بهترین ابزارهای مدیریت گذرواژه‌ها ویژه کامپیوترهای شخصی، دستگاه‌های موبایل و کامپیوترهای مک

با توجه به سیل مداوم مشکلات امنیتی که هر روز و در سطوح بالا زندگی را برای کاربران سخت می‌کند و با توجه به گزارش‌ها و اخباری که پیرامون جاسوسی‌های بزرگ در فضای ابری شاهد آن هستیم، بیش‌تر ما کاربران اینترنت درباره امنیت اطلاعات آنلاین خود نگران و دنبال راه‌کارهای امنیت هستیم. شاید با خود بگویید، من به اینترنت یا خدمات آنلاین نیازی ندارم، پس در امنیت به سر می‌برم. اما آیا از ایمیل استفاده نمی‌کنید؟ آیا خدمات بانک‌داری آنلاین در زندگی شما وارد نشده است؟ آیا در فرم‌های مختلف ثبت نام نکرده‌اید؟ آیا از فضای ذخیره‌سازی ابری (رایگان یا غیررایگان) برای پشتیبان‌گیری از داده‌های خود استفاده نمی‌کنید؟

اگر پاسخ شما تنها به یکی از موارد فوق مثبت باشد، در نتیجه به‌طور ناخواسته موضوع امنیت برای شما حایز اهمیت خواهد بود. اما چه کنیم تا فهرست بلندبالای گذرواژه‌ها را همیشه به خاطر آوریم؟ آیا این امکان وجود دارد فهرستی از گذرواژه‌هایی شبیه به ab3d8fj30fm4expo را بدون آن‌که آن را در مکانی ذخیره کنیم، به خاطر آوریم؟ پاسخ این پرسش در گروه خاصی از برنامه‌ها موسوم به Password Managers نهفته است. در این مقاله، به معرفی برنامه‌های مدیریت گذرواژه قدرتمندی خواهیم پرداخت که زندگی آنلاین را برای شما ساده می‌کند.

از هوشمندانه‌ترین و دقیق‌ترین اما در عین حال ساده‌ترین راهبردهایی که از ما در برابر مشکلات محافظت می‌کنند، به‌کارگیری یک برنامه مدیریت گذرواژه قدرتمند است. یک برنامه مدیریت گذرواژه از شما در برابر حملاتی نظیر Heartbleed یا گروه‌های هکری شبیه یک سپر محافظت به عمل نمی‌آورد، اما یکی از نخستین راه‌کارهای دفاعی است که از هویت شما محافظت می‌کند. یک برنامه مدیریت گذرواژه به شما این توانایی را می‌دهد تا قدرت گذرواژه‌های خود را افزایش دهید و به این ترتیب، از حساب‌های آنلاین شما محافظت و گذرواژه‌ها را به شما یادآوری کند. یک برنامه مدیریت گذرواژه این توانایی را دارد تا به‌طور تصادفی گذرواژه‌های قدرتمند را تولید کند، بدون آن‌که نیازی باشد آن را به خاطر آورید یا رشته تصادفی از کاراکترهای تولید شده را در مکانی یادداشت کنید. این گذرواژه‌های قدرتمند به شما کمک می‌کنند تا در مقابل حملات رایجی که از تکنیک‌هایی همچون لغت‌نامه، جداول مختلف و Brute-force استفاده می‌کنند، سپری دفاعی به وجود آورید. حملاتی که به‌آسانی گذرواژه‌های سنتی را درهم می‌شکنند. بیش‌تر برنامه‌های مدیریت گذرواژه از افزونه‌های ویژه مرورگرها پشتیبانی می‌کنند. این تکنیک به کاربر اجازه می‌دهد تا به‌طور خودکار گذرواژه‌هایی را که برای لاگین شدن به سایت‌ها از آن‌ها استفاده می‌کند، همراه با اطلاعات اعتباری خود ذخیره کند. گزینه‌های دیگری که برای تجمیع این بانک اطلاعاتی از گذرواژه‌ها می‌توانند مورد استفاده قرار گیرند، شامل صفحات گسترده اکسل یا وارد کردن دستی اطلاعات لاگین هستند. علاوه بر این،

مکانیسم افزونه‌ها به گونه‌ای طراحی شده است که فیلدهای مربوط به نام کاربری و گذرواژه‌ها را که در فرم‌های وب قرار دارند، به‌طور خودکار شناسایی کنند. هر چند تعداد زیادی از مرورگرها قابلیت مشابهی را خارج از مجموعه وظایف خود در این زمینه ارائه می‌کنند، اما اکثر قریب به اتفاق برنامه‌های مدیریت گذرواژه مزیت‌های بیش‌تری نسبت به قابلیت‌های از پیش ساخته شده مرورگرها دارند که رمزنگاری، چند پلتفرمی بودن، هم‌سان‌سازی چندپلتفرمی، پشتیبانی از دستگاه‌های همراه و به اشتراک‌گذاری امن اطلاعات اعتباری و پشتیبانی از احراز هویت چند عاملی از ویژگی‌های آن‌ها به شمار می‌رود. در بیش‌تر مواقع، نام کاربری و گذرواژه لازم است از برنامه مدیریت گذرواژه درون فیلدها کپی شود که البته سهولت استفاده از آن‌ها را کاهش می‌دهد، اما در عوض سطح امنیتی را که در ارتباط با موجودیت درخواست‌کننده است، افزایش می‌دهد (به عبارت دیگر، اجازه دسترسی مستقیم فیلدهای درون سایت‌ها را به این اطلاعات حساس نمی‌دهد).

