

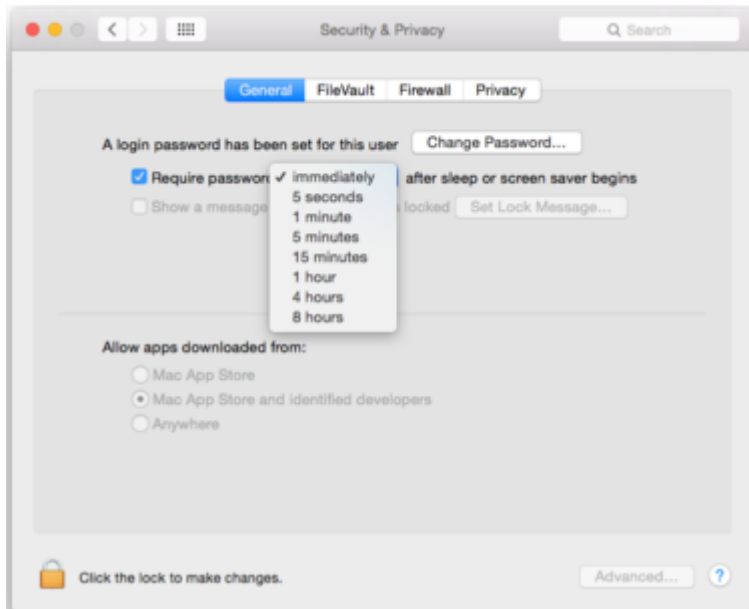


کامپیوتر به شما امکان می‌دهد که بدون توجه به مکان جغرافیایی بتوانید با همه در ارتباط باشید ولی اگر دقت کافی نداشته باشید همین کامپیوتر می‌تواند مایه دردسر و سقوط شما شود. فرقی نمی‌کند که در خانه باشید یا محل کار، در مدرسه باشید یا کافی‌شاپ و رستوران، لپ‌تاپها همه جا حاضراند. کامپیوتر قابل حمل به شما امکان می‌دهد که در هر جایی که باشید بتوانید به کارهایتان پردازید، به خصوص اگر که باتری لپ‌تاپ مدت زمان زیادی شارژ نگه می‌دارد و هم این‌که از سرویس‌ها و اپلیکیشن‌های مبتنی بر رایانش ابری استفاده کنید.

از سویی دیگر این امکان هم هست که لپ‌تاپ سرقت شود، گم شود یا مورد دسترسی غیرمجاز قرار گیرد. طبق آماري که موسسه گارتنر ارائه کرده هر 53 ثانیه یک لپ‌تاپ گم می‌شود. مطمئناً کسی دوست ندارد که لپ‌تاپش گم شود یا دزدیده شود، ولی اگر هم پیش بیاید می‌توان از قبل کارهایی انجام داد که درگیری‌های قانونی و مسائلی از این دست که زمان پیگیری اموال گم شده و سرقت شده پیش می‌آید را کاهش دهد. در ارزیابی‌های امنیتی گفته می‌شود که بهترین دفاع، تهاجم است. در اینجا 10 روش را به شما پیشنهاد می‌کنیم که می‌توانید برای جلوگیری از این مسئله انجام دهید.

### 1 - تنظیم رمز عبور و قفل شدن خودکار

اولین قدم برای محافظت از لپ‌تاپ این است که برای دستگاه خود رمز عبور تنظیم کنید. هر چند که هکرها در این زمینه مشکلی ندارند و می‌توانند از طریق جدا کردن هارد دیسک از لپ‌تاپ دسترسی مستقیم به آن داشته باشند ولی به هر حال می‌تواند به عنوان عاملی بازدارنده در برابر سارقان معمولی یا سودجویانی باشد که دنبال فرصت چند دقیقه‌ای می‌گردند تا به اطلاعات شما دسترسی پیدا کنند یا بتوانند بدافزار روی سیستم نصب کنند. فراموش نکنید که رمز عبور را هم برای بیدار شدن سیستم از حالت sleep و هم برای Screen Saver تنظیم کنید.



