Làm thế nào để kích hoạt Full-Disk Encryption trên Windows 10?

Trên hệ điều hành Windows 10, một số thì sử dụng mã hóa theo mặc định, nhưng một số thì không. Trong bài viết dưới đây Quản trị mạng sẽ hướng dẫn bạn cách kiểm tra xem bộ nhớ trên máy tính Windows 10 đã được mã hóa hay chưa.

Đôi khi việc mã hóa đóng một vai trò khá quan trọng, giúp bạn có thể bảo vệ các dữ liệu "nhạy cảm" của mình không bị người dùng khác sử dụng và truy cập trái phép.

Không giống như các hệ điều hành hiện đại khác - macOS, Chrome OS, iOS và Android, trên Windows 10 Microsoft vẫn chưa tích hợp công cụ mã hóa cho người dùng. Nếu muốn sử dụng bạn sẽ phải trả một khoản phí kha khá để mua phiên bản Windows 10 Pro hoặc sử dụng các công cụ mã hóa của bên thứ 3.

1. Nếu máy tính của bạn hỗ trợ: Windows Device Encryption

Trên nhiều dòng máy tính Windows 10 mới được tự động kích hoạt tính năng có tên gọi Device Encryption. Tính năng này được giới thiệu và tích hợp đầu tiên trên Windows 8.1, và có một số yêu cầu cụ thể về phần cứng. Không phải tất cả máy tính sẽ được tích hợp tính năng này, nhưng một số thì sẽ có.

Ngoài ra còn một số giới hạn khác bạn cần lưu ý: tính năng này chỉ thực sự mã hóa ổ của bạn khi bạn đăng nhập Windows bằng tài khoản Microsoft. Sau đó Recovery Key (mã khôi phục) của bạn sẽ được tải lên server (máy chủ) của Microsoft.

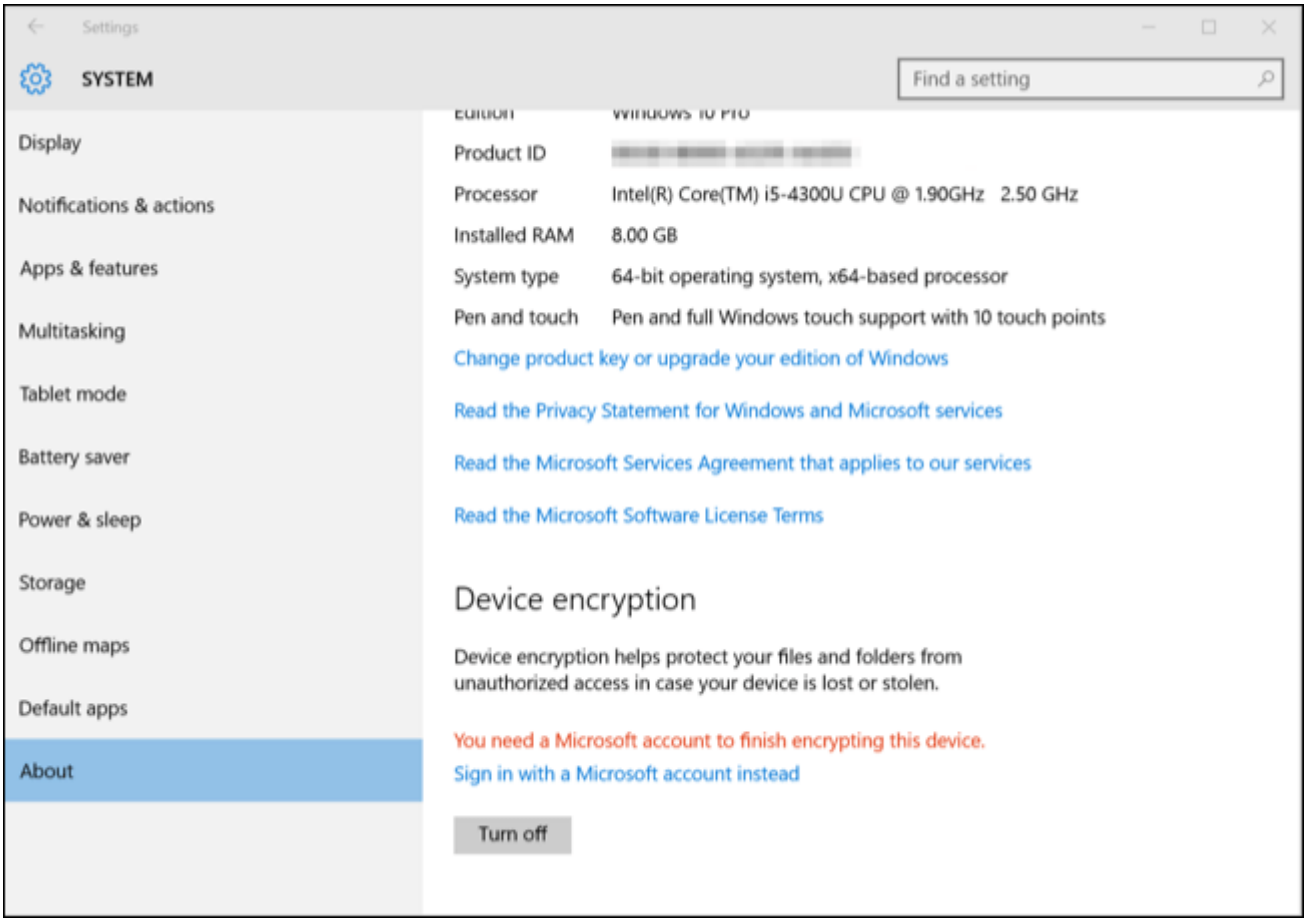
Điều này giúp bạn có thể khôi phục các tập tin của mình ngay cả khi bạn không đăng nhập máy tính. Đây là lí do tại sao FBI không quá lo lắng về tính năng này. Nhưng tuy nhiên tính năng này được khuyến cáo để mã hóa các dữ liệu trên máy tính, laptop để bảo vệ các dữ liệu của bạn khỏi các "tên trộm" mà thôi.

