AN TOÀN VÀ AN NINH THÔNG TIN

Trường Trung cấp TT-TT

Nội dung trình bày

1. Virus máy tính và cách phòng chống.
2. Bảo vệ dữ liệu máy tính
3. An Ninh Mạng
4. Bảo mật thông tin trên mạng

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…)

1.2 Lịch sử phát triển của virus máy tính

- Năm 1986: Xuất hiện loại virus đầu tiên tại Pakistan tên là **Brain**
- Năm 1987: Xuất hiện virus **Stoned**
- Năm 1990: Xuất hiện virus **Form**

1. Virus máy tính và cách phòng chống

- Năm 1991: Xuất hiện virus **Michelangelo**
- Năm 1994: Xuất hiện virus **Monkey**
- Năm 1995: Xuất hiện virus **Concept**
- Năm 1999: Xuất hiện virus **Happy99**
- Năm 2000: Xuất hiện virus **Love Letter**
- Năm 2001: Xuất hiện virus **Code Red**
- Năm 2003: Xuất hiện virus **Slammer**
- Năm 2004: Xuất hiện virus **MyDoom**
- Năm 2005: Xuất hiện virus **HaxDoor**
- Năm 2007: Xuất hiện virus **Mebroot**
- Năm 2008: Xuất hiện virus **Conficker**

1. Virus máy tính và cách phòng chống

- Năm 2010: Xuất hiện virus **Stuxnet**
- Năm 2011: Xuất hiện virus **W32.Sality.PE**
- 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
- 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

1.3 Phân loại virus

- Virus file.
- Virus boot
- **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**.

- 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).

1.4 Phương thức hoạt động của virus máy tính.

- **Qua các thiết bị lưu trữ di động.**
- **Qua thư điện tử.**
- **Qua mạng internet.**
- **Biến thể của virus.**

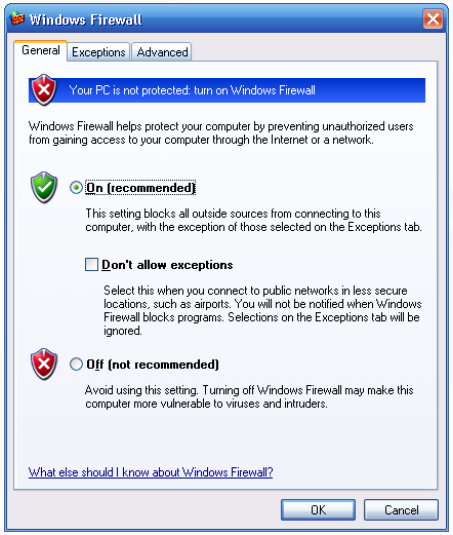
Một hình thức trong cơ chế hoạt động của virus là tạo ra các biến thể của chúng. Biến thể của virus là sự thay đổi mã nguồn nhằm các mục đích tránh sự phát hiện của phần mềm diệt virus hoặc làm thay đổi hành động của nó.

