

امنیت نوت‌بوک



هومن سیاری
Sayyari@ComputerNews.ir

نوت‌بوک‌ها برای این ساخته شده‌اند که افراد آنها را با خود به این سو و آن سو ببرند. اما اگر نوت‌بوک شما گم شد یا به سرقت رفت چه اتفاقی می‌افتد؟ چه کار باید کرد تا در این حالت از امنیت اطلاعات نوت‌بوک‌تان مطمئن شوید؟ در این مقاله راهکارهایی برای این مشکل ارائه خواهیم کرد.

که رمزنگاری کل دیسک را انجام می‌دهند نیاز به یک یا دو روش مجوز ورود به سیستم عامل دارند (نام کاربری و رمز عبور و یا اثر انگشت) تا بتوانند براساس اطلاعات مذکور رمزنگاری نمایند. اگر رمز عبور یا اثر انگشت صحیح وارد نشود، اطلاعات روی هارددیسک به صورت رمز شده و غیرقابل خواندن باقی می‌ماند.

اغلب نرم‌افزارهای رمزنگاری کل دیسک از نسخه ۱۲۸ یا ۲۵۶ بیتی استاندارد رمزنگاری پیشرفته و یا AES استفاده می‌کنند که اولین بار توسط دولت آمریکا مورد استفاده قرار گرفت و هنوز هم استفاده می‌شود. رمزنگاری کل دیسک هم به صورت دستگاه سخت‌افزاری و هم به صورت برنامه نرم‌افزاری وجود دارد. علاوه بر برنامه‌های تجاری مختلف، خود مایکروسافت هم در نسخه‌های حرفه‌ای ویندوزهای ویستا و ۷ برنامه‌ای به نام BitLocker قرار داده که کار رمزنگاری کل دیسک را انجام می‌دهد (برای اطلاع بیشتر به مقاله "با BitLocker" در شماره ۶۴ مراجعه کنید). برخی از این برنامه‌ها از جمله BitLocker امکان رمزنگاری هارددیسک اکسترنال و فلش مموری را نیز دارند.

را به رمز در آورده و کاربر فقط کافیست یک مجوز امنیتی مثل نام کاربری و رمز عبور و یا اثر انگشت خود را وارد کند. روش رمزنگاری کل دیسک از روش رمزنگاری فایل که امکان محافظت از فایل‌ها و فولدرهای دلخواه را فراهم می‌کند، امن‌تر است چرا که روش رمزنگاری کل دیسک از دسترسی غیرمجاز به سیستم عامل، فایل‌های موقتی و فایل‌های حذف شده هم جلوگیری می‌کند.



«رمزنگاری کل دیسک» همه اطلاعات روی هارددیسک را به رمز درآورده و هنگامی که داده‌ای بخواهد روی دیسک نوشته شود، ابتدا به رمز درآورده می‌شود و سپس نوشته می‌شود و برای خواندن ابتدا باید از حالت رمز خارج شده و سپس مورد استفاده قرار گیرد. نرم‌افزارهایی

در هیاهوی سفرهای تجاری حتی محتاط‌ترین افراد هم می‌توانند نوت‌بوک خود را گم کنند. از طرف دیگر زمانی که فکر می‌کنید نوت‌بوک در کنترل کامل شماست، هک‌های حرفه‌ای می‌توانند از طریق شبکه‌های عمومی مثل اینترنت به اطلاعات شما دسترسی داشته باشند! این موضوع به خصوص برای شرکت‌های تجاری به یک معضل تبدیل شده است. بنابراین اغلب شرکت‌های بزرگ اقدام به پیاده‌سازی راهکارهایی برای افزایش امنیت نوت‌بوک‌های کارمندان خود کرده‌اند تا از افشای اسرار و اطلاعات حساس آنها جلوگیری شود چرا که ممکن است به ورشکستگی و یا ضررهای هنگفت منجر شود.

در این مقاله به بررسی بعضی از این راهکارها می‌پردازیم، هر چند ممکن است تعدادی از آنها نیز مناسب کاربران خانگی هم باشد.

رمزنگاری کل دیسک (Full Disk Encryption) یکی از مهم‌ترین ملاحظات امنیتی، میزان سهولت استفاده از روش‌های آن برای کاربران است. طبیعی است که اگر به کارگیری یک روش امنیتی قوی، برای کاربران مشکل باشد از آن روش استفاده نخواهند کرد. «رمزنگاری کل دیسک» روشی ایده‌آل محسوب می‌شود چرا که این روش کل اطلاعات روی دیسک

نوت‌بوک‌هایی هستند که از طریق سیم‌کارتی که در آنها قرار داده می‌شود، از راه دور کنترل می‌شوند و به محض سرقت نوت‌بوک، با ارسال یک پیام کوتاه برای آن سیم‌کارت، کارهای متفاوتی می‌توان انجام داد، از قفل کردن نوت‌بوک گرفته تا حذف کلیه اطلاعات هارددیسک و حتی ارسال مختصات جغرافیایی در صورت مجهز بودن نوت‌بوک به GPS.