Nếu đang lo lắng về NSA, bạn có thể sử dụng các giải pháp mã hóa khác.

Device Encryption cũng được kích hoạt nếu bạn đăng nhập vào miền (domain) của tổ chức (.org hay organization). Cho ví dụ, bạn có thể đăng nhập vào một miền (domain) của doanh nghiệp, trường học. Recovery Key (mã khôi phục) của bạn sẽ được tải lên server (máy chủ) của miền tổ chức (organization domain).

Tuy nhiên cách này không áp dụng cho máy tính "trung gian" mà chỉ có máy tính gia nhập miền (domain) mà thôi.

Để kiểm tra xem Device Encryption được kích hoạt hay chưa, bạn mở ứng dụng **Settings**, sau đó điều hướng đến **System** => **About**, và tìm thiết lập có tên **Device Encryption** ở góc dưới cùng cửa sổ About. Nếu không nhìn thấy bất kỳ thông tin gì về Device Encryption tại đây đồng nghĩa với việc máy tính của bạn không hỗ trợ Device Encryption và tính năng không được kích hoạt.



Nếu Device Encryption được kích hoạt hoặc nếu bạn kích hoạt bằng tài khoản Microsoft của mình, bạn sẽ nhìn thấy một thông báo tại đó.

2. Với người dùng Windows Pro: BitLocker

Nếu Device Encryption không được kích hoạt hoặc nếu muốn sử dụng giải pháp mã hóa "mạnh" hơn để có thể mã hóa các ổ cứng di động USB, bạn có thể sử dụng BitLocker.

