HỘI ĐỒNG CHỈ ĐẠO XUẤT BẢN
SÁCH XÃ, PHƯỜNG, THỊ TRẤN

SỬ DỤNG INTERNET AN TOÀN VÀ HIỆU QUẢ

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA

NHÀ XUẤT BẢN GIAO THÔNG VẬN TẢI

https://tieulun.hopto.org

https://tieulun.hopto.org

SỬ DỤNG INTERNET AN TOÀN VÀ HIỆU QUẢ

https://tieulun.hopto.org

HỘI ĐỒNG CHỈ ĐẠO XUẤT BẢN

Chủ tịch Hội đồng

TS. NGUYỄN THẾ KỶ

Phó Chủ tịch Hội đồng

TS. NGUYỄN DUY HÙNG

Thành viên

TS. NGUYỄN AN TIÊM

TS. KHUẤT DUY KIM HẢI

NGUYỄN VŨ THANH HẢO

https://tieulun.hopto.org

https://tieulun.hopto.org

SỬ DỤNG INTERNET AN TOÀN VÀ HIỆU QUẢ

NHÀ XUẤT BẢN
CHÍNH TRỊ QUỐC GIA

NHÀ XUẤT BẢN
GIAO THÔNG VẬN TẢI

HÀ NỘI - 2012

https://tieulun.hopto.org

https://tieulun.hopto.org

LỜI NHÀ XUẤT BẢN

Internet đang ngày càng phát triển với tốc độ như vũ bão tại Việt Nam. Đến nay, số người sử dụng Internet của nước ta gần bằng 33% số dân, một mức khá cao ở khu vực Đông Nam Á và châu Á. Nhờ Internet, mọi người có thể mở rộng quan hệ đến các bạn bè trên thế giới, trong đó *Chat* là một hình thức giao lưu kết bạn thật thú vị nếu như nó được sử dụng đúng mục đích. Xét về mặt tích cực, Internet giúp ích rất nhiều cho mọi người trong cuộc sống với những tiện ích mà nó mang lại: thông tin các mặt, học tập online, trau dồi trình độ tin học, ngoại ngữ, xem phim, trò chơi trực tuyến, ứng xử giao tiếp, bày tỏ ý kiến, học hỏi kinh nghiệm... Kiến thức trên mạng thật đa dạng, rộng lớn. Internet là đòn bẩy giúp phát huy sức mạnh cộng đồng, trong đó có sức mạnh của những người trẻ, góp sức xây dựng và phát triển khoa học, công nghệ, phát triển kinh tế tri thức.

Tuy nhiên, Internet với những lợi hại khó lường có thể ví như con dao hai lưỡi đối với người sử dụng, thậm chí với cả xã hội, nhất là giới trẻ. Điều quan trọng là phải tạo cho mọi người có "sức đề kháng" với

https://tieulun.hopto.org

những ẩn họa trong các trang web. Muốn vậy, cùng với việc tăng cường giáo dục, đạo đức, nhân cách, bản lĩnh, hướng dẫn, xây dựng mục đích sử dụng Internet đúng đắn, cần trang bị những kiến thức cần thiết để truy cập web một cách an toàn và hiệu quả.

Nhằm góp phần đáp ứng những yêu cầu nêu trên, Nhà xuất bản Chính trị quốc gia - Sự thật phối hợp với Nhà xuất bản Giao thông vận tải xuất bản cuốn sách: **Sử dụng Internet an toàn và hiệu quả** trong khuôn khổ Đề án trang bị sách cho cơ sở xã, phường, thị trấn năm 2012.

Xin giới thiệu cuốn sách với bạn đọc.

Tháng 6 năm 2012

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA - SỰ THẬT

https://tieulun.hopto.org

LỜI NÓI ĐẦU

Internet đang ngày càng phát triển do khả năng truyền tải thông tin nhanh nhạy, hiệu quả và đã trở thành một phương tiện không thể thiếu được cho sự phát triển của xã hội. Internet đã đi vào cuộc sống như một nhu cầu tất yếu.

Với đủ mọi thành phần và lứa tuổi tham gia, Internet cũng có mặt trái của nó: nhiều trang web có nội dung không lành mạnh; những kẻ lừa đảo luôn rình mò để ăn trộm những thông tin cá nhân với ý đồ xấu; khi sử dụng thư điện tử luôn bị các thư rác (spam) tấn công gây nên những bức bối cho nhiều người sử dụng; những virus máy tính có thể xâm nhập làm tê liệt các máy tính cá nhân và cả các hệ thống mạng tại các công sở là những nguy hại không thể lường trước được.

Trước tình hình đó, đòi hỏi người sử dụng máy tính truy cập vào Internet cần được trang bị những kiến thức cần thiết để truy cập web một cách an toàn và hiệu quả, bảo vệ dữ liệu trên máy tính của mình, bảo vệ được thông tin cá nhân. Những gia đình có trẻ em truy cập Internet cần có những am hiểu cần thiết

https://tieulun.hopto.org

để khi sử dụng Internet, tránh được những hậu quả nghiêm trọng do mặt trái của Internet mang lại.

Nội dung của cuốn sách được chia thành 4 phần và 11 chương. Phần I: "Inernet và những chuẩn bị cần thiết trước khi cài đặt kết nối Internet". Phần II: "Những nguy cơ tiềm ẩn và cách phòng chống", Phần III: "Bảo mật khi truy cập Internet và sử dụng thư điện tử"; Phần IV: "Sử dụng Internet an toàn cho trẻ em".

Đối tượng phục vụ của cuốn sách này là tất cả những ai có nhu cầu truy cập Internet một cách an toàn, kể cả những người mới bắt đầu sử dụng, có nhu cầu bảo vệ dữ liệu, bảo vệ những thông tin cá nhân khi truy cập Internet, có nhu cầu quản lý, giúp đỡ và định hướng trẻ em sử dụng Internet đúng mục đích và hiệu quả để tránh được những hiểm họa do mặt trái của Internet mang lại.

Xin chân thành cảm ơn Nhà xuất bản Chính trị quốc gia và Nhà xuất bản Giao thông vận tải đã biên tập và xuất bản cuốn sách này. Cảm ơn các bạn đọc gần xa đã đóng góp ý kiến để cuốn sách ngày càng hoàn thiện hơn.

Hà Nội, tháng 5 năm 2012

KS. Hoàng Hồng

https://tieulun.hopto.org

Phần I

Internet và những chuẩn bị cần thiết trước khi cài đặt kết nối Internet

https://tieulun.hopto.org

https://tieulun.hopto.org

Chương I

INTERNET VÀ ĐỐI TƯỢNG PHỤC VỤ CỦA CUỐN SÁCH

1. Đối tượng phục vụ của cuốn sách này

a. Giới thiệu chung

Internet là một công cụ truyền tải thông tin nhanh nhạy và hiệu quả nhất. Nó đã trở thành một phương tiện không thể thiếu được trong cuộc sống của con người, trên thế giới nói chung và ở Việt Nam nói riêng. Internet đã đi vào cuộc sống không chỉ ở thành thị mà đã phát triển mạnh ở nông thôn, không những trong nhà trường mà còn được triển khai rộng rãi ở các điểm truy cập công cộng. Internet không chỉ cung cấp các kiến thức rộng lớn về khoa học, kỹ thuật mà còn đáp ứng các nhu cầu giải trí, thông tin văn hóa, xã hội; là một nhịp cầu giao lưu tình cảm của con người trên toàn thế giới.

Vì là một môi trường mở, với đủ mọi thành phần, tầng lớp tham gia, Internet cũng có mặt trái của nó. Không ít trang web có nội dung không lành mạnh. Những kẻ tin tặc luôn rình mò để ăn trộm những thông tin cá nhân với mục đích xấu. Những virus máy tính có thể xâm nhập làm tê liệt các máy tính cá nhân và cả các hệ

https://tieulun.hopto.org

thống mạng tại các công sở là những nguy hại không thể lường trước được...

Trước tình hình đó, đòi hỏi người sử dụng máy tính truy cập vào Internet cần được trang bị những kiến thức cần thiết để bảo vệ dữ liệu trên máy tính của mình, bảo vệ được thông tin cá nhân, truy cập web, sử dụng thư điện tử một cách an toàn và hiệu quả. Đặc biệt, cần có những cách thức cần thiết để bảo vệ con em trong gia đình khi sử dụng Internet, tránh được những hậu quả nghiêm trọng do mặt trái của Internet mang lại.

b. Đối tượng phục vụ của cuốn sách này

Cuốn sách này không đi sâu phân tích về mặt công nghệ cũng như bản chất của các vấn đề, không là tài liệu hướng dẫn sử dụng Internet cũng như cách cài đặt các ứng dụng của thư điện tử.

Với ý tưởng bảo mật dữ liệu các thông tin trên máy tính cá nhân nói chung và máy tính trong gia đình nói riêng, cuốn sách này hướng dẫn người sử dụng Internet các thao tác cần thiết để sử dụng Internet một cách an toàn, tránh được những hậu quả do mặt trái của Internet mang lại. Với cố gắng ở mức độ đơn giản nhất có thể, cuốn sách này không hướng dẫn các biện pháp bảo mật quá phức tạp đòi hỏi phải có trình độ về công nghệ ở một mức nào đó và cũng không đi sâu vào việc sử dụng Internet vào các mục đích thương mại điện tử như một số nước tiên tiến về công nghệ thông tin khác.

https://tieulun.hopto.org

Cuốn sách này là đối tượng phục vụ cho tất cả những ai đang sử dụng máy tính kết nối Internet, kể cả những người mới bắt đầu sử dụng, có nhu cầu bảo vệ dữ liệu, bảo vệ những thông tin cá nhân khi truy cập Internet. Đặc biệt là các gia đình có trẻ em sử dụng Internet với nhu cầu học tập và tìm hiểu các kiến thức về khoa học, văn hóa và xã hội cần biết được những biện pháp để việc truy cập Internet được an toàn.

2. Giới thiệu chung về Internet

a. Internet là gì?

Internet, cũng được biết với tên gọi là Net, là mạng máy tính lớn nhất thế giới, hay nói chính xác hơn, là mạng của các mạng, tức là bao gồm nhiều mạng máy tính được nối lại với nhau. Internet bao gồm nhiều máy chủ, cho phép bất kỳ một máy tính nào trong mạng có thể kết nối với bất kỳ máy tính nào khác để trao đổi thông tin với nhau. Khi đã kết nối vào Internet, máy tính của bạn là một trong số hàng chục triệu thành viên của mạng khổng lồ này.

Không ai biết Internet có bao nhiêu thành viên, các con số chỉ là ước đoán. Thực chất Internet không thuộc quyền quản lý của bất kỳ ai. Nó không có giám đốc, không có ban quản trị. Bạn có thể tham gia hoặc không tham gia vào Internet, đó là quyền của mỗi thành viên. Mỗi mạng thành phần sẽ có một giám đốc hay chủ

https://tieulun.hopto.org

tịch, một cơ quan chính phủ hoặc một hãng điều hành, nhưng không có một tổ chức nào chịu trách nhiệm về toàn bộ Internet.

Chúng được kết nối theo một giao thức đặc biệt gọi là TCP/IP (Transmission Control Protocol) thông qua các hệ thống kênh truyền thông.

b. Một số khái niệm cơ bản

(1) *Client và Server*

Cho dù ở khoảng cách xa hay gần, mạng máy tính kết nối các máy tính lại và cho phép chúng chia sẻ dữ liệu. Nhưng việc kết nối và chia sẻ dữ liệu không xảy ra một cách tự động. Các nhà lập trình đã tạo ra hai loại chương trình máy tính, đó là Server (chủ) và Client (khách).

Server: Là chương trình cung cấp thông tin trên một mạng máy tính. Chúng được thiết kế để nhiều máy tính có thể truy xuất: đọc, tải dữ liệu... một cách đồng thời.

Client: Là chương trình chạy trên máy của người sử dụng. Một chương trình Client được thiết kế để làm việc với một dạng Server nào đó.

Về cơ bản, Internet Explorer là một bộ rất nhiều các chương trình Client, mà mỗi phần mềm trong đó được thiết kế để truy cập một loại Server nào đó có mặt trên Internet.

(2) *Giao thức TCP/IP*

Giao thức TCP/IP (Transmission Control Protocol) là một giao thức chuẩn trên Internet, cho phép truyền dữ liệu từ máy tính này đến

https://tieulun.hopto.org

máy tính khác trên mạng. Nhờ giao thức này mà các máy chủ (Server) trên Internet được kết nối với nhau.

(3) *Địa chỉ IP*

Để các máy tính có thể liên lạc với nhau thì mỗi máy phải có một địa chỉ riêng biệt, gọi là địa chỉ IP (Internet Protocol). Địa chỉ IP được chia thành 4 nhóm. Các nhóm cách nhau bởi dấu chấm (.). Mỗi nhóm gồm 3 chữ số có giá trị từ 0 đến 255 và có dạng yyy.yyy.yyy.yyy, trong đó, yyy nhận giá trị từ 0 - 255 và không nhất thiết phải đủ ba chữ số.

Ví dụ: 221.16.0.2

c. Các dịch vụ trên Internet

(1) *WWW (World Wide Web)* gọi tắt là trang web

Đây là trang thông tin liên kết gồm văn bản, âm thanh, hình ảnh... Dịch vụ này cho phép liên kết từ trang web này đến trang web khác.