شیوه‌های ذخیره‌سازی گذرواژه‌ها

تعدادی از برنامه‌های مدیریت گذرواژه اقدام به ذخیره‌سازی اطلاعات کاربر به‌صورت محلی می‌کنند، در حالی که شمار دیگری از این برنامه‌ها روی سرویس‌های کلاود برای ذخیره‌سازی و هم‌سان‌سازی تأکید دارند و عده دیگری نیز از هر دو راه‌کار استفاده می‌کنند. گزینه‌هایی همچون KeePass، 1Password و... از ذخیره‌سازی محلی و اما از فرآیند هم‌سان‌سازی با استفاده از دراپ‌باکس پشتیبانی می‌کنند. تصمیم‌گیری درباره این‌که کدام برنامه مدیریت گذرواژه بهترین انتخاب برای شما خواهد بود، به ویژگی‌ها و سهولت استفاده از آن‌ها باز می‌گردد. اگر با ذخیره‌سازی اطلاعات حساس روی سرویس‌های ابری احساس نگرانی می‌کنید، در نتیجه 1Password و SplashID Safe گزینه‌های ایده‌الی برای شما به شمار می‌روند. اگر به سرویس‌های ابرمحور اعتماد دارید و بر این باور هستید که آن‌ها از داده‌های شما به بهترین شکل امنیتی و رمزنگاری قدرتمند محافظت به عمل می‌آورند، در نتیجه LastPass، Dashlane، یا PasswordBox بهترین گزینه برای شما هستند. البته KeePass بهترین گزینه برای ذخیره‌سازی محلی به شمار می‌رود و گزینه‌ای انعطاف‌پذیر است. با ترکیب افزونه‌ها، Keepass تقریباً می‌تواند هر چیزی را که از برنامه مدیریت گذرواژه انتظار دارید، در اختیارتان قرار دهد. اما در زمینه مدیریت گذرواژه در فضای ابری LastPass گزینه مناسبی است. ابتدا آن‌که قیمت آن پایین و از پیاده‌سازی پایداری برخوردار است. دوم آن‌که هر کلاینتی می‌تواند به‌راحتی از LastPass استفاده کند. سوم آن‌که با ثبات و اکثر دیدگاه‌ها درباره آن مثبت است. از جمله دلایلی که بر محبوبیت این برنامه در بین کاربران افزوده است، به قیمت آن باز می‌گردد. کاربران برای استفاده از نسخه حرفه‌ای تنها باید یک دلار در ماه پرداخت کنند. برای آن‌که بتوانید گزینه مناسب خود را انتخاب کنید، باید به طیف گسترده‌تری از گزینه‌ها دسترسی داشته باشید. در این قسمت، به‌طور مختصر و کوتاه به معرفی تعدادی از بهترین برنامه‌هایی می‌پردازیم که در زمینه مدیریت گذرواژه‌ها مورد استفاده قرار می‌گیرند. اما به‌راستی به‌کارگیری یک برنامه مدیریت گذرواژه راه‌کار اشتباهی نخواهد بود؟

1Password

زاییده افکار AglieBits سازنده ابزار محبوب رمزنگاری Knox برای OS X است. بر عکسKnox، 1Password در قالب یک ابزار چند پلتفرمی عمل می‌کند که از سیستم‌عامل‌های مک، ویندوز، آی‌اواس و آندرویید پشتیبانی می‌کند. 1Password شبیه Keepass از یک فایل محلی برای ذخیره‌سازی گذرواژه‌های رمزنگاری شده استفاده می‌کند. AglieBits هیچ سرویس ابری برای هم‌سان‌سازی با دستگاه‌های همراه ارائه نمی‌کند، اما در عوض 1Password از هم‌سان‌سازی گذرواژه‌ها با استفاده از دارپ‌باکس روی همه پلتفرم‌ها و همچنین از آی‌کلاود روی مک و آی‌اواس پشتیبانی می‌کند. 1Password به شما اجازه ساخت و محافظت از گذرواژه‌های چندگانه را می‌دهد. ویژگی به اشتراک‌گذاری ساده و ایمن تعدادی از گذرواژه‌ها با دیگر اعضای خانواده یا همکاران از جمله مزیت‌های آن به شمار می‌رود، به طوری که یک روش ایمن برای به اشتراک‌گذاری لاگین یا هر گونه داده حساس از قبیل شماره کارت‌های اعتباری یا پاسخ‌گویی به پرسش‌های امنیتی مطرح شده در سایت‌ها را با کاربرانی که مجوز دارند، از طریق یک کانال رمزنگاری شده ارائه می‌دهد. ارسال اطلاعات لاگین در قالب یک متن ساده نیز پشتیبانی شده است. اما این اطلاعات فقط روی ترافیک ایمن ایمیل شما ارسال می‌شوند.

