Họ và tên : Trần Thế Tường

Lớp : CR 210T

MSSV : 27211239157

**Virus máy tính**

- Một trong những yếu tố ảnh hưởng nhiều nhất đến an toàn của thông tin máy tính là virus máy tính.

- Khái niệm về virus : Virus máy tính là một chương trình hay một đoạn chương trình có khả năng tự nhân bản hay sao chép chính nó từ đối tượng bị lây nhiễm này sang đối tượng khác mỗi khi đối tượng bị lây nhiễm bị kích hoạt.

- Một số virus máy tính phổ biến bao gồm : Morris Worm, Nimda, ILOVEYOU, SQL Slammer, Stuxnet, CryptoLocker, Code Red, Sasser, Blaster, Conficker và Creeper virus, wanna cry virus ...

* **Biện pháp phòng tránh virus máy tính**

- Cài đặt phần mềm diệt virus, sử dụng bảng hệ thống, tắt tự động cài đặt, tạo lớp bảo vệ, không nhập vào các nút tải xuống không cần thiết và không chạy các chương trình từ Internet hoặc sao chép từ máy tính khác, sử dụng trình duyệt web an toàn, nhắc nhở các cảnh báo virus xuất hiện, cài đặt các bản cập nhật mới nhất từ Microsoft Update và luôn luôn làm mới phần mềm.

- Để phòng tránh virus, bảo vệ dữ liệu, nguyên tắc chung cơ bản nhất là: “Luôn cảnh giác và ngăn chặn virus trên chính những đường lây lan của chúng”. Cụ thể ta có các biện pháp phòng tránh sau:

- Hạn chế việc sao chép không cần thiết và không nên chạy các chương trình tải từ internet hoặc sao chép từ máy khác khi chưa đủ tin cậy.

- Cẩn thận và không nên mở những tệp gửi kèm trong thư điện tử nếu có nghi ngờ về nguồn gốc hay nội dung thư.

- Không truy cập các trang web có nội dung không lành mạnh hoặc xuất xứ không rõ ràng.

- Thường xuyên cập nhật bản sửa lỗi cho các sản phẩm phần mềm chạy trên máy tính của mình, kể cả hệ điều hành.

- Định kỳ sao lưu dữ liệu để có thể khôi phục khi bị virus phá hoại.

- Định kỳ quét và diệt virus bằng các phần mềm diệt virus.

**\* Một số biện pháp bảo vệ thông tin máy tính**

**- Sao lưu dự phòng**

- Mục đích của sao lưu dự phòng: là tạo một bản dữ liệu khác có thể được phục hồi trong trường hợp xảy ra với bản chính với bất kỳ nguyên nhân nào. Lỗi dữ liệu chính có thể là kết quả của lỗi phần cứng hoặc phần mềm, do hỏng hoặc do con người gây ra, chẳng hạn như virus tấn công (virus hoặc phần mềm độc hại) hoặc xóa nhầm dữ liệu ngẫu nhiên. Bản sao lưu cho phép dữ liệu được khôi phục từ thời điểm trước đó để giúp người sử dụng khôi phục từ những việc bất khả kháng.

- Lưu trữ bản sao của dữ liệu trên một thiết bị riêng biệt là rất quan trọng để bảo vệ chống mất dữ liệu xảy ra. Thiết bị sao lưu đơn giản nhất có thể như ổ đĩa gắn ngoài, HDD di động gắn ngoài hoặc USB hoặc bất cứ thứ gì có chức năng lưu trữ, chẳng hạn như hệ thống lổ đĩa, lưu trữ đám mây … Phương tiện thay thế có thể ở cùng vị trí với dữ liệu chính hoặc tại một vị trí ở bất cứ nơi đâu.

