

THỰC HÀNH BUỔI 4

BẢO MẬT WINDOWS

1. Sử dụng các phần mềm bảo vệ

1.1. Windows Defender

Microsoft Defender, được biết đến với tên Windows Defender Antivirus trước bản cập nhật tháng 5, 2020, do Microsoft sản xuất để cung cấp các biện pháp bảo vệ an ninh toàn diện, tích hợp sẵn và liên tục cho máy tính. Một số thành phần của nó bao gồm chống vi-rút, chống phần mềm độc hại, tường lửa,...và giữ an toàn cho máy tính cá nhân của ta tránh bị tấn công từ bên ngoài. Phần mềm này miễn phí được cài đặt sẵn và được bật mặc định trong Windows Vista và Windows 7, và tải miễn phí cho Windows XP và Windows Server 2003. Đối với những ai đã và đang sử dụng những phần mềm antivirus của bên thứ ba, ta có thể thử dùng qua Windows Defender để so sánh hiệu suất và tính bảo mật với các chương trình trước đây.

Windows Defender có chức năng quét hệ thống như các phần mềm miễn phí khác trên thị trường, phần mềm bao gồm một số tác tử bảo mật thời gian thực theo dõi sự thay đổi một vài khu vực chung của Windows có thể do bị nhiễm spyware. Phần mềm cũng có khả năng gỡ các ứng dụng ActiveX đã được cài đặt. Ngoài ra việc tích hợp vào mạng SpyNet của Microsoft cho phép người dùng thông báo cho Microsoft những gì họ cho là Spyware, và những ứng dụng hay trình điều khiển nào cho phép cài đặt trên hệ thống của họ.

1.1.1. Một số lợi ích của Windows Defender

Một trong những lợi ích chính của Microsoft Defender Antivirus là nó được tích hợp sẵn với Windows, không cần cài đặt, không phức tạp, rất ít khả năng nó xung đột với các ứng dụng khác. Cài đặt mặc định hợp lý bảo vệ ta khỏi hộp, tự động quét khi tải xuống và thực thi giúp ta an toàn trước hầu hết các mối đe dọa, đồng thời các lần quét nhân rồi và theo lịch nhằm phát hiện mọi thứ khác.

Microsoft Defender có đầy đủ các tùy chọn quét, các mối đe dọa. Bảo vệ là điều thực sự quan trọng với bất kỳ phần mềm chống vi-rút nào. Microsoft Defender đã có nhiều kết quả khác nhau từ các phòng thí nghiệm độc lập trong quá khứ, nhưng nó đã được cải thiện trong vài năm qua và hiện vượt trội hơn nhiều đối thủ cạnh tranh thương mại.

1.1.2. Các chức năng của Windows Defender

- Device performance & health: Đây là tính năng giúp ta biết được tình trạng pin, bộ máy, khả năng sử dụng của thiết bị.

- Firewall & network protection: Giúp máy tính của ta tránh bị xâm nhập bởi các phần mềm độc hại từ trình duyệt web, bảo vệ ta khỏi các cuộc tấn công mạng đến, nhưng nó ít quan tâm hơn đến việc kiểm soát truy cập ra bên ngoài.

- App & browser control: Tính năng này sẽ giúp ta thiết lập SmartScreen cho các phần mềm và thư mục. Ngoài ra, khi có sự xâm nhập của các phần mềm độc hại cho máy tính ta sẽ được cảnh báo.

- Bảo vệ thời gian thực: Tính năng này cho phép theo dõi và bảo vệ các file và chương trình khi hệ thống khởi động.

- Tích hợp với Internet Explorer: Tính năng tích hợp với Internet Explorer cho phép quét file sau khi tải xuống để đề phòng file độc hại.

- Software Explorer: Giúp tránh được các nguy cơ tiềm ẩn với Software Explorer.
- Chức năng chỉ định của Windows Vista: Windows Defender sẽ tự động chặn tất cả các ứng dụng chạy nền cần quyền quản trị.
- Tính năng bảo vệ SmartScreen: cho phép nó chặn quyền truy cập vào các trang web, tệp và ứng dụng độc hại.

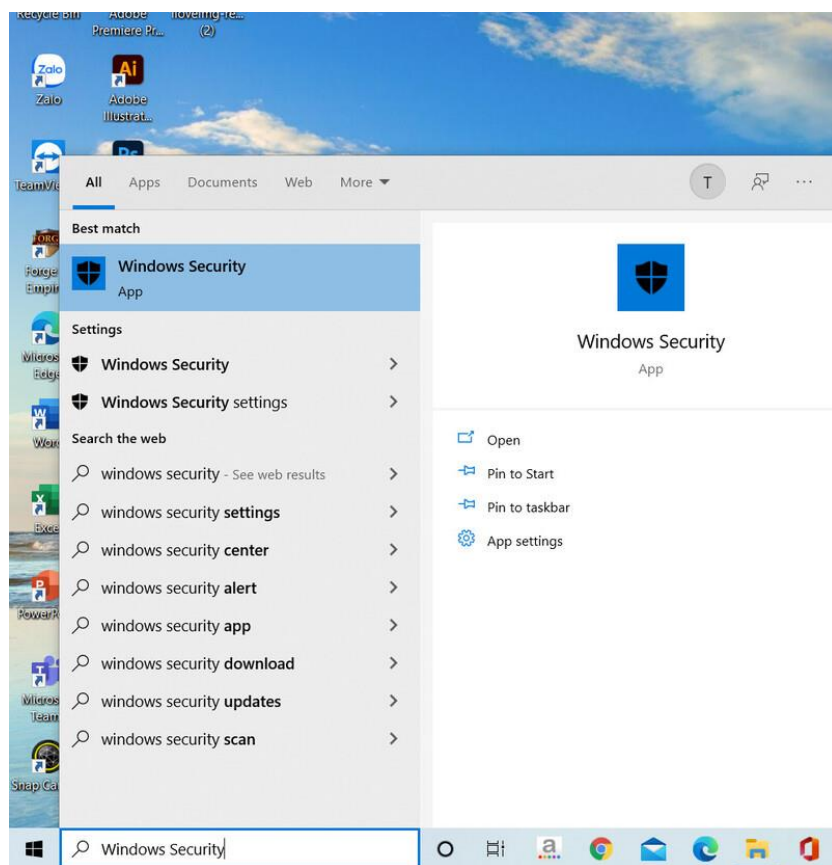
- Tùy chọn gia đình: là một bộ sưu tập các tính năng kiểm soát của phụ huynh.

Ưu điểm: Có thể tùy chỉnh khả năng lọc các trang web theo nội dung, kiểm soát thời điểm con ta có thể sử dụng thiết bị của chúng và các ứng dụng. Sau đó nhận báo cáo hoạt động thường xuyên về những gì chúng đang làm.

