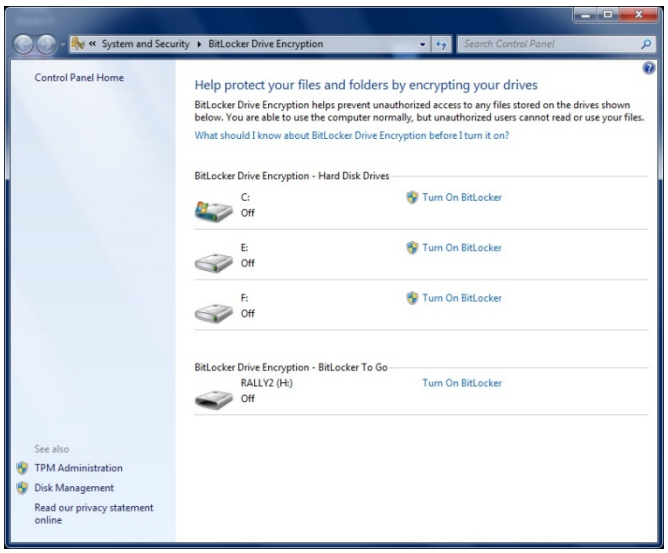
حفاظت از دیسک‌ها با استفاده از رمزنگاری BitLocker Drive Encryption

از برنامهٔ رمزنگاری دیسک BitLocker Drive Encryption برای کمک به حفاظت از فایل‌های ذخیره‌شده در دیسکی که ویندوز بر روی آن نصب شده است (دیسک سیستم‌عامل)، و بر روی دیسک‌های داده‌ای (مانند دیسک‌های سخت اینترنال) می‌توانید بهره بگیرید. از برنامهٔ BitLocker To Go برای حفاظت از داده‌های وسایل ذخیره‌گر جابه‌جاپذیر (مانند دیسک‌های سخت اکسترنال یا حافظه‌های فلش USB) می‌توانید استفاده کنید.

BitLocker برخلاف EFS[1]، که به شما امکان می‌دهد فایل‌ها را به طور تک‌به‌تک رمزنگاری کنید کل یک وسیله یا بخش ذخیره‌گر را رمزنگاری می‌کند. عملیات ورود به حساب (logon) و کار با فایل‌های‌تان را به طور عادی می‌توانید انجام دهید، اما BitLocker به شما کمک می‌کند که جلوی دسترسی هکرها به ***فایل‌های سیستمی*** را بگیرید. هکرها برای کشف گذرواژه‌ها به این نوع فایل‌ها اتکا دارند. از سوی دیگر، BitLocker جلوی دستیابی کسانی را که وسیلهٔ ذخیره‌گر شما را از کامپیوترتان جدا می‌کنند و به کامپیوتری دیگر وصل می‌کنند می‌گیرد.

هرگاه فایل‌های جدیدی را در یک وسیله یا بخش ذخیره‌گر رمزنگاری‌شده با BitLocker اضافه کنید، BitLocker آنها را به طور خودکار رمزنگاری می‌کند. فایل‌ها تا زمانی رمزنگاری می‌مانند که در بخش یا وسیلهٔ ذخیره‌گر رمزنگاری‌شده ذخیره شده باشند. اگر این فایل‌ها برای یک بخش یا وسیلهٔ ذخیره‌گر یا کامپیوتر دیگر کپی شود، رمزبرداری می‌شوند. اگر از فایل‌های‌تان به طور مشترک با کاربران دیگر بهره می‌گیرید، مثلاً از طریق یک شبکه، اگر این فایل‌ها بر روی بخش یا وسیلهٔ ذخیره‌گر رمزنگاری‌شده ذخیره شوند رمزنگاری می‌شوند، اما آنها را فقط کاربران مجاز به طور معمول می‌توانند دستیابی کنند.