(2) *Email (thư điện tử)*

Dịch vụ thư điện tử cho phép nhận và gửi thư từ máy này đến máy khác một cách nhanh chóng. Thông tin được gửi đi bao gồm: văn bản, ảnh, hình vẽ, âm nhạc...

(3) *FTP (File Transfer Protocol)*

Phương thức truyền tệp dữ liệu. Dịch vụ này cho phép truyền các tệp dữ liệu từ máy tính này đến máy tính khác.

https://tieulun.hopto.org

(4) *Chat*

Là hình thức hội thoại trực tiếp trên Internet, dịch vụ này cho phép hai hay nhiều người có thể cùng trao đổi thông tin trực tuyến bao gồm cả hình ảnh và âm nhạc.

(5) *Telnet*

Dịch vụ này cho phép truy cập đến hệ thống máy tính khác trên mạng.

(6) *Gopher*

Là công cụ cho phép duyệt các cơ sở dữ liệu và truyền các tệp dữ liệu thông qua các site tìm kiếm.

(7) *Newsgroup*

Cho phép nhóm người có thể trao đổi với nhau về lĩnh vực nào đó, chẳng hạn: kinh tế, y tế, giáo dục...

d. Một số thuật ngữ

(1) *Máy chủ web*

Một chương trình chờ các yêu cầu từ trình duyệt về một trang web cụ thể (hay một máy tính có chạy chương trình này). Máy chủ gửi lại nội dung trang đó và lại chờ cho các yêu cầu khác.

(2) *Website*

Một tập hợp các trang web (webpage). Một website có một địa chỉ Internet xác định.

Ví dụ: www.sdcvietnam.com

(3) *Webpage*

Một trang web là một phần của website được kết nối từ trang chủ hoặc từ một trang web khác. Webpage phản ánh một nội dung nào đó và có

https://tieulun.hopto.org

chiều dài có thể ngắn hơn hoặc dài hơn một trang màn hình. Thông thường, một webpage dài khoảng hai trang màn hình.

(4) *Homepage*

Là trang chủ hay thường gọi là trang chính đóng vai trò giới thiệu về trang web và liên kết tới các trang. Trang này sẽ liên kết tới các webpage trong cùng website hoặc các website khác. Khi truy cập vào website thì đa số các trường hợp, trang chủ sẽ được mở đầu tiên.

(5) *Địa chỉ website hay URL (Uniform Resource Locator)*

Website hay URL: là tập hợp các trang web. Một website hay một dịch vụ trên web có một địa chỉ duy nhất trên Internet dùng để định rõ vị trí của nó. Hầu hết các website chứa hàng chục, hàng trăm, hay hàng ngàn trang web.

e. Một số phần mở rộng của các trang web thông dụng

.com:	Tổ chức thương mại, doanh nghiệp
.gov:	Các tổ chức chính phủ
.edu:	Các tổ chức giáo dục
.int:	Các tổ chức quốc tế
.mil:	Các tổ chức quân sự
.net:	Liên quan đến mạng
.org:	Các cơ quan nhà nước

f. Các ký hiệu tên miền của một số nước trên thế giới

vn:	Việt Nam

https://tieulun.hopto.org

au: Úc
at: Áo
be: Bỉ
ca: Canađa
fi: Phần Lan
fr: Pháp
de: Cộng hòa Liên bang Đức
il: Israel
it: Italia
jp: Nhật Bản

3. Một số điều cần lưu ý khi sử dụng cuốn sách này

a. Các phần mềm sử dụng

Cuốn sách này hướng dẫn sử dụng các biện pháp bảo mật trên máy tính cài đặt hệ điều hành Windows XP là hệ điều hành đang được cài đặt thông dụng nhất hiện nay ở Việt Nam cũng như trên thế giới. Cụ thể, các hướng dẫn cài đặt lấy hệ điều hành Windows XP Professional làm cơ sở để hướng dẫn sử dụng. Trong một số thao tác có sự khác nhau ở hệ điều hành Windows XP Home Editor, chúng tôi sẽ có hướng dẫn cụ thể. Với các hệ điều hành khác, một số thao tác có thể không hoàn toàn giống với những gì chúng tôi hướng dẫn. Mong các bạn thông cảm.

Trong cuốn sách này sử dụng Internet Explorer (IE), là trình duyệt thông dụng nhất

https://tieulun.hopto.org

đang được sử dụng làm cơ sở để hướng dẫn trong thao tác, cụ thể là trên Internet Explorer 6.0. Hiện nay mới xuất hiện Internet Explorer 7.0 với nhiều ưu điểm về bảo mật và chỉ chạy trên hệ điều hành Windows XP từ Service Pack 2 trở về sau và hệ điều hành Windows phải có bản quyền. Tuy nhiên, về bảng chọn và các cách thức tạo một số tính năng về bảo mật không khác nhiều đối với Internet Explorer 6.0. Trong một thao tác nếu có sự khác nhau giữa hai trình duyệt này, chúng tôi sẽ hướng dẫn cụ thể. Ngoài ra chúng tôi còn giới thiệu các thao tác cần thiết để thiết lập chế độ bảo mật khi truy cập Internet ở các trình duyệt khác là Firefox và Opera.

Trình duyệt gửi và nhận thư điện tử làm ví dụ hướng dẫn trong cuốn sách này là Outlook Express 6.0 và Microsoft Outlook 2003. Các phiên bản trước, như Outlook Express XP, Outlook Express 2000 và Microsoft Outlook XP..., có thể hơi khác về giao diện và thao tác khi cài đặt các tham số. Mong các bạn thông cảm.

b. Một số điều lưu ý trong bảng chọn Start và hộp thoại Control Panel của Windows XP

Vì hộp thoại Control Panel dùng để thiết lập các tham số cho hệ thống nên trong cuốn sách này có nhiều thao tác ở hộp thoại này. Tùy theo cách hiển thị trong bảng chọn Start của Windows mà có hai cách để vào hộp thoại Control Panel.

https://tieulun.hopto.org

Trong hướng dẫn các chương sau, khi có thao tác: Nhấn chuột vào nút Start... các bạn nên chú ý đến nội dung của mục này.

Khi nhấn chuột vào nút Start, bảng chọn Start xuất hiện và có hai dạng như sau:

Dạng 1
Để vào hộp thoại Control Panel, đưa con trỏ đến mục Settings. Khi này một bảng chọn phụ xuất hiện. Chọn mục Control Panel.

Dạng 2
Để vào hộp thoại Control Panel, chỉ việc nhấn chuột lên biểu tượng 

.

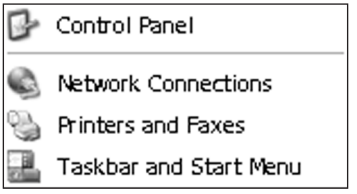
Trong các hướng dẫn ở các chương sau, chúng tôi luôn hướng dẫn theo cách ở *Dạng 1* do nhiều máy tính hiện nay đang sử dụng các phiên bản Windows 9.x.

Để thay đổi cách hiển thị từ *Dạng 1* sang *Dạng 2,* tiến hành như sau:

Nhấn chuột vào nút Start của Windows. Khi này bảng chọn Start xuất hiện. Đưa con trỏ đến

https://tieulun.hopto.org

mục Settings. Một bảng chọn phụ xuất hiện như hình sau:



Chọn mục Taskbar and Start Menu. Khi này hộp thoại Taskbar and Start Menu Properties xuất hiện. Nhấn chuột vào khung Start Menu. Khi này hộp thoại có dạng như hình sau:

- Nhấn chuột vào nút Classic Start menu.
- Nhấn chuột vào nút Apply.

https://tieulun.hopto.org

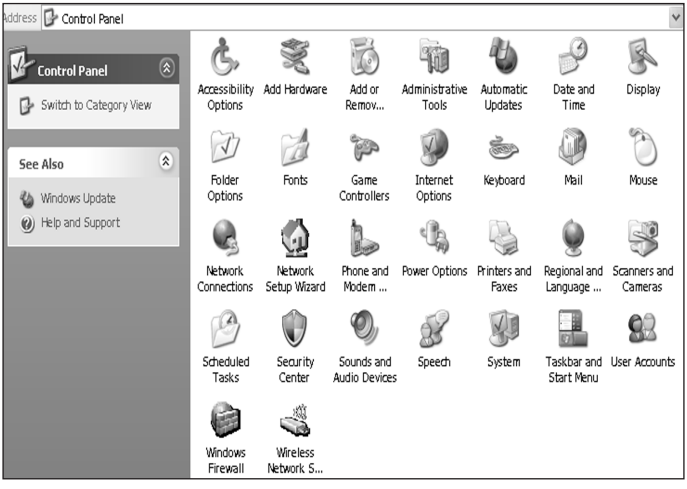
Để chuyển từ *Dạng 2* sang *Dạng 1*, tiến hành như sau:

Nhấn chuột vào nút Start của Windows, chọn Control Panel, khi này hộp thoại Control Panel xuất hiện.

Chọn biểu tượng . Khi này hộp thoại Taskbar and Start Menu Properties xuất hiện và tiến hành thao tác như trên.

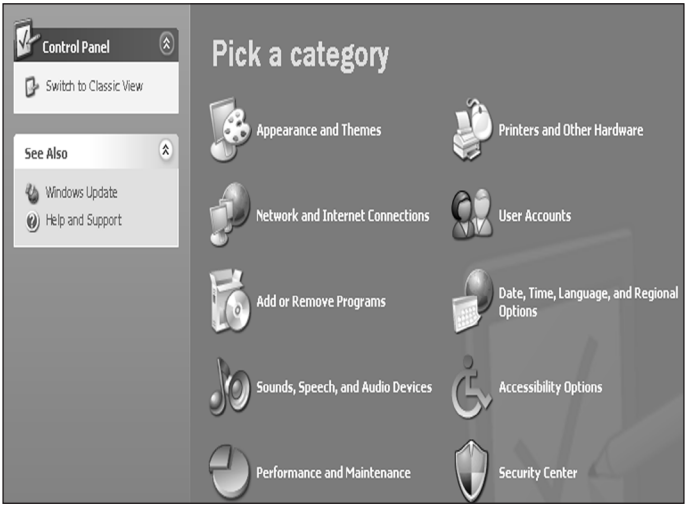
☞ *Xin các bạn lưu ý*: Hộp thoại Control Panel cũng có hai dạng hiển thị và chúng tôi sẽ giới thiệu ở dưới đây.

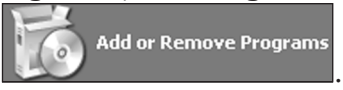
➢ *Dạng 1*: Dạng truyền thống, tương ứng Windows 9.x như hình sau:



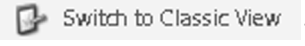
https://tieulun.hopto.org

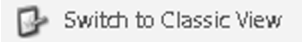
➢ *Dạng 2*: Theo chế độ đặc trưng

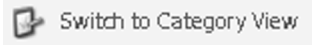


Để vào một chức năng nào đó, bạn nhấn chuột vào mục cần thiết. Ví dụ: Cài thêm hoặc ngắt một chương trình, nhấn chuột vào nút 

.

Để chuyển chế độ hiển thị từ *Dạng 2* sang *Dạng 1*, nhấn chuột vào nút 

. Khi này hộp thoại Control Panel trở về *Dạng 1* và nút 

trở thành 

để khi cần thiết thì nhấn chuột vào nút này để chuyển sang *Dạng 2*.

Trong các hướng dẫn cài đặt ở các chương sau, chúng tôi hướng dẫn bảng chọn Start ở *Dạng 1* và hộp thoại Control Panel cũng ở *Dạng 1*. Vì nhiều thao tác liên quan đến sử dụng hộp thoại

https://tieulun.hopto.org

nên chúng tôi không giới thiệu cả hai cách để mở hộp thoại. Nhìn chung, bạn nên thiết lập giao diện của hệ thống theo *Dạng 1* ở trên để tiện thiết lập các thông số cần thiết. Xin các bạn lưu ý.

https://tieulun.hopto.org

Chương II

CHUẨN BỊ TRƯỚC KHI CÀI ĐẶT KẾT NỐI INTERNET

1. Giới thiệu chung

Internet cung cấp nhiều kiến thức bổ ích cho người sử dụng nhưng đồng thời cũng là nguồn phát tán virus, trojan, spyware... Do nhiều nguyên nhân, hệ thống máy tính của bạn sẽ là đối tượng để chúng tấn công. Để bảo vệ máy tính trước những hậu quả có thể xảy ra khi cài đặt hệ thống kết nối với Internet, nên chuẩn bị những vấn đề cần thiết để phòng chống sự xâm nhập của virus, trojan, spyware... một cách tối đa. Trong trường hợp sự cố có thể xảy ra như máy bị nhiễm virus, hỏng dữ liệu, thậm chí có thể không khởi động lại được hệ thống thì đã có những đĩa CD-ROM cần thiết để khắc phục hậu quả.

2. Các bước chuẩn bị trước khi cài đặt kết nối Internet

a. Tạo đĩa khởi động CD-ROM

Nên tạo đĩa khởi động CD-ROM trước khi truy cập Internet. Bởi vì khi truy cập Internet, rất có thể sẽ bị virus xâm nhập từ mạng vào máy tính và làm hỏng hệ điều hành Windows.

https://tieulun.hopto.org

Để có thể lấy được dữ liệu và xử lý kịp thời, bạn cần phải khởi động Windows từ đĩa CD-ROM. Trong trường hợp này, hệ thống của bạn phải có ổ ghi CD.

b. Chuẩn bị các đĩa CD có chứa các chương trình chống virus

Chuẩn bị các đĩa có chứa phiên bản mới nhất của chương trình diệt virus mà bạn yêu thích. Nếu vẫn muốn giữ tính đơn giản thì sử dụng các chương trình diệt virus trong nước cũng đem lại hiệu quả cao là D32 và BKAV, những phần mềm diệt virus hàng đầu như Norton hay MacAfee thì rất tốt nhưng giá thành cao (nếu mua có bản quyền) và dung lượng lớn, việc cài đặt cũng đòi hỏi một chút kiên trì và kiến thức. Nên đưa thêm các công cụ diệt phần mềm gián điệp (spyware) như Spybot, và adware. Bạn cũng nên đưa những bản cập nhật các trình điều khiển (driver) mới nhất cho card đồ họa, âm thanh.

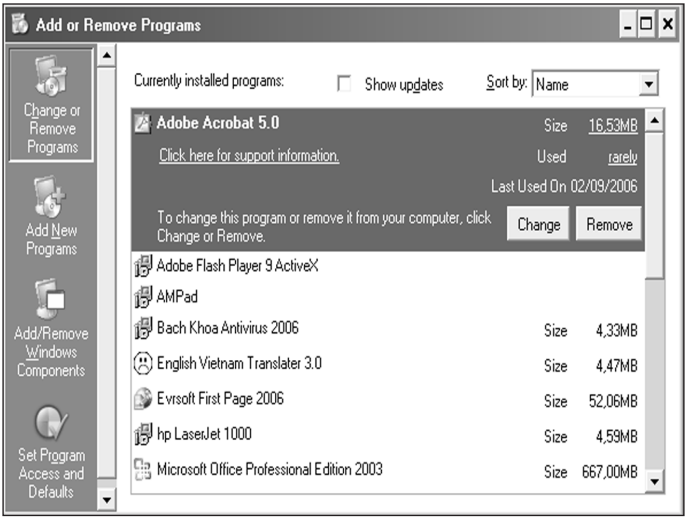
c. Loại bỏ phần mềm không sử dụng

Cần dọn sạch sẽ máy tính. Nên gỡ bỏ các phần mềm dùng thử hay những phần mềm kèm thêm mà không có ý định sử dụng vì những phần mềm này đều đòi hỏi bạn phải kích hoạt hoặc đăng ký qua kết nối Internet. Trong một số trường hợp thì chúng tự động truy cập Internet mà không hỏi người sử dụng. Do đó, máy tính cũng rất dễ bị lây nhiễm virus. Để loại bỏ những

https://tieulun.hopto.org

chương trình không sử dụng ra khỏi hệ thống, vào Control Panel, chọn biểu tượng:

Khi này hộp thoại xuất hiện như hình sau:



Chọn chương trình cần gỡ bỏ khỏi hệ thống và nhấn nút Remove.

d. Cài đặt chương trình chống virus

Hệ thống cần được cài đặt các chương trình chống virus phiên bản mới nhất và được thiết lập ở chế độ tự động phòng. Các chương trình này sẽ phát hiện và ngăn chặn kịp thời virus có thể bị nhiễm từ mạng Internet. Nhìn chung bạn nên thực hiện phương châm: "Phòng hơn chống".

https://tieulun.hopto.org

e. Cài đặt chương trình tường lửa

Trong Windows XP Service Pack 2 đã tích hợp sẵn một phần mềm tường lửa miễn phí khá tốt là Windows Firewall. Nếu muốn có thêm nhiều tính năng hơn chỉ cần chạy các phần mềm khác như ZoneAlarm hoặc SyGate. Phần mềm tường lửa cũng nên được để sẵn vào bộ đĩa CD-ROM được tạo ra trong bước 1. Hãy tiến hành cài đặt phần mềm tường lửa để bảo vệ hệ thống của bạn.

f. Cài đặt máy in và các thiết bị ngoại vi khác

Trước khi bạn kết nối vào Internet hãy cài đặt các thiết bị ngoại vi vào trong máy tính, bởi vì sau khi kết nối Internet mới tiến hành cài đặt các thiết bị ngoại vi thì chúng sẽ tự động kết nối vào trang cập nhật Windows. Chúng sẽ tự động tìm kiếm các thiết bị và đưa ra những đề nghị về nâng cấp các trình điều khiển mới. Đây là tính năng rất tốt và hữu dụng của Windows, nhưng rất có thể đó sẽ là một điểm yếu mà hacker có thể lợi dụng để xâm nhập vào máy tính.

g. Tạo tài khoản giới hạn và mật khẩu

Tài khoản quản trị cho phép quản lý truy cập vào toàn bộ hệ thống. Hacker có thể lấy cắp thông tin về hệ thống, các virus,

https://tieulun.hopto.org

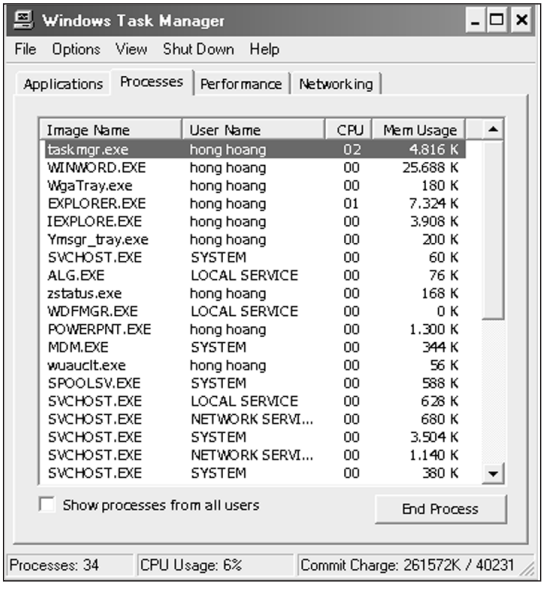
sâu, trojan, spyware... có thể tự động cài đặt và lây nhiễm vào hệ thống khi sử dụng tài khoản quản trị và vì vậy, mật khẩu của tài khoản quản trị phải có đủ tính phức tạp và khó đoán.

Hầu hết các mật khẩu đều có thể dễ dàng bị "bẻ khoá" bởi các hacker có trình độ. Để phục vụ cho hoạt động hằng ngày, bạn có thể không cần sử dụng tài khoản quản trị. Thay vào đó, sử dụng tài khoản bị giới hạn và có mật khẩu để bảo vệ (mật khẩu này phải khác với mật khẩu của người quản trị và cũng phải mạnh, không dễ đoán). Chính nhờ tài khoản bị giới hạn này mà máy tính của bạn sẽ chống lại được sự lây nhiễm hoặc cài đặt từ các phần mềm nguy hiểm do sự giới hạn về quyền truy cập.

h. Tắt những dịch vụ Windows không cần thiết

Microsoft đã cố gắng tắt một số dịch vụ không cần thiết trong bản Service Pack 2, nhưng vẫn còn một số dịch vụ không cần thiết vẫn hoạt động mặc định trên các máy tính. Khi cần biết có bao nhiêu dịch vụ đang sử dụng, nhấn tổ hợp phím Ctrl+Alt+Del và nhấn vào khung Processes. Khi này hộp thoại Windows Task Manager xuất hiện như hình sau:

https://tieulun.hopto.org

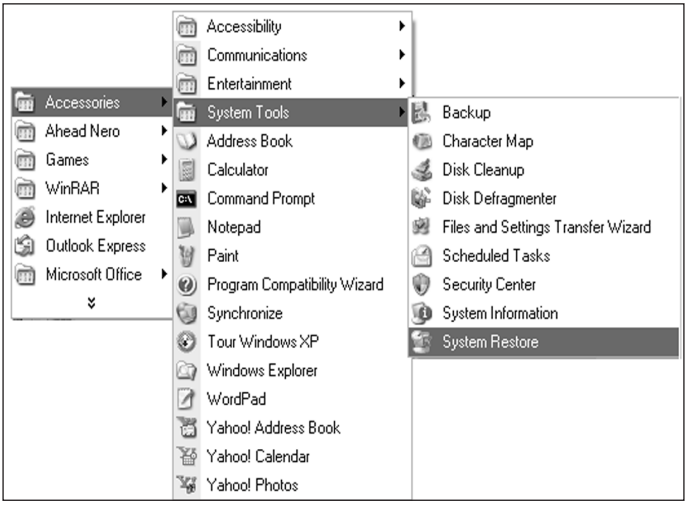


Hầu hết các ứng dụng, dịch vụ và các tiến trình... hoạt động ở chế độ nền đều sẽ hiển thị. Vấn đề ở đây chính là hầu hết những cuộc tấn công từ bên ngoài đều sử dụng và khai thác lỗ hổng từ các dịch vụ này. Hãy tắt các dịch vụ không cần thiết để tiết kiệm tài nguyên hệ thống và phòng chống các cuộc tấn công từ xa.

i. Thiết lập một điểm phục hồi

Thực hiện một điểm phục hồi bằng tiện ích System Restore là một bước thực sự quan trọng bởi lúc này hệ thống của bạn trước khi cài đặt kết nối với Internet còn rất "sạch sẽ". Nếu sau này hệ thống bị nhiễm virus, worm, spyware, trojan... hay bị các lỗi hệ thống khác thì điểm phục hồi này đúng là rất quan trọng cho máy tính của bạn.

https://tieulun.hopto.org

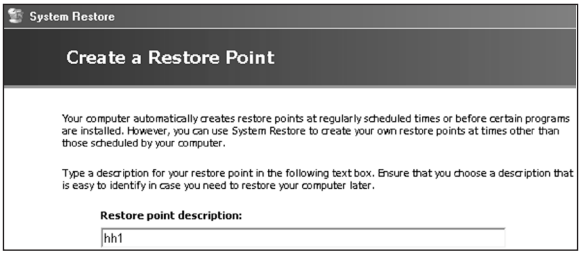


Để tạo một điểm phục hồi (Restore Point), thực hiện như sau:

- Vào bảng chọn Start, đưa con trỏ đến mục Program. Bảng chọn Program xuất hiện.
- Chọn mục Accessories.
- Chọn System Tools.
- Chọn System Restore như hình trên.

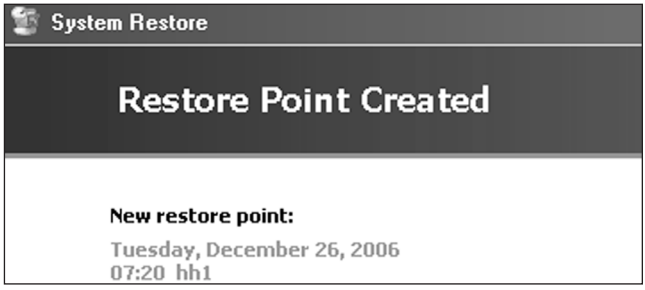
Khi này hộp thoại System Restore xuất hiện. Chọn mục Create a restore point, nhấn nút Next >.

Trong khung Restore point description nhập tên điểm phục hồi như hình sau:



https://tieulun.hopto.org

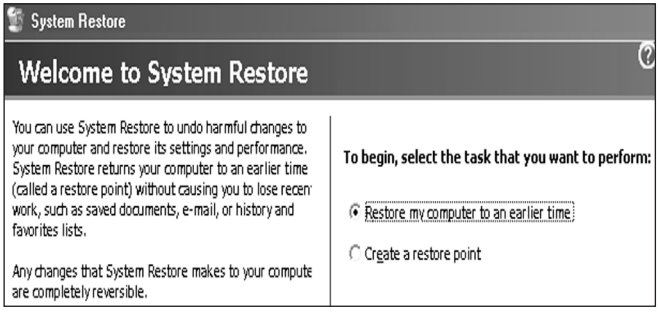
- Nhấn nút Create. Hệ thống sẽ thông báo tên điểm phục hồi cùng với thời gian tạo lập có dạng như hình sau:



- Nhấn nút Close để đóng hộp thoại và kết thúc việc cài đặt.

Khi cần khôi phục lại hệ thống từ một điểm phục hồi, tiến hành như sau:

Vào bảng chọn Start, đưa con trỏ đến mục Program. Bảng chọn Program xuất hiện. Chọn mục Accessories, chọn System Tools, chọn System Restore. Khi này hộp thoại System Restore xuất hiện như hình sau:



Nhấn chuột vào nút Restore my computer to an ealier time, hệ thống sẽ được phục hồi từ điểm phục hồi đã được lựa chọn.

https://tieulun.hopto.org

Phần II

Những nguy cơ tiềm ẩn và cách phòng chống

https://tieulun.hopto.org

https://tieulun.hopto.org

Chương III

VIRUS, WORM, TROJAN VÀ CÁCH PHÒNG CHỐNG

1. Virus và cách lây lan của virus

a. Virus là gì?

Virus máy tính là một chương trình có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác. Đối tượng cho virus hoạt động có thể là các tệp chương trình, văn bản, hệ thống máy tính, các loại đĩa.... Virus có nhiều cách lây lan và tất nhiên cũng có nhiều cách phá hoại. Cách thức hoạt động của chúng rất đa dạng và phức tạp. Tác hại của chúng cũng rất khác nhau, từ làm hỏng một tệp dữ liệu, đến làm tê liệt cả một hệ thống máy tính lớn như một công ty, ngân hàng... *Tóm lại*, virus là một đoạn chương trình và đoạn chương trình đó thường dùng để phục vụ những mục đích không tốt.

