1. ĐỀ MỤC 1: Virus máy tính và cách phòng chống.

Sau khi hoàn thành nội dung này, người sử dụng nắm được:

- Khái niệm về virus máy tính.
- Lịch sử phát triển của virus máy tính.
- Cách phân loại virus máy tính.
- Phương thức hoạt động của virus máy tính.
- Cách phòng chống virus máy tính.
- Một số phần mềm diệt virus thông dụng.

1.1. Khái niệm virus máy tính.

Virus máy tính (thường gọi tắt là virus) là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác (**file**, ổ đĩa cứng, **USB**, máy tính, vv…).

Trước đây, virus thường được viết bởi những người am hiểu về lập trình muốn chứng tỏ khả năng của mình nên khi đó virus thường có các hành động như: Làm cho một chương trình hoạt động không đúng, làm hỏng các **files,** xóa dữ liệu, làm hỏng ổ cứng hoặc gây ra những trò đùa khó chịu khác, vv…

Tuy nhiên, những virus mới được viết trong thời gian gần đây không chỉ còn thực hiện các trò đùa hay sự phá hoại đối máy tính của nạn nhân bị lây nhiễm nữa, mà đa phần hướng đến việc lấy cắp các thông tin cá nhân nhạy cảm (các mã số thẻ tín dụng, ngân hàng, mật khẩu, vv…), sử dụng máy tính bị nhiễm virus để quảng cáo bất hợp pháp, gửi thư rác, mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển hoặc các hành động khác nhằm có lợi cho người phát tán virus**.**

Trên 90% số virus đã được phát hiện là nhằm vào hệ thống sử dụng hệ điều hành **Microsoft Windows** bởi hệ điều hành này được sử dụng nhiều nhất trên thế giới. Do tính thông dụng của hệ điều hành **Microsoft Windows** nên các tin tặc thường tập trung hướng vào chúng nhiều hơn là các hệ điều hành khác.

1.2. Lịch sử phát triển của virus máy tính.

Có nhiều quan điểm khác nhau về lịch sử virus máy tính. Ở đây chỉ nêu tóm tắt và khái quát những điểm chung nhất về lịch sử phát triển của virus máy tính và sự ra đời của những virus có ảnh hưởng lớn nhất đến người sử dụng.

Năm 1986: Xuất hiện loại virus đầu tiên tại Pakistan tên là **Brain**, nó lây nhiễm trên máy tính thông qua đĩa mềm trên hệ điều hành **MS-DOS.** Tuy nhiên, đây không phải là loại virus phá hoại, tác giả là anh em nhà Alvi chỉ chèn tên tuổi và thông tin cá nhân của mình vào trong mã của virus.

Năm 1987: Xuất hiện virus **Stoned** do một sinh viên ở New Zealand tạo ra. Chỉ trong 2 năm sau đó là năm 1988, 1989, virus **Stoned** đã gây ảnh hưởng lớn ở khắp New Zealand và Australia.

Năm 1990: Xuất hiện virus **Form** có nguồn gốc từ Thụy Sĩ và tới nay vẫn chưa rõ ai là tác giả. Đây cũng là một trong những loại virus nguy hiểm nhất trong lịch sử máy tính.

Năm 1991: Xuất hiện virus **Michelangelo** ra đời muộn hơn **Form** 1 năm, virus này có nguồn gốc từ New Zealand.

Năm 1992: Xuất hiện virus **VCL** có nguồn gốc từ Mỹ . Trên thực tế, **VCL (Virus Creation Laboratory**) là một công cụ với giao diện đơn giản, cho phép người sử dụng tự tạo ra virus.

Năm 1994: Xuất hiện virus **Monkey** tại Canada, virus **Monkey** là chương trình đầu tiên có khả năng tự giấu mình trước sự phát hiện của người dùng.

Năm 1995: Xuất hiện virus **Concept** tại Mỹ, **Concept** là loại virus đầu tiên chứng tỏ khả năng xâm nhập được vào các **files** của chương trình soạn thảo văn bản **Microsoft Word.**

Năm 1999: Xuất hiện virus **Happy99**, đây là biến thể virus **e-mail** đầu tiên, nhưng không rõ nguồn gốc. Mặc dù đã lây lan nhanh chóng tới hàng triệu máy tính, nhưng **Happy99** với thông điệp "Chúc mừng năm mới 1999" không gây ra thiệt hại đáng kể nào. Cũng trong năm này, xuất hiện virus **Melissa** có nguồn gốc tại Mỹ, loại virus này được đặt theo tên một nữ vũ công nổi tiếng.

Năm 2000: Xuất hiện virus **Love Letter.** Đây là một trong những loại virus có mức độ lây lan khủng khiếp nhất trong lịch sử công nghệ. **Love Letter** hay **I Love You** có nguồn gốc từ Philippines. Những máy tính bị lây nhiễm virus này sẽ tự gửi đến danh sách bạn có trong **e-mail** những **e-mail** với tiêu đề **I Love You**, đính kèm theo những **files word** có chứa mã độc. Không chỉ có vậy, loại virus này còn phá hoại máy tính của nạn nhân. Hơn 50 triệu máy tính trên toàn cầu đã bị ảnh hưởng bởi virus **Love Letter**, thiệt hại lên tới hàng tỉ **USD**.

Năm 2001: Xuất hiện virus **Code Red** cũng không rõ nguồn gốc phát sinh như **Happy99**, đây là loại sâu tự động phát tán mà không cần quan tâm tới việc có người dùng tác động hay không.

Năm 2003: Xuất hiện virus **Slammer,** là một trong những loại virus có tốc độ lan truyền kỉ lục, với 75 ngàn máy tính bị lây nhiễm chỉ sau 10 phút. **Slammer** đã làm sập hệ thống máy **ATM** của ngân hàng Mỹ và mạng lưới 911 tại Seatles (Mỹ). Cũng trong năm này đã xuất hiện virus **Sobig** nhưng không rõ nguồn gốc xuất xứ. Một điểm tương đồng nữa là **Sobig** lây lan tới hàng triệu máy tính chỉ trong vòng vài giờ sau khi xuất hiện. Năm 2003 cũng đánh dấu sự ra đời virus đầu tiên được tạo ra với mục đích lợi nhuận là virus **Fizzer**, nó lây nhiễm thông qua các **files** đính kèm trên **e-mail**. Một máy tính sau khi bị nhiễm virus **Fizzer** có thể bị tin tặc đánh cắp quyền điều khiển và đưa vào các mạng lưới **botnet** hoặc sử dụng để gửi đi các **e-mail spam.** Ngoài ra, virus **Cabir** cũng được tạo ra trong năm này tại Philippines, **Cabir** là loại sâu điện thoại đầu tiên trong lịch sử.

Năm 2004: Xuất hiện virus **MyDoom**, loại virus này có nguồn gốc từ Nga đã được phát tán qua **e-mail** và mạng **Kazaa P2P**. Cũng trong năm này, virus **Sasser** đã xuất hiện tại Mỹ, virus **Sasser** đã đánh sập hệ thống mạng từ Australia đi Hồng Kông và Anh quốc. Năm 2004 cũng đánh dấu sự ra đời của virus **SDBot** nhưng chưa rõ nguồn gốc xuất xứ, đây là loại **trojan** có khả năng chọc thủng được mọi tuyến phòng thủ thông thường trên máy tính.

Năm 2005: Xuất hiện virus **HaxDoor,** thực chất là một loại **rootkit** có khả năng che giấu các chương trình gây hại trước mắt người sử dụng máy tính. Cũng trong năm này, virus **Sony rootkit**, một loại **rootkit** khác có nguồn gốc xác thực ở Mỹ và Anh. Hãng đĩa nhạc **Sony BMG** đã tích hợp 1 loại phần mềm trên các đĩa của mình, cho phép tự động cài đặt trên các máy tính đọc đĩa của **Sony BMG.** Mặc dù đây là động thái bảo vệ bản quyền của **Sony BMG**, nhưng phần mềm này lại tạo lỗ hổng để các phần mềm gây hại khác xâm nhập vào hệ thống.

Năm 2007: Xuất hiện virus **Mebroot**, virus này đã đánh cắp hơn 500.000 tài khoản ngân hàng cùng các thông tin thanh toán trực tuyến. Cũng trong năm này đã xuất hiện virus **Storm Worm** thực sự gây ảnh hưởng khi đã phát tán đi những bức **e-mail** kiểu "230 người đã bị thiệt mạng trong một cơn bão ở Châu Âu".

Năm 2008: Xuất hiện virus **Conficker**, virus này đã nhanh chóng phát tán ra hàng triệu máy tính trên phạm vi toàn cầu. Đây cũng là một trong những loại virus có tốc độ lây lan khủng khiếp nhất trong lịch sử công nghệ máy tính toàn cầu.

Năm 2010: Xuất hiện virus **Stuxnet** đã tốn không ít "giấy mực" của các hãng bảo mật. Loại virus này có nguồn gốc từ Mỹ và Israel, nó thuộc vào hàng nguy hiểm nhất từ trước tới nay. Hãng bảo mật **F-Secure** cho rằng, một người phải mất hơn 10 năm

nghiên cứu liên tục mới có thể hoàn thành được **Stuxnet**. Điều đó cho thấy mức độ phức tạp của loại virus này. Virus **Stuxnet** phá hoại các hoạt động hạt nhân của Iran, nó có khả năng tác động tới quá trình vận hành các cơ sở hạt nhân tại Iran, ép các máy li tâm quay ở tốc độ không an toàn, khiến các máy này có thể bị hỏng hóc.

Năm 2011: Xuất hiện virus **W32.Sality.PE,** đây là loại virus lây lan nhiều nhất năm 2011. Lý do khiến **W32.Sality.PE** có thể lây lan tới hàng triệu máy tính vì virus này có khả năng sử dụng các giải thuật di truyền để tự động lai tạo, sinh ra các thế hệ virus "đời sau" F1, F2…Càng lây nhiễm lâu trên máy tính, virus này càng sinh ra nhiều biến thể với độ phức tạp càng cao khiến cho khả năng nhận dạng và bóc lớp của các phần mềm diệt virus càng trở nên khó khăn.

