اطلاعاتی دست نیافتنی و غیر قابل مشاهده

8 ابزار برتر رمزگذاری اطلاعات

رمزگذاری یکی از بهترین روش‌های محافظت از اطلاعات است. این فناوری به ما اجازه می‌دهد از یک کلید و الگوریتمی پیچیده استفاده کرده و اطلاعات قابل رویت را به یکسری کدهای بدون معنا تبدیل کنیم. کدهایی که برای رمزگشایی و دسترسی دوباره به آن‌ها باید از کلید مخفی و الگوریتمی استفاده کنیم که پیش از آن کدها بر مبنای آن کلید رمزگذاری شده است. رمزگذاری اطلاعات از آن جهت حائز اهمیت است که می‌توانید در یک محیط عمومی همچون شرکت یا اداره داده‌های حساسی را روی سامانه خود داشته باشید که تنها شما کلید دستیابی به فایل‌ها را دارید. رمزگذاری اطلاعات به اندازه‌ای مهم است که برخی از سازمان‌های بزرگ در زمان آرشیو کردن حجم بالایی از داده‌ها، ابتدا آن‌ها را رمزگذاری کرده و سپس بایگانی می‌کنند. به ویژه زمانی‌که قرار باشد این اطلاعات روی بستر اینترنت ذخیره شوند. اما برای رمزگذاری اطلاعات به نرم‌افزارهایی حرفه‌ای و قدرتمند نیاز است که در این مقاله به هشت مورد از این نرم‌افزارها اشاره خواهد شد.

نکاتی مهم در زمینه رمزگذاری اطلاعات

رمزگذاری اطلاعات با نرم‌افزارهای کاربردی کار چندان پیچیده‌ای نیست، اما عدم توجه به برخی اصول مهم باعث می‌شود، این فرآیند سود چندانی برای شما نداشته باشد. زمانی‌که فایل‌های خود را با **ابزارهای رمزنگاری** کدگذاری می‌کنید، این ابزارها از شما گذرواژه‌ای درخواست می‌کنند که نقش یک کلید را بازی می‌کند. هر اندازه گذرواژه‌ای که انتخاب می‌کنید، قدرتمند باشد، به همان نسبت ضریب ایمنی اطلاعات شما افزایش پیدا می‌کند. گذرواژه‌ای که انتخاب می‌کنید باید منحصر به فرد بوده و ترکیبی از حروف بزرگ و کوچک، همراه با اعداد باشد. بهتر است اندازه گذرواژه انتخابی از 15 کاراکتر بیشتر باشد. از ابزارهای قدرتمندی برای ارزیابی خوب یا بد بودن گذرواژه خود استفاده کنید. البته برخی از **نرم‌افزارهای رمزگذار** و ابزارهای مدیریت گذرواژه می‌توانند گذرواژه‌های قدرتمندی برای شما ایجاد کنند. گذرواژه‌ای که انتخاب می‌کنید نباید یک کلمه یا عبارت ساده‌ای باشد که به راحتی بتوانید آن‌را به یاد آورید. ساده بودن یک گذرواژه باعث می‌شود تا هکرها بتوانند از طریق تکنیک‌هایی همچون لغت‌نامه‌ها به سرعت گذرواژه انتخابی شما را کشف کنند. تا حد امکان از گذرواژه‌ای که برای حساب‌های کاربری خود استفاده کرده‌اید، در فرآیند **رمزگذاری** اطلاعات استفاده نکنید. در صورت امکان گذرواژه‌ها را در فایل‌های متنی یا مرورگرها ذخیره‌سازی نکنید. هر گذرواژه‌ای باید تنها به یک حساب کاربری یا فایل‌های **رمزگذاری** شده تعلق داشته باشد. زمانی‌که اسناد را رمزگذاری کرده و برای شخص دیگری ارسال می‌کنید تا جایی که امکان دارد از ایمیل یا برنامه‌های پیام‌رسان برای ارسال گذرواژه استفاده نکنید.

1. LastPass

یک نرم‌افزار مدیریت گذرواژه است که گذرواژه‌های قدرتمندی را تولید می‌کند. LastPass از آن جهت در ابتدای این فهرست قرار گرفته که شما برای ذخیره‌سازی گذرواژه‌های متعلق به فایل‌های مختلفی که کدگذاری کرده‌اید، به مکانی برای ذخیره‌سازی گذرواژه‌ها نیاز دارید. LastPass به سادگی قابل استفاده بوده و انعطاف‌پذیری بالایی دارد. از افزونه‌های ارائه شده برای این برنامه مدیریت گذرواژه در مرورگرهای فایرفاکس یا کروم استفاده کنید. البته

نسخه همراه این برنامه برای اندروید و iOS ارائه شده است. زمانی‌که این ابزار را روی سیستم خود نصب می‌کنید، هر بار که قصد ایجاد یک حساب کاربری آنلاین دارید، LastPass گزینه‌ای برای ذخیره‌سازی اطلاعات پیشنهاد می‌کند. این برنامه عملکردی نسبتا هوشمند دارد. اگر گذرواژه‌های یکسانی را برای حساب‌های کاربری مختلف استفاده کرده باشید، این برنامه با نمایش پیغام هشداری این مسئله را گوشزد می‌کند. RoboForm و sticky Password ابزارهای جایگزین دیگری هستند که عملکردی همچون LastPass دارند.