Virus máy tính là do con người tạo ra, cho đến ngày nay có thể coi đã trở thành một hiểm họa đối với các máy tính cá nhân và cả với các hệ thống mạng. Như đối với một bệnh dịch, tất cả chúng ta phải luôn phòng chống, tìm ra những phương pháp mới để hạn chế và tiêu diệt chúng. Cũng như một số căn bệnh ngoài xã hội, có những

https://tieulun.hopto.org

loại virus phải mất nhiều thời gian nghiên cứu mới tiêu diệt được. Có nhiều trường hợp, những virus xuất hiện với độ phức tạp cao đã gây ra những thiệt hại nghiêm trọng do không tìm được biện pháp phòng chống ngay sau khi chúng hoạt động. Chính vì vậy, phương châm "Phòng hơn chống" là cần thiết. Biện pháp ngăn ngừa không cho virus xâm nhập vào hệ thống máy tính của bạn là một yếu tố quan trọng để có thể ngăn chặn tác hại của virus máy tính.

b. Cách lây lan của virus

Virus máy tính có thể lây vào máy tính của bạn qua thư điện tử (email), qua các tệp được tải về từ Internet hay sao chép dữ liệu từ máy này sang máy khác.

Mỗi phần mềm hệ thống đều có khả năng chứa các lỗi về bảo mật. Đây cũng là cơ hội để virus xâm nhập từ xa, cài đặt, lây nhiễm lên máy tính của bạn một cách âm thầm.

Hiện nay, email là phương tiện thông dụng dùng để trao đổi thông tin đã trở thành con đường lây nhiễm virus phổ biến nhất. Từ một máy tính, virus thu thập các địa chỉ email trong máy và gửi email giả mạo kèm theo các tệp virus để lừa người nhận thực thi các tệp này. Các email chứa virus đều có nội dung hấp dẫn, hoặc chúng tự trích dẫn nội dung của một email trong hộp thư của nạn nhân để tạo ra phần nội dung của email giả mạo, điều đó giúp cho email giả mạo có vẻ

https://tieulun.hopto.org

thật hơn và người nhận dễ bị mắc lừa hơn. Máy tính nhận được các email chứa virus sẽ bị nhiễm virus. Với cách hoàn toàn tương tự như vậy trên những máy nạn nhân khác, virus có thể nhanh chóng lây lan trên toàn cầu theo cấp số nhân.

Máy tính của bạn cũng có thể bị nhiễm virus khi bạn chạy một chương trình tải từ Internet về hay copy từ một máy tính bị nhiễm virus khác. Lý do là các chương trình này có thể đã bị lây bởi một virus hoặc bản thân là một virus giả dạng nên khi bạn chạy nó cũng là lúc bạn đã tự mở cửa cho virus lây vào máy của mình. Quá trình lây lan của virus có thể diễn ra một cách "âm thầm" (bạn không nhận ra điều đó vì sau khi thực hiện xong công việc lây lan, chương trình bị lây nhiễm vẫn chạy bình thường) hay có thể diễn ra một cách "công khai" (virus hiện thông báo trêu đùa bạn) nhưng kết quả cuối cùng là máy tính của bạn đã bị nhiễm virus và cần đến các chương trình diệt virus để trừ khử chúng. Nếu bạn vào các trang web lạ, các trang web này có thể chứa mã lệnh ActiveX hay JAVA applets, VBScript... là những đoạn mã cài đặt adware, spyware, trojan hay thậm chí là cả virus lên máy của bạn. Vì vậy, trong mọi tình huống bạn nên cẩn thận, không vào những địa chỉ web lạ.

Tuy nhiên virus cũng được phát triển theo một trình tự lịch sử tiến hóa từ thấp đến cao. Những virus hiện nay có thể lây vào máy tính

https://tieulun.hopto.org

mà bạn không hề hay biết vì bạn không nhận được email virus, không vào web lạ hay chạy bất cứ tệp chương trình lạ nào. Đơn giản là vì đó là những virus khai thác các lỗi tiềm ẩn của một phần mềm đang chạy trên máy tính của bạn (ví dụ: lỗi tràn bộ đệm) để xâm nhập từ xa, cài đặt và lây nhiễm. Các phần mềm (kể cả hệ điều hành) luôn chứa đựng những lỗi mà không phải lúc nào cũng có thể dễ dàng phát hiện ra. Các lỗi này khi được phát hiện có thể gây ra những sự cố không lớn, nhưng cũng có thể là những lỗi rất nghiêm trọng và không lâu sau đó thường sẽ có hàng loạt virus mới ra đời khai thác lỗi này để lây lan.

2. Worm và cách lây lan

a. Worm là gì?

Worm - sâu Internet là loại virus có sức lây lan rộng, nhanh và phổ biến nhất hiện nay. Worm kết hợp cả sức phá hoại của virus, sự bí mật của trojan và hơn hết là sự lây lan đáng sợ mà những kẻ viết virus trang bị cho nó - một kẻ phá hoại với vũ khí tối tân. Với sự lây lan đáng sợ, chúng đã làm tê liệt hàng loạt các hệ thống máy chủ, làm ách tắc đường truyền.

b. Cách lây lan của worm

Vào thời điểm ban đầu, worm được dùng để chỉ những virus phát tán bằng cách tìm các địa

https://tieulun.hopto.org

chỉ trong sổ địa chỉ (address book) của máy mà nó đang lây nhiễm, đó thường là địa chỉ của bạn bè, người thân, khách hàng... của chủ máy. Tiếp đến, nó tự gửi chính nó qua email cho những địa chỉ mà nó tìm thấy, tất nhiên với địa chỉ người gửi là chính bạn, chủ sở hữu của chiếc máy hay giả danh một người nào đó. Điều đó lý giải tại sao chỉ trong vòng vài tiếng đồng hồ mà Mellisa và Love Letter lại có thể lây lan tới hàng chục triệu máy tính trên toàn cầu. Cái tên worm hay "Sâu Internet" cho ta hình dung ra việc những con virus máy tính "bò" từ máy tính này qua máy tính khác trên các "cành cây" Internet.

Với sự lây lan nhanh và rộng lớn như vậy, worm thường được kẻ viết ra chúng cài thêm nhiều tính năng đặc biệt, chẳng hạn như chúng có thể định cùng một ngày giờ và đồng loạt từ các máy nạn nhân (hàng triệu máy) tấn công vào một địa chỉ nào đó. Ngoài ra, chúng còn có thể mang theo các backdoor thả lên máy nạn nhân cho phép chủ nhân của chúng truy nhập vào máy của nạn nhân và có thể làm đủ mọi thứ như ngồi trên máy đó một cách bất hợp pháp. Khái niệm "Sâu Internet" còn bao gồm các virus lây lan qua mạng chia sẻ ngang hàng, các virus lây lan qua các dịch vụ chatting và đặc biệt là các virus khai thác các lỗ hổng phần mềm để lây lan. Các phần mềm (nhất là hệ điều hành và các dịch vụ trên đó) luôn chứa đựng những lỗi mà không phải lúc

https://tieulun.hopto.org

nào cũng có thể dễ dàng phát hiện ra. Khi một lỗ hổng phần mềm được phát hiện, không lâu sau đó sẽ xuất hiện các virus có khả năng khai thác các lỗ hổng này để lây nhiễm lên các máy tính từ xa một cách âm thầm mà người chủ máy hoàn toàn không hay biết. Từ các máy này, worm sẽ tiếp tục "bò" qua các máy tính khác trên mạng Internet với một cách thức tương tự.

3. Trojan

Trojan (hay còn được gọi là Trojan horse - con ngựa thành Tơroa) được xây dựng dựa vào một điển tích cổ. Đó là cuộc chiến tranh giữa người Hy Lạp và người thành Tơroa. Thành Tơroa là một thành trì kiên cố được phòng bị cẩn mật, quân Hy Lạp không sao có thể đột nhập vào được. Người ta đã nghĩ ra một kế, đó là giả vờ giảng hòa và sau đó tặng những người trong thành Tơroa một con ngựa gỗ khổng lồ có chứa nhiều quân lính. Sau khi ngựa được đưa vào trong thành, đêm xuống những quân lính từ trong bụng ngựa xông ra và đánh chiếm thành từ bên trong.

Phương pháp trên cũng chính là cách các trojan máy tính áp dụng. Khác với virus máy tính, trojan là một đoạn mã chương trình *hoàn toàn không có tính lây lan*. Đầu tiên kẻ viết ra trojan bằng cách nào đó lừa cho người sử dụng dùng chương trình của mình hoặc ghép trojan đi kèm với các virus để xâm nhập, cài đặt lên máy

https://tieulun.hopto.org

nạn nhân. Đến thời điểm thuận lợi, trojan sẽ ăn cắp thông tin quan trọng trên máy tính của nạn nhân như số thẻ tín dụng, mật khẩu... để gửi về cho chủ nhân của nó ở trên mạng hoặc có thể sẽ ra tay xóa dữ liệu nếu được lập trình trước.

Bên cạnh các trojan ăn cắp thông tin truyền thống, hiện nay cũng xuất hiện các trojan mang tính chất riêng biệt như: Khi đã cài đặt vào máy nạn nhân sẽ tự mở ra một cổng dịch vụ cho phép kẻ tấn công (hacker) có thể kết nối từ xa tới máy nạn nhân, từ đó nó sẽ nhận lệnh và thực hiện lệnh mà kẻ tấn công đưa ra.

4. Phân biệt giữa virus, worm và trojan

Có thể khi nói về virus máy tính, bạn thường hiểu rằng worm và trojan là một. Mặc dù ba từ virus, worm và trojan horse đôi khi có thể thay thế cho nhau, cách phòng chống cũng có thể giống nhau cả về phương pháp và chương trình, nhưng chúng thực tế lại có sự khác nhau về bản chất. Cả ba loại trên đều là các chương trình nguy hiểm có thể gây hại đến cho máy tính, nhưng giữa chúng lại có sự khác nhau. Hiểu được sự khác nhau này, bạn có thể bảo vệ máy tính của mình hiệu quả hơn.

Virus có thể tự gài chính nó vào một chương trình hoặc một tệp nào đó, vì thế nó có thể phát tán ra các máy tính khác, đi đến đâu nó gây tác hại đến đấy. Không giống như virus ở người, virus

https://tieulun.hopto.org

máy tính có phạm vi tác động rộng hơn, một số virus chỉ gây ra những tác động nhỏ, trong khi một số khác thì có thể gây nguy hiểm cho ổ cứng, chương trình hay các tệp, thậm chí làm hỏng các thiết bị phần cứng. Hầu như các loại virus đều được kèm theo các tệp chương trình, điều đó có nghĩa là máy tính của bạn có thể chứa virus nhưng chưa chắc đã bị ảnh hưởng trừ khi bạn cho chạy các chương trình đó. Một điều quan trọng là virus không thể phát tán được nếu như không có sự tác động của con người, ví dụ như cho chạy các chương trình chứa nó. Mọi người thường tự phát tán virus khi chia sẻ các tệp hay gửi email có nhiễm virus.

Worm được tạo ra tương tự như virus, và nó được biết đến như là lớp con của virus. Nó cũng phát tán từ một máy tính này sang máy khác. Nhưng không giống như virus, mà giống như ý nghĩa "con sâu" tự bò được, nó có thể di chuyển mà không cần nhờ một tác động nào của người dùng. Worm lợi dụng các tính năng truyền tệp hay thông tin trên hệ thống để di chuyển không cần có tác động của con người. Sự nguy hiểm lớn nhất của worm là nó có thể tự nhân bản chính nó trong hệ thống của bạn, và nó có thể gửi đi hàng trăm, thậm chí hàng ngàn bản copy của nó ra ngoài và gây ra sự tàn phá rất lớn. Ví dụ một con worm có thể gửi chính nó tới tất cả mail trong danh sách mail của bạn. Sau đó nó tự nhân bản

https://tieulun.hopto.org

và gửi đi tất cả mail trong danh sách trên máy tính nhận, và cứ như thế. Chính vì worm có khả năng nhân bản và di chuyển trên mạng nên nó sẽ tiêu tốn bộ nhớ (hay băng thông mạng), làm cho các máy chủ web, máy chủ mạng, và cả máy tính đơn không hoạt động nữa. Gần đây nhất có loại worm tên là Blaster, nó có thể xâm nhập vào máy tính của bạn và cho phép điều khiển máy bạn từ xa.

Trojan còn nguy hiểm hơn cả hai loại trên. Trojan horse xuất hiện lúc đầu như là một phần mềm hữu ích, nhưng sẽ ngay lập tức trở nên nguy hiểm khi bạn cài nó hay chạy nó lần đầu tiên trên máy tính. Khi trojan được phát tán đến máy khác, thông thường bên nhận sẽ chạy nó vì người dùng sẽ thấy nó như là một phần mềm hay tệp đáng tin cậy và được gửi từ một nguồn đáng tin cậy. Khi trojan được kích hoạt trên máy tính của bạn thì hậu quả mà nó gây ra có thể sẽ khác nhau (như desktop thay đổi hay sẽ xuất hiện một số biểu tượng lạ trên desktop), hoặc nó có thể gây ra những hậu quả rất nghiêm trọng, như xóa các tệp, thông tin trong hệ thống của bạn. Trojan có thể tạo ra các backdoor (cổng sau) giúp cho những kẻ lạ có thể xâm nhập vào hệ thống, làm hư hại đến thông tin cá nhân và các thông tin bí mật khác. Không giống như virus và worm, trojan không phát tán bằng cách làm cho các tệp khác nhiễm cũng như không tự nhân bản nó.

https://tieulun.hopto.org

5. Triệu chứng và cách phòng chống virus, worm hay trojan. Virus macro

a. Triệu chứng khi máy bị nhiễm virus, worm hay trojan

(1) Không thoát được ra khỏi Windows hoặc không khởi động được Windows. Trong một số trường hợp, bạn nhận được các thông báo lỗi của hệ thống nhưng thực tế không phải là như vậy.

(2) Hay bị treo máy.

(3) Xuất hiện thanh công cụ lạ trên trình duyệt Internet.

(4) Máy tính chạy chậm hơn bình thường.

(5) Máy đang chạy, bạn không có nhu cầu ghi đĩa, nhưng máy lại yêu cầu bỏ nhãn chống ghi xóa của đĩa mềm.

(6) Máy đang chạy bị treo, không thể tiếp tục hoạt động được nữa.

(7) Các tệp chương trình đang sử dụng có dung lượng lớn dần lên.

(8) Kích thước đĩa trống ngày một giảm đi cho đến khi hết đĩa.

(9) Khởi động bằng đĩa mềm nhưng không nhận biết được đĩa cứng. Trong trường hợp này, cũng có thể máy của bạn đã nhiễm virus mà thời gian đầu không có biểu hiện gì đặc biệt, chỉ sau một thời gian nhất định hoặc đến một thời điểm nhất định virus mới bắt đầu hoạt động gây ảnh hưởng đến đĩa cũng như các chương trình ứng dụng và chương trình hệ thống.

https://tieulun.hopto.org

b. Chống virus, worm và trojan

(1) Virus có thể hiện diện ở bất cứ nơi đâu, dưới bất kỳ hình thức nào, và nếu bạn có nối mạng thì nguy cơ bị lây nhiễm sẽ càng cao. Để phòng chống virus, một nguyên tắc cơ bản là luôn đề cao cảnh giác.

(2) Trước tiên bạn cần đảm bảo rằng hệ điều hành đang dùng là bản nâng cấp mới nhất. Điều này rất cần thiết khi bạn đang chạy hệ điều hành Microsoft Windows. Bạn nên tạo các điểm phục hồi khi máy tính được coi là chưa bị nhiễm virus để trong trường hợp cần thiết có thể sử dụng để khôi phục lại hệ thống.

(3) Cần cài một phần mềm chống virus và cần cập nhật bản mới nhất để đảm bảo nó có thể diệt được các virus, worm và trojan mới nhất. Ngoài ra phần mềm chống virus cần phải có khả năng quét được các virus, worm, trojan trên các email và tệp khi được tải về từ Internet. Các chương trình này nên được cài thường trú trên máy tính và được cập nhật thường xuyên để có khả năng diệt các loại virus mới. Nhìn chung, bạn nên dùng từ hai chương trình trở lên, vì một chương trình không phải là diệt được tất cả các loại virus, thậm chí không thể phát hiện hết virus.

(4) Thiết lập thêm tường lửa - firewall. Firewall là một hệ thống bảo vệ hệ thống khỏi

https://tieulun.hopto.org

những truy nhập không hợp lệ. Firewall có thể là phần cứng hay phần mềm. Firewall bằng phần cứng sẽ có khả năng bảo vệ mạnh hơn đối với hầu hết các truy nhập từ bên ngoài. Khi chống virus, worm hay trojan thì firewall bằng phần cứng lại không hiệu quả bằng firewall phần mềm, vì đối với những worm được kèm vào trong email hay tệp thì nó lại lờ đi và coi chúng như là những email, tệp bình thường. Đối với những người dùng ở gia đình thì nên chọn firewall phần mềm. Một firewall phần mềm tốt sẽ bảo vệ máy của bạn khỏi sự cố gắng truy nhập có hại và còn có thêm các chức năng bảo vệ khỏi các chương trình trojan thông thường và các email worm. Nhược điểm của firewall phần mềm là nó chỉ bảo vệ được máy nào có cài đặt nó mà thôi, mà không thể bảo vệ được cả một mạng.

Cần phải nhớ là firewall không thể giải quyết được hết tất cả các vấn đề về virus, nhưng khi ta có một hệ điều hành tốt và kết hợp với một phần mềm anti-virus tốt, thì chúng ta có thể bảo vệ được máy tính của mình và cả mạng nữa.

(5) Cần truy cập Internet một cách an toàn: Không vào những trang web lạ chưa rõ nguồn gốc. Không mở những email có khả năng là thư rác...

(6) Thận trọng khi tải các ứng dụng trên mạng Internet, quét các tệp này trước khi mở

https://tieulun.hopto.org

chúng. Khi sao chép từ một đĩa khác vào máy tính cần sử dụng các chương trình chống virus để quét trước khi quyết định chép chúng vào đĩa cứng của máy.

(7) Thường xuyên sao lưu những dữ liệu quan trọng để sử dụng trong trường hợp xấu là bị virus xóa dữ liệu hoặc làm hỏng ổ đĩa.

(8) Nên trang bị cho máy tính một phần mềm diệt virus nội như D32 hoặc BKAV để chúng bổ sung với các phần mềm diệt virus ngoại vì mỗi phần mềm diệt virus có những ưu nhược điểm riêng.

(9) Thường xuyên truy cập vào các trang web thông tin virus để có thêm nhiều kiến thức về phòng chống virus. Một số trang web diệt virus đáng tin cậy:

Norton Antivirus (www.symantec.com)

McAfee Virus Scan (www.mcafee.com)

PC-cillin (www.trendmicro.com)

AVG Anti-Virus (www.grisoft.com)

Bitdefender (www.bitdefender.com)

BKAV (www.bkav.com.vn.)

D32 (www.echip.com.vn/echiproot/html/d32.html)

c. Bảo vệ máy tính khỏi virus macro

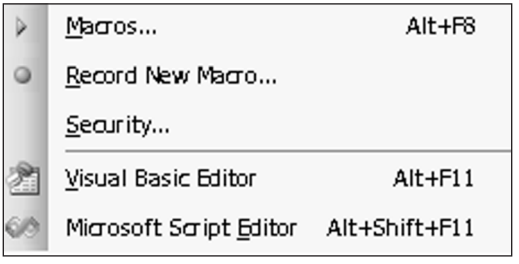
Trong một số ứng dụng của bộ Office như Word, Excel... cho phép người sử dụng tạo các macro để tự động hóa một số thao tác nhằm đẩy nhanh tiến độ công việc. Đây là những macro rất

https://tieulun.hopto.org

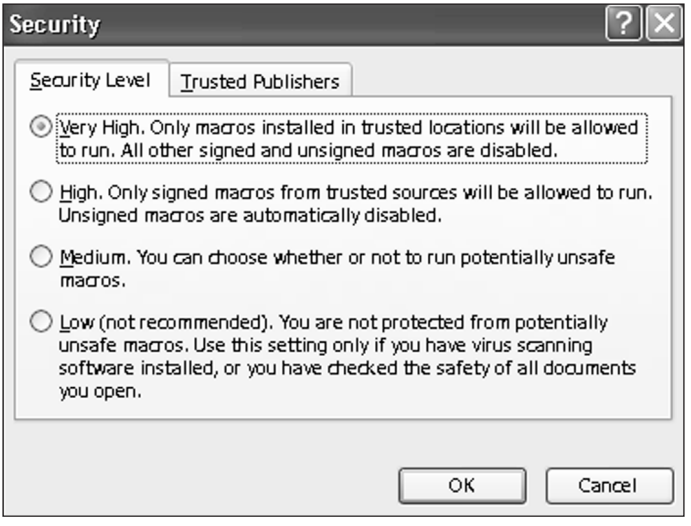
có lợi nhưng chúng cũng có thể bị kẻ xâm nhập cài thêm các virus macro. Chính vì vậy, bạn nên cân nhắc có sử dụng tính năng trên hay vô hiệu hóa toàn bộ các macro trong ứng dụng của mình bằng các bước như sau:

- Khởi động ứng dụng như Word, Excel, PowerPoint.

- Vào bảng chọn Tools, chọn mục Macros. Khi này một hộp thoại xuất hiện như hình sau:



- Chọn mục Security... Khi này hộp thoại Security xuất hiện như hình sau:



https://tieulun.hopto.org

Nếu bạn sử dụng Microsoft Office 2003, chọn mục Very High và nhấn nút 

.

6. Hiểm họa từ virus nội

Nhiều người dùng máy tính tại Việt Nam vẫn còn nhớ đến nỗi kinh hoàng của virus mang tên "Date 25/11" xuất hiện trong giai đoạn 1997 - 2000. Đây là virus có nguồn gốc từ Việt Nam, lây lan chậm nhưng cứ đến ngày 25 tháng 11 hằng năm là nó lại tàn phá dữ liệu của những máy tính bị lây nhiễm. Cũng may là sau năm 2000, virus "Date 25/11" đã bị diệt hoàn toàn.

Cuối năm 2005, dịch spyware cướp trang chủ trình duyệt và đổi thành vn-n.com cũng làm nhiều người khốn đốn. Spyware này lây nhiễm chủ yếu qua các trang web con có nội dung giải trí như âm nhạc, truyện, chat, game... Khi người dùng vào một trong các trang web này sẽ bị cài phần mềm gián điệp và bị đổi địa chỉ trang chủ của trình duyệt thành trang vn-n.com.

Cũng vào giữa năm 2005, các dịch vụ chatting trực tuyến như Yahoo!, MSN bắt đầu bị hacker lợi dụng như một công cụ để phát tán virus trên mạng. Theo các chuyên gia bảo mật nhận định: "Virus và phần mềm gián điệp có xuất xứ ở Việt Nam sẽ xuất hiện nhiều hơn. Các vụ tấn công do hacker trong nước gây ra sẽ tăng lên. Spam sẽ trở thành vấn đề nóng!". Dù đã được cảnh báo, đầu năm 2006 người dùng Internet Việt Nam vẫn

https://tieulun.hopto.org

lao đao trước "cơn bão" virus lây qua chat (Yahoo! Messenger) mang tên Xrobots (mà nhiều người quen gọi là virus "GaiXinh.jpg"). Với cơ chế lây lan hết sức đơn giản, virus trên được người viết tung lên mạng Internet thông qua tiện ích chat Yahoo! Messenger. Những tin nhắn dạng "Gai dep ne", "Phim vui phim vui" kèm theo đường link để tải virus Xrobots về máy nếu người dùng bất cẩn kích chuột vào.

Virus Xrobots lây lan theo cơ chế "đánh lừa người dùng", giả dạng một bức ảnh đẹp hay đoạn phim vui. Nguyên nhân lớn nhất dẫn đến việc Xrobots lây nhiễm tràn lan chính là nhận thức của người dùng còn chưa cao và quá chủ quan! Trong số nạn nhân của Xrobots, có cả người làm việc trong các doanh nghiệp về công nghệ thông tin. Điều đó cho thấy, nếu người dùng có ý thức tự bảo vệ mình, sẽ hạn chế được rất nhiều sự phát tán và phổ biến của các virus, spyware, website... nguy hiểm!

Điều thật tệ hại là, với các virus, spyware được tạo ra ở trong nước thì các phần mềm diệt virus, spyware nổi tiếng và phổ biến như Norton, Symantec, Bitdefender, Webroot... chưa kịp cập nhật nên không diệt được vì thế khả năng lây lan và hậu quả sẽ rất lớn.

Chính vì vậy, ngoài cảnh giác với các loại virus nói chung, người sử dụng cũng phải thật thận trọng khi nhận được các bức thư không rõ nguồn gốc, không đủ độ an toàn, các đường link đến các web có vẻ như gần gũi và thân quen bằng tiếng Việt.

https://tieulun.hopto.org

Chương IV

PHẦN MỀM QUẢNG CÁO ADWARE, PHẦN MỀM GIÁN ĐIỆP SPYWARE

1. Phần mềm quảng cáo adware

a. Adware là gì?

Là phần mềm quảng cáo bất hợp pháp, gây khó chịu cho người sử dụng. Chúng bí mật xâm nhập vào máy tính của bạn khi vô tình ghé thăm những trang web không theo dự định do bất cẩn nhấn vào một mối liên kết nào đó. Đây thường là những trang web có nội dung không lành mạnh, các trang web bẻ khóa phần mềm... Chúng biến máy tính của bạn thành nơi quảng cáo mà không ít trong số đó có nội dung không lành mạnh.

b. Tác hại của adware

Xét về góc độ ảnh hưởng của loại phần mềm này đối với hệ thống, có thể coi nó là một thứ "vô thưởng vô phạt", có nghĩa không ảnh hưởng gì tới sự an toàn của máy tính. Tuy nhiên, cũng như spyware, cái giá mà bạn phải trả chính là tốc độ hoạt động của hệ thống giảm và băng thông kết nối bị chiếm dụng. Nó có nhiệm vụ làm rối loạn máy tính của bạn và cũng có thể lấy thông tin của bạn cho chủ nhân của nó với mục đích hoàn

https://tieulun.hopto.org

toàn không tốt. Về khía cạnh nào đó, adware tương tự như spyware.

