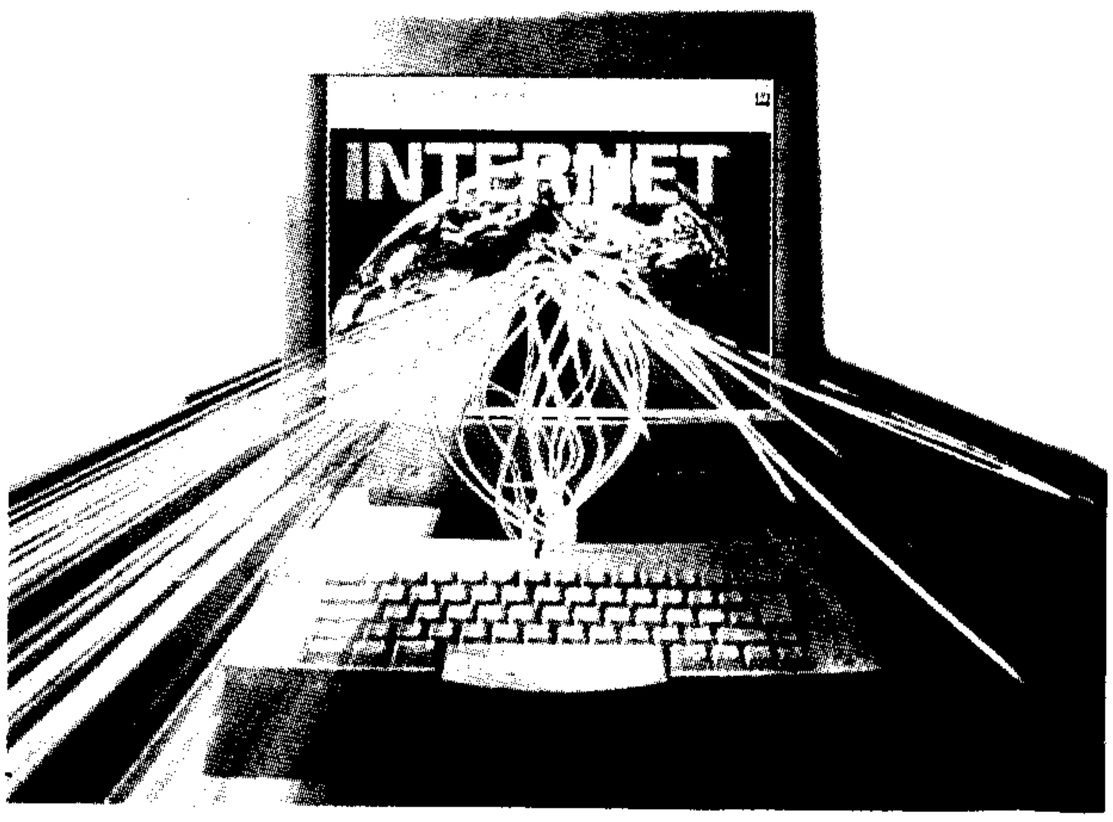
Bảo vệ máy tính KHI NỐI MẠNG INTERNET



TIẾN THÀNH

Internet luôn luôn là mối đe dọa về mọi mặt đối với bất cứ ai lướt mạng Internet, ngay cả đối với những người biết và đề phòng nó. Theo báo cáo tội phạm mạng năm 2011 của Norton, trên phạm vi toàn cầu, mỗi ngày có 1 triệu người trở thành nạn nhân của tội phạm mạng. Chính vì thế, dù là người chuyên hay không chuyên trong lĩnh vực tin học bạn cũng cần trang bị cho mình một số kiến thức cơ bản tự bảo vệ mình thật sự an toàn khi khám phá Internet.

Các mối đe dọa của Internet

Điều đáng quan tâm về mối đe dọa từ Internet hiện nay vẫn là các phần mềm gián điệp (spyware) hay virus vì thế cần nắm vững mọi chức năng hoạt động của chúng như sau:

* **Malware** (là từ viết tắt của malicious software có nghĩa là phần mềm độc hại): chúng tồn tại và hoạt động trên máy tính của bạn một cách tự do. Malware có thể hiểu là phần mềm độc hại và bao gồm: virus, spyware, keylogger, và Trojan…

* **Spyware** (phần mềm gián điệp): đây là một loại phần mềm gián điệp để thu thập thông tin về người dùng, bao gồm cả thông tin cá nhân và thói quen (các trang web mà bạn thường truy cập). Nó còn có khả năng kích hoạt các quảng cáo và cài đặt phần mềm độc hại khác.

* **Virus:** là một loại phần mềm độc hại có thể tự nhân bản và lây nhiễm các máy tính khác thông qua mạng lưới hoặc phương tiện truyền thông (chẳng hạn như một ổ đĩa flash). Virus có thể làm nhiều điều có hại cho máy tính của bạn, chẳng hạn như đi lại và sử dụng nó cho mục đích độc hại.