Ngày nay, với khả năng, trình độ cao của các tin tặc (**hacker**), virus có thể xâm nhập bằng cách bẻ gãy các rào cản an toàn của hệ điều hành hay xâm nhập vào các lỗ hổng bảo mật của các phần mềm, nhất là các chương trình thư điện tử, rồi từ đó lan tỏa khắp nơi theo các kết nối mạng hay qua thư điện tử. Do đó, việc truy tìm ra nguồn gốc phát tán virus sẽ càng trở nên khó khăn hơn nhiều.

Trong tương lai không xa virus sẽ bao gồm những điểm mạnh sẵn có, tấn công bằng nhiều cách thức, nhiều kiểu khác nhau, kết hợp với các thủ đoạn khác của phần mềm gián điệp (**spyware**), đồng thời nó có thể tấn công vào nhiều hệ điều hành khác nhau chứ không nhất thiết nhằm vào một hệ điều hành độc nhất như trong trường hợp của hệ điều hành **Microsoft Windows.**

1.3. Phân loại virus máy tính.

1.3.1. Virus file.

Là những virus lây vào những **files** chương trình, phổ biến nhất là trên hệ điều hành **Windows** như các **files** có đuôi mở rộng **.com, .exe, .bat, .pif, .sys**, vv...Khi chạy một **file** chương trình đã bị nhiễm virus cũng là lúc virus được kích hoạt và tiếp tục tìm các **files** chương trình khác trong máy tính để lây vào. Thực tế các loại virus lây **file** ngày nay cũng hầu như không còn xuất hiện và lây lan rộng nữa. Khi máy tính bị nhiễm virus lây **file**, tốt nhất người sử dụng nên sử dụng phần mềm diệt virus mới nhất để quét toàn bộ ổ cứng của mình và liên hệ với nhà cung cấp phần mềm diệt virus để được tư vấn, hỗ trợ.

1.3.2. Virus boot.

Ngày nay, hầu như không còn thấy virus **boot** trên các máy tính, vì virus **boot** có tốc độ lây lan rất chậm và không còn phù hợp với thời đại của **internet**. Tuy nhiên, virus **boot** vẫn là một phần trong lịch sử virus máy tính.

Khi máy tính được khởi động, một đoạn chương trình nhỏ trong ổ đĩa khởi động

sẽ được thực thi. Đoạn chương trình này có nhiệm vụ nạp vào hệ điều hành (**Windows, Linux** hay **Unix,** vv...). Sau khi nạp xong hệ điều hành, người sử dụng mới có thể bắt đầu sử dụng máy tính. Đoạn mã nói trên thường được để ở vùng trên cùng của ổ đĩa khởi động, và được gọi là "**boot sector**".

Virus **boot** là tên gọi dành cho những virus lây lan vào **boot sector**. Các virus **boot** sẽ được thi hành mỗi khi máy tính bị nhiễm khởi động, trước cả thời điểm hệ điều hành được nạp lên.

1.3.3. Virus macro.

Là loại virus lây vào những **files** văn bản (**Microsoft Word**), **files** bảng tính (**Microsoft Excel**) hay các **files** trình diễn (**Microsoft PowerPoint**) trong bộ **Microsoft Office**. **Macro** là tên gọi chung của những đoạn mã được thiết kế để bổ sung tính năng cho các **files** của **Microsoft Office**. Người sử dụng có thể cài đặt sẵn một số thao tác vào trong **macro**, và mỗi lần gọi **macro** là các phần cài sẵn lần lượt được thực hiện, giúp người sử dụng giảm bớt được công lặp đi lặp lại những thao tác giống nhau.

Ngày nay, trên thực tế các loại virus **macro** cũng gần như không còn xuất hiện.

1.3.4. Sâu máy tính (worm).

Sâu máy tính là một chương trình máy tính có khả năng tự nhân bản, tự tìm cách lan truyền qua hệ thống mạng (thường là qua hệ thống thư điện tử). Điểm cần lưu ý ở đây là ngoài tác động trực tiếp lên máy bị nhiễm, nhiệm vụ chính của **worm** là phá các mạng (**network**) thông tin, làm giảm khả năng hoạt động hoặc hủy hoại các mạng này. Trong khi virus máy tính bám vào và trở thành một phần của mã máy tính để có thể thi hành thì sâu máy tính là một chương trình độc lập không nhất thiết phải là một phần của một chương trình máy tính khác để có thể lây nhiễm. Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin có trên những máy tính có các đặc điểm chung như cùng hệ điều hành hoặc cùng chạy một phần mềm và được nối mạng với nhau.

Sâu máy tính thường mang theo phần mềm gián điệp để mở cửa sau trên các máy tính bị nhiễm. Các máy tính bị nhiễm được sử dụng bởi những người gửi thư rác hoặc giả danh địa chỉ trang **web**. Các cửa sau cũng có thể được các sâu máy tính khác khai thác nhằm mục đích có lợi cho tin tặc.

1.4. Phương thức hoạt động của virus máy tính.

1.4.1. Qua các thiết bị lưu trữ di động.

Trước đây đĩa mềm và đĩa **CD** chứa chương trình thường là phương tiện bị lợi dụng nhiều nhất để phát tán. Ngày nay khi đĩa mềm rất ít được sử dụng thì phương

thức lây nhiễm này chủ yếu từ các ổ **USB**, các ổ đĩa cứng di động hoặc các thiết bị giải trí kỹ thuật số.

1.4.2. Qua thư điện tử.

Khi mà thư điện tử (**e-mail**) được sử dụng rộng rãi trên thế giới thì virus chuyển hướng sang lây nhiễm thông qua thư điện tử thay cho các cách lây nhiễm truyền thống. Khi đã lây nhiễm vào máy tính nạn nhân, virus có thể tự tìm ra danh sách các địa chỉ thư điện tử sẵn có trong máy tính và tự động gửi đi hàng loạt (**mass mail**) cho những địa chỉ tìm thấy. Nếu các chủ nhân của các máy nhận được thư bị nhiễm virus mà không phát hiện được, tiếp tục để lây nhiễm vào máy tính, virus lại tiếp tục tìm đến các địa chỉ và gửi đi tiếp theo. Chính vì vậy số lượng phát tán có thể tăng theo cấp số nhân khiến cho trong một thời gian ngắn hàng triệu máy tính bị lây nhiễm.

Khi các phần mềm quản lý thư điện tử kết hợp với các phần mềm diệt virus có thể khắc phục được hành động tự gửi nhân bản hàng loạt để phát tán đến các địa chỉ khác trong danh bạ của máy nạn nhân thì người phát tán virus chuyển sang hình thức tự gửi thư phát tán virus bằng nguồn địa chỉ sưu tập được trước đó.

Phương thức lây nhiễm qua thư điện tử bao gồm:

- Lây nhiễm vào các **files** đính kèm theo thư điện tử (**attached mail**). Khi đó người dùng sẽ không bị nhiễm virus cho tới khi **file** đính kèm bị nhiễm virus được kích hoạt (do đặc điểm này các virus thường được "trá hình" bởi các tiêu đề hấp dẫn như quảng cáo bán hàng giá rẻ, phần mềm miễn phí, chương trình tặng quà, vv…).
- Lây nhiễm do mở một liên kết trong thư điện tử. Các liên kết trong thư điện tử có thể dẫn đến một trang **web** được cài sẵn virus, cách này thường khai thác các lỗ hổng của trình duyệt và hệ điều hành. Một cách khác, liên kết dẫn tới việc thực thi một đoạn mã, và máy tính có thể đã bị lây nhiễm virus.
- Lây nhiễm ngay khi mở để xem thư điện tử: Cách này vô cùng nguy hiểm bởi chưa cần kích hoạt các **files** hoặc mở các liên kết, máy tính đã có thể bị lây nhiễm virus. Cách này cũng thường khai thác các lỗ hổng bảo mật của hệ điều hành.

1.4.3. Qua mạng internet.

Với sự phát triển rộng rãi của **internet**, hiện nay các hình thức lây nhiễm virus qua mạng **internet** đã trở thành các phương thức chính của virus ngày nay. Điển hình là các hình thức lây nhiễm virus và phần mềm độc hại thông qua **internet** như sau:

- Lây nhiễm thông qua các **files** tài liệu, phần mềm: Là cách lây nhiễm cổ điển, nhưng thay thế các hình thức truyền **file** theo cách cũ (đĩa mềm, **USB**, thiết bị lưu trữ di động) bằng cách tải từ mạng **internet**, trao đổi, thông qua các phần mềm, vv...

- Lây nhiễm khi đang truy cập các trang **web** được cài đặt virus (theo cách vô tình hoặc cố ý), các trang **web** có thể có chứa các mã độc gây lây nhiễm virus và phần mềm độc hại vào máy tính của người sử dụng khi truy cập vào các trang **web** đó.

- Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba. Tin tặc có thể lợi dụng các lỗi bảo mật của hệ điều hành, phần mềm sẵn có trên hệ điều hành (ví dụ chương trình nghe nhạc **Windows media player**) hoặc lỗi bảo mật của các phần mềm của hãng thứ ba (ví dụ chương trình đọc **file Acrobat reader**) để lây nhiễm virus hoặc chiếm quyền kiểm soát máy tính nạn nhân khi mở các **files** liên kết với các phần mềm này.

1.4.4. Biến thể của virus.

Một hình thức trong cơ chế hoạt động của virus là tạo ra các biến thể của chúng. Biến thể của virus là sự thay đổi mã nguồn nhằm các mục đích tránh sự phát hiện của phần mềm diệt virus hoặc làm thay đổi hành động của nó.

Một số loại virus có thể tự tạo ra các biến thể khác nhau gây khó khăn cho quá trình phát hiện và tiêu diệt chúng. Một số biến thể khác xuất hiện do sau khi virus bị nhận dạng bởi các phần mềm diệt virus, chính tác giả của virus hoặc các tin tặc khác (biết được mã của chúng) đã viết lại, nâng cấp hoặc cải tiến chúng để tiếp tục phát tán.

1.4.5. Khả năng vô hiệu hóa phần mềm diệt virus.

Một số virus có khả năng vô hiệu hoá hoặc can thiệp vào hệ điều hành làm tê liệt phần mềm diệt virus. Sau hành động này chúng mới tiến hành lây nhiễm và tiếp tục phát tán. Một số khác lây nhiễm chính vào phần mềm diệt virus (tuy khó khăn hơn) hoặc ngăn cản sự cập nhật của các phần mềm diệt virus. Kể cả cài lại hệ điều hành và cài lại phần mềm diệt virus.

Các cách thức này không quá khó nếu như chúng nắm rõ được cơ chế hoạt động của các phần mềm diệt virus và được lây nhiễm hoặc phát tán trước khi hệ thống khởi động các phần mềm này. Chúng cũng có thể sửa đổi **file host** của hệ điều hành Windows để người sử dụng không thể truy cập vào các **website** và phần mềm diệt virus không thể liên lạc với máy chủ virus của mình để cập nhật.

1.5. Cách phòng chống virus.

Không thể khẳng định chắc chắn là bảo vệ được máy tính an toàn 100% trước những hiểm hoạ virus và các mã độc, nhưng người sử dụng có thể hạn chế đến mức tối đa và có các biện pháp bảo vệ dữ liệu của mình.

1.5.1. Cách nhận biết cơ bản.

- Máy tính chạy chậm hơn so với trước đây, truy xuất dữ liệu chậm, không cho cài đặt, gỡ bỏ phần mềm, không mở được cửa sổ **task manager** (**Ctrl + Alt + Delete**), vv…

- Các trang **web** quảng cáo hoặc trang **web** lạ tự động hiện ra (**pop up**), màn hình **desktop** bị thay đổi giao diện (thường chuyển sang màu đen).

- Duyệt **web** chậm, nội dung các trang **web** hiển thị trên trình duyệt chậm.

- Các **files** lạ tự động sinh ra khi mở ổ đĩa **USB** (**autorun.inf, new folder.exe…**). Xuất hiện **file** có phần mở rộng .**exe** có tên trùng với tên các thư mục.

- Góc phải màn hình có một biểu tượng nhỏ cùng với thông báo: “ **your computer is infected** ” hay “ **virus alert** ”, gần giống với khuyến cáo bật **firewall** hoặc yêu cầu thực hiện cài đặt **firewall**,…

- Virus có thể giả danh một phần mềm diệt virus nào đó, chương trình này có giao diện gần tương tự với phần mềm diệt virus và yêu cầu gửi thông tin để đăng ký sử dụng phần mềm.

- Đưa ra khuyến cáo máy tính đã bị nhiễm virus, đưa ra đường liên kết (**link**) hướng dẫn người sử dụng truy cập đến trang **web** đó để diệt được loại virus này (thực chất là trang **web** giả mạo chứa virus hoặc mã độc).

- Khi gõ tìm một địa chỉ trên trình duyệt **web** và chọn nút "**enter**" để bắt tìm kiếm thì trang tìm kiếm thường dùng bị thay bởi một trang tìm kiếm lạ.

- Người sử dụng tìm thấy những tên địa chỉ lạ trong danh sách "**favorites**" của trình duyệt **web** mặc dù người sử dụng chưa hề đặt vào trong mục này.

- Một công cụ tìm kiếm (**search toolbar**) hay công cụ trên trình duyệt (**browser toolbar**) xuất hiện mặc dù người sử dụng không ra lệnh để cài đặt nó và không thể xoá chúng hoặc chúng xuất hiện trở lại sau khi xoá.

- Gõ các địa chỉ quen biết vào trình duyệt mà chỉ nhận được trang trống không hay bị báo lỗi "**404 Page cannot be found**".

- Ở thời điểm mà người sử dụng không làm gì với mạng mà vẫn thấy đèn gửi/nhận chớp sáng trên **modem** hay "**board band modem**" giống như là khi đang tải một phần mềm về máy hay là các biểu tượng "**network/modem**" nhấp nháy nhanh khi mà người sử dụng không hề nối máy tính vào mạng.

- Ngoài ra, có nhiều virus chạy ẩn cùng với hệ thống mà không có dấu hiệu đặc biệt hay bất thường nên người sử dụng rất khó để nhận biết máy tính có đang bị nhiễm virus hay không.

1.5.2. Sử dụng phần mềm diệt virus.

Để đảm bảo an toàn cho máy tính, sau khi cài đặt xong hệ điều hành người sử dụng nên chọn một phần mềm diệt virus tốt để cài đặt ngay trước khi kết nối vào hệ

thống mạng, trước khi chia sẻ và sử dụng thiết bị lưu trữ ngoài (**USB**, ổ cứng cắm ngoài,…). Sau đó sử dụng phần mềm diệt virus đó thường xuyên, lâu dài cho máy tính. Phần mềm diệt virus tốt phải đáp ứng được đầy đủ các tiêu chí: Là phần mềm có bản quyền, cập nhật phiên bản mới thường xuyên để có khả năng nhận biết nhiều loại virus mới, có hỗ trợ kỹ thuật trực tiếp từ nhà sản xuất khi có sự cố liên quan tới virus.

STT	Tên virus
1	W32.Sality.PE
2	W32.AutoRunUSB.Worm
3	W32.Vetor.PE
4	W32.StuxnetQKY.Trojan
5	W32.StarterYY.Trojan
6	W32.Kawin.Trojan
7	W32.FakeUserinitIconF.Fam.Worm
8	X97M.XFSic
9	W32.SecretCNC.Heur
10	W32.SalDropFamA.Worm
11	W32.InjectAdwaredDwnMainA.Trojan
12	W32.Tmgrtext.PE
13	W32.CmVirus.Trojan
14	W32.SalDropE.Worm
15	W32.SysAntiA.Worm

Hình 1: Danh sách virus lây lan nhiều nhất năm 2011 (nguồn Bkav).

1.5.3. Sử dụng tường lửa.

Tường lửa (**firewall**): Là thiết bị phần cứng hoặc phần mềm hoạt động trong môi trường máy tính nối mạng, là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan lập ra nhằm ngăn chặn người dùng mạng **internet** truy cập các thông tin không mong muốn hoặc ngăn chặn người dùng từ bên ngoài truy cập các thông tin bảo mật nằm trong mạng nội bộ.

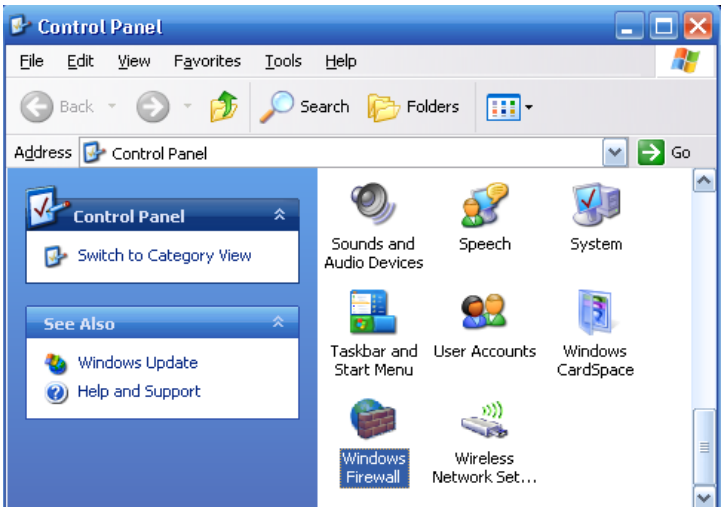
Việc sử dụng tường lửa giúp bảo vệ máy tính trước virus và các phần mềm độc hại. Khi sử dụng tường lửa, các thông tin vào và ra đối với máy tính được kiểm soát một cách vô thức hoặc có chủ ý. Nếu một phần mềm độc hại đã được cài vào máy tính có hành động kết nối ra **internet** thì tường lửa có thể cảnh báo giúp người sử dụng loại bỏ hoặc vô hiệu hoá chúng. Tường lửa giúp ngăn chặn các kết nối đến không mong muốn để giảm nguy cơ bị kiểm soát máy tính ngoài ý muốn hoặc cài đặt vào các chương trình độc hại hay virus máy tính.

Sử dụng tường lửa bằng phần cứng nếu người sử dụng kết nối với mạng **internet** thông qua một **modem** có chức năng này. Thông thường ở chế độ mặc định của nhà sản xuất thì chức năng tường lửa bị tắt, người sử dụng có thể truy cập vào **modem** để

bật chức năng tường lửa. Sử dụng tường lửa bằng phần cứng không phải tuyệt đối an toàn bởi chúng thường chỉ ngăn chặn kết nối đến trái phép, do đó cần kết hợp sử dụng tường lửa phần cứng cùng với các phần mềm tường lửa.

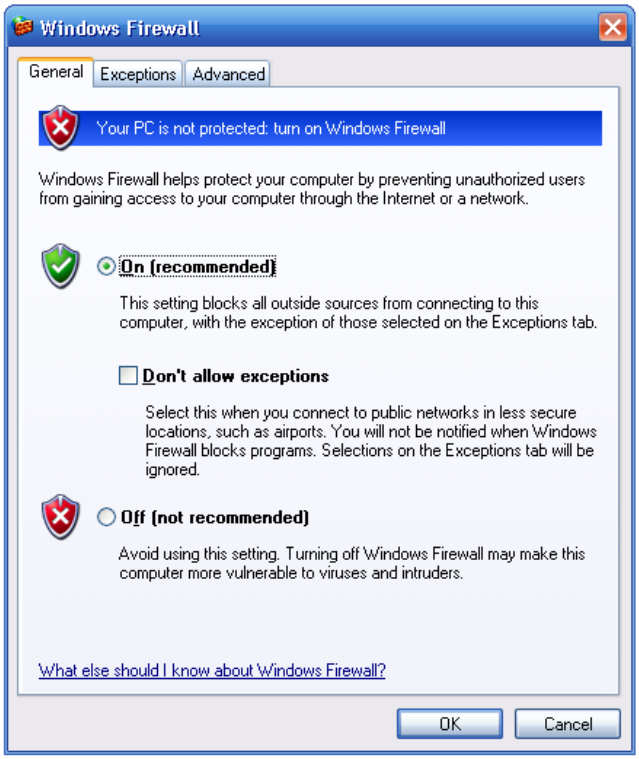
Sử dụng tường lửa bằng phần mềm: hệ điều hành **Windows** đã được tích hợp sẵn tính năng tường lửa bằng phần mềm nhằm bảo vệ dữ liệu và máy tính, để kích hoạt tính năng này người sử dụng làm như sau:

- Vào **Start \ Control Panel \ Windows Firewall**



Hình 2: Tính năng tường lửa.

- Sau khi chọn xuất hiện hộp thoại **Windows Firewall**. Trong thẻ **General** người sử dụng chọn **On (recommended)** sau đó chọn **OK.**

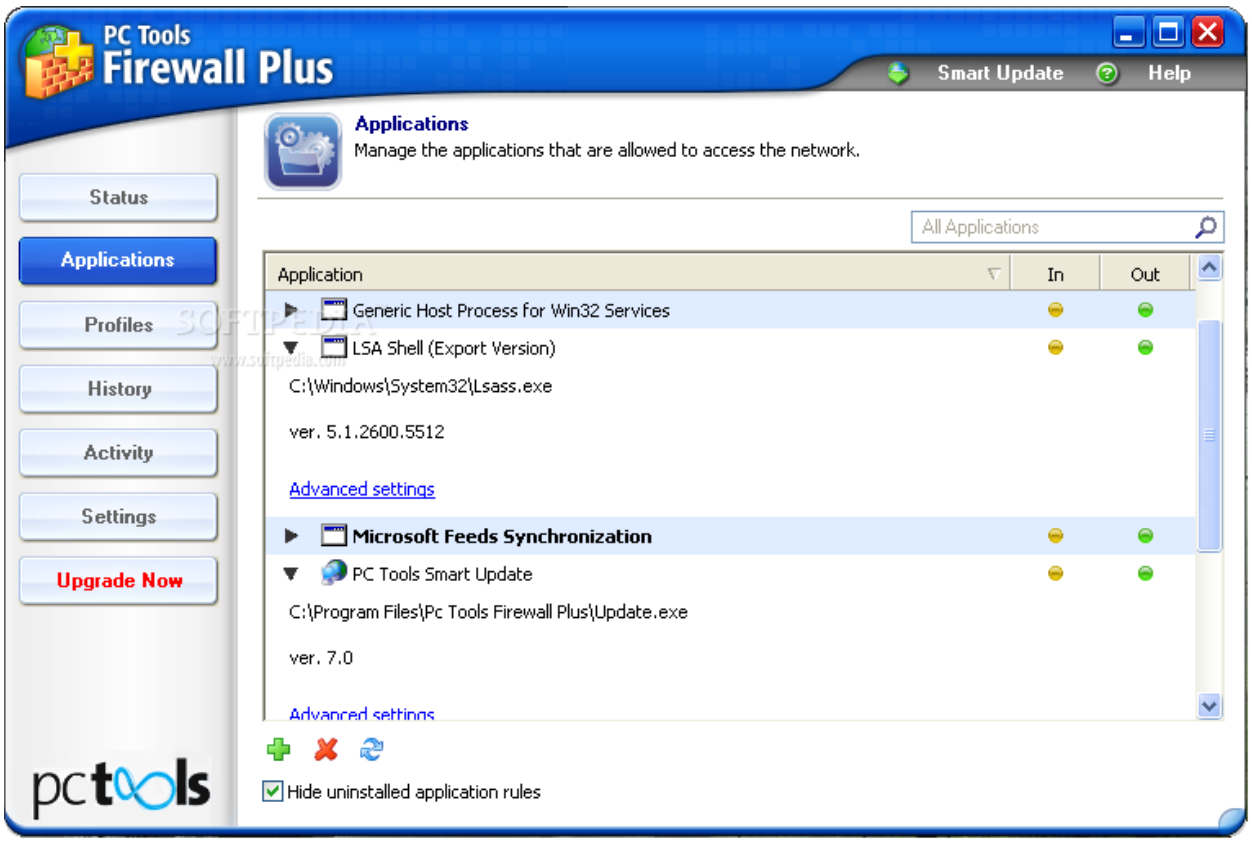


Hình 3: Bật tính năng Firewall trong Microsoft Windows XP.

Ngoài những cách trên, người sử dụng còn có thể sử dụng phần mềm tường lửa ngoài để cài đặt và bảo vệ máy tính trước virus, các phần mềm độc hại, chống **spam**, vv... Hiện nay có nhiều phần mềm tường lửa hỗ trợ cho việc này, gồm cả bản trả phí hoặc miễn phí.

Hình 4: Phần mềm Online Armor Free Firewall.

Hình 5: Phần mềm ZoneAlarm Free Firewall.



Hình 6: Phần mềm PC Tools Firewall Plus.

Hình 7: Phần mềm Comodo Firewall Personal

Hình 8: Phần mềm Outpost Pro Security Suite.

1.5.4. Cập nhật các bản sửa lỗi của hệ điều hành.

Hệ điều hành **Windows** (chiếm đa số người sử dụng) thường bị phát hiện các lỗi bảo mật chính bởi sự thông dụng của nó. Tin tặc có thể lợi dụng các lỗi bảo mật để chiếm quyền điều khiển hoặc phát tán virus và các phần mềm độc hại. Người sử dụng luôn cần cập nhật các bản vá lỗi của hệ điều hành **Windows** thông qua trang web **Microsoft update** (cho việc nâng cấp tất cả các phần mềm của hãng Microsoft) hoặc **Windows update** (chỉ cập nhật riêng cho hệ điều hành **Windows**). Cách tốt nhất hãy đặt chế độ nâng cấp (sửa chữa) tự động (**Automatic updates**) của hệ điều hành **Windows**. Tính năng này chỉ hỗ trợ đối với các hệ điều hành **Windows** có bản quyền hợp pháp.

1.5.5. Vận dụng kinh nghiệm sử dụng máy tính.

Cho dù sử dụng phần mềm diệt virus và các phương thức nêu trên thì máy tính vẫn có khả năng bị lây nhiễm virus và các phần mềm độc hại bởi mẫu virus mới nếu chưa được cập nhật kịp thời phần mềm diệt virus. Người sử dụng máy tính cần sử dụng triệt để các chức năng, ứng dụng sẵn có trong hệ điều hành và các kinh nghiệm khác để bảo vệ cho hệ điều hành và dữ liệu của mình như sau:

- Phát hiện sự hoạt động khác thường của máy tính: Đa phần người sử dụng máy tính không có thói quen cài đặt, gỡ bỏ phần mềm hoặc thường xuyên làm hệ điều hành thay đổi, có nghĩa là sử dụng máy tính ổn định. Người sử dụng có thể nhận biết được

sự thay đổi khác thường của máy tính. Mọi hoạt động khác thường này nếu không phải do phần cứng gây ra thì cần nghi ngờ sự xuất hiện của virus. Ngay khi có nghi ngờ, cần kiểm tra bằng cách cập nhật dữ liệu mới nhất cho phần mềm diệt virus hoặc thử sử dụng một phần mềm diệt virus khác để quét toàn bộ hệ thống.

- Kiểm soát các ứng dụng đang hoạt động: Người sử dụng kiểm soát sự hoạt động của các phần mềm trong hệ thống thông qua **task manager** bằng cách ấn tổ hợp phím **Ctrl + Alt + Delete** hoặc các phần mềm của hãng thứ ba để biết một phiên làm việc bình thường hệ thống thường nạp các ứng dụng nào, chúng chiếm dung lượng bộ nhớ bao nhiêu, chiếm **CPU** bao nhiêu, tên **file** hoạt động là gì, vv...ngay khi có điều bất thường của hệ thống (dù chưa có biểu hiện của sự nhiễm virus) cũng có thể có sự nghi ngờ và có hành động phòng ngừa hợp lý. Tuy nhiên cách này đòi hỏi một sự am hiểu nhất định của người sử dụng.

- Loại bỏ một số tính năng của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm virus. Theo mặc định của hệ điều hành **Windows** thường cho phép các tính năng **autorun** giúp người sử dụng thuận tiện cho việc tự động cài đặt phần mềm khi đưa đĩa **CD** hoặc ổ **USB** vào hệ thống. Chính các tính năng này được một số loại virus lợi dụng để lây nhiễm ngay khi vừa cắm ổ **USB** hoặc đưa đĩa **CD** phần mềm vào hệ thống (một vài loại virus lan truyền rất nhanh trong thời gian gần đây thông qua các ổ **USB** bằng cách tạo các **file autorun.ini** trên ổ **USB** để tự chạy các virus ngay khi cắm ổ **USB** vào máy tính). Cần loại bỏ tính năng này bằng các phần mềm của hãng thứ ba hoặc sửa đổi trong hệ thống.

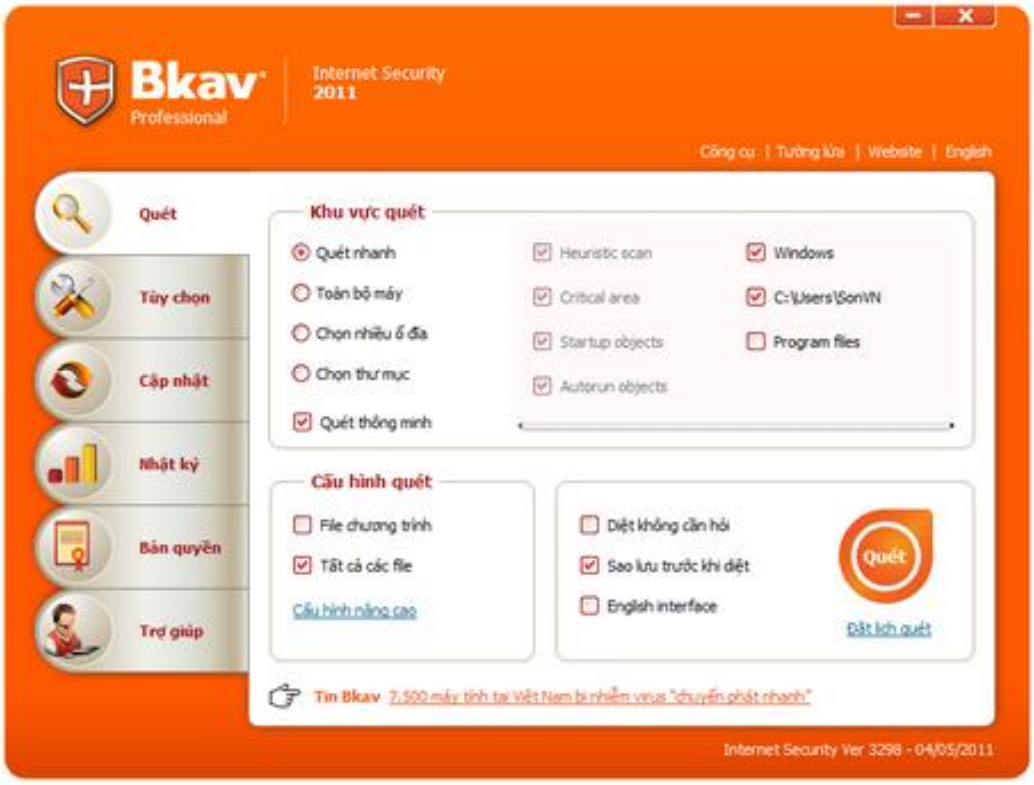
1.6. Giới thiệu một số phần mềm diệt virus.

Phần mềm diệt virus là phần mềm có tính năng phát hiện, loại bỏ các virus, khắc phục (một phần hoặc hoàn toàn) hậu quả do virus gây ra và có khả năng cập nhật để nhận biết các loại virus trong tương lai. Phần mềm diệt virus thường hoạt động trên các nguyên lý cơ bản như sau:

- Kiểm tra, quét các tập tin để phát hiện các virus đã biết trong cơ sở dữ liệu, nhận dạng mẫu virus của chúng.
- Phát hiện các hành động của phần mềm giống như các hành động của virus hoặc các phần mềm độc hại.
- Sau khi phát hiện thấy virus sẽ đưa ra các thông báo, khuyến cáo hành động thực hiện như: Khóa virus, cách ly virus, xóa bỏ virus, sao lưu **files** dự phòng,…

Trên thị trường hiện có rất nhiều phần mềm diệt virus bao gồm bản thương mại (có thu phí) và bản miễn phí hoặc diệt virus trực tuyến (khi kết nối **internet**).

- Phần mềm trong nước: Bkav, CMC.



Hình 9: Phần mềm diệt virus BKAV.

Hình 10: Phần mềm diệt virus CMC.

- Phần mềm nước ngoài: Kaspersky, AVG, Norton, Avira, McAfee, Avast, Microsoft Security Essentials, Bitdefender,…

Hình 11: Phần mềm diệt virus nước ngoài.

- Trang **web** quét virus trực tuyến: Kaspersky.com, Virustotal.com, Bitdefender.com, Cmcinfosec.com

2. ĐỀ MỤC 2: Bảo vệ dữ liệu máy tính.

Sau khi hoàn thành nội dung này, người sử dụng nắm được:

- Cách bảo vệ dữ liệu hệ thống.
- Cách bảo vệ dữ liệu đã tạo ra.

2.1. Bảo vệ dữ liệu hệ thống.

2.1.1. Tên đăng nhập và mật khẩu (userID và password).

Tên đăng nhập và mật khẩu thường là một xâu, chuỗi, loạt các kí tự mà hệ thống máy tính yêu cầu người sử dụng nhập vào bằng bàn phím trước khi có thể tiếp tục truy cập các tài nguyên trên máy tính. Một mật khẩu mạnh là mật khẩu có từ 8 ký tự trở lên, bao gồm cả chữ cái, chữ số và ký tự đặc biệt (**@,#,$,%,** vv...).

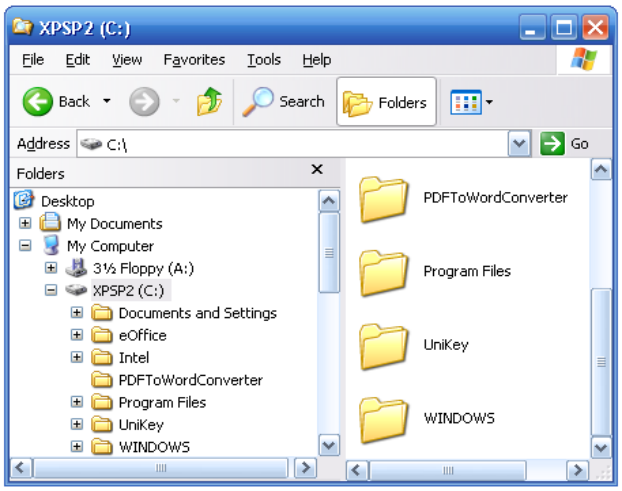
Việc đặt mật khẩu sẽ tránh được việc truy cập các tài nguyên, dữ liệu trái phép, nhất là khi phân quyền để sử dụng chung cùng một máy tính.

2.1.2. Quản lý dữ liệu ổ hệ thống.

Thông thường, hệ điều hành được cài đặt trên ổ đĩa C, nếu để dữ liệu trên ổ cài đặt hệ điều hành thì khi cài đặt lại hệ điều hành mới, dữ liệu trên phân vùng đó sẽ bị mất.

Sau khi cài đặt hệ điều hành, dữ liệu hệ thống sẽ nằm trong phân vùng cài đặt, cụ thể là thư mục **WINDOWS**, người sử dụng không nên xóa, đổi tên thư mục, di chuyển dữ liệu trên thư mục này vì có thể làm ảnh hưởng không tốt đến hệ điều hành.

Áp dụng các biện pháp sao lưu dữ liệu quan trọng trên ổ đĩa hệ thống sang một phân vùng ổ đĩa khác hoặc thiết bị lưu trữ ngoài để khôi phục khi có sự cố xảy ra.



Hình 12: Thư mục WINDOWS chứa files hệ thống.

2.2. Bảo vệ dữ liệu tạo ra.

Để đảm bảo an toàn trước sự lây nhiễm virus máy tính và các phần mềm độc hại khác thì người sử dụng nên tự bảo vệ sự toàn vẹn dữ liệu của mình trước khi dữ liệu bị hư hỏng do virus (hoặc ngay cả các nguy cơ tiềm tàng khác như sự hư hỏng của các thiết bị lưu trữ dữ liệu máy tính) theo một số cách sau:

2.2.1. Sao lưu dữ liệu theo định kỳ.

Là biện pháp đúng đắn nhất hiện nay để bảo vệ dữ liệu, việc sao lưu dữ liệu sẽ làm giảm tổn thất khi hệ thống máy tính gặp trục trặc như lỗi hệ điều hành, hỏng ổ đĩa cứng,…

Những dữ liệu cần sao lưu thông thường là tài liệu nói chung, các ứng dụng tạo và duy trì những tệp tin dữ liệu như **e-mail**, địa chỉ ưa thích của trình duyệt, lịch, sổ địa chỉ liên lạc, hình ảnh, **files video, files** nhạc,…

Người sử dụng có thể thường xuyên sao lưu dữ liệu đến một nơi an toàn như: Các thiết bị nhớ mở rộng (ổ **USB**, ổ cứng di động, ghi ra đĩa quang, vv...), hình thức này có thể thực hiện theo chu kỳ người sử dụng đặt ra tuỳ theo mức độ cập nhật, thay đổi của dữ liệu. Ngoài ra người sử dụng có thể sử dụng tiện ích sẵn có của Hệ điều hành (**system restore**) hoặc sử dụng các phần mềm của hãng khác như **Norton ghost** để tạo ra các bản sao lưu hệ thống, các phần mềm tạo ảnh ổ đĩa hoặc phân vùng khác.

Trước khi sao lưu người sử dụng nên đặt tên dữ liệu theo ngày, theo nội dung công việc để việc sao lưu và khôi phục sau này được thuận lợi.

2.2.2. Bảo vệ dữ liệu đã sao lưu.

Sau khi đã sao lưu dữ liệu thành công, người sử dụng cần bảo vệ dữ liệu đã sao lưu đó. Nếu sao lưu dữ liệu ra thiết bị lưu trữ ngoài như **USB** và ổ cứng di động thì cần sử dụng phần mềm diệt virus quét thiết bị lưu trữ trước và sau khi sao lưu.

Thiết bị lưu trữ, đĩa chương trình đã được sao lưu cần được cất giữ ở nơi an toàn, tránh việc sao chép, truy cập dữ liệu ngoài mong muốn.

2.2.3. Phục hồi dữ liệu đã sao lưu.

Tùy từng biện pháp người sử dụng đã sử dụng để sao lưu, người sử dụng có thể phục hồi lại dữ liệu đến thời điểm đã sao lưu.

Đối với dữ liệu đã sao chép ra thiết bị lưu trữ ngoài, người sử dụng sao chép (c**opy**) trở lại vào ổ đĩa cứng.

Ngoài ra, người sử dụng có thể sử dụng tính năng phục hồi dữ liệu (**system restore**) của hệ điều hành hoặc sử dụng phần mềm của hãng khác để khôi phục lại dữ liệu đã sao lưu.

3. ĐỀ MỤC 3: An ninh mạng.

Sau khi hoàn thành nội dung này, người sử dụng nắm được:

- Các khái niệm về an ninh mạng.
- Các mối nguy hiểm tấn công máy tính.
- Các hình thức tấn công trên mạng máy tính.

3.1. Khái niệm về An ninh mạng.

Trong lĩnh vực an ninh mạng, khu vực an ninh mạng bao gồm các quy định và chính sách được thông qua bởi người quản trị mạng để ngăn chặn và theo dõi truy cập trái phép, sử dụng sai, sửa đổi, hoặc từ chối các mạng máy tính và truy cập tài nguyên mạng. An ninh mạng liên quan đến việc ủy quyền truy cập dữ liệu trong một mạng, được kiểm soát bởi người quản trị mạng. Người sử dụng chọn hoặc được chỉ định một tài khoản và mật khẩu hoặc thông tin xác thực khác cho phép truy cập vào thông tin và các chương trình thuộc thẩm quyền của mình.