[illegible]

نسخه جدید 1Password به تعداد متنوعی از ابزارهای ویژه تجزیه و تحلیل گذرواژه‌ها همراه سرویس‌هایی تجهیز

شده است که به‌منظور شناسایی آسیب‌پذیری‌ها و ایمن‌سازی هویت کاربر مورد استفاده قرار می‌گیرند. هر چند بسیاری از سایت‌ها وصله مربوط به آسیب‌پذیری Heartbleed را مورد استفاده قرار داده‌اند، اما 1Password برای احتیاط بیش‌تر گذرواژه تغییر یافته شما را روی یک سایت با تاریخی مقایسه می‌کند که سایت وصله مربوط را مورد استفاده قرار داده است. اگر گذرواژه شما در این بازه زمانی تغییر نکرده باشد، به شما اعلام می‌کند بهتر است گذرواژه خود را تغییر دهید. یکی از ویژگی‌های جالبی که 1Password ارائه می‌کند، یکسان بودن ویژگی‌های عرضه شده برای کامپیوترهای شخصی و مک است. به دلیل به‌روزرسانی گسترده‌ای که روی نسخه ویندوزی انجام شده است، اکنون هر دو پلتفرم ویژگی‌های یکسانی را عرضه می‌کنند. AglieBits در گذشته وعده داده بود که دو ویژگی به اشتراک‌گذاری امن و هم‌گام‌سازی وای‌فای در نسخه جدید عرضه شود. در حال حاضر، این ویژگی‌ها روی همه پلتفرم‌ها عرضه شده‌اند. به‌طور کلی، 1Password یک مدیر گذرواژه قدرتمند به شمار می‌رود. همچنین، با توجه به ارتباط قدرتمندی که بین AglieBits و جامعه اپلی وجود دارد، این ویژگی به‌درستی در اختیار کاربران مک و آی‌اواس قرار گرفته است.

DashLane

می‌توان آن را خطی بین سرور کلاود و یک برنامه مدیریت گذرواژه محلی دانست که سعی دارد به نگرانی‌های امنیتی پاسخ دهد. می‌توانید بانک اطلاعاتی گذرواژه‌های خود را روی سرور DashLane ذخیره کنید و از مزیت‌های هم‌سان‌سازی روی دستگاه‌های مختلف بهره‌مند شوید یا صندوق گذرواژه خود را به‌طور محلی ذخیره و از هم‌سان‌سازی چشم‌پوشی کنید. این کار به انتخاب شما بستگی دارد. اگر گذرواژه بانک اطلاعاتی خود را در فضای ابری DashLane ذخیره کنید، گذرواژه اصلی همچنان فقط در اختیار شما قرار دارد. به‌جای ذخیره‌سازی یک هش از گذرواژه اصلی روی سرور، Dashlane ادعا می‌کند از گذرواژه شما صرفاً برای رمزنگاری و رمزگشایی داده‌های محلی استفاده می‌کند. به همین دلیل، بانک اطلاعاتی گذرواژه شما به‌صورت فقط خواندنی روی وب خواهد بود و تغییرات تنها می‌توانند روی یک کلاینت اعمال شوند. احراز هویت روی دستگاه‌های ثبت شده با Dashlane در دو مرحله انجام می‌شود؛ ترکیب گذرواژه اصلی که برای دستگاه ثبت شده تولید شده است و ارسال کد ثبتی از طریق ایمیل. کاربران به دو روش رایگان و غیررایگان می‌توانند از DashLane استفاده کنند. در حالت نخست، یک حساب رایگان دسترسی به گذرواژه‌ها را از طریق یک دستگاه واحد که آن را انتخاب می‌کنید، امکان‌پذیر می‌سازد. حالت دوم در ارتباط با حساب‌های حرفه‌ای هستند که باید مبلغ 99/39 دلار را در سال برای آن‌ها پرداخت کنید. این حساب‌ها امکان هم‌سان‌سازی گذرواژه‌ها روی چند دستگاه، انجام فرآیند پشتیبان‌گیری، به اشتراک‌گذاری بیش از پنج عنصر، دسترسی به یک برنامه تحت وب فقط خواندنی و بهره‌مندی از پشتیبانی خدمات مشتری DashLane را ارائه می‌دهند.

DashLane :1 [illegible]

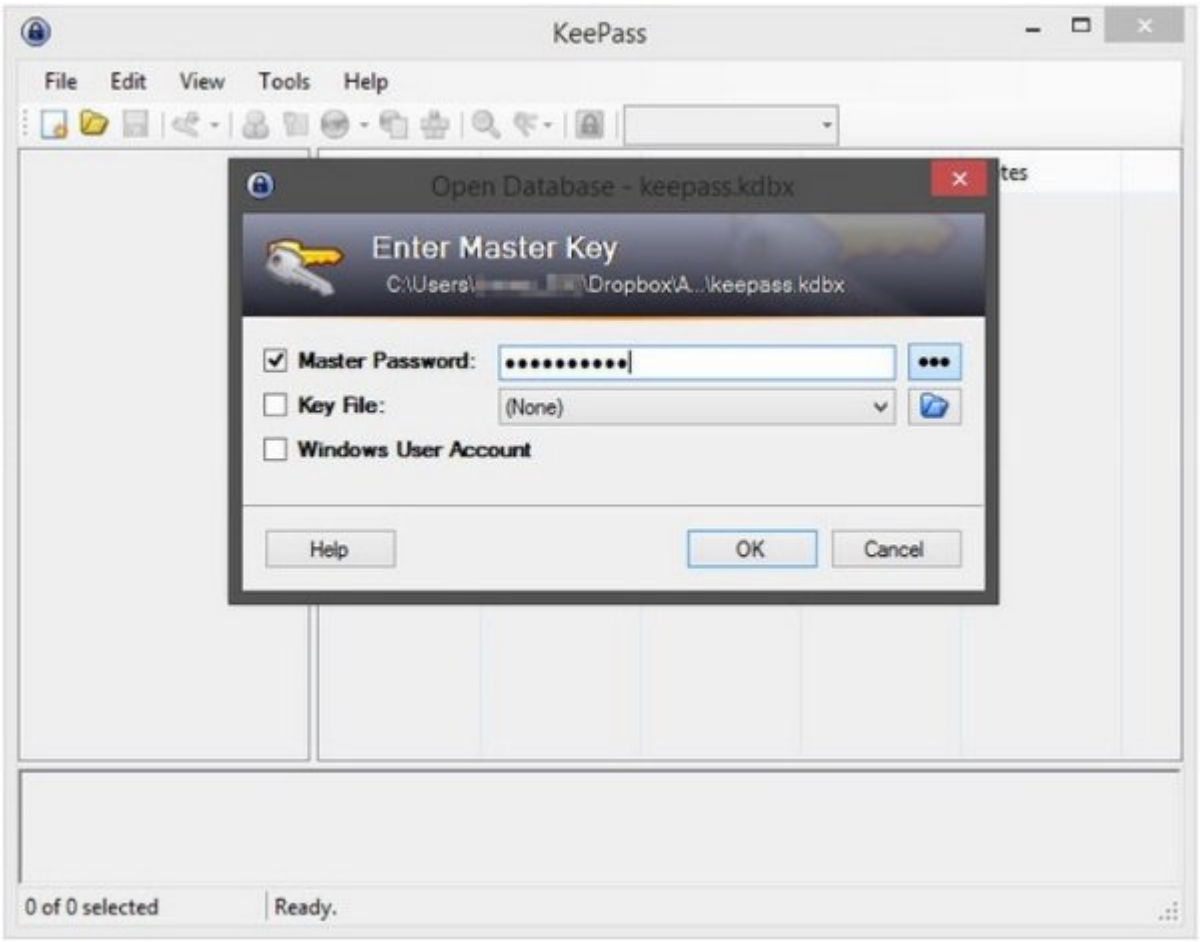
در زمان کار با DashLane حفظ گذرواژه اصلی امری حیاتی محسوب می‌شود. در صورت گم کردن گذرواژه اصلی امکان ریکاوری گذرواژه به هیچ عنوان برای شرکت وجود ندارد. DashLane از احراز هویت دوعاملی استفاده می‌کند. این احراز هویت دوعاملی با استفاده از Google Authenticator پشتیبانی می‌شود. ویژگی‌های گروهی DashLane به شما اجازه به اشتراک‌گذاری ایمن اطلاعات را با دیگر کاربران آن امکان‌پذیر می‌سازد. برای این منظور امکان تنظیم سطح دسترسی مناسب به اطلاعات وجود دارد. امکان محدودسازی عناصری که به اشتراک قرار گرفته یا تغییر سطح دسترسی به اشتراک‌گذاری یک عنصر یا امکان تخصیص مجوز کامل به داده‌ها از جمله ویژگی‌های عرضه شده از سوی Dashlane است. ویژگی دیگری که Dashlane در اختیار کاربر قرار می‌دهد، مشخص کردن مخاطبانی است که در زمان اضطراری به حساب‌های حیاتی یا اطلاعات مهم شما دسترسی داشته باشند. به دلیل این‌که DashLane سعی می‌کند مدل دورگه‌ای را بر پایه سرویس‌های ابرمحور و مدیریت محلی گذرواژه‌ها ارائه کند، در نتیجه ویژگی‌های کاملی را که در ارتباط با سرویس‌های ابری وجود دارند، ارائه نمی‌کند و ممکن است برای کاربرانی که تمایل دارند از حداکثر امکانات ابری بهره‌مند شوند، گزینه مطلوبی به شمار نرود. با این حال، اگر به سایت Dashlane مراجعه و بخش مربوط به توصیف ویژگی‌های امنیتی Dashlane را مشاهده کنید، متوجه خواهید شد این نرم‌افزار از چه تکنیک‌های امنیتی استفاده و چه جزییات مهمی را در آن لحاظ کرده است. از دیگر ویژگی‌های DashLane می‌توان به موارد زیر اشاره کرد:

- پشتیبانی از ویژگی TouchID در آی‌اواس
- رمزنگاری اطلاعات با AES-256
- ساخت و ذخیره کردن گذرواژه‌ها در زمان گشت و گذار در وب از طریق آندرویید.