اگر دیسک سیستم‌عامل را رمزنگاری کنید، BitLocker کامپیوتر را در زمان راه‌اندازی (استارت‌آپ) از لحاظ شرایطی بررسی می‌کند که ممکن است یک خطر امنیتی وجود داشته باشد (مثلاً، یک تغییر در **بایوس**[2] یا تغییرات در فایل‌های استارت‌آپ[3]). اگر BitLocker یک ریسک امنیتی را تشخیص بدهد، دیسک سیستم‌عامل را قفل خواهد کرد و یک **کلید بازسازی** BitLocker ویژه برای قفل‌برداری درخواست خواهد کرد. اطمینان یابید که هنگامی که اولین بار BitLocker را فعال می‌کنید این کلید بازسازی را بسازید؛ در غیر این صورت، ممکن است دستیابی فایل‌های‌تان را کاملاً از دست بدهید. اگر کامپیوترتان تراشهٔ TPM[4] را داشته باشد، BitLocker از آن برای تصدیق‌کردن کلیدهای مورد نیاز برای قفل‌برداری از دیسک سیستم‌عامل رمزنگاری‌شده بهره می‌گیرد. هنگامی که کامپیوترتان را راه‌اندازی می‌کنید، BitLocker کلیدهای دیسک سیستم‌عامل را از TPM می‌خواهد و از این دیسک قفل‌برداری می‌کند.



اگر دیسک‌های داده‌ای (ثابت یا جابه‌جاپذیر) را رمزنگاری کنید، با یک گذرواژه یا یک کارت هوشمند می‌توانید آنها را قفل‌برداری کنید. دیسک داده‌ای را طوری می‌توانید میزان کنید که هنگامی که وارد حساب کاربری خود می‌شوید به طور خودکار از دیسک قفل‌برداری کند.

BitLocker را در هر زمانی می‌توانید غیرفعال و خاموش کنید، چه با متوقف‌ساختن موقتی آن، چه با رمزبرداری دائمی از دیسک.

> **یادآوری:** *امکان رمزنگاری دیسک‌ها با استفاده از BitLocker Drive Encryption در همهٔ نگارش‌های ویندوز مهیا نشده است.*

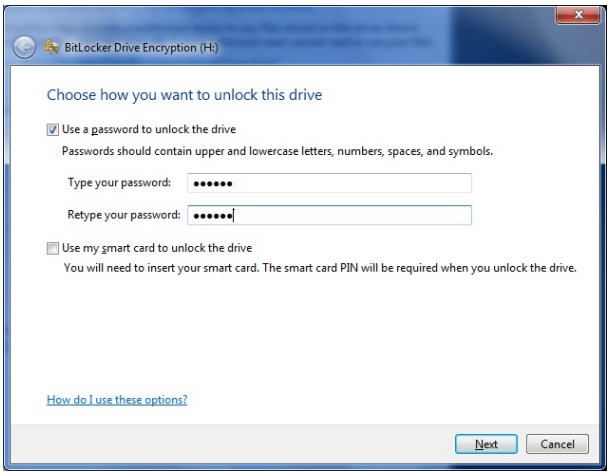
[1] Encrypting File System
[2] BIOS
[3] startup
[4] Trusted Platform Module

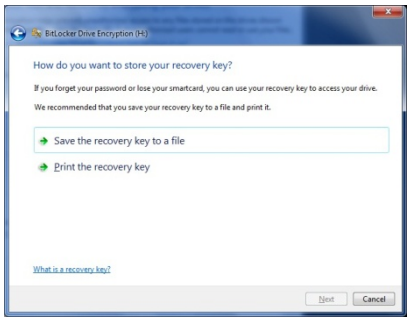
فعال‌کردن BitLocker

۱. برای اجرای برنامهٔ BitLocker Drive Encryption، روی دکمهٔ Start کلیک کنید، در کادر Search، واژه **bitlocker** را تایپ کنید، و سپس روی BitLocker کلیک کنید.