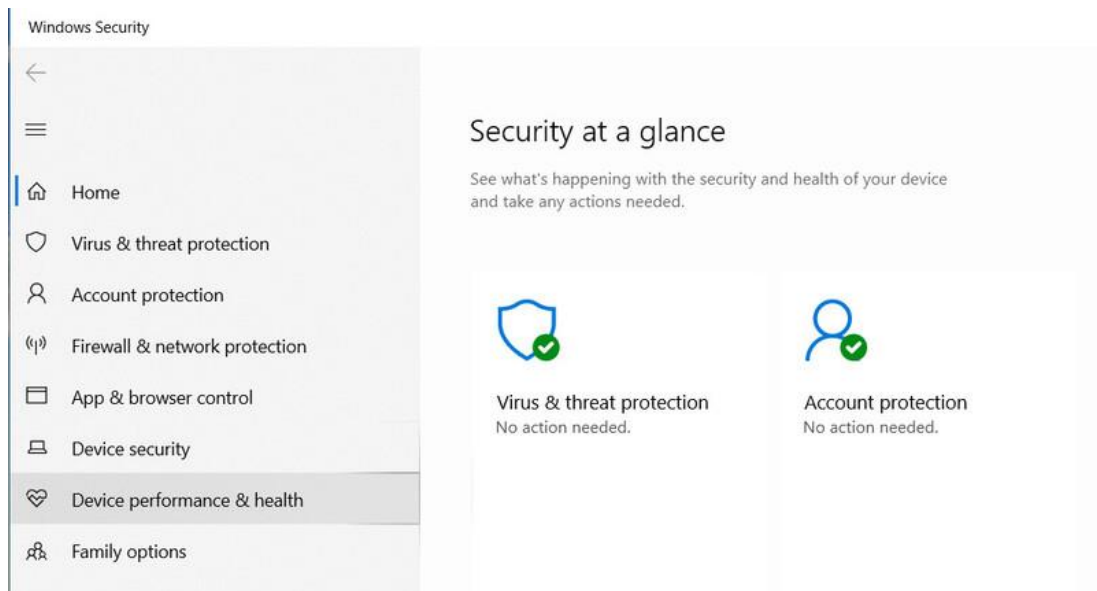
Nhược điểm: chúng hầu hết rất cơ bản và các tùy chọn trình duyệt Windows chỉ dành cho Edge.

1.1.3. Hướng dẫn quét virus bằng Windows Defender

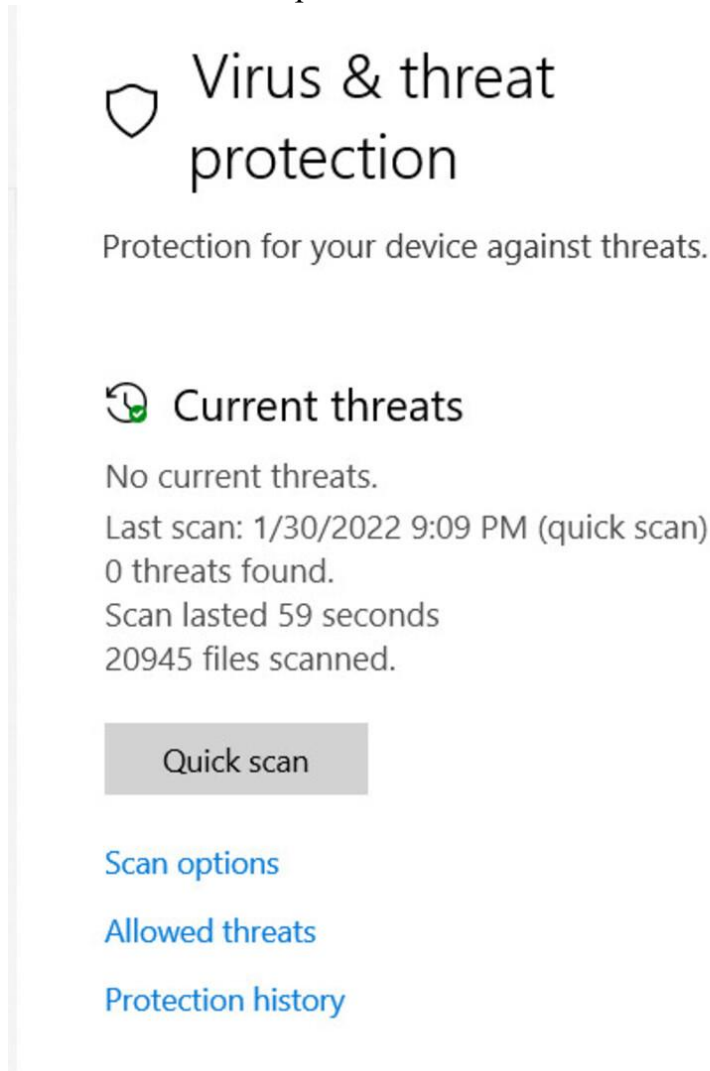
Bước 1: Bấm chữ “Windows Security” vào thanh tìm kiếm -> Chọn Windows Security.



Bước 2: Chọn mục “Virus & threat protection”



Bước 3: Bấm chọn vào “Scan options”



Bước 4: Click chọn mục “Microsoft Defender Offline Scan” -> Chọn “Scan now”

Scan options

Run a quick, full, custom, or Microsoft Defender Offline scan.

No current threats.

Last scan: 1/30/2022 9:09 PM (quick scan)

0 threats found.

Scan lasted 59 seconds

20945 files scanned.

[Allowed threats](#)

[Protection history](#)

☐ Quick scan

Checks folders in your system where threats are commonly found.

☐ Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

☐ Custom scan

Choose which files and locations you want to check.

☒ Microsoft Defender Offline scan

Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Scan now

Bước 5: Bấm “Scan Now” để tiến hành quét virus. Sau đó, ta hãy chờ máy tính quét và diệt virus.

Nhìn chung, công cụ Windows Defender không hề thua kém bất kỳ ứng dụng diệt Virus nổi tiếng nào đang có mặt trên thị trường thời điểm hiện tại. Vậy nên, nếu không có điều kiện mua những công cụ diệt Virus chính hãng đắt tiền thì các ta có thể chọn cách sử dụng công cụ Windows Defender cũng được vì đây là một giải pháp rất hiệu quả.

1.2. UAC

User Account Control hay còn gọi là UAC, là một phần trong hệ thống bảo mật Windows. UAC ngăn chặn các ứng dụng thực hiện các thay đổi không mong muốn trên máy tính. Khi một phần mềm nào đó cố gắng thay đổi hệ thống - liên quan đến một phần Registry hoặc các tập tin hệ thống, Windows 10 sẽ hiển thị hộp thoại xác nhận UAC. Nếu muốn thực hiện các thay đổi này người dùng có thể xác nhận.