An ninh mạng là bảo vệ mạng trước việc bị đánh cắp và sử dụng sai mục đích thông tin trên mạng **internet**. Nếu không có an ninh mạng được triển khai, hệ thống mạng sẽ gặp nhiều rủi ro trước sự xâm nhập trái phép, sự ngừng trệ hoạt động của mạng, sự gián đoạn dịch vụ, sự không tuân thủ quy định và thậm chí là các hành động phạm pháp. An ninh mạng không chỉ dựa vào một phương pháp mà sử dụng một tập hợp các rào cản để bảo vệ hệ thống mạng theo những cách khác nhau. Ngay cả khi một giải pháp gặp sự cố thì giải pháp khác vẫn bảo vệ được hệ thống và dữ liệu trước sự đa dạng của các loại tấn công mạng.

Trong các hệ thống thông tin, người sử dụng phải quan tâm nhiều hơn về tính an ninh, an toàn, khả năng bảo mật và tính sẵn sàng của hệ thống. Sự ngưng trệ của hệ thống thông tin có thể gây ra những thiệt hại vô cùng nghiêm trọng khi sự phụ thuộc vào các ứng dụng ngày càng tăng.

Đảng, Nhà nước và các Bộ, ban, ngành đã có các văn bản thể hiện sự chú trọng đối với vấn đề an toàn thông tin, cụ thể như sau:

- Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005 của Quốc hội Nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.

- Nghị định số 57/2006/NĐ-CP ngày 09/6/2006 của Chính phủ về Thương mại điện tử.

- Luật Công nghệ Thông tin số 67/2006/QH11 ngày 29/6/2006 của Quốc hội Nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.

- Chỉ thị số 03/2007/CT-BBCVT ngày 23/02/2007 của Bộ Bưu chính Viễn thông về việc tăng cường đảm bảo an ninh thông tin trên mạng internet.

- Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng Công nghệ Thông tin trong hoạt động của cơ quan nhà nước.

- Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác.

- Nghị định số 97/2008/NĐ-CP ngày 28/8/2008 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ **Internet** và thông tin điện tử trên **Internet**.

- Thông tư số 07/2008/TT-BTTTT ngày 18/12/2008 của Bộ Thông tin và Truyền thông hướng dẫn một số nội dung về hoạt động cung cấp thông tin trên trang thông tin điện tử cá nhân trong Nghị định số 97/2008/NĐ-CP ngày 28 tháng 08 năm 2008 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ **Internet** và thông tin điện tử trên **Internet**.

- Luật sửa đổi, bổ sung một số điều của Luật Hình sự, số 37/2009/QH12 (ATTT số: các điều 224-226b) ngày 19/6/2009 của Quốc hội Nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.

- Luật Viễn thông số 41/2009/QH12 ngày 23/11/2009 của Quốc hội Nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.

- Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020.

- Thông tư số 14/2010/TT-BTTTT ngày 29/06/2010 của Bộ Thông tin và Truyền thông quy định chi tiết một số điều của Nghị định số 97/2008/NĐ-CP ngày 28 tháng 08 năm 2008 của Chính phủ đối với hoạt động quản lý trang thông tin điện tử và dịch vụ mạng xã hội trực tuyến.

- Thông tư số 25/2010/TT-BTTTT ngày 15/11/2010 của Bộ Thông tin và Truyền thông quy định việc thu thập, sử dụng, chia sẻ, đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước.

- Nghị định số 25/2011/NĐ-CP ngày 06/4/2011 của Chính phủ quy định chi tiết và hướng dẫn thi hành một số điều của Luật Viễn thông.

- Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số.

- Công văn số 2132/BTTTT-VNCERT ngày 18/7/2011 của Bộ Thông tin và

Truyền thông hướng dẫn triển khai áp dụng tài liệu "Hướng dẫn một số biện pháp kỹ thuật cơ bản đảm bảo an toàn thông tin cho cổng/trang thông tin điện tử".

- Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

- Nghị định số 83/2011/NĐ-CP ngày 20/9/2011 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực viễn thông.

- Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng internet Việt Nam.

Bên cạnh các văn bản an toàn thông tin đã được ban hành còn có các cơ quan, tổ chức hoạt động trong lĩnh vực đảm bảo an toàn, an ninh thông tin, cụ thể như sau:

- Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam (Vietnam Computer Emergency Response Team - VNCERT)

+ Được thành lập theo Quyết định số 339/2005/QĐ-TTg ngày 20/12/2005 của Thủ tướng Chính phủ, Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam (**Vietnam Computer Emergency Response Team - VNCERT**) là đơn vị trực thuộc Bộ Thông tin và Truyền thông thực hiện chức năng điều phối và tổ chức các hoạt động phản ứng nhanh các sự cố máy tính cho mạng Internet Việt Nam.

+ Liên hệ: **Email**: office@vncert.vn; **Website**: www.vncert.gov.vn

- Hiệp hội An toàn thông tin Việt Nam (Vietnam Information Security Association - VNISA)

+ Là tổ chức xã hội nghề nghiệp phi lợi nhuận đầu tiên hoạt động trong lĩnh vực bảo mật thông tin được nhà nước Việt Nam công nhận. **VNISA** tập hợp các cá nhân, tổ chức làm công tác nghiên cứu giảng dạy, ứng dụng và phát triển an toàn thông tin nhằm hướng dẫn thực hiện các chủ trương đường lối của nhà nước trong việc ứng dụng và phát triển kỹ thuật, công nghệ, an toàn thông tin, đưa ra đề xuất, khuyến nghị với cơ quan quản lý nhà nước trong việc xây dựng cơ chế chính sách phát triển ngành.

+ Liên hệ: **Email**: infor@vnisa.org.vn; **Website:** www.vnisa.org.vn

- Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao (C50) - Bộ Công an

+ Tiến hành các biện pháp phòng ngừa, phát hiện, điều tra xử lý tội phạm sử dụng công nghệ cao, trực tiếp tiến hành các biện pháp phòng ngừa, phát hiện, đấu tranh chống các hành vi vi phạm và tội phạm sử dụng công nghệ cao theo quy định của Pháp luật.

+ Liên hệ: Điện thoại (trực ban): 069.43160; 06937126; 06937424

- Công ty an ninh mạng BKAV - Website: www.bkav.com.vn

3.2. Các mối nguy hiểm tấn công máy tính.

3.2.1. Tin tặc (hacker).

Tin tặc (**hacker**) là những người có trình độ Công nghệ Thông tin cao dùng kiến thức, kỹ năng của mình để xâm nhập vào các hệ thống máy tính, các máy chủ trong mạng **internet** với mục đích phá hoại, lấy cắp dữ liệu, chiếm quyền điều khiển, vv...

3.2.2. Mạng máy tính ma (botnet).

Mạng máy tính ma (**botnet**) là những máy tính bị bắt cóc và điều khiển bởi người khác thông qua **trojan**, virus. Những máy tính này sẽ chờ chỉ thị từ một nơi nhất định để thực hiện đồng loạt một hành vi nào đó. **Bot** là công cụ để thực hiện các cuộc tấn công từ chối dịch vụ (**DOS/DDOS**). Tấn công từ chối dịch vụ là hành động mà các tin tặc lợi dụng đặc điểm hoặc lỗi an toàn thông tin của một hệ thống dịch vụ nhằm làm ngưng trệ hoặc ngăn cản người dùng truy nhập dịch vụ đó. Thường thì tấn công từ chối dịch vụ gây cho chương trình hoặc hệ thống bị đổ vỡ hoặc bị treo, tê liệt từng phần hoặc toàn bộ, buộc người quản trị dịch vụ đó phải tạm ngừng cung cấp dịch vụ.

3.2.3. Trojan horse.

Trojan horse là loại chương trình máy tính thường ẩn mình dưới dạng một chương trình hữu ích và có những chức năng mà người dùng mong muốn, hay ít nhất chúng trông như có các tính năng này. Một cách bí mật, nó lại tiến hành các thao tác khác nhằm có lợi cho người phát tán. Những chức năng mà **trojan horse** tạo ra chỉ là phần bề ngoài nhằm che dấu cho các thao tác, mục đích xấu. **Trojan horse** cũng có tác hại tương tự như virus chỉ khác là nó không tự sao chép, nhân bản ra. Như thế, cách lan truyền duy nhất là thông qua các thư dây chuyền. Chính những kẻ tạo ra các phần mềm này sẽ sử dụng kỹ năng lập trình của mình để sao lưu thật nhiều **trojan** trước khi phát tán lên mạng. Trong thực tế, nhiều **trojan horse** chứa đựng các phần mềm gián điệp nhằm cho phép điều khiển máy tính từ xa qua hệ thống mạng.

Cách hữu hiệu nhất để phòng chống **trojan horse** là đừng bao giờ mở các tệp tin đính kèm được gửi đến một cách bất ngờ, khi mà người sử dụng chưa xác minh được độ an toàn, nguồn gốc của **file** đính kèm. Khi các **file** đính kèm không được mở ra thì **trojan horse** cũng không thể hoạt động.

3.2.4. Phần mềm ác tính (malware).

Phần mềm ác tính (**malware**) là chữ ghép của **maliciuos** và **software** chỉ chung

các phần mềm có tính năng gây hại như virus, **worm**, **trojan horse, spyware, adware, keyloger, backdoor, rootkit,** vv...Tùy theo cách thức mà tin tặc sử dụng. Sự nguy hại của các loại phần mềm ác tính có khác nhau từ chỗ chỉ hiển thị các cửa sổ khó chịu cho đến việc tấn công chiếm quyền điều khiển máy tính và lây lan sang các máy tính khác.