مشخصات خود را روی نوت‌بوک بچسبانید

اگر بدبینانه به موضوع نگاه نکنیم، این احتمال هم وجود دارد که همیشه نوت‌بوک به سرقت نرود، بلکه توسط خود شما در مکانی جا گذاشته شود و یک فرد خوب آن را پیدا کند! (تعجب کردید؟! برای این مواقع لازم است قبلاً یک لیبل با آدرس و شماره تماس‌تان را زیر نوت‌بوک بچسبانید تا آن فرد خوب را خیلی گیج نکنید و اجازه‌ی خطرات را به ذهنش ندهید!



قفل مخصوص

وقتی از نوت‌بوک‌تان استفاده نمی‌کنید، بهترین راه این است که آن را در مکانی امن مثل یک کیف قفل‌دار نگه دارید. اگر از نوت‌بوک معمولاً در مکان‌های عمومی مثل کافی‌شاپ یا لابی هتل استفاده می‌کنید، بهتر است از قفل‌های مخصوص نوت‌بوک استفاده کنید. این قفل‌ها از یک قفل کوچک و رمزدار و یک کابل بسیار محکم ساخته شده‌اند که یک طرف کابل به نوت‌بوک متصل شده و سر دیگر را به جای ثابتی مثل پایه میز محکم می‌کنند. در این صورت می‌توانید چند دقیقه‌ای از نوت‌بوکتان دور شوید! ■



و در نتیجه از ارسال اطلاعات کاربران برای هکرها جلوگیری می‌کند.



برای مثال اگر یک بدافزار برنامه‌ای keylogger (برنامه‌ای که دکمه‌های فشرد شده روی کیبورد را ثبت می‌کند و از طریق اینترنت ارسال می‌کند) را نصب کرده باشد، فایروال دوطرفه از ارسال آنچه که شما تایپ کرده‌اید (مثل رمز عبور و شماره حساب بانکی) توسط برنامه فوق جلوگیری می‌کند.

بازیابی یا پاک‌سازی

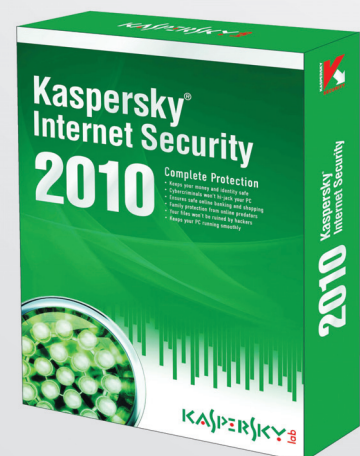
اگر برای شما مهم است که اطلاعات روی نوت‌بوک به دست دیگران نیفتد، باید به دنبال سرویسی باشید که امکان یافتن محل نوت‌بوک از راه دور را به شما داده و همچنین امکان حذف کلیه اطلاعات هارددیسک را از راه دور فراهم سازد. این قابلیت به دو صورت نرم‌افزاری و سخت‌افزاری انجام می‌شود. مثلاً نرم‌افزار LoJack به محض اینکه نوت‌بوک گمشده شما به اینترنت وصل شود، موقعیت آن را تشخیص داده و امکان حذف فایل‌های دلخواه شما را فراهم می‌کند. اما قابلیت سخت‌افزاری چیز دیگری است.



بعضی از نوت‌بوک‌ها دارای قابلیتی به نام Opal هستند که در واقع به معنای داشتن سخت‌افزاری برای رمزنگاری و از رمز خارج کردن اطلاعات هارددیسک است. در این صورت برای انجام عملیات فوق‌نیازی به استفاده از پردازنده نیست. این قابلیت سخت‌افزاری را در بعضی از مدل‌های حرفه‌ای نوت‌بوک‌های HP، Toshiba و Lenovo می‌توان دید.

Internet Security Suite

برای محافظت در مقابل ویروس‌ها، جاسوس‌افزارها و هکرها نیاز به استفاده از نرم‌افزاری جامع که شامل ضدویروس، ضدجاسوس‌افزار و فایروال باشد، دارید. از طرفی یک مزیت بزرگ Internet Security Suite این است که کاربران امکان مدیریت همه ابزارهای امنیتی را از یک رابط واحد خواهند داشت و مجبور نیستند برای هر تنظیمی به قسمت‌های متفاوت رفته و نرم‌افزارهای مختلف را باز کنند. یکی از پیشرفته‌ترین قابلیت‌های آن، اسکن فایل‌ها با الگوهای ویروس‌ها و جاسوس‌افزارهای شناخته شده است تا در صورتی که ویروس و یا جاسوس‌افزار جدیدی که الگوی مشابهی دارد و هنوز توسط سازندگان ضدویروس‌ها شناخته نشده است را تشخیص داده، از فعالیت آن جلوگیری کند. ISSها امکان محافظت کامپیوتر در مقابل بدافزارهای منتقل شده توسط نرم‌افزارهای چت، Keyloggerها، تبلیغ‌های pop-up و روت‌کیت‌ها را هم دارند. برای این منظور ISS با مرورگر وب شما ترکیب شده و به صورت همزمان شما را از خطرات ناشی از ورود به سایت‌های مشکوک مطلع می‌کند.



البته در هر حال بعضی از بدافزارها به هر حال راهی برای گذر از سیستم امنیتی شما پیدا خواهند کرد. به همین دلیل لازم است ISS از یک فایروال دوطرفه پشتیبانی کند. فایروال سنتی ترافیک وب ورودی به کامپیوتر را مانیتور می‌کند، اما فایروال دوطرفه اطلاعات خارج شده از کامپیوتر را هم بررسی می‌کند