

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

در این شماره..

- مقدمه
- برنامه های مدیریت رمز عبور چگونه کار میکنند.
- نحوه انتخاب نرم افزار مدیریت رمز عبور

OUCH!

برنامه های مدیریت رمز عبور

مقدمه

یکی از مهمترین قدمهایی که هر فرد نیاز است تا برای محافظت از خود در فضای آنلاین بردارد استفاده از رمز عبور قوی و منحصر بفرد برای هریک از حسابها و ابزارهای خود است. متأسفانه، بخاطر سپردن همه رمز عبور ها برای حسابهای کاربری مختلف امری غیر ممکن است. به همین دلیل است که بسیاری از افراد بارها و بارها از رمز عبوری یکسان استفاده میکنند. متأسفانه استفاده پیاپی از یک رمز عبور برای حسابهای کاربری مختلف بسیار خطرناک است به این دلیل که

به محض اینکه کسی رمز عبور شما را بدست آورد قادر خواهد بود که به تمام حسابهای کاربری شما دست پیدا کند. یک راه حل ساده برای حل این مشکل استفاده از ابزار های مدیریت رمز عبور است که گاهی password vault (محل امن برای نگهداری رمز عبور) نیز اطلاق میشود. این ابزارها برنامه هایی هستند که بصورت امن تمامی رمز عبورهای شما را ذخیره کرده و با استفاده از آن میتوانید برای هر حساب کاربری یک رمز عبور متفاوت داشته باشید. با استفاده از برنامه های مدیریت رمز عبور بجای اینکه تمامی رمز عبور خود را بخاطر بسپارید، کفایت تنها رمز عبور اصلی ورود به برنامه مدیریت رمز عبور را حفظ کنید.

برنامه مدیریت رمز عبور چگونه کار میکند

کارکرد برنامه مدیریت رمز عبور ذخیره کردن تمامی رمز عبورها در یک پایگاه داده (database) است که گاه به آن صندوق امن (vault) اطلاق میشود. این ابزار محتوای vault را رمزنگاری کرده و از آن با رمز عبوری که فقط شما میدانید محافظت میکند. زمانی که بخواهید با استفاده از رمز عبور خود برای ورود به ایمیل و یا حساب بانکی خود استفاده کنید، به آسانی رمز عبور برنامه مدیریت رمز عبور را وارد کرده و قفل vault (محل امن نگهداری رمز عبور) را باز میکنید. در بسیاری از موارد برنامه مدیریت رمز عبور بصورت خودکار رمز عبور را گرفته و شما را وارد سایت مربوطه میکند. به این ترتیب شما میتوانید صدها رمز عبور مختلف داشته باشید و هرگز نیاز به حفظ کردن آنها نداشته باشید.

بعضی از برنامه های مدیریت رمز عبور محتویات vault را بر روی کامپیوتر یا موبایل شما ذخیره میکنند و برخی دیگر بر روی ابر (cloud). علاوه بر این، بسیاری از برنامه های مدیریت رمز عبور این قابلیت را دارند تا به صورت خودکار محتویات vault را بر روی دستگاه هایی که از طرف شما مجاز شناخته شده اند بروزرسانی کنند. به این ترتیب اگر شما رمز عبوری را بر روی لب تاپ خود تغییر داده باشد، آن تغییرات بر روی کلیه دستگاه های مجاز به روز خواهد شد. صرف نظر از اینکه اطلاعات رمز عبور در چه جایی ذخیره شده باشند، لازم است برنامه مدیریت

سر دبیر مهمان

کریس کریستائسون مشاور امنیت اطلاعات در کالیفرنیا، با 20 سال سابقه با تعداد بسیاری مدارک فنی میباشد. وی در بسیاری از کنفرانس ها سخنرانی کرده و در بسیاری از مقالات صنعتی مشارکت داشته است. کریس از طریق سایت <https://ismellpackets.com> و [@cchristianson](mailto:cchristianson) قابل دسترس است.

برنامه های مدیریت رمز عبور



برنامه های مدیریت رمز عبور روشی ساده برای ذخیره سازی و استفاده امن از رمز عبور های مختلف است.

رمز عبور را بر روی سخت افزاری که می خواهید از این ابزار استفاده کنید نصب کنید.

در زمان تنظیم برنامه مدیریت رمز عبور برای بار اول، میبایست کلیه رمز عبور ها را بصورت دستی وارد کرد. پس از آن، هنگامی که شما در حال ثبت یک حساب کاربری جدید و یا بروزرسانی رمز عبور های یک حساب موجود هستید، برنامه مذکور بصورت خودکار محتویات vault را بروزرسانی میکند. این کار به این دلیل امکان پذیر است که این برنامه ها بصورت یکپارچه با مرورگرها در ارتباط هستند. این ارتباط به شخص اجازه میدهد تا بصورت خودکار به وب سایتها وارد شوند.