3.2.5. Phần mềm gián điệp (spyware).

Phần mềm gián điệp (**spyware**): Là chữ viết tắt của **spy** (gián điệp) và **software** (phần mềm máy tính). Là phần mềm có khả năng thâm nhập trực tiếp, theo dõi những hoạt động trên máy tính mà không có sự nhận biết và cho phép của người sử dụng máy tính. Một cách điển hình, **spyware** được cài đặt một cách bí mật như là một bộ phận kèm theo của các phần mềm miễn phí (**freewares**) và phần mềm chia sẻ (**shareware**) mà người sử dụng có thể tải về từ **internet**. Một khi đã cài đặt, **spyware** điều phối các hoạt động của máy chủ trên **internet** và lặng lẽ chuyển các dữ liệu thông tin đến một máy khác, chúng thu thập tất cả các thông tin cá nhân, thói quen cá nhân, thói quen truy cập **web** của người sử dụng và gửi về cho tác giả. Ngoài ra, **spyware** còn sử dụng các tài nguyên của bộ nhớ (**memory resource**) để ăn cắp băng thông khi nó gửi thông tin trở về tác giả của các **spyware** qua các liên kết **internet**. Vì **spyware** dùng tài nguyên của bộ nhớ và của hệ thống, các ứng dụng chạy trong nền (**background**) có thể dẫn tới hệ điều hành bị lỗi hoặc máy tính chạy không ổn định.

Để phòng ngừa **spyware** thì người sử dụng có thể dùng phần mềm chống **spyware**. Quét thường xuyên để loại bỏ **spyware**. Khởi động lại máy tính và kiểm tra lại lần nữa sau mỗi lần bị nhiễm **spyware** mới để chống sự tái nhiễm (**tickler**). Phần mềm chống **spyware** nổi tiếng trên thị trường là phần mềm **spy sweeper**.

3.2.6. Phần mềm quảng cáo (adware).

Phần mềm quản cáo (**adware**): Là chữ viết tắt của **advertisement** (quảng cáo) và **software** (phần mềm máy tính). Là phần mềm thu thập thông tin duyệt **web** của người dùng, được lén lút cài đặt vào máy tính người dùng hoặc cài đặt thông qua một phần mềm miễn phí, hay phần mềm dùng thử được người dùng cho phép (nhưng không ý thức được mục đích của chúng). Một số phần mềm vô hại, nhưng một số có khả năng hiển thị thông tin trên màn hình gây khó chịu cho người sử dụng. Tuy nhiên chúng không dừng lại ở tính đơn giản là quảng cáo mà sẽ kết hợp với những loại virus khác nhằm tăng hiệu quả phá hoại.

3.2.7. Bắt ký tự gõ trên bàn phím (keylogger).

Bắt ký tự gõ trên bàn phím, hay còn gọi là "trình theo dõi thao tác bàn phím" là phần mềm ghi lại mọi thao tác thực hiện trên bàn phím vào một tập tin nhật ký (**log**) để cho người cài đặt nó khai thác, sử dụng thông tin trái phép.

3.2.8. Lừa đảo trực tuyến (phishing).

Lừa đảo trực tuyến (**phishing**) là một hoạt động phạm tội dùng các kỹ thuật lừa đảo thường được thực hiện qua thư điện tử hoặc tin nhắn nhanh hay yêu cầu người dùng nhập thông tin vào một **website** giả mạo gần như giống hệt với **website** thật. Kẻ lừa đảo cố gắng lừa lấy các thông tin nhạy cảm, chẳng hạn như mật khẩu và thông tin về thẻ tín dụng, bằng cách giả là một người hoặc một doanh nghiệp đáng tin cậy trong một giao dịch điện tử. **phishing** thường được thực hiện bằng cách sử dụng thư điện tử hoặc tin nhắn, đôi khi còn sử dụng cả điện thoại.

Tấn công giả mạo là một đơn cử của những kĩ thuật lừa đảo trực tuyến (**social engineering**) nhằm đánh lừa người dùng và khai thác những lỗ hổng hiện nay của công nghệ bảo mật **web**. Để chống lại những hình thức tấn công, lừa đảo ngày càng tăng thì cần hoàn chỉnh hành lang pháp lý, huấn luyện cho người dùng, cảnh báo và tăng cường an ninh kĩ thuật.

3.2.9. Cửa hậu (backdoor).

Trong một hệ thống máy tính, cửa hậu là một phương pháp vượt qua thủ tục chứng thực người dùng thông thường hoặc để giữ đường truy nhập từ xa tới một máy tính trong khi cố gắng không bị phát hiện bởi việc giám sát thông thường. Đây cũng là một loại **trojan** nhưng nhiệm vụ chính là mở thông một số cổng nào đó trên máy tính để lây lan, truy cập và điều khiển máy tính từ xa. Cửa hậu có thể có hình thức là một chương trình được cài đặt hoặc có thể là một sửa đổi đối với một chương trình hợp pháp.

3.2.10. Rootkit.

Rootkit là một bộ công cụ phần mềm do kẻ xâm nhập đưa vào máy tính nhằm mục đích cho phép tin tặc quay lại xâm nhập máy tính đó và dùng nó cho các mục đích xấu mà không bị phát hiện như thu thập dữ liệu về máy tính (kể cả các máy tính khác trong cùng mạng) và những người sử dụng chúng (chẳng hạn mật khẩu và thông tin tài khoản) hoặc gây ra lỗi sai trong hoạt động máy tính. Đây cũng là một loại **trojan** nhưng tự giấu mình, hoạt động ở tầng thấp của hệ thống nên có thể ngăn cản một số dịch vụ. **Rootkit** đã bị sử dụng ngày càng nhiều bởi các phần mềm ác tính, giúp kẻ xâm nhập hệ thống giữ được đường truy nhập vào hệ thống. Các **rootkit** thường sửa đổi một số phần của hệ điều hành hoặc tự cài đặt chúng thành các trình điều khiển (**driver**) hay các **module** trong nhân hệ điều hành (**kernel module**).

Máy tính có thể bị lây nhiễm **rootkit** bằng nhiều con đường, trong đó có việc lây nhiễm qua các chương trình được tải xuống từ **internet**, qua tệp gắn kèm tại **e-mail**, hoặc khi truy cập vào một số trang **web** nhất định. **Rootkit** còn có thể được đưa vào máy tính qua ổ đĩa cắm ngoài hoặc ổ **USB**. **Rootkit** không tự nhân bản và không có cơ

chế hoạt động độc lập tự chủ. **Rootkit** nằm hoàn toàn dưới quyền kiểm soát của một kẻ tấn công.

3.2.11. Spam (thư rác).

Spam (thư rác) là thư được gửi tới nhiều người mà những người đó không yêu cầu được nhận. Nói cách khác, thư rác chủ yếu là những thư không phù hợp, không có ý nghĩa với người sử dụng máy tính, vv…Nguy hiểm hơn là virus và các hành vi lừa đảo có thể ẩn mình dưới dạng thư rác. Người gửi thư rác thường gửi một loạt tới danh sách các địa chỉ thư và được gửi từ nhiều địa chỉ khác nhau. Các thư này thường được gửi dưới dạng "nặc danh" để giấu thông tin về người gửi thật.

3.3. Các hình thức tấn công trên mạng máy tính.

Tội phạm mạng đang diễn ra với tốc độ nhanh hơn, quy mô hơn, tính chuyên nghiệp, trình độ kỹ thuật ngày càng cao hơn và khả năng để lại dấu vết, chứng cứ trên không gian ảo ngày càng ít hơn. Tính mở của các dịch vụ tiện ích, các mạng xã hội (**facebook**, **twitter**, **yahoo chat, yahoo mail,** vv…), các thiết bị di động thông minh (**smartphone**, máy tính bảng, vv…) đã được giới tội phạm mạng lợi dụng để lừa đảo. Việc nắm bắt được tâm lý, sự nhẹ dạ của người sử dụng, thông qua các lỗ hổng dịch vụ, tội phạm mạng có thể nghe lén các cuộc đàm thoại, truy cập, lấy dữ liệu quan trọng (thông tin thẻ tín dụng, thông tin cá nhân, vv…), mạo danh người sử dụng để lừa đảo (Nhờ mua thẻ điện thoại, mượn địa chỉ **e-mail** để gửi thư, vv…). Người sử dụng cần cẩn trọng khi tiếp nhận các thông tin qua các kênh giao tiếp trên mạng. Đặc biệt, cần cảnh giác trước các đường liên kết tới **website** hoặc các **files** nhận được, thậm chí nên gọi điện hỏi lại nếu thấy tài khoản **chat, e-mail**, vv…của họ đang yêu cầu cung cấp tiền hoặc các thông tin nhạy cảm khác, vv…

Có rất nhiều hình thức tấn công đã biết cũng như chưa biết, tuy nhiên hiện nay có thể chia ra làm 4 loại chính:

3.3.1. Tấn công trực tiếp.

Phần lớn sự tấn công là trực tiếp, tức là dùng một máy tính tấn công trực tiếp máy tính khác.

Dò tìm **user name** và **password**, bằng cách thử với một số từ khóa thông dụng như "xinchao", ""**hello**", “123456”, dùng tên người thân, ngày sinh, số điện thoại, vv...Vì vậy người sử dụng nên tránh việc đặt mật khẩu quá đơn giản hoặc thuộc những kiểu kể trên.

Dùng chương trình để giải mã các **files** chứa mật khẩu trên máy tính để tìm ra mật khẩu, thường những mật khẩu đặt quá ngắn sẽ bị phát hiện bằng cách này. Người sử dụng nên đặt mật khẩu của mình tối thiểu là 8 ký tự, càng dài càng tốt, nên có cả số, chữ cái, ký tự đặc biệt, vv…

Dùng lỗi của chương trình ứng dụng hay hệ điều hành để làm cho các ứng dụng hay hệ điều hành đó bị tê liệt.

3.3.2. Nghe trộm.

Không cần can thiệp trực tiếp vào máy tính mà thông qua các dịch vụ mạng, bằng cách này tin tặc có thể nghe trộm được những thông tin được truyền qua lại trên mạng.

Nghe trộm **password:** Cũng với cách như trên, tin tặc có thể lấy được mật khẩu của người sử dụng, sau đó chúng truy cập một cách chính quy vào hệ thống.

3.3.3. Giả mạo địa chỉ.

Thường thì các mạng máy tính nối mạng **internet** đều được bảo vệ bởi bức tường lửa. Bức tường lửa có thể coi như cánh cửa duy nhất mà người đi vào nhà hay đi ra cũng đều bắt buộc phải qua đó.