2. BitLocker

ابزارهای رمزنگار متنوع و قدرتمندی در اختیار کاربران قرار دارند که هر یک قابلیت‌های منحصر به فردی را ارائه می‌کنند، BitLocker یکی از مولفه‌های داخلی ویندوز است و روی هر سیستم‌عامل ویندوزی قرار دارد. بیت‌لاکر در گروه ابزارهای رمزگذار با توانایی بالا قرار می‌گیرد، زیرا برای رمزگذاری کل دیسک استفاده می‌شود. ابزار فوق از الگوریتم رمزگذاری AES برای کدگذاری فایل‌هایی که روی درایوها قرار دارند. استفاده می‌کند. الگوریتم AES به این دلیل از سوی **ابزارهای رمزگذار** استفاده می‌شود که بالاترین سطح از ایمنی را ارائه کرده و به دقت ارزیابی شده است. اما چرا باید از بیت‌لاکر استفاده کنیم؟ در پاسخ به این پرسش دلایل زیر را می‌توان ارائه کرد:

• به‌کارگیری بیت‌لاکر ساده بوده و روی سیستم‌عامل‌های مختلف مایکروسافت قرار دارد. در نتیجه نیازی ندارید تا ابزاری را روی سامانه‌ای نصب کرده و از آن استفاده کنید.

• ابزار فوق رایگان بوده و در نتیجه برای **رمزگذاری** اسناد مهمی که روی هارددیسک ذخیره کرده‌اید، ایده‌آل است.

• بیت‌لاکر یک درایو را به‌طور کامل **رمزگذاری** کرده و در نتیجه اگر لپ‌تاپ‌تان مفقود یا گم شود دیگر از بابت افشای اطلاعات خود نگران نخواهید بود.

• زمانی که بیت‌لاکر را روی سامانه خود فعال می‌کنید، هر زمان فایل جدیدی به درایو خود اضافه کنید، بیت‌لاکر به شکل خودکار آن‌را **رمزگذاری** می‌کند.

مطلب پیشنهادی

آخر هفته با شبکه: نگاهی به فیلم بازی تقلید در باره کار و زندگی آلن تورینگ
بازی تقلید: زندگی ناتمام نابغه‌ای که بازی را تمام کرد

3. VeraCrypt

نرم‌افزار رمزگذاری که رایگان در اختیار کاربران قرار می‌گیرد چندسکویی است و روی سیستم عامل‌های ویندوز، لینوکس و مک قابل استفاده است. عملکرد این نرم‌افزار شباهت زیادی به ابزار TrueCrypt دارد که عرضه نسخه‌های جدیدتر آن از سال 2014 میلادی متوقف شد. این نرم‌افزار همانند بیت‌لاکر از استاندارد AES برای **رمزگذاری** اطلاعات استفاده می‌کند و بخش‌های **رمزگذاری** شده را به شکلی قدرتمند در میان سایر بخش‌ها پنهان می‌کند تا هکرها به راحتی موفق نشوند از طریق نرم‌افزارهای کدشکن اطلاعات را دومرتبه به وضعیت اولیه خود باز گردانند. مهم‌ترین مزیت این نرم‌افزار در به‌روزرسانی‌های مستمر آن است.

4. FileVault

این ابزار رایگان برای کاربرانی است که از سیستم‌عامل مک استفاده می‌کنند و قصد **رمزگذاری** داده‌های خود را دارند. ابزار FileVault از استاندارد **رمزگذاری** XTS-AES-128 با کلید 256 بیتی برای رمزگذاری اطلاعات دیسک استفاده می‌کند. این ابزار قدرتمند 8 سال پیش و همراه با سیستم‌عامل X Lion برای بهبود امنیت کاربران مک عرضه شد.

5. DiskCryptor

یکی دیگر از ابزارهای رمزگذاری رایگانی که برای ویندوز ارائه شده DiskCryptor است. شما می‌توانید از این ابزار برای رمزگذاری درایوهای داخلی، خارجی و حتی ایمیج‌های ایزو ایجاد شده از سیستم‌عامل استفاده کنید. ابزار فوق برای بهبود ضریب ایمنی رمزگذاری از چند الگوریتم قدرتمند همچون AES، Twofish و Serpent استفاده می‌کند. تنها کاری که برای رمزگذاری یک داریو باید انجام دهید، انتخاب درایو موردنظر و انتخاب گزینه رمزگذاری است. با کلیک روی این گزینه فرآیند رمزگذاری آغاز می‌شود.

