نسخه پشتیبان دارید؟

مقدمه

اگر به صورت طولانی مدت از یک کامپیوتر یا دستگاه موبایل استفاده میکنید، دیر یا زود مشکلی رخ خواهد داد. ممکن است به صورت تصادفی فایلهای اشتباهی را پاک کرده،مشکل سخت افزاری پیدا کرده و یا دستگاهی را گم کنید. شاید حتی بدتر از آن، ممکن است بدافزار فایلها را آلوده کرده و آنها را پاک و یا رمزگذاری کنند. در چنین زمانهایی، اکثرا نسخه های پشتیبان (Backup) تنها راهی است که میتوانید زندگی دیجیتال خود را بازسازی کنید.

نسخه های پشتیبان کپی هایی از اطلاعات شما هستند که در جایی جدا از روی کامپیوترتان یا دستگاههای موبایل شما ذخیره میشوند. زمانیکه شما اطلاعات با ارزش خود را روی آن دستگاهها از دست داده و یا دسترسی به آنها ندارید، میتوانید با استفاده از نسخه های پشتیبان اطلاعات خود را بازیابی نمائید. بسیاری از فایلهایی که ما امروزه ایجاد میکنیم به صورت خودکار در فضای ابری ذخیره و پشتیبان گیری میشوند،مانند مدارک Microsoft Word که در Dropbox، Microsoft OneDrive، یا Google Drive ذخیره شده اند، یا عکسهای شخصی که در Apple iCloud ذخیره شده اند. اما ممکن است فایلهایی دیگری که ساخته اید نیز وجود داشته باشند که به صورت خودکار در فضای ابری ذخیره نشده اند، یا شاید شما بخواهید نسخه های پشتیبان اضافی برای استفاده شخصی خود داشته باشید.

چه چیز، چه زمان، و چگونه

قدم اول این است که تصمیم بگیرید چه چیزی را میخواهید پشتیبان گیری کنید: (1) اطلاعات خاصی که برای شما مهم هستند، یا (2) همه چیز، شاید با احتساب کل سیستم عامل تان. بسیاری از راهکارهای پشتیبان گیری به صورت پیش فرض برای رویکرد اولیه تنظیم شده اند وفقط پرکاربردترین پوشه ها را پشتیبان گیری میکنند. اگر مطمئن نیستید که میخواهید از چه چیزی پشتیبان تهیه کنید یا میخواهید بیشتر مراقب باشید، پشتیبان گیری از همه چیز را در نظر بگیرید.

دوم، تصمیم بگیرید که میخواهید چند مرتبه از اطلاعات پشتیبان بگیرید. برنامه های پشتیبان گیری خود سیستم عامل، مانند Time Machine اپل یا برنامه Backup and Restore ویندوز به شما اجازه میدهند که نسخه پشتیبان خودکار "تنظیمش کن و فراموشش کن" زمانبندی شده بسازید. گزینه های زمان بندی مرسوم شامل موارد ساعتی، روزانه و هفتگی میباشند. راهکارهای دیگر میتوانند "حفاظت مداوم"پیشنهاد دهند که در آن فایلها به محض تغییر یا ذخیره شدن پشتیبان گیری شوند. در حداقل حالت، پیشنهاد ما پشتیبان گیری روزانه خودکار از فایلهای حساس است .
در انتها، تصمیم بگیرید که چگونه میخواهید پشتیبان گیری نمائید. دو راه موجود است: پشتیبان گیری های محلی یا ابری. پشتیبان گیری های محلی به تجهیزاتی که شما از لحاظ فیزیکی میتوانید کنترل میکنید وابسته است، مانند درایوهای خارجی(USB) یا دستگاههایی که از طریق شبکه قابل دسترسی هستند. مزیتی که پشتیبان گیریهای محلی دارند این است که به شما این امکان را میدهند که داده هایی با حجم بالا را به سرعت پشتیبان گیری و بازیابی کنید. عیب آن این است که در صورتی که به بدافزار آلوده شوید، ممکن است که آلودگی به نسخه های پشتیبان شما نیز گسترش یافته و آنها را آلوده نماید. همچنین، اگر یک فاجعه داشته باشید، مانند آتش سوزی یا دزدی، ممکن است نسخه های پشتیبان خود را مانند رایانه خود از دست بدهید.
اگر شما از تجهیزات بیرونی برای پشتیبان گیری استفاده میکنید، یک نسخه کپی خارج از محل در یک مکان امن ذخیره نموده و مطمئن شوید که نسخه های پشتیبان شما به درستی برچسب گذاری شده اند .برای امنیت مضاعف، رمزگذاری برای پشتیبان گیریهای خود در نظر بگیرید.