UAC cung cấp một môi trường bảo mật cụ thể cho tài khoản người dùng hạn chế quyền truy cập và có thể nâng cao một quá trình cụ thể với các quyền truy cập đầy đủ khi cần thiết. Tuy nhiên, nhiều người dùng cảm thấy không hài lòng khi trên màn hình cứ xuất

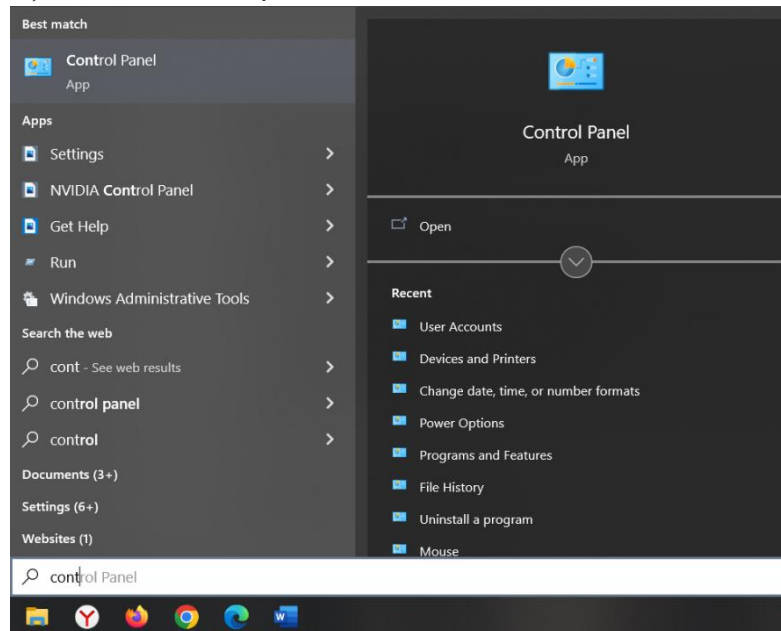
hiện các cửa sổ UAC thông báo. Nếu là người dùng Windows 10 không muốn hiển thị cửa sổ UAC, khi đó có thể vô hiệu hóa UAC đi.

1.2.1. Vô hiệu hóa UAC thông qua Control Panel

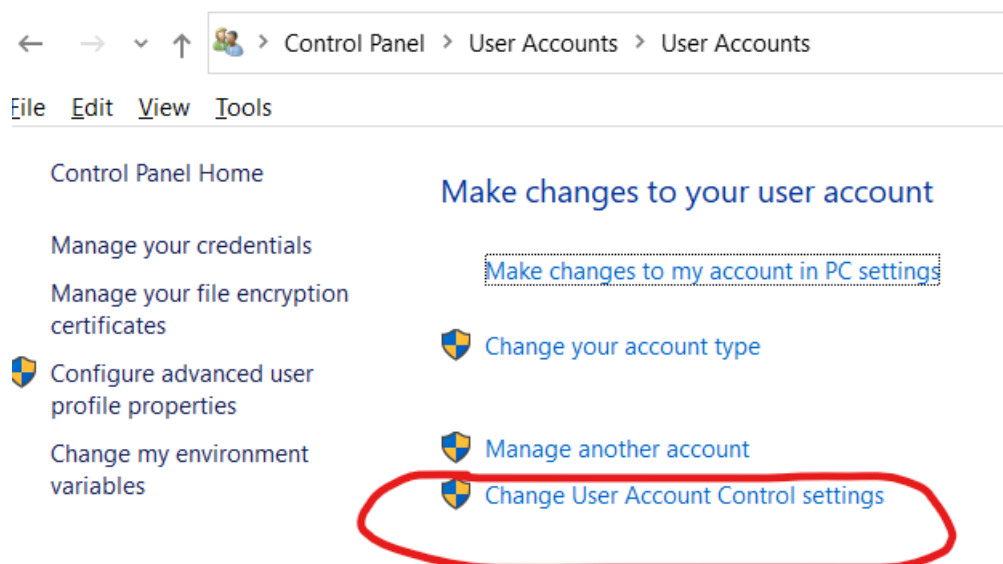
Để vô hiệu hóa UAC thông qua Control Panel, ta thực hiện theo các bước dưới đây:

1. Mở Control panel.

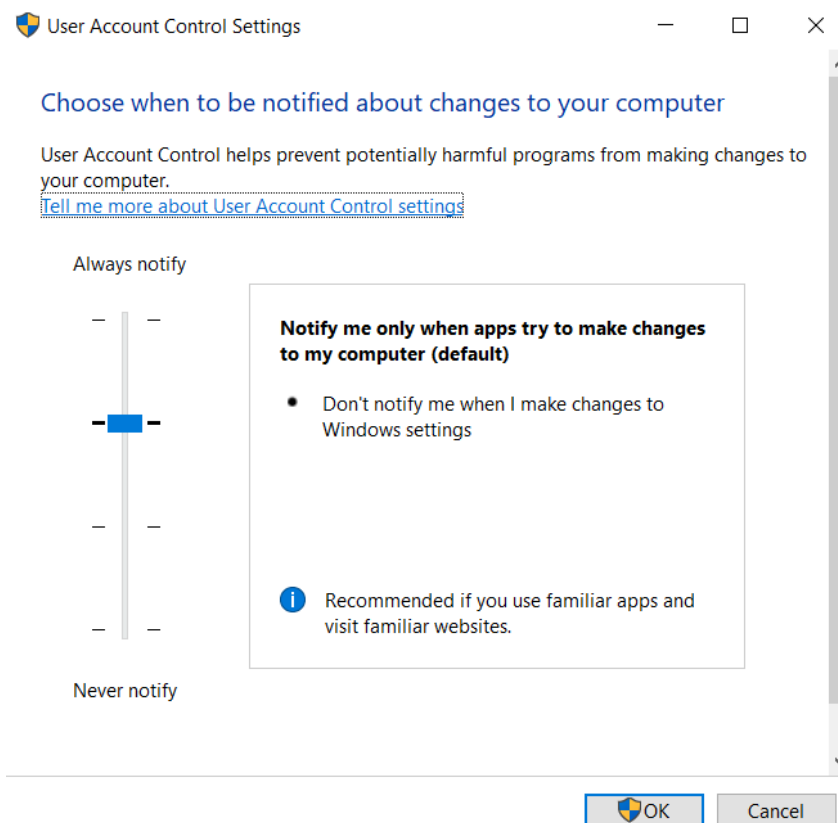
Để mở Control Panel trên Windows 10, bạn nhấn tổ hợp phím Windows + X để mở Power User Menu, sau đó click chọn Control Panel.



2. Trên cửa sổ Control Panel, truy cập theo đường dẫn dưới đây: Control Panel > User Accounts. Tại đây tìm và click chọn link Change User Account Control settings.