6. Zip-7

ابزار قدرتمند دیگری که بسیاری از کاربران برای آرشیو کردن و از آرشیو خارج کردن فایل‌ها از آن استفاده می‌کنند. ابزار Zip-7 برای کاربرانی ایده‌آل است که به دنبال **رمزگذاری** فایل‌ها و اسناد خاصی هستند و نیازی ندارند کل یک درایو را رمزگذاری کنند. این ابزار رایگان به شکل متن‌باز عرضه شده و از **الگوریتم رمزگذاری** AES-256 با الگوی 256 بیتی برای کدگذاری آرشیوهای ساخته شده استفاده می‌کند. از ویژگی‌های شاخص این نرم‌افزار می‌توان به رابط کاربری ساده و ارائه بهترین فرمت برای فشرده‌سازی فایل‌ها اشاره کرد. Zip-7 چند سکویی بوده و روی ویندوز و لینوکس قابل استفاده است.

7. AxCrypt

این ابزار همچون ابزار Zip 7 یک ابزار **رمزگذاری** رایگان و متن‌باز است که برای ویندوز ارائه شده است و حجمی در حدود 1 مگابایت دارد و برای **رمزگذاری** گروهی از فایل‌ها یا پوشه‌ها یا **رمزگذاری** تک فایلی استفاده می‌شود. ابزار Axcrypt فایل‌ها را برای مدت زمان مشخصی رمزگذاری کرده و پس از آن‌که فایل‌ها به مقصد می‌رسد به شکل خودکار رمزگشایی می‌شوند. البته طرف مقابل نیز باید این ابزار را روی سامانه خود نصب کرده باشد.

8. پروتکل انتقال ابر متن ایمن (HTTPS)

رمزگذاری فایل‌ها تنها بخشی از فرآیند محافظت از اطلاعات شخصی است. در زمان اتصال به اینترنت و به ویژه زمانی‌که با سایت‌ها به تعامل می‌پردازید، این احتمال وجود دارد که ترافیک مبادله شده در میانه راه شنود شده و اطلاعات شما دچار نشتی شوند. برای آن‌که اطمینان حاصل کنید، داده‌های شما در زمان انتقال روی بستر اینترنت به شکل مطمئنی انتقال پیدا می‌کنند باید از راهکارهایی که برای این منظور ارائه شده است، استفاده کنید. در ادامه با سه مورد از این راهکارها آشنا خواهید شد.

امروزه به‌کارگیری پروتکل انتقال ابرمتن ایمن(HTTPS) به یک اجبار تبدیل شده است، با این حال برخی از سایت‌ها هنوز هم تمایلی ندارند از پروتکل فوق استفاده کنند. برای آن‌که مطمئن شوید ارتباط شما همواره ایمن خواهد بود، پیشنهاد می‌کنیم از افزونه‌هایی شبیه
HTTPS in Anywhere که برای کروم، فایرفاکس و اپرا عرضه شده، استفاده کنید. زمانی‌که از افزونه HTTPS in Anywhere استفاده می‌کنید، مرورگری که از آن استفاده می‌کنید یک ارتباط ایمن برقرار کرده و زمانی‌که اطلاعات حساسی همچون گذرواژه‌ها و نام کاربری را در فیلدهای متنی یک سایت وارد می‌کنید، از تکنیک‌های **رمزگذاری** برای ارسال اطلاعات استفاده می‌کند.

مطلب پیشنهادی

الگوریتم‌ها، بنیاد دانش کامپیوتر

سخن پایانی

راهکارها و ابزارهایی که به آن‌ها اشاره شد، به تنهایی نمی‌توانند از حریم خصوصی شما محافظت کنند. برای به حداقل رساندن تهدیدات امنیتی پیشنهاد می‌کنیم جدیدترین وصله‌های امنیتی ارائه شده برای مرورگرها و سیستم‌عامل‌ها را نصب کرده و مطمئن شوید که جدیدترین نسخه از نرم‌افزارهای کاربردی را دریافت کرده‌اید. هکرها می‌دانند که بیشتر کاربران تمایلی به نصب وصله‌ها ندارند، در نتیجه شانس خود را امتحان می‌کنند و بر مبنای آسیب‌پذیری‌های شناسایی اکسپولیت‌هایی را با هدف آسیب رساندن به سامانه‌های کاربران ایجاد می‌کنند، با این توصیف نصب وصله‌ها را حتما جدی بگیرید. در زمان اتصال به شبکه‌های بی‌سیم عمومی هیچ‌گاه اطلاعات حساس را انتقال ندهید. با توجه به این‌که در یک شبکه بی‌سیم عمومی هر کاربری قادر به اتصال به شبکه است، احتمال آن‌که اطلاعات حساس شما از سوی هکری شنود شود زیاد است.

برای آن‌که از گزند هکرها دور باشید باید حلقه‌ای چند لایه از مکانیسم‌های امنیتی همچون ضدویروس‌ها، ضدبدافزارها و **رمزگذاری** اطلاعات را پیرامون سامانه‌های خود بکشید تا خطر نفوذ را به حداقل برسانید.

تاریخ انتشار:

25 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15296/8-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%D8%A8%D8%B1%D8%AA%D8%B1-%D8%B1%D9%85%D8%B2%DA%AF%D8%B0%D8%A7%D8%B1%DB%8C-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA