

## ***I. Khái niệm virus máy tính***

Virus máy tính (gọi tắt là virus) cũng là một chương trình máy tính, những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng khác (file, ổ đĩa, các chương trình máy tính khác...) mà không có sự cho phép của người dùng. Sau đó Virus thường thực hiện một số loại hoạt động có hại trên máy tính bị nhiễm. Các khu vực bị ảnh hưởng được cho là "bị nhiễm" virus.

## ***II. Tác hại của virus máy tính***

### ***Tiêu tốn tài nguyên hệ thống:***

Virus chiếm dụng các tài nguyên CPU, bộ nhớ, dung lượng đĩa cứng và băng thông mạng. Các máy bị nhiễm virus thường có triệu chứng như: chạy rất chậm, đèn mạng báo liên tục. Trong nhiều trường hợp thậm chí virus chiếm hết băng thông khiến người dùng không thể kết nối mạng.

### ***Phá hủy dữ liệu:***

Có rất nhiều loại virus xóa file. Các tài liệu thường bị tấn công nhiều nhất là các file .doc (Word), .xls (Excel) thường là các tệp chứa dữ liệu quan trọng của người dùng.

### ***Đánh cắp dữ liệu:***

Có rất nhiều loại virus, spyware, keylogger sử dụng các thông tin quan trọng đánh cắp được trên máy tính người dùng để trục lợi. Ngày nay mọi người lưu trữ hầu hết các thông tin quan trọng trên máy tính, từ: sổ sách, chứng từ, thẻ tín dụng.

### ***Mã hóa dữ liệu tống tiền:***

Đây là một hiện tượng mới xuất hiện trong một vài năm gần đây. Khi virus xâm nhập vào máy nạn nhân sẽ mã hóa tất cả các dữ liệu quan trọng của người dùng và yêu cầu họ phải trả tiền để có thể khôi phục lại hệ thống.

### ***Phá hủy hệ thống:***

Một số virus cố tình phá hủy hệ thống (Các virus phá hủy BIOS, làm giảm tuổi thọ của ổ cứng, gây ra lỗi xung đột hệ thống dẫn đến màn hình BSD), thậm chí khiến máy tính trở nên vô dụng.

### ***Gây các khó chịu khác cho người dùng:***

Thiết lập các chế độ ẩn cho tập tin, thư mục, chặn registry, Task Manager... Thay đổi cấu trúc hoạt động của các phần mềm như trình duyệt, office, thậm chí thay đổi hệ điều hành.

### ***Các ví dụ:***

- Vào tháng 1 năm 2004, virus Mydoom đã lây nhiễm gần 1/4 triệu máy tính trong một ngày.
- Vào tháng 1 năm 2007, một loại sâu có tên "Storm" đã lây nhiễm vào khoảng 50 triệu máy tính.
- Hơn 6000 loại virus máy tính mới được tạo ra và phát hành mỗi tháng.
- Virus MyDoom, nó gây thiệt hại 38,5 tỷ USD.

- Năm 1999, một loại virus siêu nhỏ mạnh được gọi là “Melissa” đã buộc Microsoft và các công ty lớn khác phải đóng cửa hệ thống mail của họ.

### ***III. Các loại virus máy tính***

Phân loại virus tùy thuộc vào đã là phân tích xem chúng có cư trú trong tệp thực thi nhị phân (như tệp .EXE hoặc .COM), tệp dữ liệu (như tài liệu Microsoft Word hoặc tệp PDF) hoặc trong khu vực khởi động của ổ cứng của máy chủ (hoặc một số kết hợp của tất cả những điều này).

- Macro Virus
- File Virus
- Boot Sector Virus
- Multipartite Virus
- Polymorphic Virus
- Overwrite Viruses
- FAT Virus

Một cách phân loại virus là phân tích xem chúng có cư trú trong tệp thực thi nhị phân (như tệp .EXE hoặc .COM), tệp dữ liệu (như tài liệu Microsoft Word hoặc tệp PDF) hoặc trong khu vực khởi động của ổ cứng của máy chủ (hoặc một số kết hợp của tất cả những điều này).

