OUCH!
SANS SECURITY AWARENESS
ماهنامه آگاهی از امنیت اطلاعات برای شما

مدیریت گذرواژه ها را ساده کنیم

مقدمه

اغلب به شما گفته میشود که رمزهای عبور شما کلیدی برای محافظت از حساب های کاربری شما هستند (که حرف درستی است!)، اما به ندرت به شما راهی ساده برای ایمن سازی و مدیریت تمام رمزهای عبور خود داده می شود. در زیر ما سه مرحله ساده را برای ساده کردن گذرواژه های شما، قفل کردن حساب های خود و محافظت از آینده خود را پوشش می دهیم.

عبارت عبور

دوران رمزهای عبور پیچیده و عجیب غریب تمام شده است. این رمزهای عبور سخت است که به خاطر سپرد سخت است که تایپ شوند، و با استفاده از رایانه های فوق العاده سریع امروز مهاجم سایبری به راحتی میتواند آنها را بشکند. کلید رمزهای عبور قوی این است که طولانی باشند، اگر رمز عبور کاراکترهای بیشتری دارد رمز بهتری است. اینها را passphrases مینامند، یک نوع رمز عبور قوی است که از یک جمله کوتاه یا کلمات تصادفی استفاده می کند. در اینجا دو نمونه است

وقت خوردن قهوه قوی است!
ساحل حلزون خزنده گم شده

هر کدام از اینها با بیش از بیست کاراکتر قوی هستند، آسان برای بخاطر سپردن و ساده برای تایپ اما مشکل برای هک کردن. شما ممکن است به وب سایت ها یا شرایط برخورد کنید که باید در گذرواژه علامت ها، شماره ها یا حروف بزرگ بکا ر برید، که خوب است. به یاد داشته باشید همیشه طول رمز عبور مهم ترین است.

نرم افزار مدیریت رمز عبور

برای هر حساب یک رمز عبور منحصربفرد نیاز دارید. اگر چندین رمز یکسان را برای چندین بار استفاده کنید، شما خود را در معرض خطر بزرگ قرار می دهید. یک مهاجمین سایبری تنها کاری که باید انجام دهد این است که وبسایتی را که از آن استفاده میکنید را هک کنند، تمام رمزهای عبور از جمله رمز شما را سرقت کنند، سپس از گذرواژه شما برای ورود به همه حسابهای دیگر شما استفاده کنند. این خیلی بیشتر از آنچه شما بدانید اتفاق میافتد. باور نمیکنید؟ وب سایت www.haveibeenpwned.com را بررسی کنید تا ببینید کدامیک از سایت هایی که استفاده می کنید هک شده اند و کلمه عبور شما به طور بالقوه در خطر است. پس باید چکار کنید؟ از یک نرم افزار مدیریت رمز عبور استفاده کنید.

این برنامه های کامپیوتری مخصوصی هستند که به طور ایمن تمام گذرواژه های شما را در یک گاوصندوق دیجیتال رمزگذاری ذخیره می کند. شما فقط به یک رمز عبور نیاز دارید، رمزی برای نرم افزار مدیریت رمز عبور. مدیر رمز عبور به طور خودکار هر وقت که به آنها نیاز دارید، کلمه عبور شما را بازیابی می کند و شما را به وب سایت ها وارد می کند. آنها همچنین قابلیت های دیگری مانند ذخیره پاسخ های به سوالات مخفی هم را ذخیره میکنند، هشدار دادن هنگامی که شما رمز عبور تکراری استفاده میکنید یک ژنراتور رمز عبور که تضمین می کند از کلمات عبور قوی استفاده میکنید و بسیاری از ویژگی های دیگر. بیشتر نرم افزار های مدیریت رمز عبور هم ایمن در تقریبا هر کامپیوتر یا دستگاه همگام سازی می شوند، بنابراین صرفنظر از سیستم که استفاده می کنید، دسترسی آسان و امن به تمام رمزهای عبور شما وجود دارد.

در نهایت، مطمئن شوید رمز عبور ورود به نرم افزار مدیریت رمزعبورها یادداشت کنید و آن را در یک مکان امن در خانه ذخیره کنید. برخی از نرم افزارهای مدیریت رمز عبور حتی اجازه کپی بازیابی رمز عبور مدیر را چاپ می کنند. به این ترتیب اگر رمز عبور را به مدیر رمز عبور خود بسپارید، پشتیبان دارید. یا اگر بیمار هستید یا در شرایط اضطراری پیدا کنید، همسر یا اعضای خانواده تان اطمینان می توانید اطلاعات را از طرف شما بازیابی کنید.

تأیید دو مرحله ای

تأیید صحت دو مرحله ای (اغلب به نام تأیید دو عامل یا تایید هویت چند عامل) یک لایه امنیتی اضافی را ایجاد میکند. در هنگام وارد شدن به حسابهایتان، لازم است دو چیز داشته باشید. گذرواژه و کد عددی که توسط گوشی هوشمند شما تولید شده یا به تلفن شما ارسال می شود. این فرآیند تضمین می کند که حتی اگر مهاجم سایبری رمز عبور شما را دریافت کند، هنوز نمی تواند به حساب شما وارد شود. تأیید صحت دو مرحله ای خیلی ساده میشود تنظیم کرد و شما معمولا فقط هنگامی که از یک رایانه یا دستگاه جدید وارد سیستم می شوید فقط باید آن را استفاده کنید. هر زمان که ممکن است، به ویژه برای مهمترین حسابهایتان مانند حساب بانکی یا حسابهای بازنشستگی یا دسترسی به ایمیل خود، این امکان را فعال کنید. اگر از مدیر رمز عبور استفاده می کنید، به شدت توصیه می کنیم آن را با یک عبارت عبور قوی و تأیید دو مرحلهای محافظت کنید.

این ممکن است به نظر احمقانه باشد، اما این سه مرحله ساده راه زیادی برای محافظت از کار، شهرت و آینده مالی شما می گذارد.

سردبیر مهمان

جاستین هندرسون (@SecurityMapper) یکی از بنیانگذاران H & A Security Solutions است، مدرس معتبر موسسه SANS و نویسنده مطالب دوره های SANS Cyber Defense و SIEM است. او همه چیزهای درباره دفاع سایبری را دوست دارد و برای پانزده سال در این زمینه مشاورت بوده است.

منابع

من هک شده ام: https://haveibeenpwned.com/

سایت تصدیق دو عامل: https://twofactorauth.org/

NIST SP800-63B: https://pages.nist.gov/800-63-3/sp800-63b.html

پوستر: هدف شما: https://www.sans.org/u/OGi