلمه عبور و سایر داده های حساس مانند شماره کارت های اعتباری است. با این حال، حتما از یک عبارت اصلی منحصر به فرد و قوی استفاده کنید و همیشه آخرین نسخه برنامه را بکار ببرید.

سردبیر مهمان

راسل یوبانکس یک پیشرو در امنیت اطلاعات از اتالانتا است که با بیش از *20* سال تجربه، مدارک بسیاری را کسب کرده است. او مربی یک مرکزاطلاعات طوفان اینترنت *SANS* است و در کنترل های امنیتی بحرانی همکاری دارد. برای دسترسی به راسل میتوانید از *@russelleubanks* و آدرس *https://www.securityeverafter.com*. استفاده کنید.

منابع

آسان سازی گذرواژه ها http://www.sans.org/u/Y63

وراثت دیجیتال: http://www.sans.org/u/Z2G

نظرات مستقیم مرتبط با بهترین برنامه های مدیریت رمزعبور: /https://www.wired.com/story/best-password-managers