- **Khả năng vô hiệu hóa phần mềm diệt virus.**

1.5 Cách phòng chống virus.

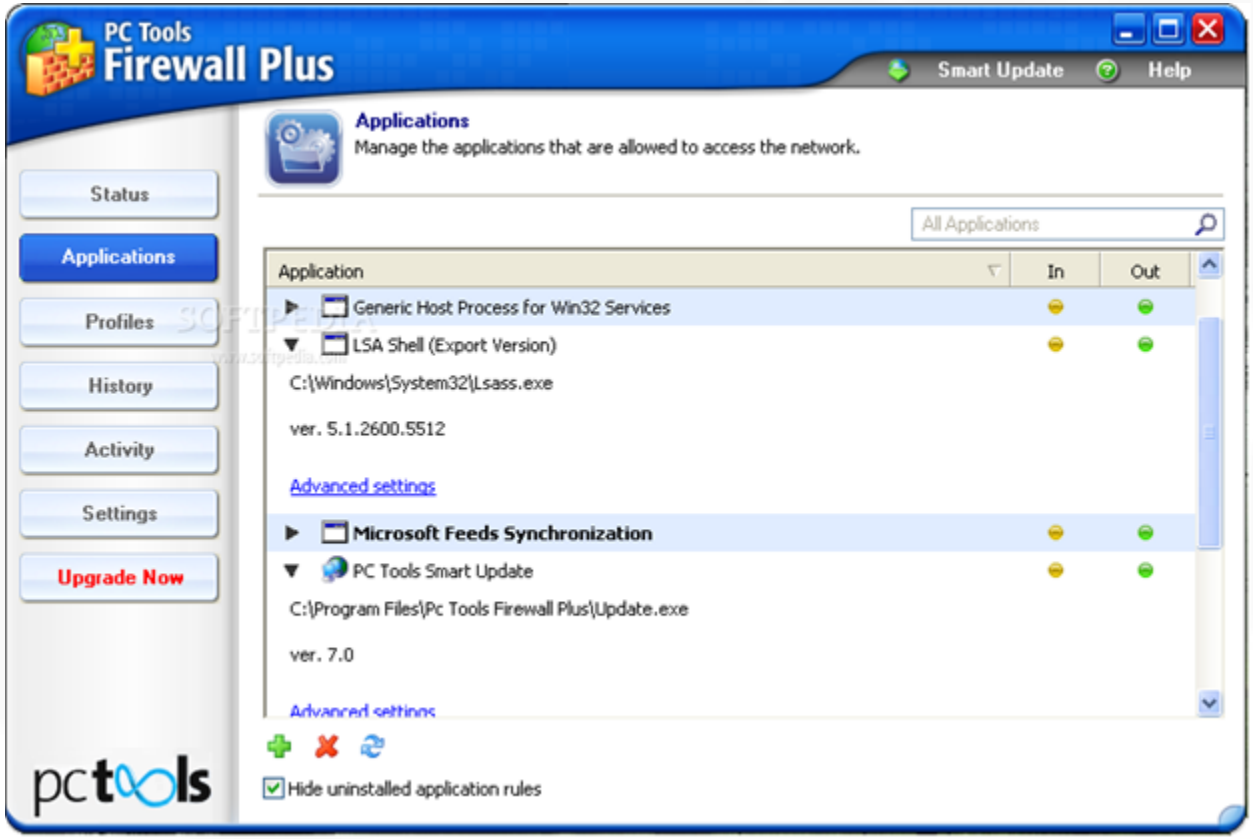
- **Cách nhận biết cơ bản**
- **Sử dụng phần mềm diệt virus.**
- **Sử dụng tường lửa.**

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



1. Virus máy tính và cách phòng chống

Sử dụng các công cụ tường lửa khác



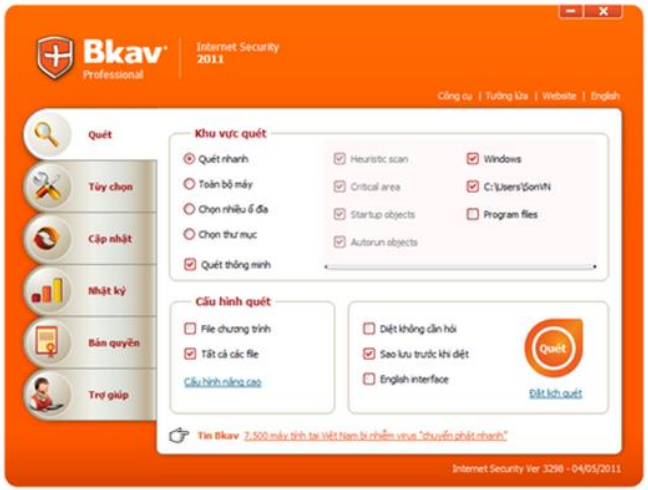
- **Cập nhật các bản sửa lỗi của hệ điều hành.**
- **Vận dụng kinh nghiệm sử dụng máy tính.**

- Phát hiện sự hoạt động khác thường của máy tính
- Kiểm soát các ứng dụng đang hoạt động với **task manager**
- Loại bỏ một số tính năng của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm virus như autorun

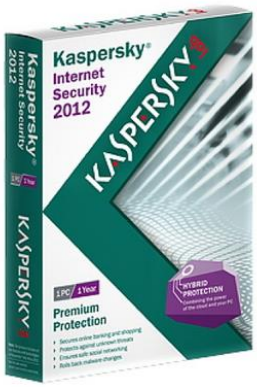
1.6 Giới thiệu một số phần mềm diệt virus.