2. Phần mềm gián điệp spyware

a. Phần mềm gián điệp spyware là gì?

Đây là loại phần mềm chuyên thu thập các thông tin từ các máy (thông thường vì mục đích thương mại) qua mạng Internet mà không được phép của chủ nhân máy tính đó. Spyware được cài đặt một cách bí mật do đánh lừa người sử dụng cài đặt hoặc kèm theo các phần mềm khác mà người ta 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 (của những kẻ hacker). Spyware cũng thu thập tin tức về địa chỉ email và ngay cả mật khẩu cũng như là số thẻ tín dụng!

b. Tác hại của phần mềm gián điệp spyware

Ngoài các vấn đề nghiêm trọng về đạo đức và tự do cá nhân bị xâm phạm, spyware còn đánh cắp từ các tài nguyên của bộ nhớ, chiếm băng thông khi gửi thông tin về cho chủ nhân của chúng qua đường truyền Internet. Chúng ăn cắp các thông tin quan trọng: số tài khoản, mật khẩu của người sử dụng gây nên những tác hại không lường hết được như: dựa vào các thông tin thu thập được, chủ nhân của các spyware sẽ rút tiền

https://tieulun.hopto.org

từ ngân hàng của người bị hại, sử dụng để mua hàng trực tuyến... Chúng có thể ăn trộm nội dung của các bức thư điện tử khi đã biết mật khẩu truy cập, thậm chí có thể chiếm toàn bộ hộp thư khi chúng thay đổi mật khẩu khác mà chính chủ nhân của các hộp thư này không thể truy cập vào được nữa. Spyware có thể thay đổi trang web mặc định, đọc các thông tin trên ổ cứng... Là một chương trình độc lập và chiếm bộ nhớ nên khi máy bị nhiễm spyware, sẽ làm giảm tốc độ của máy tính có thể dẫn tới tình trạng máy chạy không ổn định, thậm chí có thể làm hỏng máy hoặc không chạy được các ứng dụng khác.

c. Các triệu chứng khi máy bị nhiễm spyware

(1) Máy tự nhiên chạy chậm hơn bình thường do các chương trình spyware chạy thường trực trong máy.

(2) Trình duyệt đột ngột bung ra một trang web không theo ý muốn, một cửa sổ pop-up xuất hiện ngay cả khi không duyệt web, hoặc trình duyệt web xuất hiện thêm các thanh công cụ mới thì chắc chắn máy tính bị nhiễm spyware.

(3) Trang chủ của trình duyệt web bị thay đổi thành một trang web khác, thường là trang web có nội dung không lành mạnh, trong một số trường hợp bạn còn không thể thay đổi lại được trang chủ bằng trang web khác thay cho trang này.

https://tieulun.hopto.org

(4) Bạn liên tục nhận được các thông báo một cách không bình thường, tệ hại hơn là có thể bị ngừng các quá trình kết nối mạng hoặc tự động bị tắt trình duyệt web.

(5) Khi bạn sử dụng một trang tìm kiếm nào đấy như Google thì trình duyệt lại tự ý đưa ra một trang web tìm kiếm khác mà hầu hết các trang tìm kiếm này đều có nội dung vô bổ.

(6) Khi sử dụng các dịch vụ email, bạn thường xuyên bị spam, nghĩa là nhận quá nhiều các thư điện tử không mong muốn.

(7) Bạn có thể nhận thấy các liên kết lạ được tự ý thêm vào danh sách Favorites hoặc trong bảng chọn Start.

(8) Trên màn hình Windows xuất hiện các shortcut liên kết đến các trang web lạ, thường là những trang web có nội dung không lành mạnh.

(9) Cước sử dụng Internet gia tăng khác thường.

(10) Ở thời điểm không làm việc với mạng mà vẫn thấy đèn gửi/nhận chớp sáng trên modem giống như khi đang tải một phần mềm về máy.

d. Cách lây nhiễm và tác hại của phần mềm gián điệp (spyware)

Có nhiều cách để một phần mềm gián điệp xâm nhập vào hệ thống máy tính của bạn và gây ra những hậu quả không lường trước được, nhưng chúng thường lây vào máy tính của bạn bằng các cách sau đây:

https://tieulun.hopto.org

(1) Khi vô tình nhấn chuột vào một mẫu quảng cáo, spyware có thể được tải xuống máy tính của bạn.

(2) Spyware ẩn trong các tệp âm nhạc MP3 hay các tệp phim ảnh không hợp pháp.

(3) Spyware ẩn trong các phần mềm miễn phí không rõ nguồn gốc.

(4) Một số chương trình giả mạo chống spyware nhưng thực chất chúng cài đặt spyware. Để không bị mắc bẫy trò lừa bịp này, bạn nên cài đặt phần mềm chống spyware tin cậy và có nguồn gốc rõ ràng.

(5). Cũng giống như virus, spyware có thể được cài vào máy tính khi mở một tệp đính kèm khi nhận thư điện tử.

(6). Một khả năng nữa là chính hệ thống của bạn bị những kẻ xâm nhập trực tiếp cài đặt spyware khi chúng có điều kiện tiếp xúc máy tính.

e. Cách phòng chống khi máy bị nhiễm phần mềm gián điệp

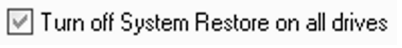
Spyware là một trong những thách thức lớn và gây mệt mỏi, chán nản cho người sử dụng máy tính và nhà quản trị hệ thống. Phải làm cách nào để tiêu diệt spyware an toàn, đó là một bài toán đau đầu cho nhiều người sử dụng máy tính hiện nay.

Để loại bỏ hoàn toàn spyware ra khỏi hệ thống, các bạn tiến hành các bước sau đây:

https://tieulun.hopto.org

Bước 1: Trước khi cố gắng xóa bỏ các phần mềm gián điệp, bạn cần phải sao lưu những dữ liệu quan trọng. Một số spyware có thể làm thay đổi lớn tới những thiết lập hệ thống và khi thực hiện loại bỏ chúng có thể gây ra lỗi, hoặc ảnh hưởng tới toàn bộ hệ thống. Một cách tốt nhất là sử dụng các phần mềm sao lưu toàn bộ ổ đĩa cứng. Tối thiểu, bạn cũng nên sao chép các tập tin quan trọng trong thư mục My Documents và các thư mục chứa dữ liệu quan trọng khác. Một số chương trình như Spybot Search & Destroy được tải từ địa chỉ http://www.safer-networking.org/en/index.html cũng thực hiện một số chức năng sao lưu, nhưng tạo bản sao lưu bằng tay là một bước rất cần thiết. Hãy sử dụng chức năng System Restore của Windows XP, tiện ích này cho phép hệ thống có thể phục hồi trạng thái ổn định khi gặp sự cố. System Restore có thể giúp bạn quay trở lại điểm sao lưu khi hệ thống còn "sạch sẽ" - chưa bị nhiễm spyware. Nếu tin rằng spyware đã ở trong hệ thống của bạn từ vài tuần nay, rất có thể những điểm phục hồi được tạo bởi System Restore cũng đã bị nhiễm. Do đó, bạn hãy xóa hết những điểm phục hồi gây nghi ngờ này. Một số phần mềm chống virus, spyware có thể phát hiện các điểm phục hồi bị nhiễm, nhưng hầu hết các phần mềm này không thể "dọn" sạch spyware. Cách tốt nhất để xóa sạch mọi điểm phục hồi là:

https://tieulun.hopto.org

Nhấn chuột phải vào My Computer. Khi này một hộp thoại xuất hiện. Chọn Properties, và chọn khung System Restore. Đánh dấu vào lựa chọn: 

và nhấn nút 

.

Hãy đợi vài phút để Windows xóa bỏ toàn bộ các điểm phục hồi.

Sau khi đã hoàn thành xóa điểm phục hồi từ hệ thống, hãy quay trở lại khung hội thoại và bỏ chọn 

. Điều này cho phép khởi động lại System Restore nhưng không có bất kì điểm sao lưu nào.

Để chắc chắn có một bản phục hồi tốt được sử dụng trong thời gian tới, bạn cần tạo một điểm phục hồi mới. *Xem mục 2.i Chương 2*.

Bước 2: Một cách diệt spyware nhanh chóng nhất là xóa một số chương trình trong Add or Remove Programs. Đây là một nơi đặc biệt quan trọng giúp phân tích các vấn đề về hệ thống Windows, và các phần mềm cài đặt trên máy tính. Danh sách các phần mềm trong Add or Remove Programs sẽ cho bạn biết máy tính đang sử dụng phần mềm nào và xác định được chương trình nào cần phải sao lưu. Tiếp đó, Add or Remove Programs cũng cho phép xác định các ứng dụng chia sẻ tệp như phần mềm âm nhạc, phim ảnh... và cũng là môi trường "nuôi dưỡng" và phát tán spyware. Vì vậy, hãy sử dụng Add or Remove Programs để loại bỏ những ứng dụng chia sẻ tập

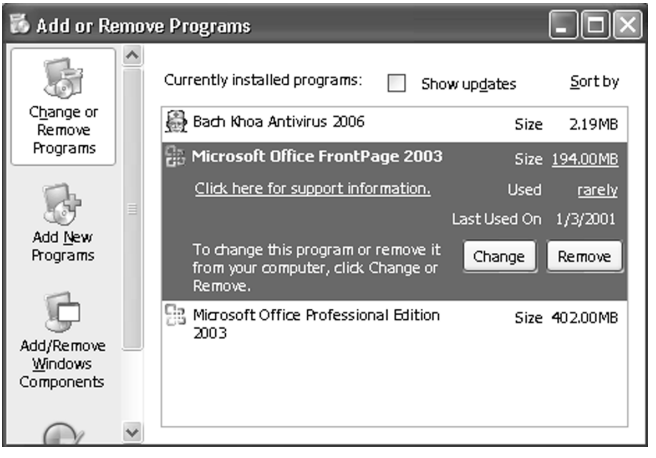
https://tieulun.hopto.org

tin ngang hàng. Bởi chẳng có tác dụng gì nếu đã quét sạch virus, spyware mà vẫn tiếp tục duy trì nơi phát sinh ra chúng. Cuối cùng, bằng cách xem xét kỹ danh sách Add or Remove Programs, có thể tìm được các chương trình được cài đặt bí mật, hoặc trong quá trình cài đặt một ứng dụng thì các phần mềm quảng cáo bị cài đặt lén lút.

Để ngắt bỏ một chương trình khỏi hệ thống, các bạn tiến hành như sau:

- Nhấn chuột vào nút Start, chọn Setting. Khi này một bảng chọn phụ xuất hiện.
- Chọn Control Panel. Khi này hộp thoại Control Panel xuất hiện.

- Chọn nút . Khi này hộp thoại Add or Remove Programs xuất hiện như hình sau:



https://tieulun.hopto.org

- Chọn chương trình cần ngắt khỏi hệ thống và nhấn nút Remove.

Trong danh sách các chương trình được tìm thấy, hãy cẩn thận loại bỏ những phần mềm khả nghi. Những phần mềm dưới đây thường là những phần mềm không mong muốn cho người sử dụng, chúng thường đưa ra những quảng cáo và thay đổi những giao diện trong trình duyệt:

Media Access
Media Gateway
My Web Search
MySearch
Search Assistant - My Search
Secure Delivery
Select CashBack
Surf Accuracy
The Best Offers
v.v..

Khi những phần mềm trên đã bị loại bỏ, chúng sẽ yêu cầu khởi động lại máy. Nếu chỉ một trong số chúng yêu cầu khởi động lại máy, hãy trả lời "No" cho đến khi toàn bộ đã bị loại ra khỏi danh sách Add or Remove. Nên sử dụng Google (http://www.google.com.vn) làm công cụ để tìm kiếm và loại bỏ những phần mềm không mong muốn ra khỏi danh sách. Nếu muốn biết những chương trình nào đang chạy trong hệ thống, hãy xem chúng trong Task Manager bằng cách nhấn Ctrl+Shift+Esc. Khi này hộp thoại Task Manager xuất hiện có dạng như hình sau:

https://tieulun.hopto.org

Trong trường hợp không chắc chắn có phải là spyware hay không, thì tốt hơn hết hãy tạm để chương trình đó lại. Bạn vẫn có cơ hội để xóa chúng ở những bước sau.

Bước 3: *Lựa chọn phần mềm tiêu diệt spyware*: Nếu hệ thống chỉ bị nhiễm adware thì Add or Remove Programs có thể đem lại hiệu quả. Nhưng khi đã bị lây nhiễm nặng hơn, tốt nhất hãy sử dụng phần mềm chống spyware. Những phần mềm này có thể xóa bỏ hoàn toàn những tập tin bị lây nhiễm và bảo vệ hệ thống không bị lây

https://tieulun.hopto.org

nhiễm lại. Trước khi cân nhắc mua một chương trình diệt spyware đắt tiền, bạn hãy dùng thử một số tiện ích diệt spyware miễn phí. Những phần mềm miễn phí sau thực sự rất mạnh, và được đánh giá rất cao như Ad-Aware SE Personal (địa chỉ: http://www.lavasoftusa.com/software/adaware), Spybot Search & Destroy (địa chỉ: http://www.safer-networking.org/en/index.html), Microsoft Windows AntiSpyware (địa chỉ: http://www.microsoft.com/downloads/details.aspx? FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671).