Bảo mật bên trong máy tính

* **Đặt mật khẩu cho file:** Một số người lưu các mật khẩu, chi tiết tài khoản ngân hàng và những thông tin cá nhân khác trong tài liệu Word. Sau đó họ nhét file đó vào một thư mục nào đó như Backup trong ổ cứng. Chuyện gì sẽ xảy ra nếu như laptop của họ bị mất cắp? Giải pháp là khóa tài liệu đó bằng mật khẩu. Cách làm là vào **File**, chọn **Save As**, kích chuột vào **Tools**, chọn **Security Options**. Kích vào thẻ **Advanced**, chọn **Microsoft Enhanced Cryptographic Provider**, nhấn nút Ok. Sau đó, bạn nhập mật khẩu vào ô **"Password to open"**, rồi nhấn tiếp Ok. Bạn sẽ được đề nghị nhập lại mật khẩu lần nữa. Sau khi hoàn tất động tác đó, bạn kích chuột vào nút **Save**. Như vậy, file đó đã được mã hóa nhưng điều quan trọng là đừng có quên mật khẩu.

* **Khóa máy tính tự động:** Máy tính văn phòng thường được bảo vệ cẩn thận bằng mật khẩu để chống thâm nhập trái phép. Tuy nhiên, máy tính đó vẫn có nguy cơ bị thâm nhập trong khoảng thời gian ngắn khi bạn ra ngoài. Cách đối phó với vấn đề này là bật tính năng bảo vệ màn hình bằng mật khẩu. Vào **Start**, chọn **Control Panel**, chọn **Display**. Chọn thẻ **Screen Saver**, kích vào ô **"On resume, password protect"**.

Bảo mật máy tính khi truy cập Internet

* **Cài đặt phần mềm bảo vệ:** Hãy chắc rằng

hệ điều hành của bạn được cập nhật tự động và bức tường lửa (**firewall**) được bật lên và Sử dụng các chương trình bảo mật bao gồm phần mềm chống virus và **spyware**, đăng ký cập nhật các phần mềm này. Quét toàn bộ máy ít nhất một tháng một lần.

*** Sử dụng Email:** Không mở các file đính kèm hay ấn chuột vào những đường link trong email từ những ngươi bạn không quen biết. Sử dụng mật khẩu ít nhất 8 ký tự hoặc số và biểu tượng và thường xuyên thay đổi chúng.

*** Bảo mật tài khoản Gmail:** Theo Google, nếu người dùng truy cập dịch vụ thư điện tử Gmail trên mạng công cộng không mã hóa hay trên mạng không dây, các tài khoản Gmail của họ có thể dễ bị tấn công hơn. Giải pháp cho vấn đề này là chỉ cần thay đổi vài thiết lập của tài khoản. Vào mục **Settings** nằm ở góc trên bên phải cửa sổ Gmail window, tìm đến mục "**Browser connection**" trong thẻ **General**, kích chuột vào ô "**Always use https**", sau đó nhấn vào nút **Save Changes**. Với động tác đó, bạn đã kích hoạt tính năng mã hóa của Gmail. Việc kích hoạt tính năng bảo mật email này có thể khiến cho việc mở Gmail lâu hơn một nhưng nó sẽ gây ra khó khăn với những hacker muốn ăn cắp thông tin.

*** Đóng cổng mạng không dây:** Mở mạng không dây tự do cũng tương tự như một ngôi nhà không có khóa. Bất kỳ ai trong phạm vi phủ sóng không dây (dài ngắn khác nhau tùy vào chuẩn kết nối không dây) của router đều có thể nhìn thấy mạng của bạn, ăn cắp băng thông hoặc nguy hiểm hơn là thâm nhập trái phép vào các máy tính bên trong mạng. Giải pháp cho vấn đề này là đóng cửa mạng không dây. Đầu tiên hãy mở trình duyệt Internet, gõ địa chỉ của router (ví dụ như 192.168.1.1) vào thanh địa chỉ rồi nhấn Enter để mở nó. Sau đó nhập tên tài khoản và mật khẩu để mở tiện ích thiết lập của router. Để đổi mật khẩu mới, bạn sẽ phải nhập mật khẩu cũ. Nếu bạn chưa bao giờ đổi tên người dùng và mật khẩu của router, tên người dùng và mật khẩu mặc định là admin với router của Linksys và D-link. Cách thức đổi mật khẩu router của mỗi hãng khác nhau. Ví dụ, với router Linksys, bạn có thể đổi mật khẩu ở thẻ Administration. Trong router Belkin, có thể vào System Settings. Còn trong D-Link, bạn có thể đổi mật khẩu ở mục Admin trong thẻ Tools. Chọn mật khẩu mới cho router nên dài hơn 8 ký tự và sử dụng kết hợp cả số, chữ hoa và chữ thường hoặc có thêm ký tự đặc biệt thì càng tốt. Sau khi đổi mật khẩu, bạn nên vô hiệu hóa tính năng phát tín hiệu SSID. Mỗi loại router có cách vô hiệu hóa khác nhau do sự khác biệt về giao diện. Ví dụ, với router D-Link thì vào Wireless, chọn thẻ Home, chọn nút Off ở lựa chọn Wireless Radio. Tương tự với router LinkSys, chọn Wireless, rồi Basic Wireless Settings và nhấn chuột vào nút Disable.

*** Kết nối internet**: Không kết nối Internet và sử dụng mạng không dây mà không có mật khẩu. Không gửi thông tin nhạy cảm tới một trang Web mà không bắt đầu bằng "http", cụm từ "http" có nghĩa là nó được bảo vệ.

T.T