#### ***Macro Virus:***

Là loại virus lây nhiễm các tệp được tạo bằng các ứng dụng hoặc chương trình nhất định có chứa macro (Microsoft Word, Microsoft Excel...). Macro là tên gọi chung của những đoạn mã được thiết kế để bổ sung tính năng cho các file của Office các chương trình nhỏ giúp tự động hóa một loạt các thao tác để chúng được thực hiện dưới dạng một hành động, giúp người dùng không phải thực hiện chúng một cách riêng lẻ .

Những ví dụ bao gồm:

- Relax
- Bablas
- Melissa.A

#### ***File Virus:***

Đây là một loại phần mềm độc hại lây nhiễm các tệp thực thi với mục đích gây ra thiệt hại vĩnh viễn hoặc làm cho chúng không thể sử dụng được

Vi rút lây nhiễm tệp ghi đè mã hoặc chèn mã bị nhiễm vào tệp thực thi chẳng hạn như .exe, .vbs hoặc tập tin .com. Hai loại file virus bao gồm *direct action* và *resident virus*.

#### ***Direct Action Virus:***

Direct Action Virus là một loại vi rút lây nhiễm tệp hoạt động bằng cách tự gắn vào tệp .exe hoặc .com. Khi được cài đặt hoặc thực thi virus có thể lây lan sang các tệp hiện có khác và có thể khiến chúng không thể truy cập được.

### ***Resident Virus:***

Resident Virus tương tự như Direct Action Virus, vì cả hai đều là loại virus lây nhiễm tệp. Tuy nhiên, trong khi Direct Action Virus yêu cầu người dùng cài đặt hoặc thực thi tệp bị nhiễm để vi-rút được kích hoạt, thì Resident Virus sẽ tự cài đặt trên máy tính và do đó được coi là nguy hiểm và khó diệt hơn.

Ví dụ: Cleevis and Cascade

### ***Boot Sector Virus:***

Khi máy tính của bạn khởi động, một đoạn chương trình nhỏ trong ổ đĩa khởi động của bạn sẽ được thực thi. Đoạn chương trình này có nhiệm vụ nạp hệ điều hành (Windows, Linux hay Unix...). Sau khi nạp xong hệ điều hành, bạn mới có thể bắt đầu sử dụng máy. Đoạn mã nói trên thường được để ở vùng trên cùng của ổ đĩa khởi động, và chúng được gọi là "Boot sector". Virus Boot là tên gọi dành cho những virus lây vào Boot sector. Các Virus Boot sẽ được thực thi mỗi khi máy bị nhiễm khởi động và trước thời điểm hệ điều hành được nạp.

Những ví dụ bao gồm:

- AntiEXE
- Polyboot.B

### ***Multipartite Virus***

Virus có thể tấn công cả hai khu vực khởi động và các tệp thực thi cùng một lúc, trong khi các vi-rút khác thường lây lan qua một trong các phương pháp này.

Một vi rút đa nhân lây nhiễm các hệ thống máy tính nhiều lần và vào các thời điểm khác nhau. Để loại bỏ nó, toàn bộ virus phải được loại bỏ khỏi hệ thống. Ví dụ, các tệp chương trình có thể được dọn sạch, nhưng khu vực khởi động có thể không, khi đó virus đa nhân sẽ sinh sản như đã từng xảy ra khi khởi động hệ thống.

Virus đa nhân đầu tiên là virus Ghostball.

### ***Polymorphic Virus***

Có thể thích nghi với mọi hình thức phòng thủ của phần mềm diệt virus, bằng cách liên tục thay đổi chữ ký (một chuỗi các byte tạo nên mã vi rút) của chính nó để tránh bị phát hiện. Vì vậy một phần mềm diệt virus không thể phát hiện sự hiện diện chính xác của nó.