3. Trên cửa sổ User Account Control settings, di chuyển thanh trượt xuống phía dưới cùng (Never Notify):



Click chọn OK và UAC sẽ bị vô hiệu hóa

2. Thiết lập chính sách bảo mật khác - BitLocker

BitLocker là một phương thức bảo mật và mã hóa dữ liệu, giúp chúng ta bảo vệ dữ liệu trên máy tính khỏi bị kẻ xấu đánh cắp thông tin. Công cụ BitLocker có sẵn và miễn phí trên Windows, sau khi cài đặt phương pháp mã hóa dữ liệu này, máy tính của chúng ta vẫn hoạt động bình thường.

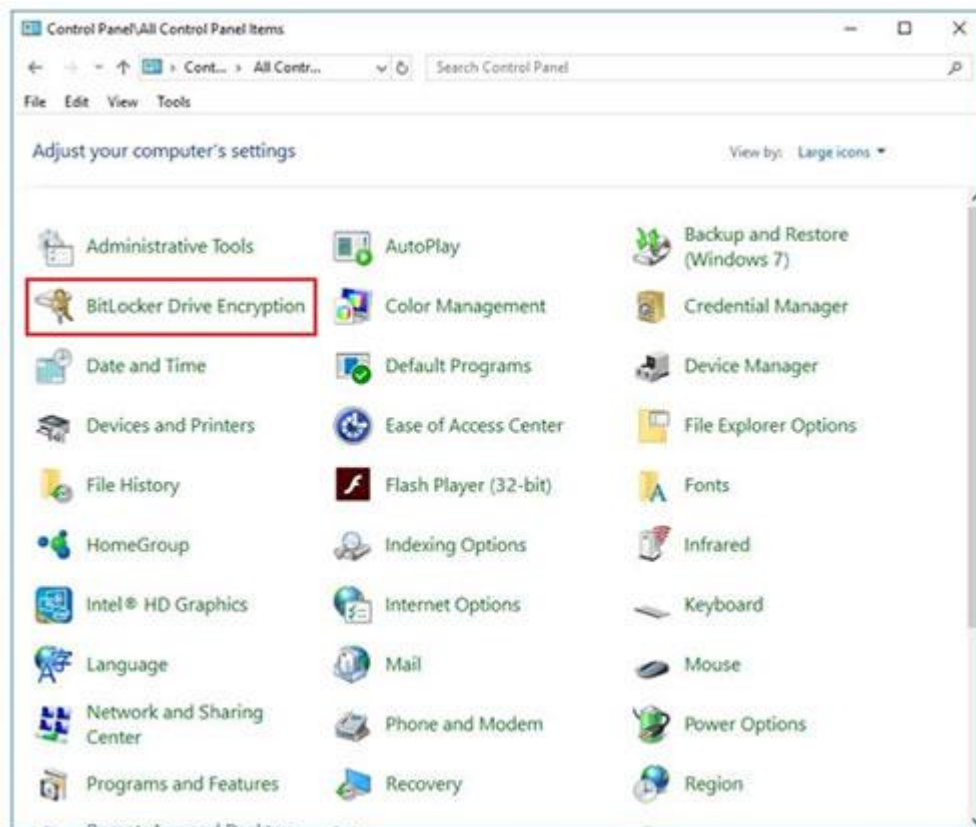
BitLocker trên Windows cung cấp khả năng bảo vệ bổ sung cho các tập tin. Bất kỳ ai, ngay cả với thiết bị của đang sử dụng, đều không thể đọc dữ liệu trên các ổ đĩa được mã hóa. Các ổ đĩa chỉ có thể mở khóa khi cung cấp thông tin đăng nhập, chẳng hạn như mật khẩu Windows hoặc khóa bí mật.

Việc kích hoạt BitLocker mang lại cho máy tính khả năng bảo mật bổ sung mà không phải trả thêm phí. Tác động hiệu suất đối với mã hóa này là tối thiểu đối với phần cứng hiện đại. Khi người dùng cung cấp mật khẩu mở khóa Windows, BitLocker sẽ tự động mở khóa ổ đĩa.

Để sử dụng BitLocker thì máy tính của chúng ta phải hỗ trợ Trusted Platform Module 1.2.

2.1. Mở BitLocker

1. Kết nối thiết bị lưu trữ di động của bạn với máy tính.
2. Truy cập vào Control Panel và chọn BitLocker Drive Encryption.



Chọn BitLocker Drive Encryption

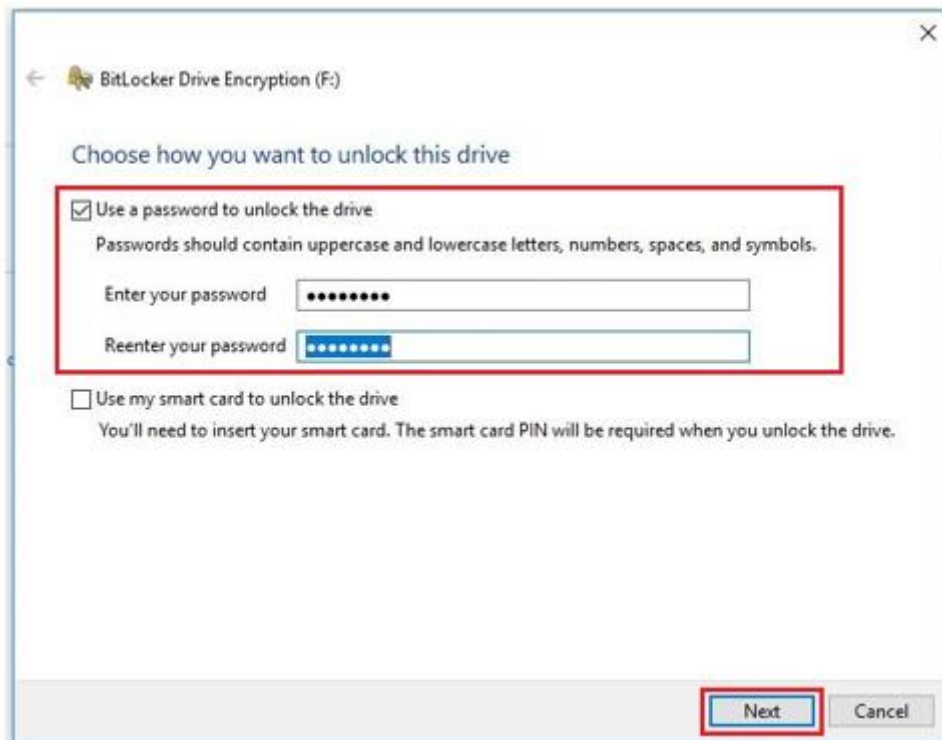
3. Chọn ổ lưu trữ di động mà bạn muốn mã hóa và sau đó nhấp vào Turn on BitLocker.