KeePass

این برنامه یک پروژه منبع باز تحت مجوز GNU GPL است که راه‌حل رایگانی برای مدیریت گذرواژه‌ها در سیستم‌عامل‌های ویندوز، OS X و لینوکس فراهم می‌کند. این نرم‌افزار به‌طور بومی روی ویندوز اجرا می‌شود، اما برای اجرا روی دیگر پلتفرم‌ها به Mono نیاز است. همه مزایای پروژه‌های منبع باز در KeePass قرار دارند که شامل اکوسیستم قدرتمند افزونه‌ها و انتقال روی سیستم‌عامل‌های مختلف است. با توسعه افزونه‌های KeePass توانایی تغییر الگوی رمزنگاری، ورود خودکار از طریق مرورگر، ادغام شدن با صفحه‌کلیدهای لمسی یا حتی ساخت

اسکریپت‌هایی را دارید که روی KeePass اجرا می‌شوند. طراحی KeePass به گونه‌ای است که اقدام به ذخیره کردن یک کپی محلی از صندوق گذرواژه‌ها می‌کند. پشتیبان‌گیری ابری و پشتیبانی از هم‌سان‌سازی روی چند دستگاه از طریق افزونه‌هایی به دست می‌آید که با سرویس‌های ذخیره‌سازی ابری همچون دراپ‌باکس، Google Docs و وان‌درایو کار می‌کنند. از جمله مزیت‌هایی که ذخیره‌سازی محلی KeePass در اختیار کاربران قرار می‌دهد، به اشتراک‌گذاری بانک اطلاعاتی ساخته شده توسط کاربران KeePass یا به اشتراک‌گذاری چند بانک اطلاعاتی توسط یک کاربر و دیگر عناصر است.



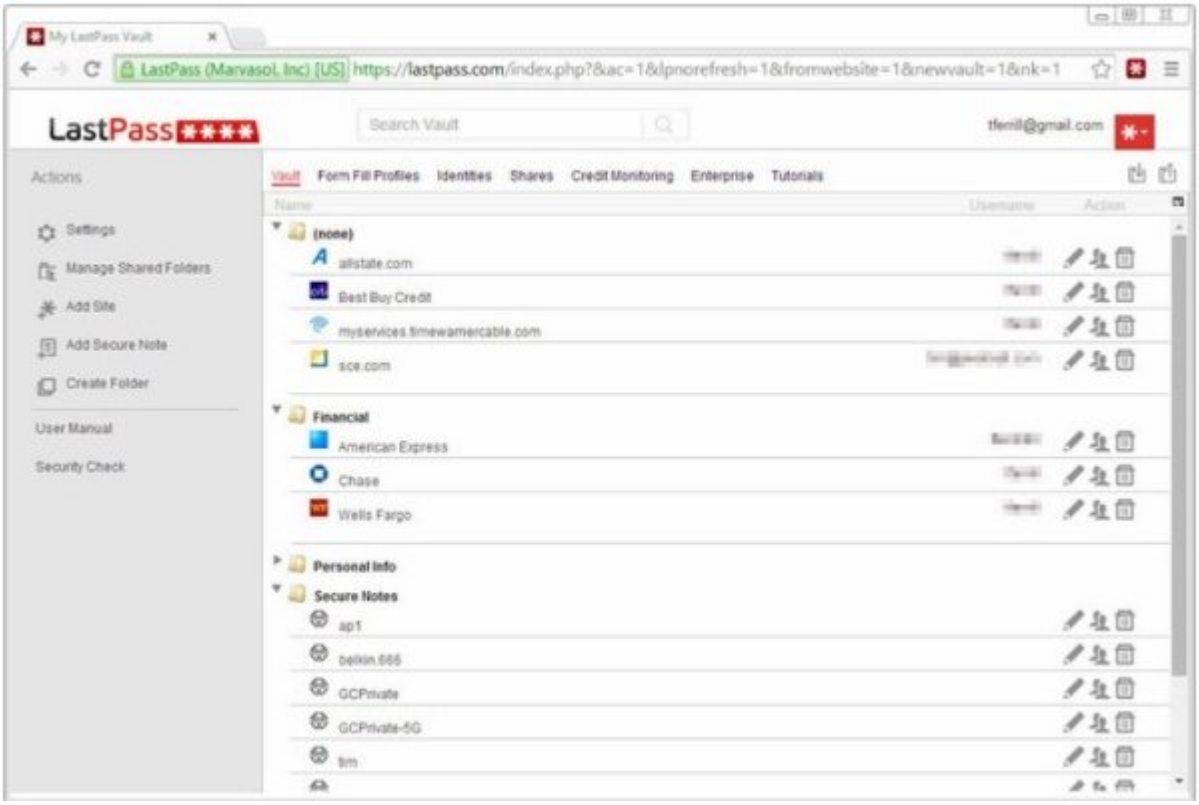
□□□ 2: □□ *KeePass* □□□□□□□□ □□□ □□□□ □□□□□ □□□□□□□□ □□ □□ □□□□□□□□ □□ □□□□□□ □□□□□□□□□ □□□□ □□□□□□ □ □□□□□ □□□□ □□□□□□□ □□□□□□□ □□□□□.