۲. روی Turn On BitLocker کلیک کنید. برنامهٔ هدایت‌کنندهٔ برپایی BitLocker به اجرا در می‌آید. اگر از شما یک گذرواژهٔ administrator یا تأییدیه درخواست شد، گذرواژه یا تأییدیه را فراهم کنید.

۳. دستورالعمل‌های برنامهٔ هدایت‌کننده را دنبال کنید.





غیرفعال‌کردن BitLocker

۱. برای اجرای برنامهٔ BitLocker Drive Encryption، روی دکمهٔ Start کلیک کنید، در کادر Search، واژه **bitlocker** را تایپ کنید، و سپس روی BitLocker کلیک کنید.

۲. یکی از دو کار زیر را انجام دهید:

- برای متوقف‌کردن موقتی BitLocker، روی Suspend Protection کلیک کنید، و سپس روی Yes کلیک کنید.
- برای غیرفعال‌کردن BitLocker و رمزبرداری از دیسک، روی Turn Off BitLocker کلیک کنید، و سپس روی Decrypt Drive کلیک کنید.

پیش‌نیازهای سخت‌افزاری

برای استفاده از BitLocker Drive Encryption، برای دیسکی که ویندوز بر روی آن نصب شده است کامپیوترتان باید پیش‌نیازهای زیر را برآورده کند:

- یک کامپیوتر مجهز به تراشهٔ TPM، که در بسیاری از کامپیوترها برای پشتیبانی از امکانات ایمن‌سازی پیشرفته تعبیه می‌شود. اگر کامپیوترتان مجهز به TPM version 1.2 یا مابعد آن باشد کلید خود را در این تراشه ذخیره خواهد کرد.
- یک ذخیره‌گر جابه‌جاپذیر USB مانند یک حافظهٔ فلش USB. اگر کامپیوترتان TPM version 1.2 یا مابعد آن را نداشته باشد کلید خود را در حافظهٔ فلش ذخیره خواهد کرد. این گزینه فقط هنگامی قابل دستیابی است که مدیر سیستم شما شبکهٔ شما را طوری برپا کرده باشد که استفاده از یک کلید راه‌انداز به جای TPM مجاز باشد.

برپایی دیسک‌سخت برای BitLocker Drive Encryption

برای رمزنگاری دیسکی که ویندوز بر روی آن نصب شده است، کامپیوترتان باید دو پارتیشن داشته باشد: یک **پارتیشن سیستمی** (که حاوی فایل‌های مورد نیاز برای راه‌اندازی کامپیوتر است)، و یک **پارتیشن سیستم‌عامل** (که حاوی ویندوز است). **پارتیشن سیستم‌عامل** رمزنگاری خواهد شد و **پارتیشن سیستمی** رمزنگاری‌نشده باقی خواهد ماند تا کامپیوترتان بتواند راه‌اندازی بشود.

در نگارش‌های پیشین ویندوز، مجبور بودید که به طور دستی این پارتیشن‌ها را بسازید. در **ویندوز۷**، این پارتیشن‌ها به طور خودکار ساخته می‌شوند. اگر کامپیوترتان یک **پارتیشن سیستمی** نداشته باشد، برنامهٔ هدایت‌کنندهٔ BitLocker با استفاده از ۲۰۰مگابایت از فضای دیسک موجود یک **پارتیشن سیستمی** برای شما خواهد ساخت. برای **پارتیشن سیستمی** هیچ حرف نمایندهٔ دیسکی نسبت داده نخواهد شد و در پوشهٔ Computer به نمایش در نخواهد آمد.

پیش‌نیازها برای ذخیره‌گرهای داده‌ای

برای رمزنگاری دیسک‌های داده‌ای ثابت مانند دیسک‌های سخت اینترنال از برنامهٔ BitLocker و برای رمزنگاری ذخیره‌گرهای جابه‌جاپذیر، مانند یک حافظهٔ فلش USB، از برنامهٔ BitLocker To Go می‌توانید بهره بگیرید.