Nhấp vào Turn on BitLocker

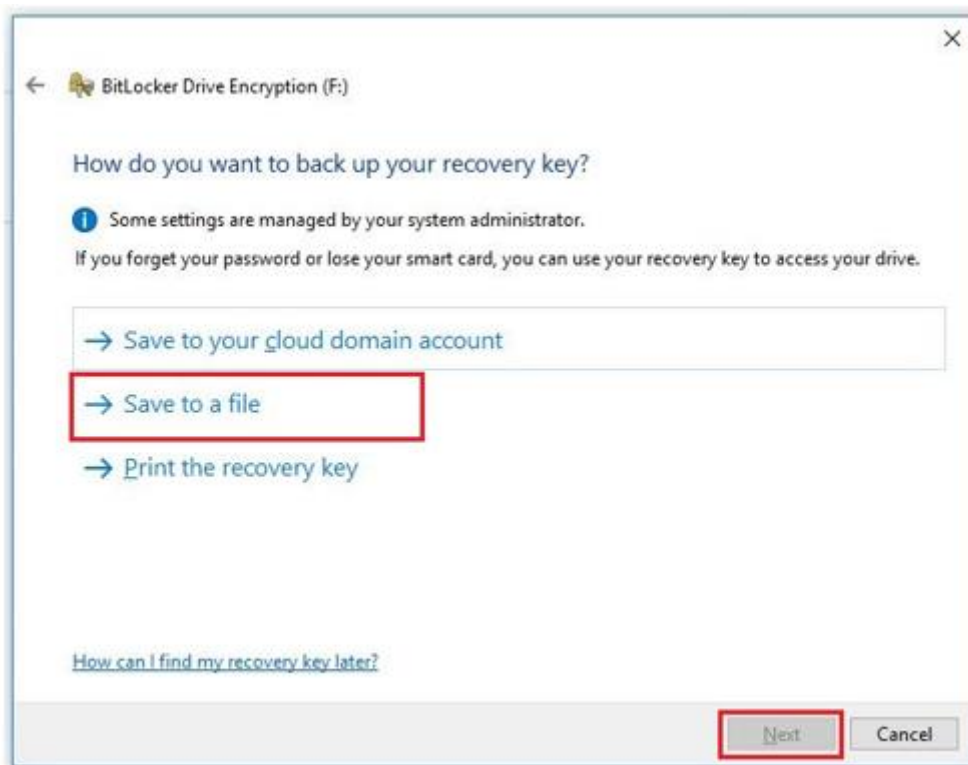
4. Đợi một lúc để việc khởi tạo BitLocker hoàn tất.

5. Chọn Use a password to unlock the drive và xác định mật khẩu của bạn. Nhập lại mật khẩu để xác nhận và sau đó nhấp vào Next.



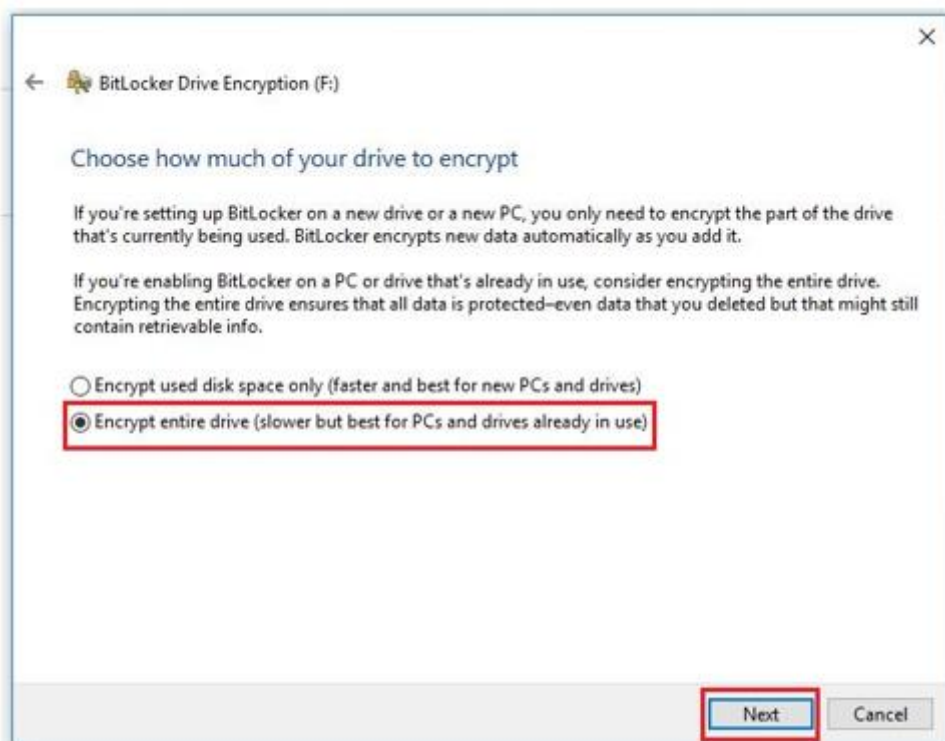
Chọn Use a password to unlock the drive

6. Chọn nơi bạn muốn lưu khóa khôi phục cần thiết để truy cập ổ đĩa trong trường hợp bạn quên mật khẩu. Không nên sử dụng tùy chọn **Save to your cloud domain account**, vì nó yêu cầu máy tính của bạn tham gia Microsoft Azure Active Directory hiện không được cung cấp. Thay vào đó, bạn nên sử dụng tùy chọn **Save to a file** và lưu trữ khóa khôi phục ở nơi an toàn. Sau khi lưu khóa khôi phục, nhấp vào **Next**.