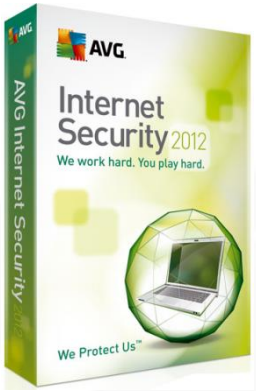
Phần mềm diệt virus là phần mềm có tính năng phát hiện, loại bỏ các virus, khắc phục hậu quả do virus gây ra và có khả năng cập nhật để nhận biết các loại virus trong tương lai.

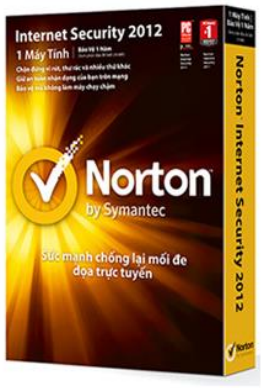
1. Virus máy tính và cách phòng chống

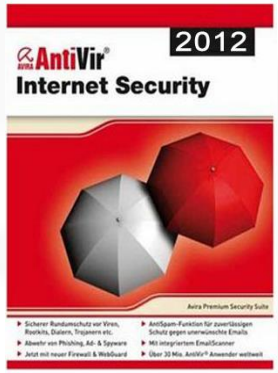


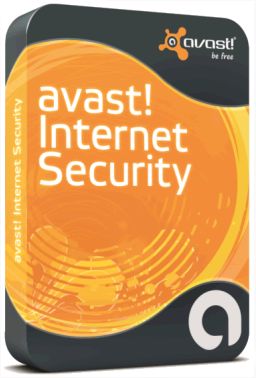
1. Virus máy tính và cách phòng chống

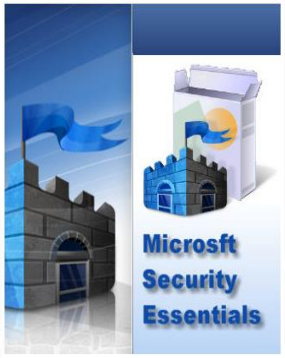


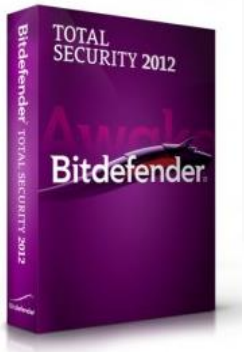








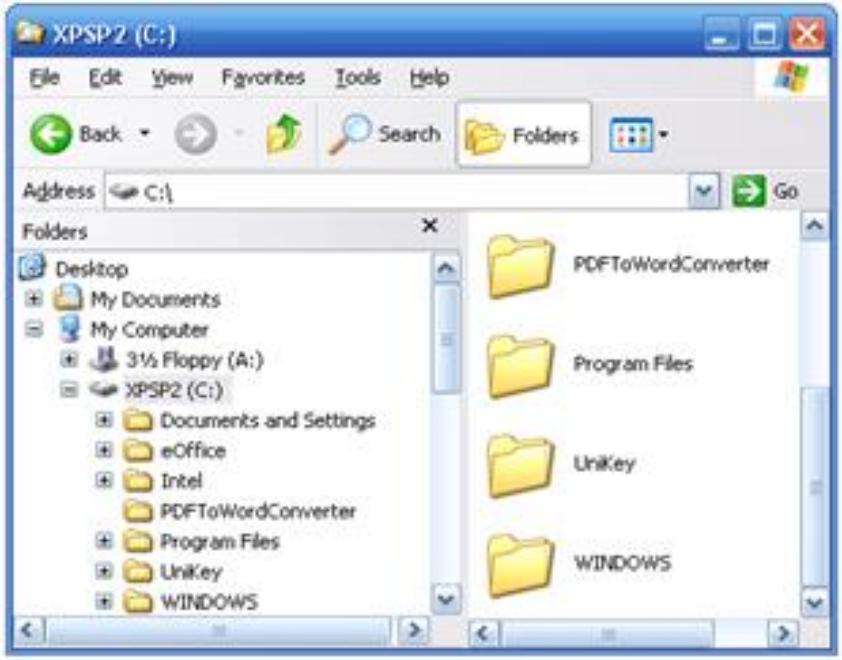




2. Bảo vệ dữ liệu máy tính

2.1 Bảo vệ dữ liệu hệ thống.

- Tên đăng nhập và mật khẩu (userID và password).
- Quản lý dữ liệu ổ hệ thống.



2.2 Bảo vệ dữ liệu tạo ra.

- Sao lưu dữ liệu theo định kỳ

- Bảo vệ dữ liệu đã sao lưu.

- Phục hồi dữ liệu 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. An ninh mạng

3.1 Khái niệm về An ninh mạng.

- An ninh mạng là bảo vệ mạng trước việc bị đánh cắp và sử dụng sai mục đích thông tin trên mạng **internet**.
- 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

3.2 Các mối nguy hiểm tấn công máy tính

- Tin tặc **(**hacker**)**.
- Tin tặc (hacker).
- Trojan horse.

3. An ninh mạng

- Phần mềm ác tính (malware).
- Phần mềm gián điệp (spyware).
- Phần mềm quảng cáo (adware)
- Bắt ký tự gõ trên bàn phím (keylogger).
- Lừa đảo trực tuyến (phishing).
- Cửa hậu (backdoor).
- Rootkit.

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

- Spam (thư rác).

3.2 Các hình thức tấn công trên mạng máy tính.

- **Tấn công trực tiếp**

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...

- **Nghe trộm.**

Nghe trộm **password**

- **Giả mạo địa chỉ IP.**
- **Vô hiệu hoá các dịch vụ.**

DoS (Denial of Service)

- **Yếu tố con người.**

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
- Tính nguyên vẹn
- Tính xác thực
- Tính không thể từ chối
- Tính chống lặp lại

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**)
- Không nên sử dụng chung một mật khẩu cho những dịch vụ quan trọng
- Không nên sử dụng chức năng nhớ mật khẩu, hãy nhập mật khẩu cho mỗi lần đăng nhập
- Ghi nhớ mật khẩu của mình, không nên lưu trữ mật khẩu trên máy tính
- Kiểm tra về thông tin trang web sắp truy cập

4. Bảo mật thông tin trên mạng

- Không nên kích chuột trực tiếp lên các **files** đính kèm
- Không tải về, cài đặt các chương trình lạ chưa rõ nguồn gốc
- Khi cài đặt một phần mềm bất kỳ trên máy tính hoặc truy cập vào **website** cần đọc kỹ các điều khoản đưa ra trước khi **next** (chuyển), hoặc **accept**, **OK** (chấp nhận), vv…
- Không nên lưu giữ các **files** tạm (**cache**) trên trình duyệt
- Nên sử dụng hoặc cập nhật phiên bản mới nhất cho trình duyệt **web**
- Bật tính năng tường lửa (**firewall**)
- Bảo mật các thông tin quan trọng trên hệ điều hành như: Địa chỉ **IP**, tên máy tính, vv…

4. Bảo mật thông tin trên mạng

- Tắt chế độ điều khiển máy tính từ xa (**remote desktop**)
- Cài đặt và sử dụng phần mềm diệt virus, cập nhật các mẫu virus mới, quét virus thường xuyên
- Nên sử dụng phần mềm chứng thư điện tử, mã hóa, mật khẩu định kỳ thay đổi.
- Nên sử dụng phần mềm chứng thư điện tử, mã hóa, đặt mật khẩu dữ liệu