Một số trang web trong nước cũng cung cấp phần mềm miễn phí để diệt spyware như BKAV (www.bkav.com.vn), D32 được cập nhật từ một số trang web. Một số phần mềm diệt spyware như SpySweeper có giá rẻ và tỉ lệ tiêu diệt spyware thành công rất cao.

☞ *Xin các bạn lưu ý*: Một số phần mềm chống spyware rất nguy hiểm. Rất nhiều phần mềm loại này được đưa ra trên Internet thường không hiệu quả, và thường chúng được quảng cáo qua Google. Thậm chí chính những phần mềm này không tiêu diệt được bất cứ spyware nào mà lại là nơi phát tán spyware. Hãy thận trọng bởi vì có những phần mềm đòi hỏi bạn phải trả tiền trong khi chúng không đáng tin cậy.

https://tieulun.hopto.org

Bước 4: *Tiêu diệt spywar*e: Nói chung, phần mềm chống spyware hoạt động theo những nguyên tắc cơ bản như sau: Khi được nạp, những phần mềm này sẽ quét các tiến trình đang chạy, các tập tin và các khóa trong Registry để tìm các chương trình, các thiết lập không mong muốn. Sau khi đã hoàn thành quét tệp, chúng cung cấp một báo cáo về những gì tìm thấy và bạn có thể lựa chọn xóa bỏ spyware tại bước này. Người dùng cũng có quyền lựa chọn xóa bỏ toàn bộ spyware ngay lập tức, hoặc đưa chúng vào kho cách ly trong trường hợp muốn sử dụng sau này. Tuy nhiên, cũng đừng thực sự tin tưởng quá mức vào những công cụ này. Một tệp hoặc một tiến trình được xác định là một spyware, nhưng chưa chắc chúng đã là một spyware. Thực tế, mỗi công cụ diệt spyware đều có những khả năng cũng như tiêu chuẩn khác nhau trong việc loại trừ phần mềm gián điệp. Vì vậy, bạn nên sử dụng hai hay nhiều hơn phần mềm chống spyware là cách tốt nhất và hiệu quả nhất để đề phòng trường hợp một chương trình diệt spyware thậm chí còn không phát hiện được. Khi hệ thống đã làm việc tốt, bạn hãy chắc chắn là kích hoạt lại System Restore, và tạo một điểm phục hồi sạch sẽ. Điều này rất có ích nếu bạn muốn quay trở lại một điểm phục hồi sạch khi hệ thống lại bị nhiễm.

Lưu ý về cookie: Một số phần mềm gián điệp quét, tìm những cookie và sử dụng với mục đích quảng cáo của một trang web nào đó. Những

https://tieulun.hopto.org

cookie này theo dõi hành vi lướt web và đưa ra những quảng cáo thích hợp với sở thích của bạn. Tuy nhiên, người dùng cũng sẽ chẳng được hưởng lợi gì từ những quảng cáo vô bổ và đầy phiền toái này. Vì vậy, khi phát hiện cookie loại này, tốt nhất bạn hãy để phần mềm chống spyware dọn sạch chúng.

Bước 5: *Giải quyết khó khăn với Internet*. Một vài công cụ diệt spyware vẫn không thể loại bỏ hoàn toàn chúng. Hãy cập nhật thường xuyên những bản cập nhật mới nhất từ các hãng cung cấp. Đa số các phần mềm chống spyware đều hỗ trợ tính năng cập nhật tự động các mẫu spyware mới nhất và những bản vá trong các gói phần mềm. Tiếp đó, hãy cập nhật thông tin về bảo mật mà đặc biệt là thông tin về spyware.

Những nhà cung cấp công cụ chống spyware, virus hàng đầu như Symantec, McAfee, và Computer Associates đều thường xuyên đưa ra những thông tin cảnh báo về những hiểm họa lớn nhất từ trang web của họ. Nếu cần trợ giúp và phương pháp tiêu diệt spyware thì một số diễn đàn trên Internet là nơi tuyệt vời mà bạn nên ghé thăm. Hai trang web tốt nhất trong số đó là Spyware Warrior, địa chỉ: http://spywarewarrior.com/ và PC Pitstop, địa chỉ: http://support.pcpitstop.com/. Bạn cũng có thể tìm hiểu ở các trang web trong nước như PCWorld, địa chỉ:

https://tieulun.hopto.org

http://www.pcworld.com.vn và một số trang web khác như:

• Bkav: www.bkav.com.vn.

• D32:

www.echip.com.vn/echiproot/html/d32.html.

• VnExpress:

www.vnexpress.net/Vietnam/Vi-tinh/Hacker-Virus/.

• Tuổi trẻ Online:

www.tuoitre.com.vn/Tianyon/Index.aspx?ChannelID=65.

• VnMedia:

www.vnmedia.vn/ShowCat.asp?CatId=34.

Trước khi đưa vấn đề của mình lên diễn đàn, bạn hãy tìm đọc những câu hỏi có liên quan tới vấn đề đang tìm hiểu, rất có thể câu trả lời đã có sẵn cho bạn.

https://tieulun.hopto.org

Chương V

NHỮNG TRÒ LỪA ĐẢO TRÊN MẠNG NGUY CƠ MẠNG KHÔNG DÂY

1. Những trò lừa đảo trên mạng

a. Phishing là gì?

Phishing là một thuật ngữ được dùng để chỉ các âm mưu trực tuyến lừa gạt mọi người bằng những thông tin nhạy cảm kiểu như những bức email được ngụy trang dưới các vỏ bọc rất đáng tin cậy, với mục đích ăn cắp những thông tin cá nhân của người bị hại nhằm mục đích xấu.

Hiện nay, những kẻ tạo ra thư rác, lừa đảo đã tạo thành những tổ chức để thâm nhập vào máy tính và tấn công thẳng vào hệ thống an ninh máy tính của công ty. Trong những năm qua, các hãng an ninh Internet đã phát hiện ra vô số kẻ phá hoại và chúng gần như đã thò tay khắp nơi trên thế giới.

Dù quy mô khác nhau, nhưng có thể mô phỏng một quá trình phạm tội theo bốn bước: Bắt đầu là dò lỗ hổng. Một nhóm tội phạm (đương nhiên phải là các chuyên gia máy tính có trình độ cao về công nghệ) tìm vào mạng của một tập đoàn hay một công ty. Một khi phát hiện chỗ rò rỉ, chúng lập tức tạo phần mềm để khoét rộng cực

https://tieulun.hopto.org

đại chỗ rò. Sau đó, sẽ sử dụng hệ thống bị tổn thương này để thâm nhập vào các máy tính khác. Một khi cây cầu này được thiết lập, chúng sẽ viết phần mềm để đặt tất cả các máy tính có vấn đề dưới sự kiểm soát của chúng và bắt đầu gây tội ác. Bọn chúng tung ra đủ thứ từ virus, trojan đến spam và thư phishing. Những loại virus mới nhất có thể quét một vòng các máy tính dễ xâm nhập nhất, sau đó truyền bá virus sang các máy chủ khác qua đường Internet. Do đó, các chuyên gia an ninh mạng cho rằng, tội phạm Internet đang phát triển hẳn một hệ thống riêng.

b. Các kiểu lừa đảo

(1) Một dạng tội phạm phổ biến khác của các kẻ lừa đảo là thiết lập các website trông hoàn toàn giống với một ngân hàng trực tuyến hoặc một trang web bình thường có những dịch vụ trực tuyến. Chúng gửi email đến các khách hàng, dụ họ đăng ký và cung cấp thông tin tài khoản. Những website này chỉ tồn tại trong vài tuần, thu thập đủ thông tin, khách hàng, rồi đột nhiên biến mất. Trong một số trường hợp khác, chúng lợi dụng sự bảo mật không tốt của một số trang web và cài đặt các mã để khi người sử dụng nhập các user name và mật khẩu thì các thông tin này được chuyển đến chúng. Thậm chí chúng còn cài đặt để khi truy cập vào trang web này thì được tự động chuyển đến trang web khác với mục đích xấu.

https://tieulun.hopto.org

(2) Sử dụng con ngựa thành Tơroa (Trojan horse). Thông qua trojan, bọn hacker tiếp cận đến mạng lưới máy tính để đánh cắp trực tiếp các thông tin tài khoản. Trojan là một phương tiện để tội phạm Internet thiết lập phần mềm keylogging (ghi nhận những thao tác trên bàn phím nhằm mục đích đánh cắp mật khẩu của bạn và gửi cho chủ nhân của nó). Một nghiên cứu thực hiện gần đây đã phát hiện ra hàng ngàn chương trình keylogging đang vận hành, với hàng trăm ngàn máy tính bị nhiễm. Những chương trình đó thường ẩn đằng sau các bức email phishing hoặc các ứng dụng gián điệp, có khả năng tránh né các phần mềm chống virus và bức tường lửa.

(3) Gửi các thư điện tử giả mạo và cố ngụy trang để người nhận nhầm rằng thư hợp lệ, được gửi đi từ các ngân hàng, công ty thẻ tín dụng hoặc các hãng bán lẻ. Đường link trong những bức thư này thường đưa người nhận tới những website giả mạo. Tại đó, nạn nhân sẽ được yêu cầu khai báo thông tin cá nhân để nâng cấp tài khoản. Những dữ liệu như số tài khoản và thẻ tín dụng mà người nhẹ dạ để lộ qua con đường này sẽ được tội phạm sử dụng để ăn cắp tiền của khổ chủ.

(4) Kẻ lừa đảo gửi thư với nội dung lừa đảo đại loại như:

"Bạn đã mua một sản phẩm của một cửa hàng trực tuyến X, Y nào đó và được trúng thưởng hay

https://tieulun.hopto.org

khuyến mại sản phẩm hoặc một số tiền cụ thể là X, Y...".

"Bạn là khách hàng thứ một triệu truy cập website của chúng tôi và bạn được quà tặng...".

Hầu hết các dạng email lừa đảo này đều yêu cầu người nhận gửi đến địa chỉ, thường là tài khoản nhà băng quốc tế một số tiền để làm thủ tục. Và từ đó, người dùng cả tin, không tỉnh táo, nên dễ rơi vào những bẫy này.

Kẻ xấu còn lợi dụng các tên miền miễn phí, tạo ra các website có địa chỉ gần giống như website của nhà cung cấp dịch vụ game online, hoặc ngân hàng... gửi đến người dùng một email nói rằng mật khẩu email, hoặc tài khoản games của bạn có độ bảo mật thấp. Yêu cầu bạn thay đổi bằng cách nhập lại các thông tin mật khẩu, câu hỏi bí mật... Kiểu lừa đảo này khá tinh vi và phức tạp, có thể cướp email, account, items games, thậm chí chiếm quyền quản lý tên miền, hosting hay tài khoản ngân hàng...

(5) Những kẻ lừa đảo còn đưa ra các tình huống để lừa đảo những người nhẹ dạ như:

+ Cá độ trên mạng: Bạn thắng một giải xổ số ảo trên mạng, nhưng để nhận giải, bạn phải trả trước một khoản chi phí.

+ Tài khoản không có người thừa kế: Một người ngoại quốc có tài khoản tại một ngân hàng ở châu Phi hay châu Á chết mà không có người thừa kế. Nạn nhân được yêu cầu tham gia với vai

https://tieulun.hopto.org

trò bà con giả, nhưng trước hết phải trả những khoản phí hối lộ.

+ Doanh nhân bị ám sát: Kẻ lừa đảo núp dưới bóng một công ty bảo hiểm, sau khi một doanh nhân bị ám sát, sẽ tìm cách giải ngân một tài sản kếch xù cho người thừa kế. Bạn được hứa hẹn một phần của tài sản nếu cùng tham gia phi vụ, nhưng phải trả một khoản phí.

(6) Chúng mạo nhận là một tổ chức quyên tiền đóng góp từ thiện như thiên tai, hoặc một ca phẫu thuật cần nhiều kinh phí cho một cá nhân khó khăn nào đó và yêu cầu gửi tiền hỗ trợ.

(7) Nhiều người thường xuyên tham gia các diễn đàn trên mạng và có công bố hòm thư Yahoo! sau đó đã bị kẻ xấu lợi dụng các nick gần giống để lừa đảo bạn bè họ qua chat. Phương pháp này khá đơn giản và nhanh chóng, một nick ảo tương tự với nick thật để giả mạo kiểu như "phamnhatminh26" thành "phannhatminh26"... Nếu không tinh ý rất khó nhận ra.

(8) Chúng sử dụng tên miền gần giống với tên miền của công ty thật để dụ người sử dụng vào website giả của mình, sau đó cuỗm sạch thông tin cá nhân của họ. Thậm chí chúng còn rao bán các tên miền gần giống với các tên miền có thương hiệu lớn để lừa đảo những người không thận trọng và cả tin.