اگر درباره امنیت گذرواژه‌های خود بیش از هم‌سان‌سازی نگران هستید، باید بدانید KeePass به‌طور پیش‌فرض از روش‌های احراز هویت چندگانه استفاده می‌کند. فایل‌های بانک اطلاعاتی KeePass با ترکیب چند عامل قفل می‌شوند. این عوامل عبارتند از یک فایل کلید، گذرواژه و حساب کاربری ویندوزی. فایل کلید روی یک رسانه قابل حمل همچون حافظه فلش ذخیره‌سازی می‌شود. احراز هویت دوعاملی دسترسی ایمن به گذرواژه‌های حساس را امکان‌پذیر می‌سازد. شاید بزرگ‌ترین مشکل KeePass در پیچیدگی آن قرار داشته باشد. به‌کارگیری همه ویژگی‌های پیش‌رفته توسط یک کاربر به تحقیق، تنظیم، تعمیر و نگهداری نیاز دارد. در حالی که KeePass یک راه‌حل عالی برای طرف‌داران منبع باز به شمار می‌رود، انعطاف‌پذیری زیادی دارد و یک نرم‌افزار رایگان است، اما به‌سادگی سرویس‌های ابرمحور نیست.

LastPass

شاید یکی از شناخته شده‌ترین و محبوب‌ترین ابزارهای مدیریت گذرواژه‌ها است. نرم‌افزاری که مجموعه گسترده‌ای از ویژگی‌ها را در اختیار کاربران قرار می‌دهد و از طیف گسترده‌ای از پلتفرم‌های همراه پشتیبانی می‌کند. برعکس KeePass، LastPass یک نرم‌افزار وب‌محور است و از سرویس ابری محلی خود برای ذخیره‌سازی اطلاعات کاربران و هم‌سان‌سازی داده‌ها استفاده می‌کند. LastPass هم به‌صورت رایگان و هم در قالب پرداخت حق اشتراک ماهانه یک دلار قابل استفاده است. کاربران نسخه رایگان به بیش‌تر ویژگی‌های اصلی که از یک سرویس ابرمحور انتظار

می‌رود، دسترسی دارند. ویژگی‌هایی همچون پشتیبانی از افزونه‌ها برای مرورگرهای مختلف، دسترسی از هر مکان و حتی پشتیبانی از احراز هویت چندگانه که با استفاده از Google Authenticator روی آندرویید یا دستگاه آی‌اواس و Microsoft Authenticator روی ویندوزفون قرار دارند، از دیگر قابلیت‌های LastPass هستند.



□□□ *3: LastPass* □□ □□□□□□□□□ □□□□□□□ □□□ □□ □□□□□□□□ □□□□□□□ □□ □□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□ □□□□□□ □□□□□□□.

LastPass یک سری ویژگی‌ها و قابلیت‌های دم دستی در ارتباط با به اشتراک‌گذاری حساب‌ها را با دوستان یا افراد خانواده در اختیار یک کاربر قرار می‌دهد. سرویس رایگان به شما اجازه می‌دهد به‌طور انتخابی اطلاعات لاگین را با دیگر افراد LastPass به اشتراک قرار دهید، به طوری که به آن‌ها اجازه می‌دهد با استفاده از اطلاعات شما به احراز هویت برنامه‌های تحت وب بپردازند بدون آن‌که به گذرواژه شما دسترسی داشته باشند. کاربرانی که حق اشتراک پرداخت می‌کنند، به پوشه Family Folder دسترسی خواهند داشت. این ویژگی امکان تعیین نوع اطلاعاتی را که با دیگر کاربران LastPass به اشتراک گذاشته شود، در اختیار کاربر قرار می‌دهد. پشتیبانی دسکتاپ LastPass کمی گیج‌کننده است. LastPass از شکل‌های مختلفی از احراز هویت دوعاملی همچون Microsoft Authenticator و Google Authenticator پشتیبانی می‌کند. اگر نیازمند یک ابزار مدیریت گذرواژه ساده تحت وب هستید، نسخه رایگان LastPass انتخاب اشتباهی نخواهد بود.

