**CHỦ ĐỀ 2. MẠNG MÁY TÍNH VÀ INTERNET**

# **BÀI 9. AN TOÀN TRÊN KHÔNG GIAN MẠNG**

**A/ Bài học**

**1. MỘT SỐ NGUY CƠ TRÊN MẠNG**

-  Những nguy cơ trên Internet có thể gặp:

+ Tin giả và tin phản văn hóa

+ Lừa đảo trên mạng

+ Lộ thông tin cá nhân

+ Bắt nạt trên mạng

+ Nghiện mạng

- Các biện pháp bảo vệ thông tin cá nhân:

+ Không ghi chép thông tin cá nhân ở nơi người khác có thể đọc.

+ Giữa cho máy tính không bị nhiễm các phần mềm gián điệp.

+ Cẩn trọng khi truy cập mạng qua wifi công cộng.

- 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 từ kẻ bắt nạt.

+ 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 bằng chứng.

**2. PHẦN MỀM ĐỘC HẠI**

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

- Virus không phải là 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.

- Worm, sâu máy tính là phần mềm hoàn chỉnh, lây qua những lỗ hổng bảo mật của hệ điều hành, hoặc lừa người dùng cài đặt vào máy của nạn nhân.

- Trojan là phần mềm nội gián và có thể mang những tên khác nhau như:

+ Spyware: có mục đích ăn trộm thông tin để chuyển ra bên ngoài.

+ Keylogger: 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, thực hiện được mọi hoạt động kể cả xóa dấu vết.

**b. Tác hại của phần mềm độc hại**

- Không chỉ gây khó chịu, mà còn có thể làm hỏng các phần mềm khác trong máy tính, xóa dữ liệu hay làm tê liệt hệ thống máy tính.

- Một số thiệt hại lớn do phần mềm độc hại gây ra:

+ Sâu Melissa (1999) cơ chế lừa để lây gây thiệt hại hơn 1 tỉ đô la.

+ Sâu Code Red (2001) lợi dụng khiếm khuyến bảo mật Windows, chiếm quyền các máy chủ trong 10 ngày gây thiệt hại khoảng 2 tỉ đô.

**c. Phòng chống phần mềm độc hại**

- Để phòng ngừa độc hại cần thận trọng khi chép các tệp chương trình hay dữ liệu vào máy từ ổ cứng rời, thẻ nhớ hoặc tải từ mạng.

- Để tránh bị lừa, không mở các liên kết trong email hay tin nhắn mà không biết an toàn hay không.

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

- Sử dụng các phần mềm phòng chống các phần mềm độc hại.

**THỰC HÀNH**

**Dùng phần mềm phòng chống virus Windows Defender.**

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

**Hướng dẫn:**

Bước 1. Từ nút Start chọn Setting, màn hình xuất hiện tương tự như sau:



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



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

**Quick scan**: phần mềm sẽ quét tất cả các tệp chương trình ở các thư mục mà virus thường lây nhiễm.

Bước 3. Quét virus. Nháy vào **Quick scan** hoặc lựa chọn **Scan options** để lựa cọn kiểu quét và quét.

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

- Quét nhanh: quét các thư mục có nguy cơ cao.

- Quét hết: quét tất cả các ô đĩa.

- Quét theo yêu cầu: chỉ quét trên thư mục nào mà em muốn quét.

- Quét ngoại tuyến: Chúng ta không bàn đến lựa chọn này vì đòi hỏi hiểu biết sâu.



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, ta nháy chuột vào tên thư mục xuất hiện bảng chọn tắt, chọn lệnh **Scan with Microsoft Defrender**.



**B/ Trắc nghiệm**

**Câu 1.**Khi truy cập mạng, mọi người có thể bị kẻ xấu lợi dụng, ăn cắp thông tin hay không?

**A.** Có.

**B.** Không.

**C.** Tùy trường hợp.

**D.** Không thể.

**Câu 2.**Biện pháp nào bảo vệ thông tin cá nhân **không** đúng khi truy cập mạng?

**A.** Không ghi chép thông tin cá nhân ở nơi người khác có thể đọc.

**B.** Giữ máy tính không nhiễm phần mềm gián điệp.

**C.** Cẩn trọng khi truy cập mạng qua wifi công cộng.

**D.** Đăng tải tất cả thông tin cá nhân lên mạng cho mọi người cùng biết.

**Câu 3.**Biện pháp nào phòng chống hành vi bắt nạt trên mạng?

**A.** Không kết bạn dễ dãi trên mạng.

**B.** Không trả lời thư từ với kẻ bắt nạt trên diễn đàn.

**C.** Chia sẻ với bố mẹ, thầy cô.

**D.** Cả 3 ý trên.

**Câu 4.**Theo cơ chế lây nhiễm, có mấy loại phần mềm độc hại?

**A.** 3.

**B.** 2.

**C.** 4.

**D.** 5.

**Câu 5.**Tác động của virus đối với người dùng và máy tính?

**A.** Gây khó chịu với người dùng.

**B.** Làm hỏng phần mềm khác trong máy.

**C.** Xóa dữ liệu, làm tê liệt máy tính.

**D.** Cả A, B, C.

**Câu 6.**Bản chất của virus là gì?

**A.** Các phần mềm hoàn chỉnh.

**B.** Các đoạn mã độc.

**C.** Các đoạn mã độc gắn với một phần mềm.

**D.** Là sinh vật có thể thấy được.

**Câu 7.**Bản chất của Worm, sâu máy tính là gì ?

**A.** Phần mềm hoàn chỉnh.

**B.** Một đoạn mã độc.

**C.** Nhiều đoạn mã độc.

**D.** Cả 3 ý trên.

**Câu 8.**Trojan gọi là gì?

**A.** Phần mềm độc.

**B.** Mã độc.

**C.** Ứng dụng độc.

**D.** Phần mềm nội gián.

**Câu 9.**Phần mềm độc hại viết ra có tác dụng gì?

**A.** Dùng để hỗ trợ các ứng dụng.

**B.** Dùng với ý đồ xấu, gây ra tác động không mong muốn.

**C.** Cải thiện khả năng xử lí của máy tính.

**D.** Cả 3 ý trên.

**Câu 10.**Có mấy kiểu quét trong Window Defender?

**A.** 1.

**B.** 2.

**C.** 3.

**D.** 4.