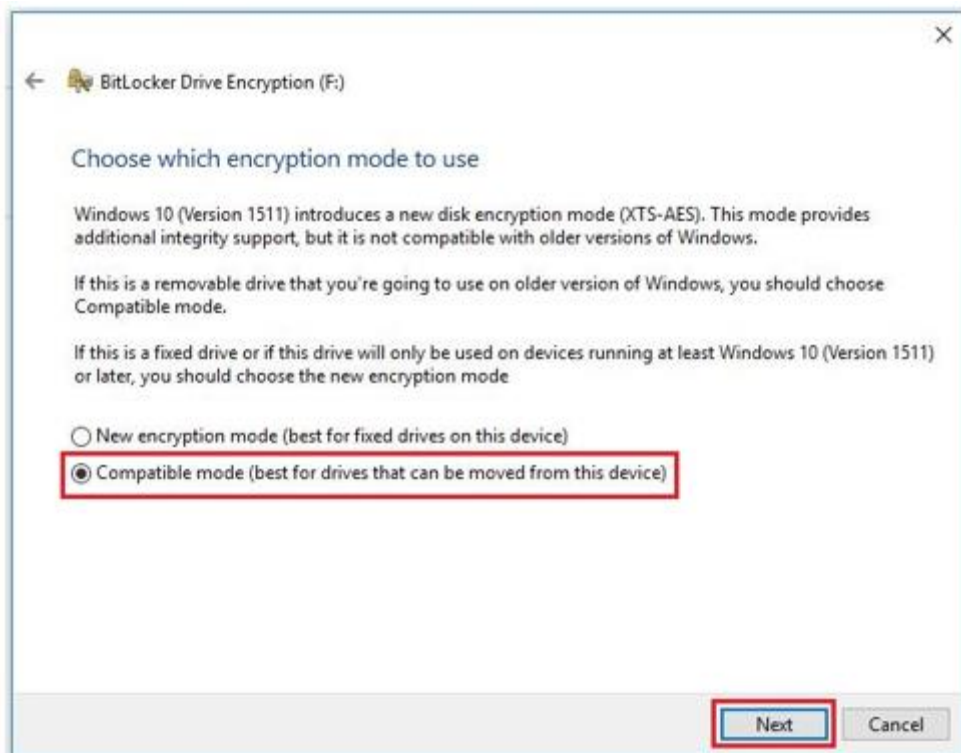
Sử dụng tùy chọn Save to a file

7. Chọn cách bạn muốn mã hóa ổ. Nếu bạn đang sử dụng một ổ mới, hãy chọn Encrypt used disk space only. Nếu bạn đang sử dụng một ổ có dữ liệu, hãy chọn Encrypt entire drive. Sau đó nhấp vào Next.



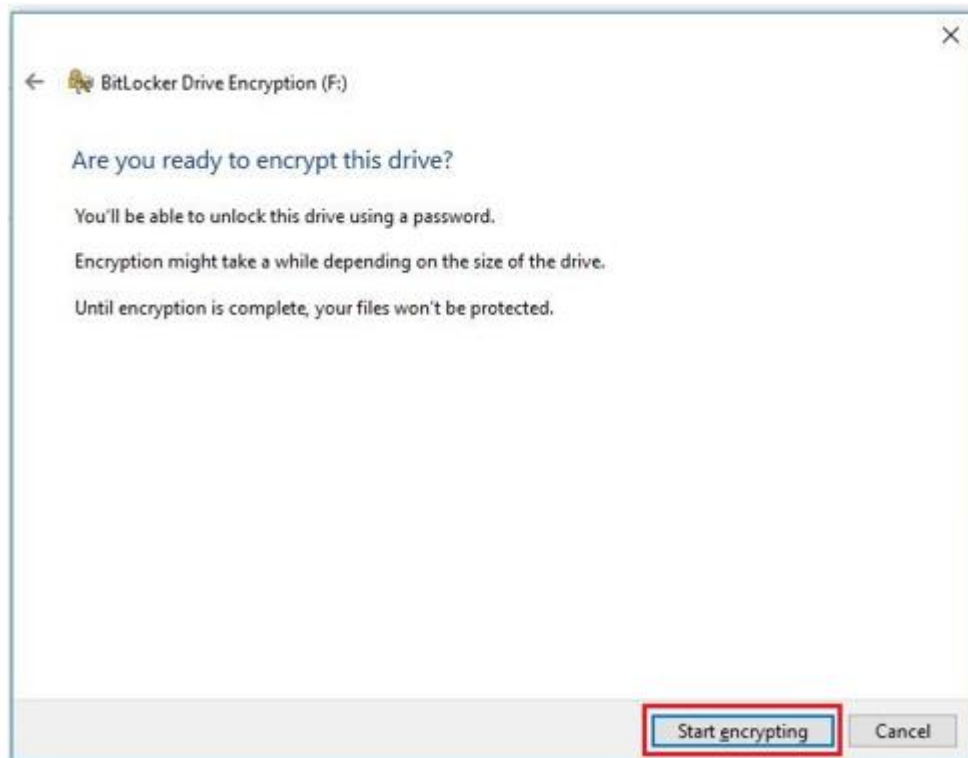
Chọn cách bạn muốn mã hóa ổ

8. Chọn chế độ mã hóa. Nếu dự định sử dụng ổ được mã hóa trên các phiên bản Windows cũ, hãy chọn Compatible mode. Nếu bạn sẽ chỉ sử dụng ổ trên máy Windows 10, hãy chọn New encryption mode, chế độ mã hóa tốt hơn. Sau đó nhấp vào Next.



Chọn chế độ mã hóa

9. Nhấp vào **Start encrypting** khi đã sẵn sàng.

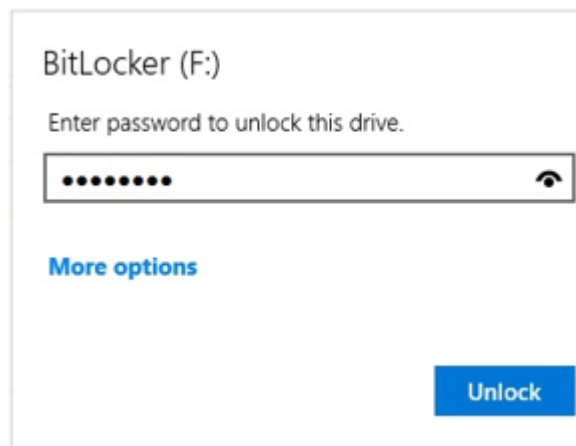


Nhấp vào Start encrypting

10. Quá trình mã hóa có thể mất một chút thời gian, tùy thuộc vào các yếu tố khác nhau, bao gồm tốc độ của thiết bị lưu trữ, hiệu suất của PC,... (Microsoft ước tính tốc độ mã hóa là khoảng 500MB/phút). Làm gián đoạn quá trình có thể dẫn đến hỏng/mất dữ liệu.

11. Nhấp vào Close khi việc mã hóa hoàn tất.

Lần tới khi bạn kết nối ổ được mã hóa với máy tính, hãy nhập mật khẩu để mở khóa.

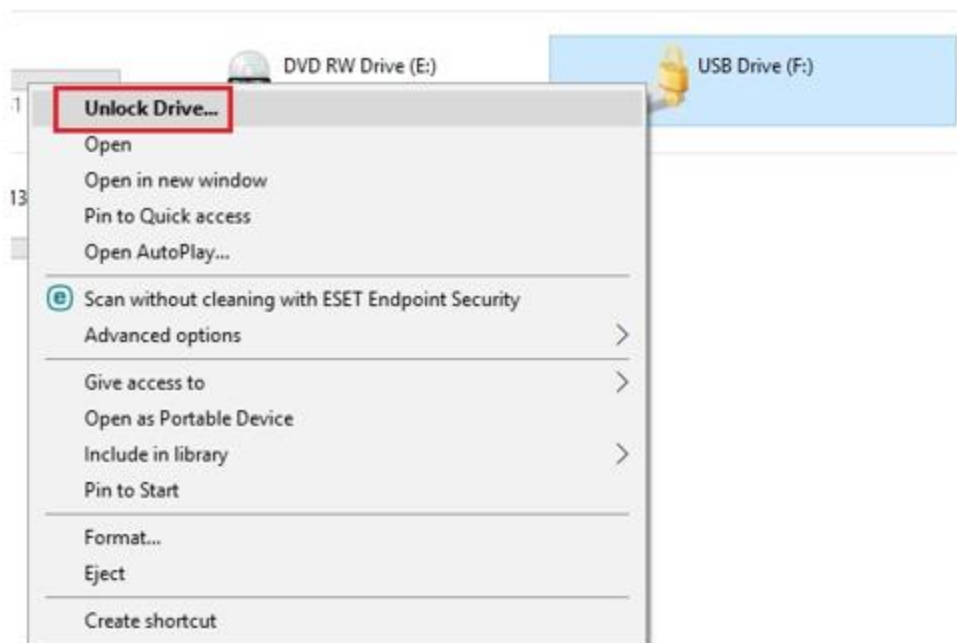


Hãy nhập mật khẩu để mở khóa ổ

2.2. Sử dụng khóa khôi phục để mở khóa ổ

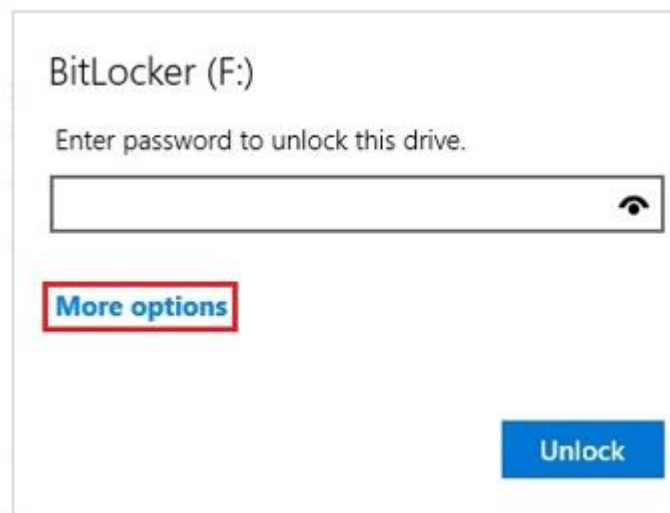
Trong trường hợp bạn quên mật khẩu mở khóa hoặc vì bất kỳ lý do gì bạn không thể truy cập vào ổ được mã hóa, bạn có thể mở khóa ổ bằng khóa khôi phục.

1. Nhấp chuột phải vào ổ được mã hóa từ File Explorer, sau đó nhấp vào Unlock Drive.



Nhấp vào Unlock Drive

2. Nhấp vào **More options** trong cửa sổ pop-up.



BitLocker (F:)

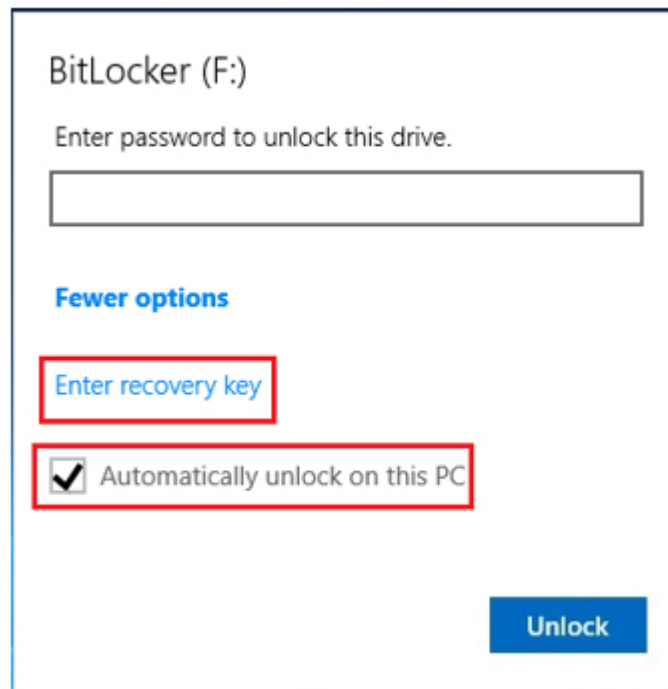
Enter password to unlock this drive.

[More options](#)

[Unlock](#)

Nhấp vào More options

3. Hãy chắc chắn rằng “**Automatically unlock on this PC**” đã được chọn và nhấp vào **Enter recovery key**.



BitLocker (F:)

Enter password to unlock this drive.

[Fewer options](#)

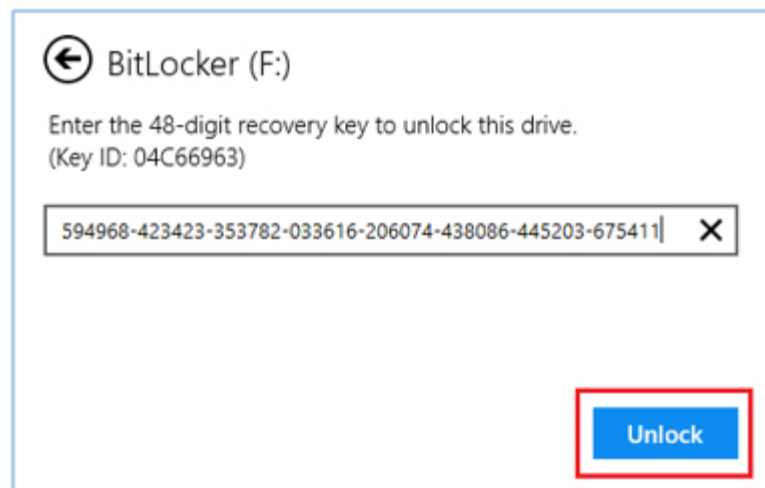
[Enter recovery key](#)

☒ Automatically unlock on this PC

[Unlock](#)