راهکارهای ذخیره ابری، خدمات آنلاینی هستند که فایلهای شما را در شبکه اینترنت پشتیبان گیری و ذخیره میکنند. معمولا، شما یک نرم افزار روی رایانه خود نصب میکنید. سپس نرم افزار به صورت خودکار فایلهای شما را در بازه زمانی مشخص شده توسط شما یا در زمان تغییر و یا ذخیره آنها پشتیبان گیری میکند. برخی از مزیتهای راهکارهای ابری کاربری ساده آنها، تنظیم خودکار پشتیبان گیری ها و دسترسی به فایلهای شما تقریبا از هر مکانی میباشد. همچنین، از آنجایی که داده‌های شما در فضای ابری قرار میگیرد، سوانح خانگی مانند آتش‌سوزی یا سرقت تأثیری بر پشتیبان‌گیری شما نخواهد داشت. عیب اصلی آن پهنای باند مصرفی آن است. توانایی شما برای تهیه نسخه پشتیبان و بازیابی آن به میزان اطلاعاتی که پشتیبان گیری می کنید و سرعت شبکه شما بستگی دارد. مطمئن نیستید که می خواهید از پشتیبان گیری محلی یا ابری استفاده کنید؟ ایمنی بیشتری در نظر گرفته و از هر دو استفاده کنید.

با دستگاه‌های تلفن همراه، بیشتر اطلاعات شما مانند ایمیل‌ها، پیام‌های متنی یا عکس‌هایی که می‌گیرید به طور خودکار در فضای ابری ذخیره می‌شوند. اگرچه، تنظیمات برنامه تلفن همراه، تنظیمات اصلی سیستم و سایر فایل‌ها ممکن است در فضای ابری ذخیره نشوند. با پشتیبان‌گیری خودکار از دستگاه تلفن همراه تان ، نه تنها این اطلاعات را حفظ می‌کنید، بلکه هنگام ارتقا به یک دستگاه جدید، انتقال اطلاعاتتان ساده تر خواهد شد.

نکات کلیدی دیگر

- با بازیابی و باز کردن یک فایل، به طور مرتب آزمایش کنید که نسخه های پشتیبان شما درست کار می کنند.
- اگر سیستمی را از پشتیبان گیری از جمله سیستم عامل بازسازی می کنید، مطمئن شوید که آخرین وصله های امنیتی و به روز رسانی ها را قبل از استفاده دوباره مجدداً اعمال کرده اید.
- اگر از یک راه کار ابری استفاده می کنید، راه حلی را انتخاب کنید که استفاده از آن برای شما آسان بوده و در مورد گزینه های امنیتی آن تحقیق کنید. به عنوان مثال، آیا شرکت فروشنده پشتیبانگیری ابری شما از احراز هویت دو مرحله ای برای ایمن سازی حساب آنلاین شما پشتیبانی می کند؟

پشتیبان گیری ها یک راه ساده و کم هزینه برای محافظت از زندگی دیجیتال شما است.

سردبیر مهمان

گرگ شیدل، مدیر ارشد امنیت سایبری در Iron Vine Security است که بیش از 30 سال تجربه در زمینه فناوری اطلاعات و امنیت فناوری اطلاعات دارد. او همچنین یک مربی SANS است که معماری امنیتی، مهندسی و اعتماد صفر را در SEC530 تدریس می کند. میتوانید در توئیتر با او در ارتباط باشید @greg_scheidel

منابع

احراز هویت چند مرحله ای: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts
استفاده ایمن از فضای ابری: https://www.sans.org/newsletters/ouch/securely-using-the-cloud
برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers
وراثت دیجیتالی: https://www.sans.org/newsletters/ouch/digital-inheritance

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو

OUCH! توسط SANS Security Awareness منتشر شده است و تحت مجوز Creative Commons BY-NC-ND 4.0 میباشد. شما آزاد هستید که این ماهنامه را برای بقیه اشتراک گذاشته یا آن را توزیع نمائید به شرطی که آن را به فروش نرسانده یا تغییری در آن ایجاد نکنید. هیئت تحریریه: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.