Bảo mật

Bởi:
Đỗ Ngọc Minh

Bảo mật thông tin

Thuật ngữ bảo mật thông tin và lợi ích của nó

Bảo mật thông tin là gì

Đây là thuật ngữ chung chỉ *tất cả các hình thức an toàn trong máy tính* bao gồm cả việc bảo vệ chống lại virút, tin tặc và các truy cập trái phép.Bạn cần học cách điều khiển máy tính đúng quy cách, tránh rủi ro mất mát dữ liệu do thao tác không đúng gây ra. Bạn cũng cần phải thiết lập cho mình các quy tắc bảo mật như quyền truy cập hay lịch quét vi rút hàng ngày.

Sự quan trọng của việc tắt máy tính đúng quy cách

Việc tắt máy tính không giống như tắt các thiết bị điện tử khác trong nhà như Tivi, đài, quạt…bởi máy tính khi bật thì thường làm việc với dữ liệu. Việc tắt máy tính không đúng cách sẽ gây ra mất dữ liệu do hệ điều hành chưa kịp sao lưu. Để tránh trường hợp tắt máy đột ngột, nhiều hãng sản xuất đã thiết kế nút công tắc điện trên vỏ máy gắn với chức năng tắt hệ điều hành (shutdown). Trong những trường hợp này, người dùng có thể yên tâm khi nhấn nút công tắc nguồn trên vỏ máy sau khi hoàn thành công việc và muốn tắt máy đi. Tuy nhiên, nếu sử dụng hệ điều hành Windows, cách thông dụng nhất để tắt máy tính đúng cách là nhấn vào nút Start, chọn Shutdown.

Bộ lưu điện (UPS) là gì?

Bộ lưu điện UPS (Un-interruptible Power Supply) là một thiết bị bảo vệ máy tính tránh trường hợp nguồn điện bị tắt đột ngột. Bộ lưu điện có các bộ ắc quy để cung cấp điện cho máy tính đủ thời gian để người dùng thực hiện lệnh shutdown và tắt máy đúng cách. Điều này đặc biệt quan trọng cho các máy tính trong một mạng mà ở đó dữ liệu được cung cấp cho nhiều người sử dụng đồng thời.

Sử dụng ổn áp bảo vệ quá điện

Điện áp cung cấp cho máy tính có thể lên xuống thất thường, nhất là việc tăng điện áp đột ngột. Để tránh những trường hợp này, cần sử dụng các thiết bị ổn áp nhằm điều chỉnh cường độ dòng điện hợp lý và an toàn.

Điều kiện môi trường phù hợp với máy tính

- Thoáng gió
- Môi trường sạch
- Bề mặt rộng rãi ổn định

Điều kiện môi trường hoặc những công việc không phù hợp khi làm việc với máy tính

- Bụi
- Người sử dụng đặt đồ ăn hoặc đồ uống lên bàn phím
- Nhiệt độ quá cao hoặc quá thấp
- Ẩm ướt
- Không di chuyển máy tính trong khi máy vẫn đang bật, điều này có thể làm hỏng đĩa cứng trong máy.
- Không để đồ vật lên màn hình.
- Không để đĩa mềm gần màn hình vì trường điện từ mạnh của màn hình sẽ làm hỏng đĩa mềm.

Phải làm gì khi máy tính bị hỏng

Trong một tổ chức lớn, nếu máy tính bị hỏng, bạn cần báo cho bộ phận phụ trách công nghệ thông tin và bộ phận này sẽ có trách nhiệm giải quyết. Còn nếu trong tổ chức nhỏ, không có bộ phận chuyên trách, bạn nên gọi bộ phận kỹ thuật hoặc thợ đến sửa chữa. Lưu ý rằng chừng nào bạn chưa chắc chắn là sẽ tự sửa được, chừng đó không nên tự mở máy ra kiểm tra. Công việc sửa chữa máy khi máy bị hỏng là việc của những người có chuyên môn..

Bảo vệ sự riêng tư trong tin học

Tên đăng nhập và mật khẩu (UserID và passwords)

Tên đăng nhập cùng với mật khẩu được sử dụng để đăng nhập vào máy tính hoặc mạng máy tính. Tên đăng nhập cho phép định rõ vị trí và vai trò của người dùng trong khi mật khẩu đảm bảo rằng không ai có thể truy cập vào mạng và mạo nhận bạn

Tên đăng nhập và mật khẩu có thể do bạn tự tạo ra nếu bạn sử dụng máy tính riêng hoặc có thể do quản trị mạng cấp phát cho bạn khi bạn có nhu cầu đăng nhập vào hệ thống

mạng theo quyền truy nhập rất cụ thể. Ý tưởng của quyền truy cập là bạn chỉ có khả năng kết nối hoặc chia sẻ với những nơi mà bạn có quyền sử dụng.