- Để có kết quả tốt nhất, các bản sao lưu được thực hiện trên cơ sở nhất quán, thường xuyên để giảm thiểu số lượng dữ liệu bị mất giữa các bản sao lưu. Càng nhiều thời gian trôi qua nếu dữ liệu chưa được sao lưu, càng có nhiều khả năng mất dữ liệu xảy ra khi khôi phục từ bản sao lưu chính. Giữ lại một bản sao lưu là linh hoạt cần làm để khỏi mất mác dữ liệu có thể xảy ra.

**\* Các biện pháp sao lưu dự phòng**

Trong máy tính, hệ điều hành và các phần mềm ứng dụng thường được cài đặt trên ổ C, các kết quả làm việc cũng thường được lưu trong thư mục My Documents và cũng trên ổ C. Trong quá trình làm việc máy tính có thể xảy ra trục trặc với hệ điều hành và các phần mềm ứng dụng, từ đó có thể dẫn đến hư hỏng các tệp trên ổ C và làm mất thông tin. Các tệp trên ổ khác thường ít bị hư hỏng hơn. Nên ta có thể thực hiện sao lưu dữ liệu từ ổ C sang các ổ đĩa khác hoặc sao lưu từ máy tính sang các ổ đĩa di động khác (USB).

- Cách thực hiện:

+ Tạo một thư mục có tên Sao\_luu tại ổ đĩa khác ngoài ổ C trên máy tính hoặc ở ổ đĩa di động khác (USB).

+ Sao chép dữ liệu cần sao lưu dự phòng từ ổ C sang thư mục Sao\_luu hoặc từ máy tính sang thư mục Sao\_luu ở ổ nhớ di động bằng các lệnh Copy và Paste.

Đây là cách phổ biến và dễ thực hiện nhất.

* **Sao lưu dữ liệu trực tuyến**

Sao lưu trực tuyến là cách tiếp cận dễ dàng hơn để sao lưu và phục hồi. Dữ liệu được đọc hoặc phát trực tuyến từ máy chủ trực tiếp hoặc thông qua máy chủ dự phòng đến một phương tiện thứ cấp hoặc hệ thống lưu trữ nào đó.

Máy chủ sao lưu chịu trách nhiệm nhập dữ liệu và thực hiện các hoạt động bổ sung để tối ưu hóa dữ liệu trước khi ghi lưu nó vào thiết bị thứ cấp. Lập chỉ mục dữ liệu để dễ dàng tìm kiếm và khôi phục và giảm thiểu dữ liệu xuống bằng cách nén file, mã hóa dữ liệu để bảo vệ dữ liệu trong quá trình di chuyển và chuyển đổi.

*- Sao lưu dữ liệu và khôi phục theo cách này cung cấp nhiều lợi ích, bao gồm:*

Khả năng hợp nhất và quản lý sao lưu và phục hồi từ nhiều hệ thống chính với một giao diện sao lưu và mục tiêu lưu trữ là duy nhất.

Khả năng an toàn dữ liệu với tính năng nén và nén toàn bộ.

Quản lý dữ liệu thông minh để cải thiện việc thu thập dữ liệu để phục hồi. Tích hợp ứng dụng để dữ liệu được khôi phục.

*- Tuy nhiên bên cạnh đó cũng có một số nhược điểm, bao gồm:*

Sao lưu dữ liệu trực tuyến yêu cầu máy chủ ứng dụng phải có hiệu suất cao đòi hỏi CPU và bộ nhớ RAM để đọc và truyền dữ liệu từ bộ nhớ cục bộ hoặc từ xa để xử lý các công việc sao lưu. Trong trường hợp dữ liệu nhiều hình ảnh cũng cần phải có HDD lớn và dẫn đến thời gian khôi phục dữ liệu sẽ lâu hơn.

Phần mềm sao lưu doanh nghiệp có thể rất tốn kém, đặc biệt khi dữ liệu phát triển và mở rộng trong tương lai. Trong nhiều trường hợp, chi phí của phần mềm sao lưu có thể lớn hơn chi phí của cơ sở hạ tầng lưu trữ cơ bản.