Giải pháp phát hiện virus này là:

- Quét heuristic: Thay vì tìm kiếm sự trùng khớp chính xác với mã độc được xác định, quét heuristic tìm kiếm một số thành phần quan trọng mà mỗi đe dọa có thể chia sẻ, làm tăng cơ hội phát hiện và ngăn chặn một biến thể mới của virus.

- Phát hiện dựa trên hành vi: Loại chức năng chống vi-rút này phân tích hành vi của vi-rút thay vì chỉ nhìn vào mã thực tế của nó.

Ví dụ: Taureg

### **Overwrite Viruses**

Những virus này xóa thông tin có trong các tệp mà chúng lây nhiễm, khiến chúng trở nên vô dụng một phần hoặc hoàn toàn. Cách duy nhất để "dọn dẹp" một tệp tin bị nhiễm virus ghi đè là xóa nó hoàn toàn, điều này sẽ khiến bạn mất nội dung gốc.

Ví dụ: Trj.Reboot, Way

### **FAT Viruses**

là virus máy tính tấn công bảng cấp phát tệp (FAT), một hệ thống được sử dụng trong các sản phẩm của Microsoft và một số loại khác của hệ thống máy tính để truy cập thông tin lưu trữ trên máy tính. Thiệt hại gây ra có thể dẫn đến mất thông tin từ các tệp tin cá nhân hoặc thậm chí toàn bộ thư mục.

### **Bảng tóm tắt các loại virus:**

	Cách lây nhiễm	Tác hại	Ví dụ
Resident Viruses	Được lưu trữ trong bộ nhớ	làm gián đoạn tất cả các hoạt động được thực hiện bởi hệ thống	Randex, CMJ, Meve, and MrKlunky
Boot sector virus	thi hành mỗi khi máy bị nhiễm khởi động	Phá hủy hoặc thay đổi chương trình và dữ liệu.	Disk Killer, Stone virus.
Program or File Virus	thực thi khi các tệp tin như .exe, .com, .bin, .sys được mở	Phá hủy hoặc thay đổi chương trình và dữ liệu	Sunday and Cascade
Multipartite Virus	kết hợp giữ Boot sector virus và File Virus	Phá hủy hoặc thay đổi chương trình và dữ liệu	Invader, Flip, and Tequila
Macro Virus	khi mở hoặc thực thi câu lệnh của 1 file office	- ảnh hưởng đến các file office - khi các file được đính kèm trong email thì nó có thể	DMV, Nuclear, Word Concept, Melissa, ILOVEYOU, Love Bug

		truy cập địa chỉ email để spam	
--	--	--------------------------------	--

#### ***IV. Cách thức phòng phòng tránh:***

- Luôn cập nhật bản vá bảo mật mới nhất của hệ điều hành.
- Luôn cập nhật bản phát hành mới nhất của trình duyệt web
- Cài đặt 1 firewall và luôn cập nhật
- Đừng mở email từ các nguồn không xác định, luôn quét các tệp tin đính kèm trong email trước khi mở
- Quét máy tính định kỳ, Không cắm và mở USB mà chưa quét virus cho chúng.
- Đừng tìm kiếm và tải xuống các phần mềm miễn phí không rõ nguồn gốc.
- Luôn kiểm tra phần mở rộng của tệp trước khi mở nó.
- Mã hóa thông tin trên máy tính, máy tính Windows có thể dùng BitLocker, Veracrypt
- Sử dụng trình quản lý mật khẩu như Lastpass/Dashlane, Sử dụng 1 VPN có uy tín như PIA, Express VPN, F-Secure Freedome.
- Sử dụng xác thực hai yếu tố ở mọi nơi bạn có thể
- Không bao giờ lưu trữ thông tin tài chính hoặc tài liệu của bản thân mà không có sự bảo vệ thích hợp. Lưu chúng trong các thư mục được mã hóa nếu cần.

#### ***V. Nhận biết máy bị nhiễm virus***

**Kiểm tra hoạt động của ổ cứng của bạn:** nếu bạn không chạy bất kỳ chương trình nào và đèn ổ cứng của bạn liên tục bật và tắt hoặc bạn có thể nghe thấy tiếng ổ cứng đang hoạt động, có thể bạn có vi-rút đang hoạt động trong nền.

**Xem xét thời gian để máy tính của bạn khởi động:** Nếu bạn bắt đầu nhận thấy rằng máy tính của mình mất nhiều thời gian hơn bình thường để khởi động, thì có thể vi-rút đang làm chậm quá trình khởi động.

**Nhìn vào đèn modem của bạn:** Nếu bạn không có bất kỳ chương trình nào đang chạy và đèn chuyển modem của bạn liên tục nhấp nháy, bạn có thể có vi-rút đang truyền dữ liệu qua mạng.

**Lưu ý về sự cố chương trình:** Nếu các chương trình thông thường của bạn bắt đầu gặp sự cố thường xuyên hơn, vi-rút có thể đã lây nhiễm vào hệ điều hành. Các chương trình mất nhiều thời gian tải hơn hoặc hoạt động quá chậm cũng là dấu hiệu của điều này.

**Cửa sổ bật lên:** Nếu bạn bị nhiễm vi-rút, bạn có thể bắt đầu thấy thông báo xuất hiện trên màn hình, ngay cả khi không có chương trình nào khác đang chạy. Chúng có thể bao gồm quảng cáo, thông báo lỗi, v.v.

**Hãy cảnh giác với việc cấp quyền truy cập tường lửa cho chương trình:** Nếu bạn nhận được thông báo liên tục về một chương trình yêu cầu quyền truy cập vào tường lửa của bạn,

chương trình đó có thể đã bị nhiễm. Bạn nhận được những thông báo này vì chương trình đang cố gắng gửi dữ liệu qua bộ định tuyến của bạn.

**Xem các tệp của bạn:** Vi rút thường xóa các tệp và thư mục của bạn hoặc các thay đổi được thực hiện mà không có sự đồng ý của bạn. Nếu tài liệu của bạn biến mất, rất có thể bạn đã bị nhiễm vi-rút.

**Kiểm tra trình duyệt web của bạn:** Trình duyệt web của bạn có thể mở các trang chủ mới hoặc không cho phép bạn đóng các tab. Cửa sổ bật lên có thể xuất hiện ngay khi bạn mở trình duyệt của mình. Đây là một dấu hiệu tốt cho thấy trình duyệt của bạn đã bị virus hoặc phần mềm gián điệp xâm nhập.

**Nói chuyện với bạn bè và đồng nghiệp của bạn:** Nếu bạn có vi-rút, danh sách gửi thư của bạn có thể nhận được các thư mà bạn không gửi. Những tin nhắn này thường chứa nhiều vi-rút hoặc quảng cáo hơn. Nếu bạn biết rằng những người khác đang nhận những thứ này từ bạn, rất có thể bạn đã bị nhiễm vi-rút.