## 2 - هارد دیسک را رمزگذاری کنید

ساده‌ترین راه برای اطمینان از اطلاعات روی هارد دیسک این است که با استفاده از نرم‌افزارهایی نظیر FileVault (برای سیستم‌عامل مک) و BitLocker (برای ویندوز) آن را رمزگذاری کنید. نرم‌افزار BitLocker روی نسخه‌های Enterprise و Ultimate و ویندوز 7، نسخه‌های Pro و Enterprise و ویندوز 8 و ویندوز 10 کار می‌کند. به خاطر داشته باشید که حتماً کلید بازیابی اطلاعات رمزگذاری شده را در جایی مطمئن قرار دهید، زیرا شاید روزی احتیاج داشته باشید که اطلاعات را بازیابی کنید یا ممکن است مادربرد لپ‌تاپ به هر دلیلی خراب شود.

## 3 - فایل‌های مهم خود را در سرویس‌های ابری ذخیره کنید

از دست دادن لپ‌تاپ همیشه امری غیرقابل انتظار است و بدترین حالت زمانی رخ می‌دهد که فایل‌های خود را فقط روی لپ‌تاپ ذخیره کرده باشید و همچنان برخی از آنها نیاز به کار داشته باشند، فایل‌هایی که جای دیگری ذخیره نشده‌اند (مثلاً به حجم عظیم عکس‌های‌تان فکر کنید که جای دیگری هم از آنها کپی ندارید). گاهی اوقات درد از دست دادن چنین اطلاعاتی از خود لپ‌تاپ بیشتر است، پس عقلانی به نظر می‌رسد که آنها را در جای دیگری هم نگه داشت. سرویس‌های مبتنی بر رایانش ابری زیادی در حلال حاضر وجود دارند مانند دراپ‌باکس، باکس و وان درایو. همچنین می‌توانید با استفاده از ابرهای عمومی و خصوصی پشتیبان بسیار خوبی از اطلاعات خود درست کنید.

## 4 - از لپ‌تاپ پشتیبان بگیرید

حتی در صورت استفاده از سرویس‌های پشتیبان‌گیری مبتنی بر رایانش ابری، باز هم لازم است که به طور مداوم از اطلاعات خود نسخه پشتیبان بگیرید. چنین کاری باعث آرامش خاطر بیشتر شما شده و خیالتان را راحت می‌کند؛ خصوصاً اگر که برنامه‌های جدید نصب کرده باشید یا فایل‌هایی داشته باشید که خارج از پوشه‌های سینک شده قرار داشته باشد. فایده دیگری که این مدل پشتیبان گرفتن دارد آن است که تمام تنظیمات و پیکربندی‌های شما در سیستم‌عامل و نرم‌افزارهای نصب شده ذخیره خواهد شد؛ در نتیجه زمانی که بازیابی می‌کنید خیلی سریع‌تر می‌توانید به جریان کار برگردید.

کاربران مک برای این کار برنامه‌ای به نام سرویس Time Machine اپل را در اختیار دارند که در سیستم‌عامل وجود دارد. کاربران ویندوز می‌توانند از Acronis True Image استفاده کنند که برنامه‌ای شناخته شده و کاملاً کاربردی برای این منظور است. یکی از مهم‌ترین ویژگی‌های Acronis آن است که می‌توانید تمام اطلاعات را روی یک لپ‌تاپ جدید حتی با مارکی دیگر و مدلی متفاوت بازیابی کنید.

## 5 - به پلتفرم ایمیل مبتنی بر ابر یا سرور سوئیچ کنید

برغم وجود پلتفرم‌های ایمیلی مبتنی بر ابر و سرور مانند Outlook، Gmail و Exchange کاربران خیلی کمی هستند که ایمیل‌های داندلود شده را در سرویس‌های دیگر ذخیره کنند، همین امر باعث می‌شود زمانی که بر حسب اتفاق لپ‌تاپ گم شود یا دزدیده شود و اطلاعات از بین برود راهی برای بازیابی آن‌ها وجود نداشته باشد. در نهایت باید گفت که پلتفرم‌های ایمیلی مبتنی بر ابر و سرور بیشتر قابل اطمینان هستند و سینک کردن تمام ایمیل‌ها بین چند

دستگاه مختلف غیرضروری به نظر می‌رسد.