PasswordBox

شباهت‌های زیادی به Dashlane دارد. هرچند PasswordBox از تکنیک‌هایی همچون احراز هویت دوعاملی یا پشتیبانی از احراز هویت اثر انگشت پشتیبانی نمی‌کند، اما شرکت سازنده اعلام کرده است این دو ویژگی به‌زودی به این نرم‌افزار افزوده خواهند شد. همچنین، اقدام به عرضه برنامه‌های جداگانه برای ویندوز و مک نکرده است، اما در عوض افزونه‌هایی را برای مرورگرهای مختلف ارائه کرده است. برنامه‌های همراه آن برای آندرویید و آی‌اواس وجود دارند. PasswordBox هیچ برنامه تحت وبی برای مشاهده یا ویرایش گذرواژه‌ها یا مدیریت حساب کاربری عرضه نکرده است و همه این فرآیندها از طریق برنامه‌های موبایل و افزونه‌های مرورگرها انجام می‌شود. نسخه رایگان این ابزار امکان ذخیره‌سازی 25 گذرواژه را همراه با هم‌سان‌سازی و قابلیت‌های به اشتراک‌گذاری کامل در اختیار کاربران قرار می‌دهد. هزینه نسخه غیررایگان 12 دلار در سال است که امکان ذخیره‌سازی نامحدود را در اختیار کاربران قرار می‌دهد. PasswordBox به کاربران هر دو گروه رایگان و غیررایگان امکان به اشتراک‌گذاری اطلاعات لاگین ذخیره شده را می‌دهد، بدون آن‌که گذرواژه قابل رؤیت باشد. Legacy Locker یکی دیگر از ویژگی‌های PasswordBox است. این ویژگی به کاربر اجازه می‌دهد تا افرادی را به‌عنوان وارث رسمی حساب خود تعیین کند.

در نتیجه اگر کاربری در قید حیات نبود، کنترل و مدیریت حساب او توسط این افراد انجام خواهد شد. البته لازم به توضیح است انتقال حساب با استفاده از Legacy Locker تا زمانی که تاریخ رسمی فوت کاربر اعلام نشده است، وجود ندارد و از آن زمان به بعد این ویژگی معتبر و قانونی می‌شود. در حال حاضر، PasswordBox بخشی از Intel Security Family است.

□□□ *PasswordBox :4* □□□□□□□□□□□□ □□□ □□ □□□ □□□□ □□□ □□□□□ □□□□□□ □□□□□□□□□□ □□□ □□□□□□□ □□□□□□□□□ □□□□ □□□□□□□□□□ □□□□□□□□.
□□□□□□□□□□ □□□ □□ □□□□□□□□ □□ □□□□□□□□□ □□ □□□□□□□ □□□□ □□□□□□□ □□□□□□□ □ □□□□□□□ □□□□□□.

SplashID Safe

SplashID یکی از شناخته شده‌ترین نام‌های تجاری در ارتباط با مدیریت گذرواژه‌ها است. محصول این شرکت، SplashID Safe به‌ویژه در ارتباط با دستگاه‌های همراه کاربرد دارد. به‌تازگی SplashID Safe از برنامه‌های کلاینت و تحت وب در پلتفرم‌های ویندوز، مک، آی‌اواس، آندروید، بلک‌بری 10 و ویندوزفون پشتیبانی می‌کند. در حالی که بیش‌تر برنامه‌های مدیریت گذرواژه بر مبنای تکنیک ابری یا محلی کار می‌کنند، این برنامه از هر دو ویژگی پشتیبانی می‌کند. حساب اصلی SplashID به‌صورت رایگان در دسترس کاربران قرار دارد، اما کاربر را به یک دستگاه محدود می‌کند و امکان به اشتراک‌گذاری یا پشتیبان‌گیری را در اختیار کاربر قرار نمی‌دهد.
یک حساب SplashID Pro امکان هم‌سان‌سازی گذرواژه‌ها را در ازای پرداخت 99/1 دلار در ماه و 99/19 دلار در سال در اختیار کاربران قرار می‌دهد. همچنین، هم‌سان‌سازی روی تعداد نامحدودی از دستگاه را با استفاده از اینترنت و وب، به اشتراک‌گذاری و پشتیبان‌گیری خودکار پشتیبانی می‌کند. امکان دریافت کمک از گروه پشتیبان فنی شرکت نیز وجود دارد. SplashID Safe ویژگی محبوبی را که همه ما از سرویس‌های ابرمحور نیاز داریم، ارائه می‌کند. توانایی پیکربندی یک لاگین تنها به‌صورت محلی این توانایی را در اختیار کاربر قرار می‌دهد که از ذخیره‌سازی داده‌های حساس خود روی اینترنت ممانعت به عمل آورد. این ایده بر این اساس است که اگر شما اطلاعات لاگین مهم یا داده‌های حساسی در اختیار دارید، نباید به اینترنت اعتماد کنید. برای این منظور، می‌توانید مانع از آپلود شدن داده‌هایتان روی سرور SplashID Safe شوید.
SplashID safe از دو روش برای به اشتراک‌گذاری اطلاعات لاگین استفاده می‌کند. در روش نخست، می‌توانید اطلاعات لاگین را با کاربری که از حساب کاربری ابری SplashID استفاده می‌کند، به اشتراک قرار دهید. این اطلاعات به‌طور مستقیم درون حساب کاربری او وارد می‌شود. روش دوم به کاربرانی مربوط است که فاقد حساب