Nhấp vào Enter recovery key

4. Nhập khóa khôi phục và nhấp vào **Unlock**.



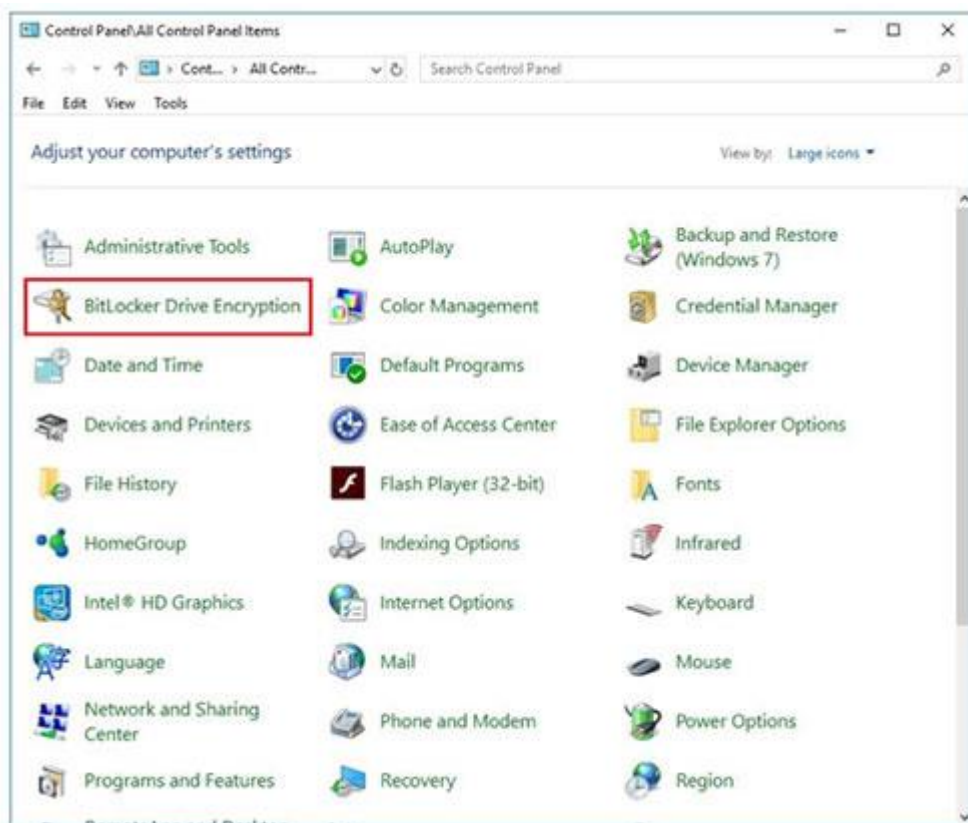
Nhấp vào Unlock

5. Ổ sẽ được mở khóa.

2.3. Thay đổi mật khẩu mở khóa

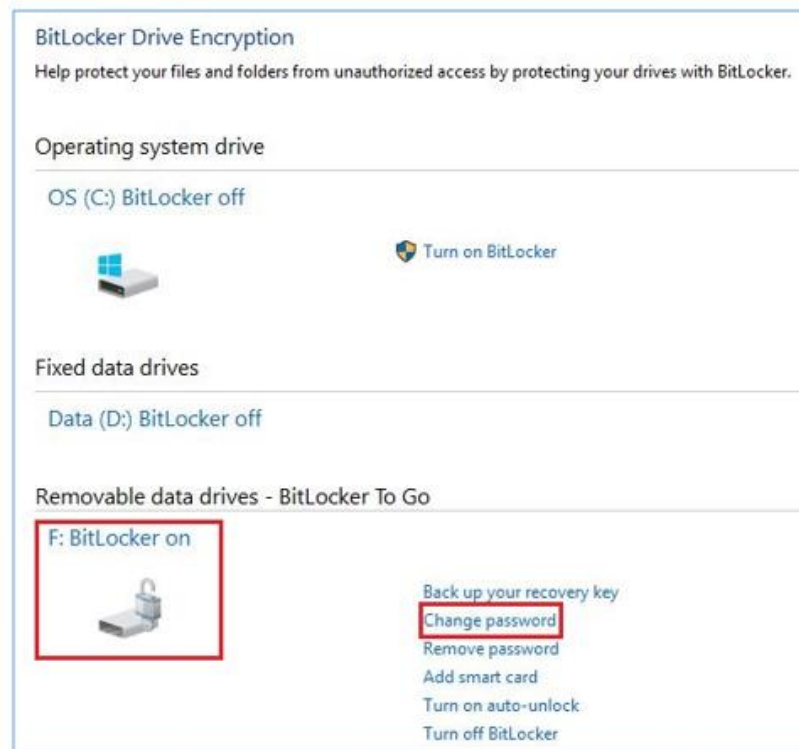
1. Mở khóa ổ được mã hóa với mật khẩu hiện có.

2. Chuyển đến **Control Panel** và sau đó chọn **BitLocker Drive Encryption**.



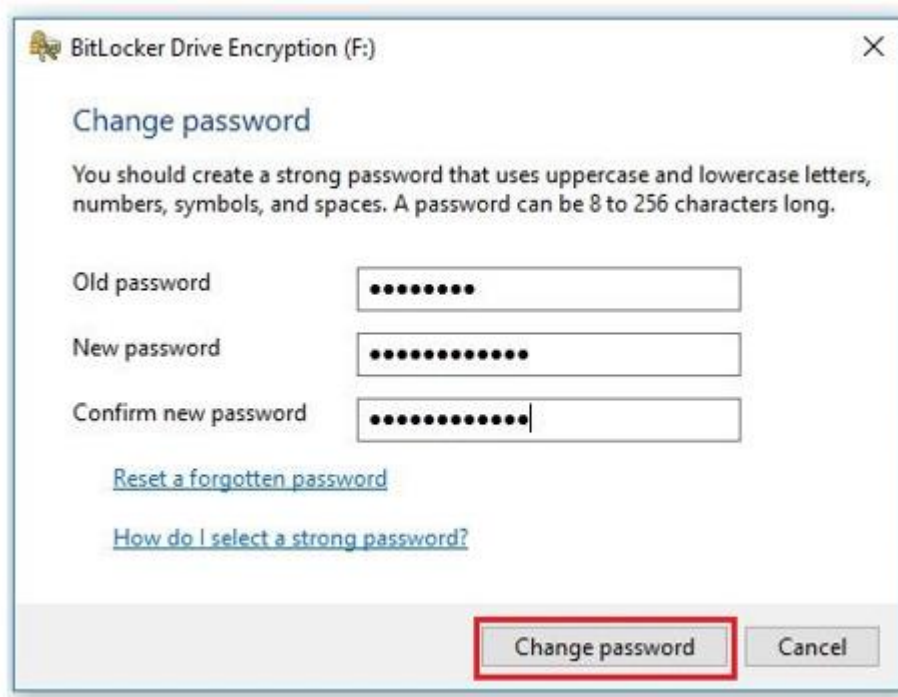
Chọn BitLocker Drive Encryption

3. Xác định vị trí ổ được mã hóa và nhấp vào **Change password**.



Nhấp vào Change password

4. Nhập mật khẩu cũ. Xác định mật khẩu mới và nhập lại để xác nhận. Sau đó bấm vào **Change password**.



Xác định mật khẩu mới và nhập lại để xác nhận

5. Mật khẩu được thay đổi. Nhấp vào **Close**.