Chọn một mật khẩu an toàn

Mật khẩu cùng với tên đăng nhập tạo thành một chiếc chìa khóa có thể mở máy tính của bạn hoặc các khu vực thông tin riêng tư của bạn. Tên đăng nhập thường là công khai nên việc lựa chọn một mật khẩu an toàn là điều hết sức quan trọng và cần thiết.

Mật khẩu nên có ít nhất là 8 ký tự và có cả chữ và số. Bạn nên thường xuyên thay đổi mật khẩu. Chính sách mật khẩu đúng đắn nhất là không bao giờ cho bất kỳ ai biết mật khẩu của mình. Ngoài ra, không nên viết mật khẩu ra giấy, không nên đặt mật khẩu đơn giản quá… Điều cuối cùng cần nói đến là hãy nhớ mật khẩu của mình; trong một số trường hợp dữ liệu không thể khôi phục lại được một khi bị mất mật khẩu

Huỷ dữ liệu

Đôi khi, huỷ dữ liệu cũng là một vấn đề lớn. Bạn nên chú ý rằng dữ liệu có thể được khôi phục rất dễ dàng bởi những phần mềm chuyên dụng nếu bạn chỉ dùng những lệnh xoá thông thường, kể cả những lệnh xoá mà bạn nghĩ đó là lệnh xoá vĩnh viễn hay lệnh format - định dạng lại đĩa.

Có hai cách sau được coi như là cách huỷ dữ liệu an toàn và bạn có thể yên tâm rằng sau khi huỷ, khó ai có thể sử dụng phần mềm khôi phục lại được

- Dữ liệu sẽ bị huỷ vĩnh viễn nếu bạn thực sự phá hỏng nó về mặt vật lý. Tuy nhiên, cách thức này có vẻ không hay lắm khi mà thực sự muốn huỷ dữ liệu nào, bạn lại phải phá huỷ thiết bị lưu trữ đó đi.
- Bạn nên sử dụng các phần mềm huỷ dữ liệu chuyên dụng (như Norton Wipe). Phần mềm này làm việc giống như cách thức mà máy huỷ giấy làm, có nghĩa là dữ liệu của bạn sẽ bị xử lý rất vụn ra rồi mới bị xoá hẳn.

Quản lý khách thăm quan?

Khi bạn cho khách vào cơ quan của bạn, họ phải được quản lý hoặc được để mắt tới. Ngày nay, với sự phát triển của các thiết bị lưu trữ tiện dụng như các thiết bị lưu trữ cầm tay chuẩn USB, nếu máy tính của bạn đang bật và lại không có mật khẩu bảo vệ, khách có thể nhanh chóng lấy dữ liệu từ máy tính đó khi không có người quản lý.

Mục đích và giá trị của việc sao lưu dữ liệu

Tại sao phải sao lưu?

Thứ quan trọng nhất mà bạn lưu trữ trong máy tính là thông tin. Thông thường chúng được lưu trong ổ đĩa cứng qua nhiều năm. Nếu đĩa cứng không may bị hỏng, toàn bộ dữ liệu sẽ bị mất. Vì lý do này mà bạn nên sao lưu dữ liệu ra các thiết bị sao lưu chuyên dụng. Trong những tổ chức lớn thủ tục sao lưu được thực hiện tự động bởi đội ngũ hỗ trợ máy tính và dữliệu được giữ trong một máy tính trung tâm hoặc trong các khu chứa chuyên dụng.

Trong các tổ chức nhỏ hơn, sao lưu các tệp tin của bạn sang đĩa mềm hoặc đĩa CD và cất vào chỗ khác. Trong trường hợp có vấn đề, máy tính bị hỏng và ổ cứng không hoạt động, lấy lại thông tin đã sao lưu ra để có thể tiếp tục làm việc.

Thiết lập máy tính để sao lưu hiệu quả

Bạn nên có các chính sách sao lưu dữ liệu của riêng mình sao cho hiệu quả và phù hợp với nhu cầu. Ví dụ, thư mục chứa tài liệu của bạn luôn được cập nhật tài liệu mới, như vậy, bạn có thể thiết đặt máy tính của mình hàng ngày sao lưu thư mục đó ra vùng nhớ khác vào một thời điểm nhất định.