ابری SplashID هستند. این گروه از کاربران ایمیلی دریافت خواهند کرد که یک لینک امن برای دریافت این اطلاعات دارد. لینک‌هایی که این اطلاعات را به اشتراک قرار می‌دهند، با استفاده از یک گذرواژه محافظت می‌شوند. این لینک‌ها تنها 24 ساعت اعتبار دارند و بعد از سپری شدن این مدت اعتبار آن‌ها منقضی می‌شود.
احراز هویت دوعاملی در SplashID فقط از یک لایه اضافی از امنیت در زمانی که یک دستگاه جدید ثبت می‌شود، استفاده می‌کند که نیاز دارد یک کد شش رقمی را که از طریق ایمیل ارسال می‌شود، مورد استفاده قرار دهید. SplashID به‌جای استفاده از یک گذرواژه اصلی از الگوی باز کردن قفل اصلی نیز پشتیبانی می‌کند که البته هنوز جای کار بیش‌تری دارد.

انتخاب‌های دیگر

همیشه عرضه یک محصول امنیتی از سوی نام‌های آشنا خبر خوبی محسوب می‌شود. Norton Identity Safe متعلق به شرکت سیمانتک از این ویژگی بهره‌مند است. Identity Safe گزینه دیگری در زمینه مدیریت گذرواژه‌ها است که به‌طور رایگان در اختیار کاربران قرار دارد. انتخاب‌های رایگان زیادی در ارتباط با نرم‌افزارهای مدیریت گذرواژه‌ها وجود دارد، اما کدام یک از سرویس‌های ابری فعال در این زمینه قابل اعتمادتر از شرکتی هستند که بیش از یک دهه در این زمینه تجربه دارد؟ Norton Identity Safe یکی از ابزارهای قرار گرفته در بسته امنیتی نورتون است. اکنون سرویس مستقل مبتنی بر وب و کلاینت ویژه ویندوز، آی‌اواس و آندرویید را عرضه کرده است.
RoboForm گزینه محبوب دیگری است که در ارتباط با مدیریت گذرواژه و پرکننده فرم‌ها مورد استفاده قرار می‌گیرد. این ابزار هم‌سان‌سازی را روی دستگاه‌های مختلف عرضه می‌کند، اما هیچ برنامه وبی احراز هویت دوعاملی یا قابلیت به اشتراک‌گذاری را عرضه نمی‌کند. KeePass تنها برنامه منبع باز در ارتباط با مدیریت گذرواژه‌ها نیست. Password Safe به‌تازگی هم به‌صورت قابل حمل و هم به‌صورت نصبی برای کاربران ویندوز و نسخه بتای آن برای کاربران لینوکس عرضه شده است. ویژگی‌های آن همانند KeePass نیستند، در نتیجه نمی‌توان آن را به‌عنوان جایگزینی برای KeePass پیشنهاد کرد. اما اگر تصمیم دارید از یک برنامه مدیریت گذرواژه به‌صورت محلی استفاده کنید، گزینه ایده‌آلی به شمار می‌روند.
My1Login هم به‌صورت رایگان و هم غیررایگان در اختیار کاربران قرار دارد. در حالت رایگان، تبلیغات و لینک‌های وابسته به شرکای شرکت سازنده را مشاهده خواهید کرد. در حالت غیررایگان، این لینک‌ها و تبلیغات دیگر وجود نخواهند داشت. My1Login ویژگی‌های نام‌آشنایی همچون به اشتراک‌گذاری و تولید گذرواژه‌های قدرتمندی را که دیگر سازندگان عرضه می‌کنند، در اختیار کاربران قرار می‌دهد. تنها ایرادی که درباره My1Login وجود دارد، به وب‌محور بودن آن باز می‌گردد. به دلیل نبود نسخه کلاینتی My1Login، این ابزار به کم‌ترین تنظیمات نیاز دارد. تجربه نشان داده است این شیوه وب‌محور بودن در درازمدت دردسرهای خاص خود را دارد.
Keeper Backup یک مدیر گذرواژه کامل دیگر است که از پلتفرم‌های مختلفی همچون مک، ویندوز، آی‌اواس، آندرویید و ویندوزفون پشتیبانی می‌کند. ویژگی امنیتی عرضه شده توسط آن شامل احراز هویت دوعاملی و به اشتراک‌گذاری ایمن هستند. نسخه رایگان آن فاقد به اشتراک‌گذاری است و از داده‌های محدودی پشتیبانی می‌کند. نسخه غیررایگان از هم‌سان‌سازی، ذخیره‌سازی نامحدود و به اشتراک‌گذاری پشتیبانی می‌کند.
DirectPass محصول ترند مایکرو گزینه رایگان دیگری است که تنها از پنج گذرواژه و اما نسخه غیررایگان آن از تعداد نامحدودی گذرواژه پشتیبانی می‌کند. این نرم‌افزار از همه پلتفرم‌ها پشتیبانی می‌کند و چیزی کم‌تر از دیگر برنامه‌های مدیریت گذرواژه ندارد.

منبع:
اینفوورلد
تاریخ انتشار:
28 آبان 1394

نشانی منبع: https://www.shabakeh-mag.com/security/2243