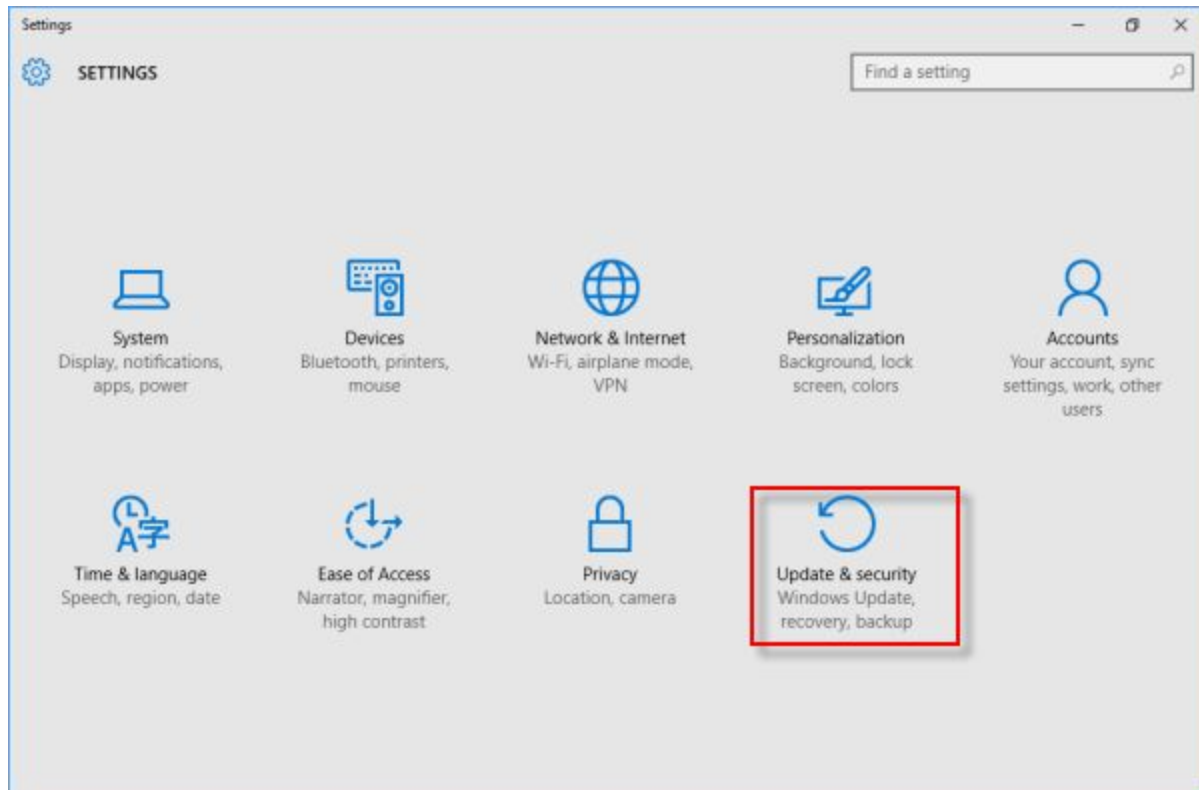
**Chạy chương trình chống vi-rút:** Bạn phải luôn cài đặt và chạy chương trình chống vi-rút trên máy tính của mình

## ***VI. Phát hiện và tiêu diệt các mối đe dọa trong Windows 10***

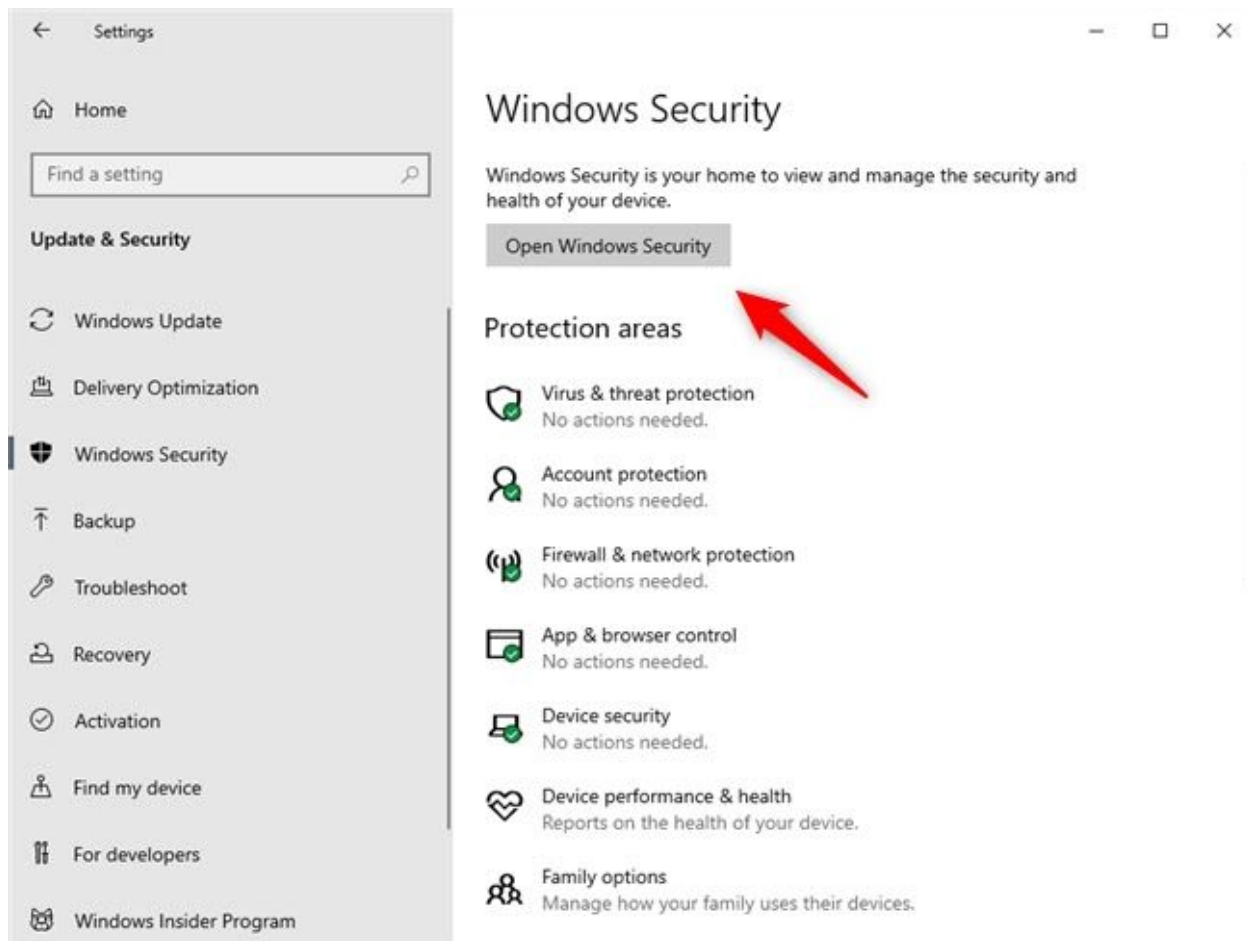
Sử dụng bộ công cụ Windows Defender trong Windows 10

Bước 1:

Chọn menu **Start > Setting > Update & Security**.



Bước 2: Nhấn vào **Windows Security**( Nó ở bảng điều khiển bên trái ) > **Open Windows Security**.





Bước 3: Nhấn vào **Virus & threat protection**







 Home


 Virus & threat protection


 Account protection

 Firewall & network protection

 App & browser control

 Device security

 Device performance & health

 Family options

## Security at a glance

See what's happening with the security and health of your device and take any actions needed.



**Virus & threat protection**  
Tamper protection is off. Your device may be vulnerable.

Turn on

Dismiss



**Device performance & health**



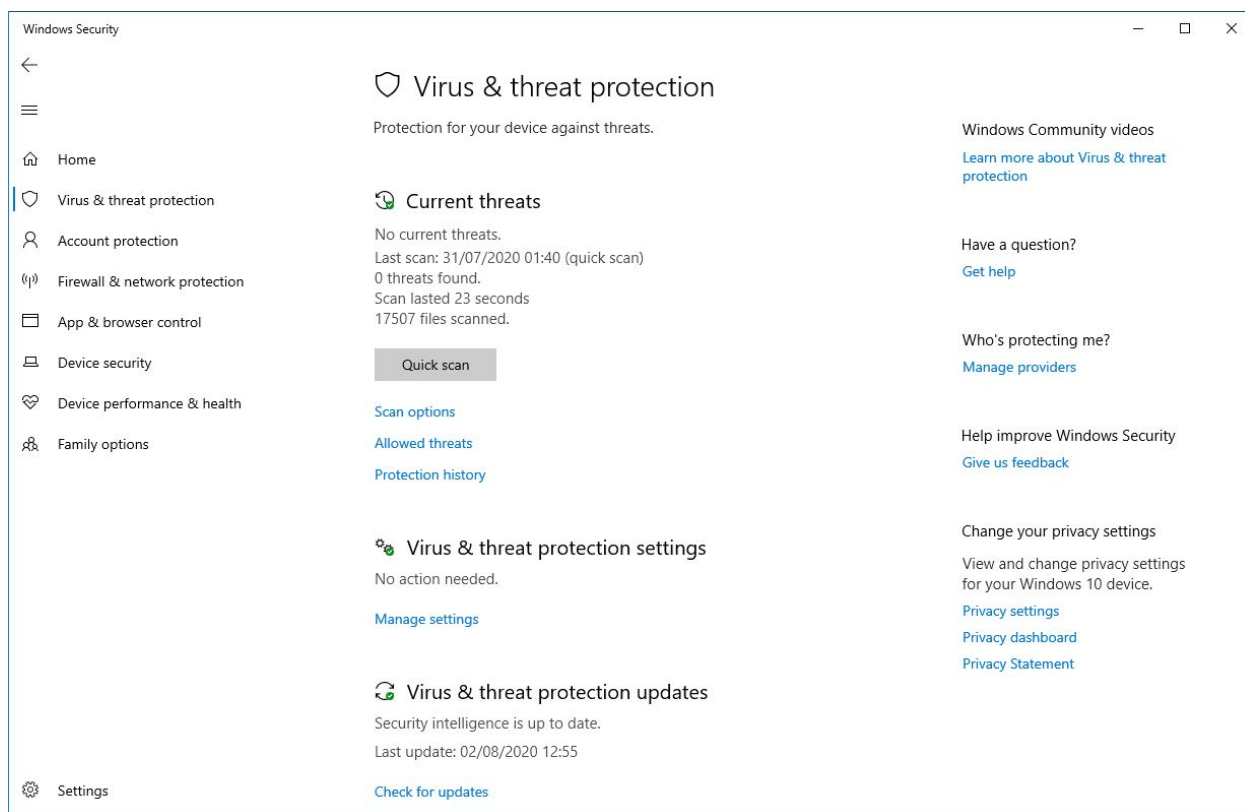
**Account protection**  
No action needed.



**Firewall & network protection**  
No action needed.



**Family options**  
Manage how your family



Bước 4: Như đã đề cập virus được tạo mới mỗi ngày, do đó trước khi thực hiện việc quét và tiêu diệt virus chúng ta nên cập nhật các định nghĩa mới nhất về virus.

Trong bảng **Virus & threat protection** > click **Check for updates** ( trong mục **Virus & threat protection updates** ).

Bước 5: Sau khi update xong > click **Quick scan**.

kết quả quét

**Current threats**  
No current threats.  
Last scan: 31/07/2020 01:40 (quick scan)  
0 threats found.  
Scan lasted 23 seconds  
17507 files scanned.

nếu kết quả quét phát hiện có các mối đe dọa thì làm theo hướng dẫn để loại trừ. Trong trường hợp này hệ thống không phát hiện bất kỳ mối đe dọa nào.

<b>I. Khái niệm virus máy tính</b>	<b>1</b>
<b>II. Tác hại của virus máy tính</b>	<b>1</b>
Tiêu tốn tài nguyên hệ thống:	1
Phá hủy dữ liệu:	1
Đánh cắp dữ liệu:	1
Mã hóa dữ liệu tổng tiền:	1
Phá hủy hệ thống:	1
Gây các khó chịu khác cho người dùng:	1
Các ví dụ:	1
<b>III. Các loại virus máy tính</b>	<b>2</b>
Overwrite Viruses	2
Macro Virus:	2
File Virus:	2
Direct Action Virus:	2
Resident Virus:	3
Boot Sector Virus:	3
Multipartite Virus	3
Polymorphic Virus	3
Overwrite Viruses	4
FAT Viruses	4
Bảng tóm tắt các loại virus:	4
<b>IV. Cách thức phòng phòng tránh:</b>	<b>5</b>
<b>V. Nhận biết máy bị nhiễm virus</b>	<b>5</b>
<b>VI. Phát hiện và tiêu diệt các mối đe dọa trong Windows 10</b>	<b>6</b>