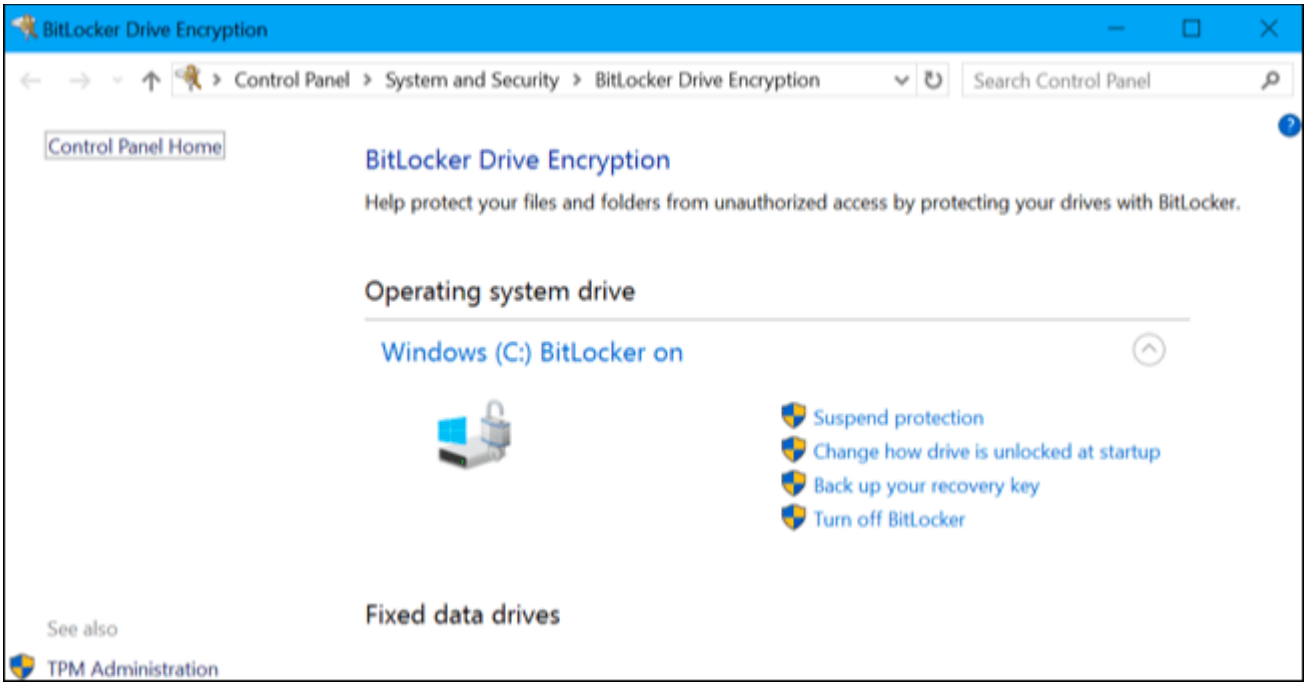
Công cụ mã hóa BitLocker của Microsoft là một phần của Windows và được tích hợp trên nhiều phiên bản hiện nay. Tuy nhiên, Microsoft vẫn hạn chế BitLocker trên các phiên bản Professional, Enterprise, và Education của Windows 10.

BitLocker là giải pháp an toàn nhất cho máy tính của bạn, công cụ có chứa Trusted Platform Module (TPM) - được tích hợp trên các máy tính hiện đại. Bạn có thể nhanh chóng kiểm tra máy tính của mình có Trusted Platform Module (TPM) hay

không ngay trên Windows, hoặc có thể kiểm tra nhà sản xuất máy tính của bạn nếu không chắc chắn.

Windows thường nói rằng BitLocker yêu cầu phải có TPM, nhưng tuy nhiên bạn có thể kích hoạt BitLocker mà không cần TMP bằng cách sử dụng tùy chọn ẩn. Để làm được điều này bạn sẽ phải sử dụng một ổ USB Flash làm "Startup Key" để khởi động mỗi khi bạn kích hoạt tùy chọn này.

Nếu đang sử dụng phiên bản Windows 10 Pro, BitLocker được tích hợp sẵn trên hệ thống, bạn có thể tìm kiếm BitLocker bằng cách nhập từ khóa **BitLocker** vào khung **Search** trên Start Menu rồi nhấn **Enter** và sử dụng BitLocker Control Panel để kích hoạt công cụ.



Nếu không sử dụng phiên bản Windows 10 Pro, bạn sẽ phải trả một khoản phí, rơi vào khoảng 99$ để nâng cấp phiên bản Windows 10 Home thành phiên bản Windows 10 Pro. Chỉ cần mở ứng dụng **Settings**, sau đó điều hướng đến **Update & security** =>**Activation** và click chọn nút **Go to Store**.