بسیار مهم است که رمز عبور اصلی که برای محافظت از محتویات برنامه مدیریت رمز عبور استفاده میکنید بسیار قوی و غیر قابل حدس زدن باشد. پیشنهاد ما استفاده از عبارت عبور (passphrase)، بعنوان یکی از قوی ترین روش های تعیین رمز عبور، برای رمز عبور اصلی است. اگر برنامه شما از روش های احراز هویت دوعاملی

پشتیبانی میکند از آن برای استفاده از رمز عبور اصلی استفاده کنید. در انتها حتما رمز عبور اصلی خود را به خاطر بسپارید. در صورتیکه آن را فراموش کنید، هرگز قادر نخواهید بود به سایر رمز عبور های خود دسترسی پیدا کنید.

نحوه انتخاب یک برنامه مدیریت رمز عبور

برنامه های بسیاری برای مدیریت رمز عبور وجود دارد. در بخش منابع لینکی قرار دادیم که میتوانید این برنامه ها را مرور کنید. در عین حال زمانیکه در حال پیدا کردن بهترین برنامه هستید، نکات ذیل را به خاطر بسپارید:

- کار با برنامه مدیریت رمز عبور باید برای شما آسان باشد. اگر برنامه ای پیدا کردید که کار با آن پیچیده است از آن صرف نظر کنید و راه حلی بیابید که با تخصص و تجربه شما مناسبت داشته باشد.
- مدیریت رمز عبور میبایست بر روی کلیه وسایل الکترونیکی (رایانه و موبایل و تبلت) که رمز عبور بر روی آنها استفاده میشوند کار کند. این برنامه میبایست به آسانی بر روی کلیه دستگاه های شما بروزرسانی شود.
- همیشه از برنامه های قابل اعتماد و معروف استفاده کنید. از برنامه هایی که برای مدت طولانی در این حوزه نبودند و یا بازخورد کمتری از کاربران دارند استفاده نکنید. مجرمان سایبری میتوانند برنامه های مدیریت رمز عبور بنویسند که اطلاعات شما را بدزدند. همچنین کسانی که ادعا میکنند که راهکار رمزنگاری را خودشان ایجاد کردند بسیار مشکوک باشید.
- از برنامه های مدیریت رمز عبوری که ادعا میکنند میتوانند رمز عبور اصلی را بازیابی کنند استفاده نکنید. این به این معناست که آنها رمز عبور اصلی شما را میدانند.

برنامه های مدیریت رمز عبور

- از برنامه ای استفاده کنید که فروشنده آن بطور مرتب برنامه را بروزرسانی میکند و مطمئن باشید که همیشه از آخرین نسخه نرم افزار استفاده میکنید.
- برنامه مدیریت رمز عبوری استفاده کنید که قابلیت ایجاد خودکار رمز عبور های قوی را برای شما فراهم کند و به شما قدرت رمز عبور انتخاب شده را نشان دهد.
- برنامه مدیریت رمز عبور میبایست برای شما گزینه های دیگری برای ذخیره سازی اطلاعات حساس نظیر پاسخ های مربوط به سوالهای امنیت محرمانه و یا کارت های اعتباری را فراهم کند

برنامه مدیریت رمز عبور یک روش عالی برای ذخیره کردن کلید رمزهای عبور و یا اطلاعات حساس شماست. با این وجود، از آنجا که این برنامه ها از اطلاعات مهمی مراقبت میکنند، مطمئن شوید که از رمز عبور اصلی استفاده میکنید که بسیار قوی است بطوریکه برای مجرمان غیر قابل حدس زدن بوده و شما به راحتی آن را به خاطر میسپارید.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل های افزایش آگاهی های امنیتی موسسه SANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاوره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

بهترین برنامه های مدیریت رمز عبور سال 2017: <https://www.pcmag.com/article2/0,2817,2407168,00.asp>

رمز عبارتگونه: <https://securingthehuman.sans.org/ouch/2017#april2017>

احراز هویت دو عاملی: <https://www.securingthehuman.org/ouch/2015#september2015>

ورود خود را قفل کنید: <https://www.lockdownyourlogin.org/>

نکات روز SANS Security: <https://www.sans.org/tip-of-the-day>

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفاً با ouch@securingthehuman.org تماس بگیرید.

هیأت تحریری: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

ترجمه شده توسط: سعید میرجلیلی، مجید هدایتی



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus