BÀI 9

AN TOÀN TRÊN KHÔNG GIAN MẠNG

SAU BÀI NÀY EM SẼ:

- Nêu được những nguy cơ và tác hại khi tham gia các hoạt động trên Internet một cách thiếu hiểu biết và bất cẩn. Trình bày được một số cách đề phòng những tác hại đó.
- Nêu được một vài cách phòng vệ khi bị bắt nạt trên mạng. Biết cách bảo vệ dữ liệu cá nhân.
- Trình bày được sơ lược về các phần mềm xấu (mã độc). Biết sử dụng một số công cụ để phòng chống phần mềm xấu.

Không gian mạng – (trong một số hoàn cảnh cụ thể được gọi vắn tắt là "mạng") chính là Internet, là một môi trường rất mở. Trên mạng mọi người có thể liên lạc, chia sẻ thông tin với nhau một cách dễ dàng nhưng chính điều đó lại bị những kẻ xấu lợi dụng khiến mạng cũng là nơi đầy rẫy những cạm bẫy. Cần tự bảo vệ mình như thế nào?

1. MỘT SỐ NGUY CƠ TRÊN MẠNG

Hoạt động 1 Nguy cơ trên mạng

Hãy thảo luận và cho ví dụ minh hoạ về những nguy cơ có thể khi lên Internet để:

a) Kết bạn.

b) Xem tin tức.

c) Tải các phần mềm.

Tin giả và tin phản văn hoá. Ai cũng có thể đưa tin bài lên mạng kể cả các tin bài xấu. Có nhiều tin giả, tin bài phản cảm như những tình tiết có tính bạo lực trong một vụ án hoặc có nội dung dẫn đến các nhận thức lệch lạc.

Lừa đảo trên mạng. Nhiều người lợi dụng mạng để lừa đảo. Một ví dụ là kẻ xấu lấy các ảnh, tin tức trên trang facebook của một người để lập một trang giống hệt rồi kết bạn với những người bạn của nạn nhân. Cuối cùng chúng mạo danh vay mượn để chiếm đoạt tài sản.

Lộ thông tin cá nhân. Thông tin cá nhân bao gồm tên tuổi, số điện thoại, tài khoản email, tài khoản ngân hàng,... và các tài khoản của các ứng dụng trên mạng. Khi lộ tài khoản các ứng dụng phần mềm, ta có thể bị mạo danh. Còn khi lộ tài khoản của ngân hàng, ta có thể mất tiền.

Các biện pháp bảo vệ thông tin cá nhân:

- Không ghi chép thông tin cá nhân ở những nơi mà người khác có thể đọc;
- Giữ cho máy tính không bị nhiễm các phần mềm gián điệp;
- Cẩn trọng khi truy cập mạng qua wifi công cộng vì hầu hết những trạm wifi công cộng không mã hoá thông tin khi truyền.

Bắt nạt trên không gian mạng. Một trong những vấn nạn trên mạng là bắt nạt. Mức thấp là xỉ vả, lăng nhục. Mức cao là đe doạ tung thông tin cá nhân, đưa tin bịa đặt, vu khống, thậm chí tống tiền hoặc ép buộc làm điều xấu. Hành vi bắt nạt trên mạng ảnh hưởng nghiêm trọng tới tâm lí của nạn nhân vì:

- Việc bắt nạt có thể xảy ra dai dẳng, bất cứ lúc nào;
- Người bắt nạt có thể ẩn danh, không biết là ai để đối phó;
- Số người theo dõi, bình luận có thể rất đông gây áp lực nặng nề, khiến nạn nhân có nguy cơ tự cô lập;
- Nhiều người không tự giải quyết được nhưng không dám nói ra, dẫn đến trầm cảm và có các hành vi tiêu cực. Bắt nạt là một kiểu khủng bố trên không gian mạng.

Một số biện pháp phòng chống hành vi bắt nạt:

- Không nên kết bạn dễ dãi qua mạng.
- Không trả lời thư từ hay tin nhắn, không tranh luận với kẻ bắt nạt trên diễn đàn.
- Hãy lưu giữ tất cả các bằng chứng.
- Hãy chia sẻ với bố mẹ hoặc thầy cô.
- Khi sự việc nghiêm trọng hãy báo cho cơ quan công an kèm theo bằng chứng.

Nghiện mạng. Có một số người dành rất nhiều thời gian cho mạng, đặc biệt là chơi game đến mức nghiện, ảnh hưởng nghiêm trọng tới sức khoẻ. Đã từng có những thanh niên chơi trò chơi điện tử liên tục nhiều ngày và đột quỵ ngay trên bàn máy tính.

- Mạng là môi trường giao tiếp nhanh chóng, thuận tiện nhưng ẩn chứa nhiều nguy cơ gây mất an toàn thông tin.
- Chỉ truy cập các trang web tin cậy, hãy cảnh giác với các thông tin giả, lừa đảo.
- Hãy giữ bí mật thông tin cá nhân.
- Chỉ nên kết bạn với những người quen biết trong mạng xã hội. Khi bị bắt nạt, hãy chia sẻ với người thân hoặc thầy cô.
- Không nên sử dụng Internet quá nhiều.

1. Em hãy đưa ra một số tình huống có thể làm lộ mật khẩu tài khoản.
2. Em có biết một hành vi lừa đảo nào trên mạng không? Nếu có, em hãy kể cách thức lừa đảo.

2. PHẦN MỀM ĐỘC HẠI

Hoạt động 2 **Có những loại phần mềm độc hại nào?**

Em hiểu gì về virus máy tính? Có phải tất cả phần mềm độc hại đều là virus?

Một đối tượng gây mất an toàn là phần mềm độc hại (malicious software, viết tắt là malware), những phần mềm được viết ra với ý đồ xấu, gây hại cho người dùng.

Những phần mềm độc hại có mục đích gây ảnh hưởng trên quy mô lớn thường có cơ chế lây nhiễm. Theo cơ chế lây nhiễm, có hai loại phần mềm độc hại là virus và worm. Còn một loại phần mềm độc hại khác là trojan chỉ nhằm chiếm đoạt thông tin hay chiếm quyền sử dụng máy tính sẽ ít chú trọng đến tính năng lây nhiễm.

a) Tìm hiểu về virus, trojan, worm và cơ chế hoạt động

Virus. Virus không phải là các phần mềm hoàn chỉnh, mà chỉ là các đoạn mã độc và phải gắn với một phần mềm mới phát tác và lây lan được. Khi chạy một phần mềm đã nhiễm virus, đoạn mã độc sẽ được đưa vào bộ nhớ, chờ khi thi hành một phần mềm khác sẽ chèn vào để hoàn thành một chu kì lây lan.

Worm, sâu máy tính. Khác với virus, worm là một phần mềm hoàn chỉnh. Để lây, worm lợi dụng những lỗ hổng bảo mật của hệ điều hành hoặc dẫn dụ, lừa người dùng chạy để cài đặt vào máy của nạn nhân. Cách lừa thông thường là để một liên kết ngầm trong email hoặc tin nhắn với vỏ bọc là một nội dung lành mạnh, ví dụ "bấm vào đây để nhận tin" nhưng khi bấm vào, ngoài bản tin thì chính phần mềm độc hại cũng được tải vào máy.

Trojan. Phần mềm nội gián, gọi là trojan, theo truyền thuyết "Con ngựa thành Troa" (Trojan Horse) trong truyện thần thoại Hy Lạp. Tuỳ hành vi, trojan có thể mang những tên khác nhau như:

- Spyware: (phần mềm gián điệp) có mục đích ăn trộm thông tin để chuyển ra ngoài.
- Keylogger: là một loại spyware ngầm ghi hoạt động của bàn phím và chuột để tìm hiểu người sử dụng máy làm gì.
- Backdoor: tạo một tài khoản bí mật, giống như cửa sau, để có thể truy cập ngầm vào máy tính.
- Rootkit: chiếm quyền cao nhất của máy, có thể thực hiện được mọi hoạt động kể cả xoá các dấu vết. Rootkit cũng có tài khoản truy nhập ngầm.

b) Tác hại của phần mềm độc hại

Như vậy, hai đặc trưng chính của virus hay worm là lây lan và gây ra các tác động không mong muốn, còn trojan thì thực hiện các hoạt động nội gián.

Tác động không mong muốn có khi chỉ gây khó chịu, nhưng các virus hay worm "dữ" có thể làm hỏng các phần mềm khác trong máy, xoá dữ liệu hay làm tê liệt hệ thống máy tính.

Virus có thể bị phát hiện theo hành vi, nhưng các worm (sâu) thường do chính nạn nhân bị lừa cài đặt nên rất khó phát hiện. Nhiều sâu đã gây ra những thảm hoạ, ví dụ:

- Sâu Melissa (1999) có cơ chế lừa để lây rất hiệu quả đã từng gây thiệt hại hơn 1 tỉ đô la.
- Sâu Code Red (2001) lợi dụng một khiếm khuyết bảo mật của Windows, chiếm quyền các máy chủ Windows, trong 10 ngày đã gây thiệt hại khoảng 2 tỉ đô la.
- Sâu WannaCry (2017) tống tiền bằng cách mã hoá toàn bộ thông tin có trên đĩa cứng và đòi tiền chuộc mới cho phần mềm hoá giải.
- Một số loại virus hay worm được phát tán rộng rãi, trở thành các đội quân ngầm, mỗi khi nhận được lệnh là truy cập đồng thời vào một máy chủ định trước, gây quá tải, làm tê liệt máy chủ. Hình thức tấn công này gọi là tấn công từ chối dịch vụ (Denial of Service – DOS) rất khó chống.

c) Phòng chống phần mềm độc hại

Để phòng ngừa phần mềm độc hại, điều quan trọng đầu tiên là cần thận trọng khi chép các tệp chương trình hay dữ liệu vào máy từ ổ cứng rời, thẻ nhớ hoặc tải về từ mạng. Rất nhiều phần mềm bẻ khoá cho lấy tự do trên mạng là các phần mềm bị gắn mã độc một cách cố ý.

Để tránh bị lừa, không mở các liên kết trong email hay tin nhắn mà không biết rõ có an toàn hay không. Ngay cả khi nhận thư từ hộp thư của bạn bè, nếu thấy có yêu cầu nháy vào liên kết thì tốt nhất hãy liên lạc qua một phương tiện khác, ví dụ gọi điện cho bạn để xác minh trước khi tải xuống.

Đừng để lộ mật khẩu các tài khoản của mình để tránh bị kẻ xấu chiếm quyền, mạo danh.

Ngoài ra, hãy sử dụng các phần mềm phòng chống các phần mềm độc hại.

- Phần mềm độc hại là phần mềm viết ra với ý đồ xấu, gây ra các tác động không mong muốn.
- Virus và worm là các phần mềm độc hại có khả năng lây nhiễm; Trojan là phần mềm nội gián để ăn cắp thông tin và chiếm đoạt quyền trên máy.
- Để phòng ngừa phần mềm độc hại, không lấy từ trên mạng hoặc sao chép qua các thiết bị nhớ những phần mềm mà mình không biết rõ. Khi nhận được email hay tin nhắn có liên kết, nếu không rõ về nguồn gốc thì không nên mở.
- Hãy sử dụng các phần mềm chống phần mềm độc hại để bảo vệ máy tính.

Em hãy tổng kết về ba loại phần mềm độc hại theo bảng sau:

	Tính hoàn chỉnh	Cơ chế lây nhiễm	Tác hại
Virus	?	?	?
Trojan	?	?	?
Worm	?	?	?

THỰC HÀNH

Dùng phần mềm phòng chống virus Windows Defender.

Có hàng trăm phần mềm phòng chống virus như Kapersky, AVG, Avast, McAfee, Norton Antivirus, Panda hay một phần mềm của Việt Nam là BKAV. Thực tế, các phần mềm này không chỉ phát hiện và diệt virus mà còn phòng chống nhiều nguy cơ làm mất an toàn khác như kiểm tra các tệp tải về, cảnh báo truy cập các website có mã độc,… Chính vì thế, các phần mềm này còn được gọi là Firewall (bức tường lửa) với ý nghĩa ngăn chặn các nguy cơ từ ngoài.

Bài thực hành này giới thiệu sử dụng phần mềm Defender Firewall được tích hợp sẵn trong hệ điều hành Windows phiên bản 10, tự động chạy ngầm để bảo vệ các máy tính dùng hệ điều hành Windows. Defender tự động cập nhật các mẫu virus mới mỗi khi hệ điều hành được cập nhật (theo tiện ích Windows Update).

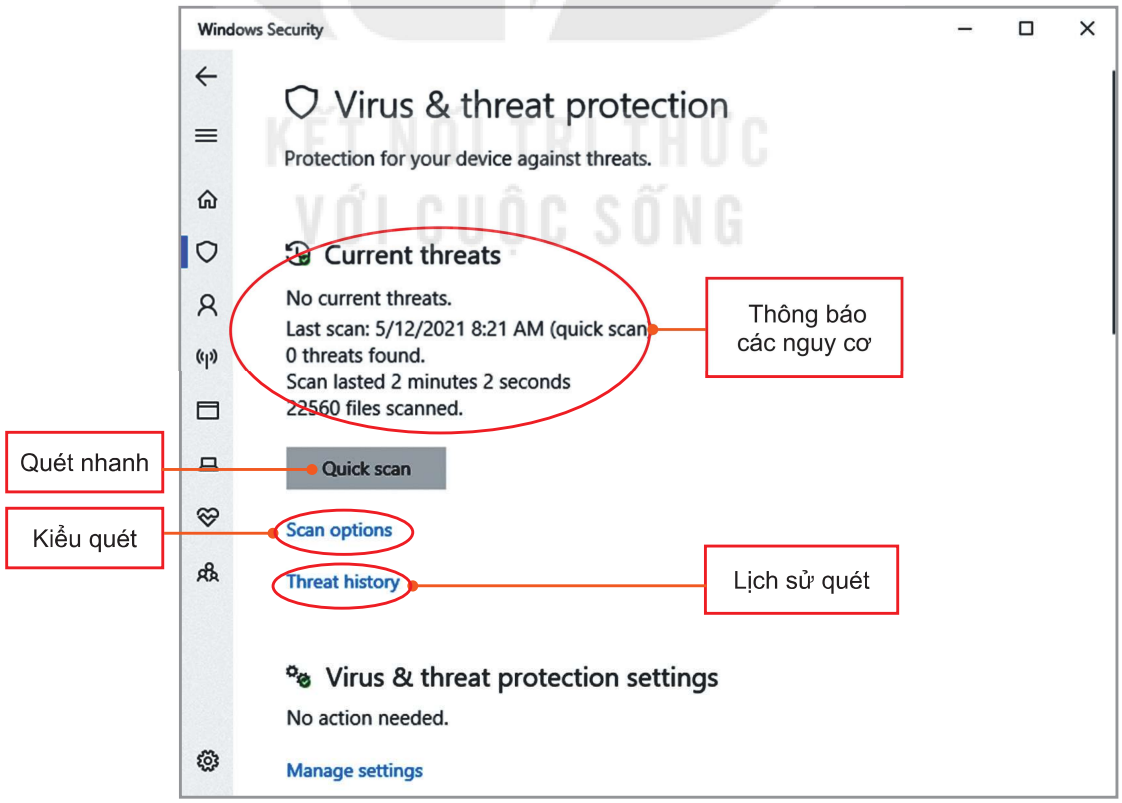
Nhiệm vụ: Thiết lập các lựa chọn và quét virus với Windows Defender.

Hướng dẫn.

Bước 1: Từ nút **Start** chọn **Setting** (có thể dùng cách nhanh hơn là gõ chữ "Defender" vào hộp tìm kiếm nằm ở thanh trạng thái), màn hình xuất hiện tương tự như sau:

Hình 9.1. *Truy cập chức năng bảo vệ chống virus*

Bước 2: Thực hiện các thao tác như hướng dẫn ở Hình 9.1 sẽ xuất hiện cửa sổ như Hình 9.2.



Hình 9.2. *Chức năng bảo vệ chống virus và các nguy cơ*

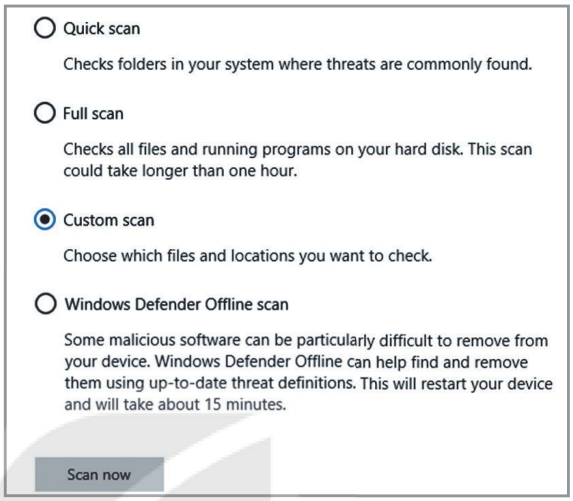
Current threats: thống kê những nguy cơ tìm thấy trong thời gian gần nhất khi các tệp được quét kiểm tra.

Quick scan: nếu nháy vào nút này phần mềm sẽ quét tất cả các tệp chương trình ở các thư mục mà virus thường lây nhiễm.

Bước 3: Quét virus. Ta có thể nháy vào nút Quick scan hoặc vào lựa chọn Scan options để lựa chọn kiểu quét và quét.

Trong Scan options, ta có thể lựa chọn các kiểu quét, có bốn lựa chọn:

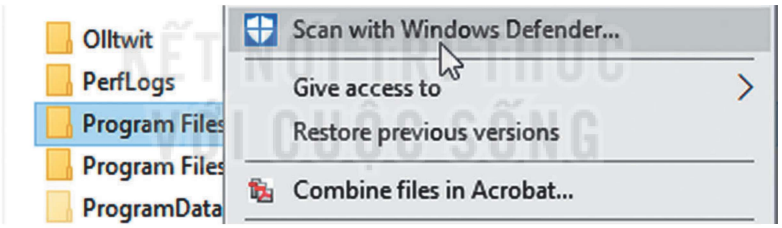
1. Quét nhanh (Quick scan): quét các thư mục có nguy cơ cao.
2. Quét hết (Full scan): quét tất cả các ổ đĩa.
3. Quét theo yêu cầu (Custom scan), chỉ quét trên một thư mục nào đó. Khi đó, Defender sẽ yêu cầu chỉ ra thư mục em muốn quét.
4. Quét ngoại tuyến (Windows Defender Offline scan). Chúng ta sẽ không bàn đến lựa chọn này vì nó là trường hợp đòi hỏi những hiểu biết rất sâu.



Hình 9.3. *Các lựa chọn trong scan options*

Sau khi chọn một lựa chọn, nháy nút Scan now và đợi kết quả.

Nếu đang làm việc ở thư mục mà muốn quét thư mục đó thì không cần truy cập vào Defender, ta có thể nháy nút phải chuột vào tên thư mục để xuất hiện bảng chọn tắt, chọn lệnh Scan with Microsoft Defender (Hình 9.4).



Hình 9.4. *Truy cập nhanh lệnh quét trên thư mục*

LUYỆN TẬP

1. Em hãy kể ra các nguy cơ mất an toàn khi tham gia các mạng xã hội.
2. Em hãy kể ra những trường hợp có thể bị nhiễm phần mềm độc hại và biện pháp phòng, chống tương ứng.

VẬN DỤNG

1. Em hãy tìm hiểu qua Internet các cách thức tấn công từ chối dịch vụ.
2. Em hãy tìm trên mạng thông tin về worm, kể một worm với tác hại của nó.