Sao lưu toàn bộ và sao lưu một phần

Sao lưu toàn bộ (Complete backup) có nghĩa là sao lưu tất cả dữ liệu trong máy tính của bạn. Điều này có thuận lợi là toàn bộ đĩa cứng có thể được sao lưu, nhưng điểm không thuận lợi là quá trình này có thể mất nhiều thời gian.

Sao lưu một phần (Incremental backup) có nghĩa là bạn chỉ sao lưu những tệp tin mà bạn vừa mới tạo hoặc sửa từ lần sao lưu lần trước, tiết kiệm thời gian. Với phần mềm sao lưu, quá trình này là tự động và thông thường bạn chỉ phải chọn full hay incremental.

Nên lưu ý việc sao lưu dữ liệu bằng cách chuyển dữ liệu sang máy tính khác. Nếu một người nào đó ăn cắp máy tính của bạn thì bạn cũng mất luôn cả những dữ liệu đã sao lưu. Nếu có sự cố hoả hoạn, bạn cũng mất dữ liệu đã lưu trong máy tính đó. Cho nên kết quả sao lưu nên được đặt ở những nơi an toàn. Tốt nhất là lưu ở những nơi chống được hoả hoạn

Thận trọng khi sao lưu các tệp tin đang mở

Bạn nên thực thiện sao lưu vào buổi tối (lúc không làm việc). Nếu bạn sao lưu trong lúc làm việc thì tệp tin chương trình hoặc dữ liệu của bạn mà đang được sử dụng sẽ không được sao lưu, chương trình sao lưu sẽ bỏ qua các tệp tin đang mở.

Khả năng mất cắp máy tính xách tay, PDA, điện thoại di động

Trường hợp mất cắp máy tính xách tay

Máy tính xách tay rất linh hoạt và tiện dụng nên phần lớn thông tin quan trọng bạn đều lưu giữ trong đó. Tuy nhiên chính vì sự nhỏ gọn và việc bạn hay mang đi theo này mà trong trường hợp rủi ro bị mất, nếu không có mật khẩu hoặc chính sách bảo vệ thì tất cả dữ liệu trong máy tính có thể bị xâm phạm. Chính vì vậy, điều đầu tiên là bạn cần bảo quản máy thật tốt và thứ đến là hãy thiết lập các tính năng bảo vệ dữ liệu cho máy bằng các hình thức thiết đặt mật khẩu truy nhập.

Trường hợp mất cắp PDA hay điện thoại di động.

PDA hay điện thoại di động cũng giống như máy tính xách tay, lưu trữ rất nhiều thông tin cá nhân, đòi hỏi bạn phải cẩn thận và có thiết lập cơ chế an toàn, bảo mật đề phòng trong trường hợp bị mất điện thoại.

Virút máy tính

Virút máy tính và những tác hại

Virút là những chương trình nhỏ, xâm nhập bất hợp pháp vào trong máy tính của bạn, có khả năng tự sao chép bản thân nó và tự ẩn nấp trên ổ đĩa (cả đĩa cứng, đĩa mềm, đĩa CD, đĩa ZIP…).

Chính nhờ khả năng tự sao chép bản thân mà vivút máy tính có thể lây nhiễm đến các máy tính khác thông qua các con đường như sao chép tệp tin bằng đĩa mềm hay qua việc truyền thông tin từ máy này đến máy khác trên môi trường mạng.

Ngoài phần có khả năng tự lây nhiễm và nhân bản, virút máy tính còn có phần ngòi nổ, đây chính là phần thực hiện công việc đặc thù của virút và thường là phá hoại. Ví dụ, virút có thể xoá một phần hoặc hoàn toàn ổ cứng của bạn.

Để biết được sự tồn tại của virút, ngoài các hậu quả rõ rệt do bạn phát hiện ra đối với các tài nguyên trong máy hoặc thấy máy có những triệu trứng bất thường như chạy chậm, hay bị treo… bạn cần sử dụng chương trình phần mềm phát hiện và tiêu diệt virút. Các phần mềm đó sẽ thông báo rằng máy bạn có bị nhiễm virút hay không, nếu có thì tên của con virút đó là gì.