## 6 - کد رجیستر کردن نرم‌افزارهایی که به سختی پیدا می‌شوند را در جایی نگه دارید

به جرأت می‌توان گفت احتمال پیدا نکردن کد رجیستر برای نرم‌افزارهایی که به صورت آنلاین وجود ندارند بسیار کم شده است ولی به هر حال ممکن است که اتفاق بیفتد. برای همین لازم است که به تناوب از کد رجیستر نرم‌افزارهایی که نصب کرده‌اید با برنامه‌هایی نظیر Evernote نسخه پشتیبان تهیه و در جایی ذخیره کنید.

## 7 - هارددیسک‌های قابل حمل و فلش دیسک‌ها را هم کدگذاری کنید

اگر عادت دارید اطلاعات را روی هارددیسک‌های قابل حمل یا فلش دیسک ذخیره کنید؛ حتما باید اطلاعات را کدگذاری کنید. چرا که احتمال گم شدن یا دزدیده شدن آن‌ها به اندازه لپ‌تاپ است. برای جلوگیری از این مسئله دو راه وجود دارد: استفاده از نرم‌افزار BitLocker To Go که به صورت نرم‌افزاری کدگذاری می‌کند یا استفاده از دیسک‌های سخت اکسترنال که به صورت سخت‌افزاری کدگذاری می‌کنند.

## 8 - روش‌های امنیتی اضافه

برای محافظت از لپ‌تاپ می‌توان از روش‌های سخت‌افزاری دیگری استفاده کرد مثل قفل کنزینگتون که می‌تواند دستگاه شما را در اتاق هتل یا سایر مکان‌های نیمه عمومی محافظت کند. با این‌که هر قفلی می‌تواند شکسته شود ولی وجود یک قفل فیزیکی خیلی ساده هم کمک می‌کند تا خطر از شما دور شده و احتمالا سارقین را به دنبال هدف دیگری بفرستد. استفاده از سیستم اعلان خطر مانند Proximo هم می‌تواند در صورتی که دستگاه شما از محدوده خاصی خارج شود به شما در پیدا کردن آن کمک کند.



## 9 - از نوشته‌ای برای بازگرداندن لپ‌تاپ استفاده کنید

در کنار تمام تلاش‌های نرم‌افزاری و سخت‌افزاری که برای محافظت از لپ‌تاپ و خصوصا اطلاعات انجام می‌دهید؛ بهتر است که نوشته‌ای هم برای نحوه بازگرداندن لپ‌تاپ در کنار آنها قرار دهید، مثلا آدرس شرکت، تلفن تماس یا آدرس ایمیل را روی Screen Saver قرار دهید یا روی کاغذ بنویسید و زیر دستگاه خود بچسبانید. مطمئنا اگر دزدیده شده باشد این روش کمکی به شما نمی‌کند ولی اگر آن را گم کرده باشید، می‌توانید خوشبین باشید که شاید انسان نیکوکاری آن را پیدا کند و بخواهد آن را به شما بازگرداند.

## 10 - لپ‌تاپ را برای ردیابی از راه دور یا حتی پاک کردن اطلاعات تنظیم کنید

و سرانجام آخرین راهی که برای بازیابی اطلاعات به شما پیشنهاد می‌کنیم، نصب نرم‌افزارهایی مانند Prey یا LoJack است. با توجه به طرح و برنامه‌ای که شما دارید و نوع تنظیم، قادر خواهید بود که دستگاه دزدیده شده خود را ردیابی کنید یا حتی از راه دور آن را پاک کنید. ولی بهتر است در چنین مواقعی حتی اگر می‌دانید که لپ‌تاپ در نزدیکی شما است به تنهایی اقدام به بازیابی نکنید و حتما از پلیس کمک بگیرید. اگر که امکان بازیابی لپ‌تاپ وجود

ندارد می‌توانید از راه دور اقدام به پاک کردن اطلاعات کنید تا حداقل فکرتان راحت باشد که کسی به اطلاعات شما دسترسی پیدا نکرده است.

**منبع:**

[آی‌تی‌ورلد](#)

**تاریخ انتشار:**

27 شهریور 1394

---

**نشانی منبع:** <https://www.shabakeh-mag.com/information-feature/1563>