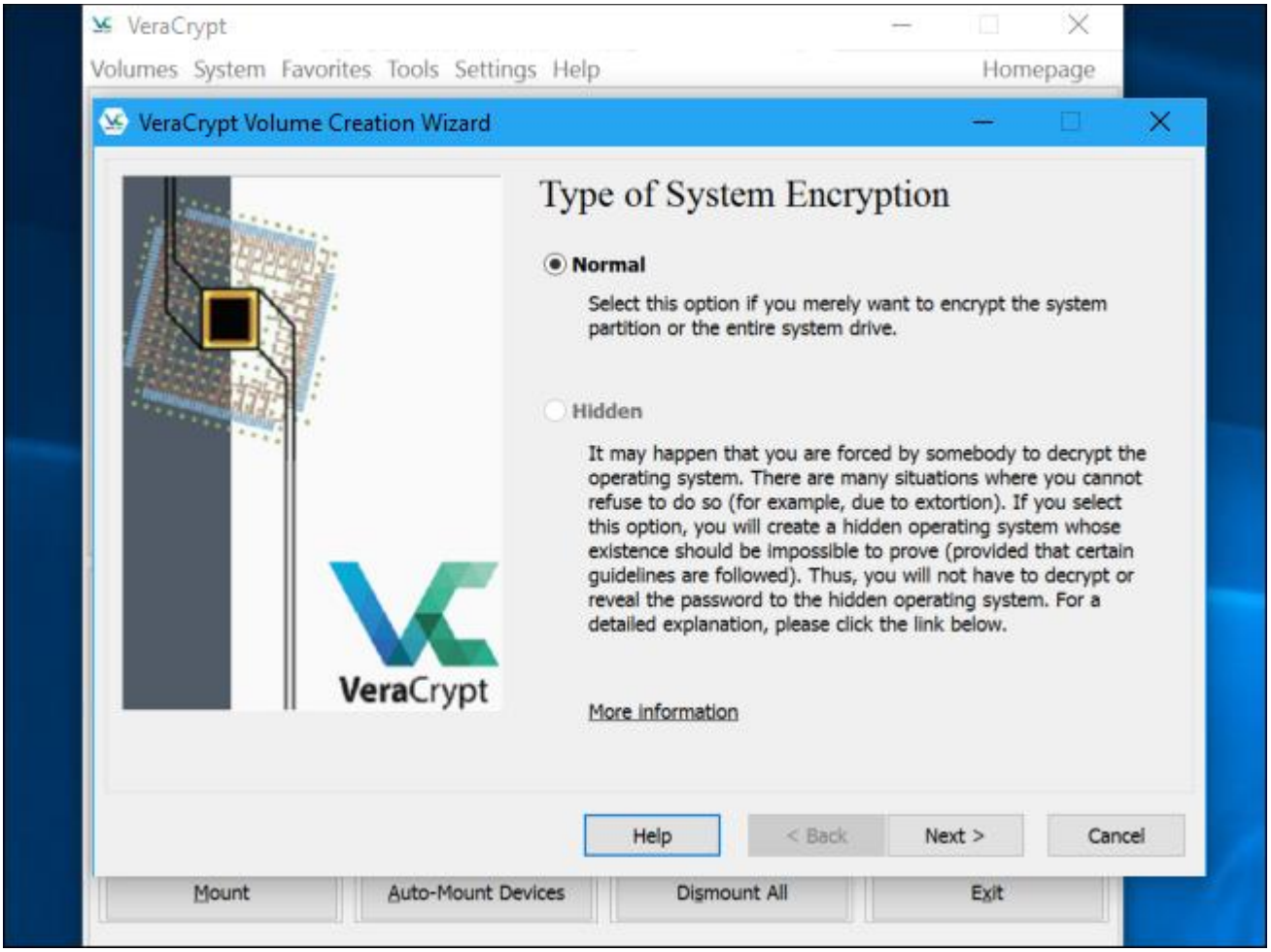
Bạn sẽ phải gán quyền truy cập cho BitLocker và các tính năng khác có trong phiên bản Windows 10 Pro.

3. Lựa chọn khác: VeraCrypt

BitLocker không phải là lựa chọn duy nhất, do đó nếu không muốn mất khoản phí kha khá để sử dụng BitLocker, bạn có thể sử dụng các công cụ mã hóa khác để thay thế.

TrueCrypt là công cụ mã hóa có mã nguồn mở mà bạn có thể sử dụng để thay thế BitLocker. Mặc dù được phát triển cách đây chưa lâu nhưng TrueCrypt có một vài điểm hạn chế là công cụ không thể mã hóa phân vùng hệ thống GPT và sử dụng UEFI để khởi động.

VeraCrypt cũng là công cụ mã hóa có mã nguồn mở khác được phát triển dựa trên nền tảng mã code TrueCrypt. Công cụ này hỗ trợ mã hóa phân vùng hệ thống EFI trên các phiên bản 1.18a và 1.19. Hiểu theo cách khác nôm na, VeraCrypt cho phép bạn có thể mã hóa phân vùng hệ thống máy tính Windows 10 miễn phí.



Xét về độ bảo mật thì VeraCrypt tốt hơn TrueCrypt. Do đó nếu có ý định mã hóa một vài tập tin hoặc toàn bộ phân vùng hệ thống, Quản trị mạng khuyên bạn nên sử dụng VeraCrypt.