Bạn có thể hình dung con đường lây lan trên toàn thế giới của một con virút như sau: Đầu tiên, nó tự phát tán bằng cách gửi thư điện tử tới tất cả những địa chỉ thư mà nó biết trên mạng. Sau đó, nếu ai đó nhận được những bức thư này và vô tình mở thư cũng như tệp tin đính kèm ra (virút nằm trong tệp tin đính kèm này), hộp thư của người đó sẽ bị

nhiễm virút và tất cả những người nằm trong sổ địa chỉ của hộp thư đó sẽ lại nhận được một bức thư chứa virút với nội dung tương tự (thường là có nội dung rất hấp dẫn và kích thích người nhận tò mò mở ra). Cứ như thế, trong một giờ đồng hồ, con virút này có khả năng lây lan trên toàn thế giới.

Phần mềm diệt virút và công việc ngăn cản sự phá hoại của virút

Để ngăn cản sự phá hoại của virút, tốt hơn hết là phải phòng tránh ngay từ đầu sự xâm nhập và lây lan của virút bằng cách sử dụng các phần mềm cho phép phát hiện và diệt virút để kiểm tra dữ liệu trước khi vào hoặc ra khỏi máy. Nhưng điều cơ bản để có thể sử dụng các phần mềm này một cách hiệu quả là chúng cần phải được thường xuyên cập nhật bởi mỗi ngày lại có một loại virút mới và phần mềm diệt virút ngày hôm nay thì chỉ biết những virút từ hôm nay về trước mà thôi.

Các tập tin cập nhật virút cho phép chương trình có thể phát hiện ra nhiều loại virút mới và các tệp tin này được đặt trên trang web của nhà cung cấp trên Internet. Bạn cần tải chúng về hàng ngày từ những địa chỉ này.

Ở Việt Nam, có hai phần mềm diệt virút khá hiệu quả là BKAV của tác giả Nguyễn Tử Quảng, Đại học Bách Khoa Hà Nội và D2 của tác giả Trương Minh Nhật Quang, Đại học Cần Thơ. Hai phần mềm này đều được tải về miễn phí từ Internet (có kích thước rất gọn nhẹ) và quan trọng hơn là chúng vẫn đang được cập nhật danh sách virút hàng ngày nên bạn luôn có thể có được những phiên bản mới nhất.

Địa chỉ tải về của BKAV là http://www.bkav.com.vn và của D2 là http://www.ctu.edu.vn

Ngoài các phần mềm của Việt Nam kể trên, bạn nên kết hợp cùng các phần mềm có tên tuổi của nước ngoài. Norton Antivirus của hãng Symantec là một trong những sản phẩm hàng đầu thế giới về nhận dạng và tiêu diệt virút. Nếu bạn có bộ cài đặt của phần mềm này thì cách thức sử dụng gồm hai bước như sau :

- Cài đặt phần mềm
- Tải về và chạy tệp tin cập nhật danh sách virút mới nhất cho phần mềm đó từ địa chỉ http://www.symantec.com

Bảo vệ máy tính khỏi virút và phải làm gì khi máy tính bị nhiễm virút

Cách an toàn nhất là sử dụng một máy tính không nối mạng nội bộ hoặc Internet, không sử dụng đĩa mềm đã được sử dụng bởi các máy tính khác. Tuy nhiên, không thể cô lập máy tính của mình như vậy được. Bạn vẫn phải mở cửa để máy tính của mình giao lưu với thế giới bên ngoài, tất nhiên là trong một tư thế cảnh giác cao độ, ví dụ như:

- Sử dụng phần mềm quét virút để quét tất cả các tệp tin vào/ra khỏi máy tính của bạn
- Thiết đặt các chế độ bảo vệ (security) cho các chương trình như trình duyệt, chương trình soạn thảo văn bản... theo các chỉ dẫn của các chương trình này.
- Nên sử dụng tất cả các bản sửa lỗi của Microsoft để hạn chế các lỗ hổng bảo mật. Virút máy tính thường tận dụng những lỗ hổng này để xâm nhập vào máy tính của bạn

Nếu bạn nhận được thông báo có một virút trong máy tính thì bạn đừng hoảng sợ bởi nếu chương trình tìm virút đưa ra thông báo như vậy thì chứng tỏ là chương trình đã nhận diện ra virút rồi và có khả năng sẽ khống chế được virút này. Trong mọi trường hợp, bạn nên đọc kỹ thông báo xem chương trình diệt virút đã xử lý thế nào, sau đó bạn nên làm theo hướng dẫn của phần mềm diệt virút để có thể có thao tác đúng với những virút đang có trong máy