Giả mạo địa chỉ là người bên ngoài (máy tính của tin tặc) sẽ giả mạo mình là một người ở trong nhà (tự đặt địa chỉ **IP** của mình trùng với một địa chỉ nào đó ở mạng bên trong). Nếu làm được điều đó thì tin tặc sẽ được đối xử như một người (máy) bên trong, tức là được làm mọi thứ để từ đó tấn công, lấy trộm, phá huỷ thông tin, vv...

3.3.4. Vô hiệu hoá các dịch vụ.

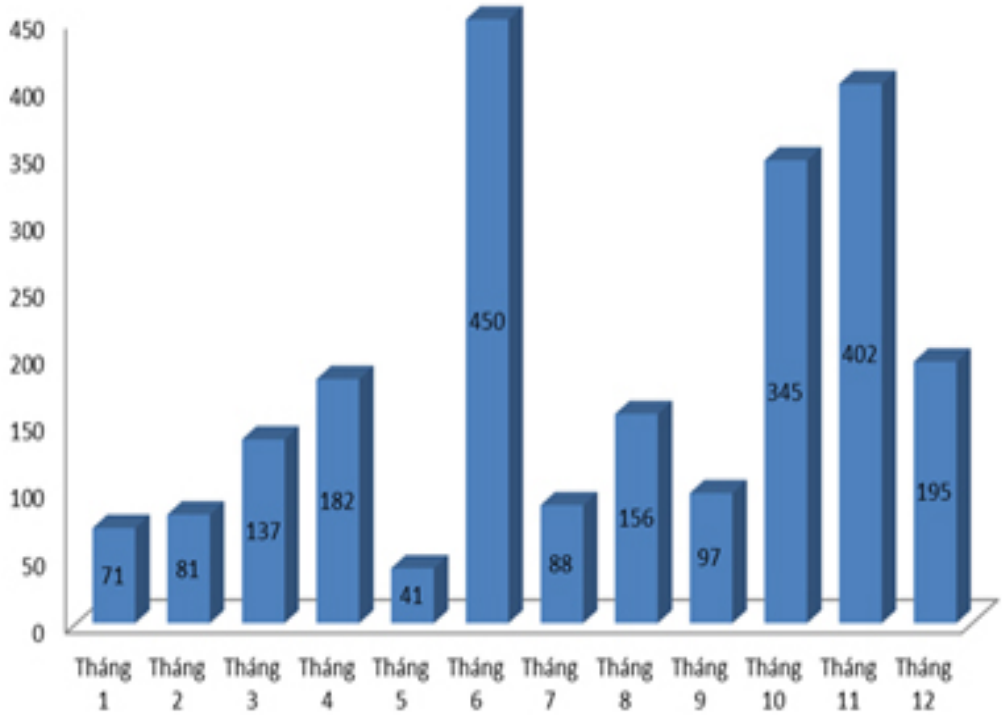
Làm tê liệt một số dịch vụ nào đó. Thường cách tấn công này được gọi là **DoS (Denial of Service)** hay "từ chối dịch vụ". Cách tấn công này lợi dụng một số lỗi của phần mềm. Tin tặc cho máy tính của chúng đưa ra những yêu cầu "lạ" tới những máy chủ trên mạng. Với yêu cầu "lạ" như vậy các máy chủ tiếp nhận yêu cầu sẽ không xử lý được dẫn đến bị tê liệt.

Tấn công từ chối dịch vụ cũng có thể hoàn toàn là những yêu cầu hợp lệ. Ví dụ như virus máy tính được cài đặt chức năng tấn công như đã nói tới trong phần về virus (**botnet**). Tại một thời điểm, hàng triệu máy tính trên mạng tất cả đồng thời gửi yêu cầu tới máy chủ phục vụ. Những yêu cầu này là hoàn toàn hợp lệ, nhưng tại cùng một thời điểm có quá nhiều yêu cầu như vậy, thì máy chủ không thể phục vụ được nữa dẫn đến không thể tiếp nhận các yêu cầu tiếp theo dẫn đến bị tấn công từ chối dịch vụ.

3.3.5. Yếu tố con người.

Kẻ tấn công giả vờ liên lạc với người quản trị mạng yêu cầu đổi mật khẩu của người sử dụng (**user**) nào đó, nếu người quản trị mạng làm theo thì vô tình đã tiếp tay cho tin tặc.

Tương tự kẻ tấn công có thể yêu cầu quản trị mạng thay đổi cấu hình hệ thống để tiếp đó chúng có thể tiến hành được các cuộc tấn công.



Hình 13: Số lượng các website bị tấn công năm 2011 (nguồn Bkav)

4. ĐỀ MỤC 4: Bảo mật thông tin trên mạng.

Sau khi hoàn thành nội dung này, người sử dụng nắm được:

- Khái niệm về bảo mật thông tin.
- Mục đích của bảo mật thông tin.
- Các phương pháp bảo mật thông tin.

4.1. Khái niệm về bảo mật thông tin.

Bảo mật thông tin là hình thức bảo vệ máy tính, thông tin cá nhân được an toàn. Giúp người sử dụng kiểm soát và bảo vệ thông tin tránh khỏi việc vô tình hoặc cố ý sửa đổi, xóa cũng như tiết lộ thông tin trái phép.

4.2. Mục đích của bảo mật thông tin.

Tính bí mật: Chỉ có người nhận đã xác thực mới có thể lấy ra được nội dung của thông tin chứa đựng trong dạng đã mã hóa của nó. Nói khác đi, nó không thể cho phép thu lượm được bất kỳ thông tin đáng kể nào về nội dung của thông điệp.

Tính nguyên vẹn: Người nhận cần có khả năng xác định được thông tin có bị thay đổi trong quá trình truyền thông hay không, tránh khỏi việc bị thay đổi, chỉnh sửa trái phép.

Tính xác thực: Người nhận cần có khả năng xác định người gửi và kiểm tra xem người gửi đó có thực sự gửi thông tin đi hay không.

Tính không thể từ chối: Người gửi không thể từ chối hay phủ nhận việc mình đã gửi thông tin đi.

Tính chống lặp lại: Không cho phép bên thứ ba sao chép lại văn bản và gửi nhiều lần đến người nhận mà người gửi không hề hay biết.

4.3. Các phương pháp bảo mật thông tin.

- Không nên đưa các thông tin cá nhân lên mạng.

- Không nên dùng các thông tin cá nhân để làm mật khẩu (**password**), nên đặt mật khẩu mạnh bao gồm các yếu tố: Có từ 8 ký tự trở lên, bao gồm cả chữ cái, chữ số và ký tự đặc biệt (**$,%,@,&,*,** vv…) và đổi mật khẩu tối thiểu 3 tháng 1 lần.

- Không nên sử dụng chung một mật khẩu cho những dịch vụ quan trọng trên mạng như thư điện tử, tài khoản, vv…

- Không nên sử dụng chức năng nhớ mật khẩu, hãy nhập mật khẩu cho mỗi lần đăng nhập, nhất là những máy tính được sử dụng chung.

- Ghi nhớ mật khẩu của mình, không nên lưu trữ mật khẩu trên máy tính và các thiết bị khác.

- Kiểm tra về thông tin trang web sắp truy cập.

- Không nên kích chuột trực tiếp lên các **files** đính kèm, các đường liên kết (**links**) được gửi đến người sử dụng qua thư điện tử, phần mềm chat, vv…khi người sử dụng chưa biết rõ nguồn gốc, độ an toàn của đường liên kết đó. Những đường liên kết đó có thể vô hại nhưng cũng có thể đã được cài đặt sẵn virus, mã độc, chương trình ăn cắp thông tin cá nhân, vv…

- Không tải về, cài đặt các chương trình lạ chưa rõ nguồn gốc vì nó có thể chứa virus, trojan, mã độc, vv…(đặc biệt chú ý các tập tin có đuôi ***.exe**, ***.com**, ***.bat**, ***.scr**, ***.swf**, ***.zip**, ***.rar**, ***.js**, ***.gif,** vv…). Cần kiểm tra (**scan**) bằng một chương trình diệt virus và một chương trình diệt **spyware**, vì nhiều chương trình diệt virus chỉ có thể tìm thấy virus chứ không thể nhận biết ra **spyware**.

- Khi cài đặt một phần mềm bất kỳ trên máy tính hoặc truy cập vào **website**, có thể sẽ có yêu cầu, điều khoản kèm theo để được cài đặt phần mềm, truy cập **website** đó. Khi đó cần đọc kỹ các điều khoản đưa ra trước khi **next** (chuyển), hoặc **accept**, **OK** (chấp nhận), vv…Tránh trường hợp bị ràng buộc điều kiện trong điều khoản mà người sử dụng không để ý tới.

- Không nên lưu giữ các **files** tạm (**cache**) trên trình duyệt, các thông tin về những trang **web** đã ghé thăm.

- Nên sử dụng hoặc cập nhật phiên bản mới nhất cho trình duyệt **web** (**internet browser**).

- Bật tính năng tường lửa (**firewall**) có trên hệ điều hành, có thể cài đặt thêm phần mềm tường lửa từ một hãng khác.

- Bảo mật các thông tin quan trọng trên hệ điều hành như: Địa chỉ **IP**, tên máy tính, vv…

- Tắt chế độ điều khiển máy tính từ xa (**remote desktop**) trên hệ điều hành.

- Cài đặt và sử dụng phần mềm diệt virus, cập nhật các mẫu virus mới, quét virus thường xuyên trên toàn bộ hệ thống và khi sử dụng các thiết bị lưu trữ ngoài.

- Nên sử dụng phần mềm chứng thư điện tử, mã hóa, đặt mật khẩu dữ liệu trước khi chia sẻ tài nguyên trên mạng.

- Khi không có nhu cầu kết nối **internet,** người sử dụng có thể tắt tính năng **network connection** trên hệ điều hành hoặc tắt thiết bị mạng nhằm đảm bảo an toàn, bảo mật cho máy tính.

MỤC LỤC