(9) Chúng có thể gửi email đến những người từng tham gia đấu giá một mặt hàng nào đó tại

https://tieulun.hopto.org

một trang web đấu giá trực tuyến (như eBay chẳng hạn). Thư điện tử mạo danh này có thể tuyên bố rằng nạn nhân đã thắng trong cuộc đấu giá và đề nghị họ cung cấp các thông tin cá nhân chi tiết để hoàn tất thương vụ. Một dạng tấn công khác là khai thác trên mạng để tìm hiểu các mối quan hệ cá nhân, sau đó dùng họ tên trong đó để tạo nên các email ngụy tạo, làm nạn nhân tưởng rằng đó là thư của bạn bè hoặc thân nhân. Kiểu tấn công thứ ba có thể ngụy tạo một trục trặc trong việc truy cập mạng của người dùng, sau đó gửi email đến cho họ, lấy danh nghĩa một công ty dịch vụ đề nghị khắc phục.

(10) Ngoài những kiểu lừa đảo gây thiệt hại về kinh tế, uy tín của một công ty, một kiểu lừa đảo mang tính chất rộng lớn hơn và cũng gây nhiều hậu quả nghiêm trọng, đó là lừa đảo về tình cảm và quan hệ. Hiện nay có vô số các trang web không có địa chỉ, không có người chịu trách nhiệm có các chuyên mục về làm quen, tư vấn tình cảm, giới thiệu việc làm... và những kẻ xấu đã lợi dụng chúng để lừa đảo không ít người sử dụng mạng, biến họ thành những trò đùa tai hại.

Không chỉ giới hạn với những trò bịp trên, những kẻ lừa đảo trên mạng viết ra ngày càng nhiều kịch bản mới, tinh vi hơn nhằm đánh vào lòng tham: tham tình, tham tiền, tham danh của cộng đồng những người dùng mạng.

https://tieulun.hopto.org

c. Những khó khăn trong việc phát hiện các trò lừa đảo trên mạng

Lần theo dấu vết loại tội phạm này rất khó, bởi nó thường vượt ra khỏi biên giới một quốc gia, do đó cũng vượt khỏi tầm thực thi pháp luật của một nước, trong khi luật ở mỗi nước lại khác nhau. Bọn tội phạm đã tận dụng triệt để khó khăn này.

Thông thường, nhân viên của các tổ chức tội phạm trực tuyến không hề biết mình đang nhúng tay vào việc phi pháp. Vô tình, những người này, có thể là những chuyên gia có trình độ cao, đã cộng tác với kẻ xấu. Họ được các ông trùm tuyển dụng thông qua các trang web việc làm. Đây là một biện pháp tuyển dụng rất đặc trưng và phổ biến của các tổ chức tội phạm. Bắt đầu vào vụ án lừa đảo, các ông trùm sẽ chuyển thông tin tài khoản bị mất cắp đến nhân viên, những người ngây thơ nghĩ rằng họ đang hợp tác với các ngân hàng. Nhân viên được hướng dẫn cụ thể để hoàn thành các giao dịch ngân hàng khác nhau trên mạng và không nghĩ rằng, mình đang làm những việc bất hợp pháp.

Các nhà thực thi pháp luật không phải lúc nào cũng lần theo được dấu vết của những vụ lừa đảo để tóm cổ được tội phạm đích thực. Ngay cả khi có người bị phát hiện, thì họ cũng không biết chính xác kẻ đầu sỏ là ai, bởi chúng thường liên

https://tieulun.hopto.org

lạc với họ thông qua thẻ điện thoại ăn cắp hoặc qua địa chỉ email.

Các chuyên gia bảo mật cũng rất khó khăn trong việc ngăn chặn chúng, vì những kẻ hacker, rất có thể lại cũng là các chuyên gia có trình độ cao, và luôn tận dụng những kẽ hở, cả về luật pháp và công nghệ, để thực hiện những ý đồ đen tối của chúng. Theo các chuyên gia về bảo mật thì: "*Hầu hết các phương pháp lừa đảo trực tuyến, kẻ xấu chỉ dựa vào một xác suất rất nhỏ sự nhẹ dạ, hoặc hám lợi của người dùng để thành công*". Cách tốt nhất chính là ý thức của người sử dụng mạng.

2. Các biện pháp tránh bị lừa đảo trên mạng

Ngoài việc thực hiện cài đặt bảo mật cho Windows, bảo vệ trình duyệt Internet, bảo vệ trình duyệt email được cài trong hệ thống và cài đặt các chương trình chống virus, spyware sẽ được chúng tôi giới thiệu ở các chương sau, các bạn cần chú ý thêm các vấn đề sau:

a. Thận trọng khi đọc email

+ Không mở một bức thư khi nghi ngờ là thư rác. Trong trường hợp cần thiết, chỉ mở ở mức độ hạn chế.

+ Đừng trả lời một bức thư bằng cách nhấn nút Reply khi chưa thật an tâm về địa chỉ nơi gửi.

https://tieulun.hopto.org

+ Không nên nhấn chuột vào các đường liên kết trong các email lạ. Điều này đặc biệt quan trọng đối với các email có vẻ đến từ một tổ chức tài chính.

+ Đọc email ngoại tuyến (ngắt kết nối Internet). Điều này ngăn chặn việc tải về máy tính những nội dung nếu vô tình nhấn vào một mối liên kết.

b. Truy cập Internet thận trọng

Không truy cập vào các trang web lạ, nhất là các trang web có nội dung về cờ bạc, phim ảnh bất hợp pháp. Trong các trang web có độ an toàn cao, cũng nên thận trọng khi nhấn chuột vào các mối liên kết, nhất là trên các cửa sổ quảng cáo. Vấn đề này chúng tôi sẽ giới thiệu đầy đủ hơn ở *Chương VII: Truy cập web an toàn*.

c. Cài đặt thanh công cụ chống "phishing"

Một số công ty cung cấp các thanh công cụ phần mềm miễn phí có thể thêm vào trình duyệt Internet nhằm bảo vệ bạn tránh khỏi truy cập vào những trang web lừa bịp.

• http://toolbar.netcraft.com

Đối với Internet Explorer và Firefox tải miễn phí

• http://www.trustwatch.com

• http://www.cloudmark.com

Chỉ đối với Internet Explorer tải miễn phí.

https://tieulun.hopto.org

3. Mạng không dây

a. Giới thiệu chung

Trong những năm gần đây, giới công nghệ thông tin đã chứng kiến sự bùng nổ của nền công nghiệp mạng không dây. Khả năng liên lạc không dây đã gần như tất yếu trong các thiết bị cầm tay, máy tính xách tay, điện thoại di động và các thiết bị số khác. Với các tính năng ưu việt về vùng phục vụ kết nối linh động, khả năng triển khai nhanh chóng, giá thành ngày càng giảm, mạng không dây đã trở thành một trong những giải pháp cạnh tranh có thể thay thế mạng Ethernet LAN truyền thống. Tuy nhiên, sự tiện lợi của mạng không dây cũng đặt ra một thử thách lớn về vấn đề bảo mật trên đường truyền.

Trong khuôn khổ của cuốn sách này, nhằm mục đích cho các cá nhân sử dụng Internet an toàn tại cơ quan hoặc gia đình, nhất là các gia đình có con em còn nhỏ có nhu cầu truy cập Internet, chúng tôi không đi sâu vào mặt công nghệ của mạng không dây mà chỉ giới thiệu những nguy cơ tiềm ẩn và một số vấn đề cần quan tâm khi sử dụng.

b. Các khái niệm cơ bản về mạng không dây

Mạng không dây rất gọn nhẹ, đơn giản và dễ lắp đặt. Để thiết lập một mạng không dây, chủ yếu có hai thiết bị sau:

https://tieulun.hopto.org

* Access point (AP) có vai trò tương tự như Hub hay Switch trong mạng LAN có dây. Điểm truy cập này có thể hỗ trợ từ 15-250 users trong khoảng cách 20-500m, tùy thuộc vào công nghệ và môi trường.

* Wireless card đóng vai trò như một bộ thu phát tín hiệu giúp các thiết bị số trao đổi dữ liệu với nhau hoặc truy cập Internet trong bán kính khoảng 100m (nếu ở trong nhà) và khoảng 300m (nếu ở ngoài trời) tùy theo loại. Lợi điểm lớn nhất của wireless card chính là việc giúp người dùng loại bỏ các sợi cáp lằng nhằng bất tiện, người dùng có thể mang máy tính đến bất cứ đâu có "phủ sóng" để kết nối Internet mà không cần cáp cũng như các khai báo phức tạp.

c. Kết nối không dây dùng Wi-Fi

Có hai loại mạng không dây cơ bản:

Kiểu Ad-hoc: Hai hay nhiều máy tính liên kết trực tiếp với nhau thông qua các thiết bị card mạng không dây mà không dùng đến các thiết bị định tuyến (Wireless Router) hay thu phát không dây (Wireless Access Point).

Kiểu Infrastructure: Các máy tính trong hệ thống mạng sử dụng một hoặc nhiều thiết bị định tuyến hay thiết bị thu phát để thực hiện các hoạt động trao đổi dữ liệu với nhau và các hoạt động khác.

https://tieulun.hopto.org

d. Những nguy cơ tiềm ẩn

Công nghệ Wi-Fi sử dụng sóng radio tầm ngắn, cho phép phát sóng ra xung quanh bán kính lên tới cả trăm mét, dễ dàng xuyên qua một số vật cản. Dữ liệu không dây được truyền trong không khí nên tin tặc dễ phát hiện hơn là dữ liệu tải trên dây cáp. Những kẻ xâm nhập mạng Ethernet sẽ tốn rất nhiều công sức để đột nhập vào mạng này hoặc phải truy cập vào cáp Ethernet vốn đã bị khóa mã. Tuy nhiên, để thâm nhập mạng không dây, tin tặc chỉ cần nằm trong tầm phủ sóng của Wi-Fi, chúng có thể ung dung dò tìm và truy cập vào mạng dễ hơn nhiều so với mạng thông thường.

Những kẻ xâm nhập thường la cà ở những khu công nghiệp, những khu có nhiều văn phòng đang hoạt động và với một máy tính xách tay có card mạng Wi-Fi, chúng dựa trên tên của các access point, có thể dễ dàng xác định chủ nhân của các điểm truy cập vì có nhiều trường hợp tên này được đặt theo tên doanh nghiệp đang sử dụng.

Ngay cả đối với các chuyên viên tin học, bảo vệ an ninh cho mạng không dây luôn là vấn đề cần quan tâm thường xuyên. Người sử dụng bình thường, nhất là trong các gia đình, lại càng đáng ngại hơn vì ít ai để ý các lỗ hổng chết người này.

https://tieulun.hopto.org

Ngoài việc dùng miễn phí Internet, từ cửa ngõ access point, chúng còn đi ngược trở vào mạng nội bộ (LAN) của các đơn vị này, lấy đi các thông tin trong mạng, thậm chí còn thả virus, trojan, spyware để có thể thay đổi các thông số mạng, làm tê liệt hệ thống mạng.

Mặc dù các thông báo về bảo mật luôn được khuyến cáo, cũng ít người dùng tại gia đình và doanh nghiệp nhỏ quan tâm đúng mức đến việc bảo vệ mạng không dây. Nguyên nhân chủ yếu là do người sử dụng ngại đụng đến các thiết lập thông số kỹ thuật rắc rối nên chỉ cần lắp thiết bị Wi-Fi và cho máy tính kết nối Internet là xem như được.

Nguy hiểm hơn nữa, khi phát hiện mất dữ liệu, người bị mất cắp dữ liệu không thể biết mình đang ở đâu vì một access point nếu được đặt ở vị trí thuận lợi có thể phát sóng đi xa cả trăm mét.

Các chuyên gia tin học từng cảnh báo nhiều về nguy hiểm tiềm ẩn từ Wi-Fi đối với người sử dụng máy tính. Kẻ xấu có thể lợi dụng những sơ hở của người sử dụng để làm chuyện phi pháp, trộm cắp thông tin cá nhân hay phá hoại trên mạng Internet kiểu "ném đá giấu tay".

Khoa học kỹ thuật không ngừng phát triển, nhiều thiết bị tin học ứng dụng cuộc sống đến với người sử dụng máy tính đơn thuần ngày càng

https://tieulun.hopto.org

phổ biến do giá thành rẻ so với nhiều năm trước. Thế nhưng sử dụng chúng như thế nào an toàn nhất cũng như tránh rủi ro không cần thiết thì lại hoàn toàn cần sự hiểu biết về bảo mật tin học.

Khi sử dụng các loại thiết bị công nghệ cao không dây nói chung, đừng ngần ngại xin lời tư vấn hay giúp đỡ từ các chuyên gia, nhân viên bán hàng hay người am hiểu về lĩnh vực nói trên để có được giải pháp bảo mật an toàn, tránh rủi ro có thể xảy ra.

e. Những vấn đề cần quan tâm khi sử dụng bảo mật mạng không dây

(1) Mã hóa: Tất cả các thiết bị Wi-Fi đều hỗ trợ công nghệ mã hóa WEP (Wired Equivalent Privacy). WEP sẽ quản lý tất cả dữ liệu trên mạng không dây nên các thiết bị dò sóng sẽ không thể bắt được tín hiệu. Khi cài đặt WEP, bạn nên nhập mật khẩu cho các cấu hình của từng thiết bị trên mạng. Những thiết bị này sẽ sử dụng mật khẩu để tạo ra khóa WEP - được dùng để mã hóa và giải mã dữ liệu truyền trên mạng.

(2) Dùng phần mềm firewall trên từng thiết bị trong mạng.

(3) Dùng phần mềm chuyên dụng để kiểm tra các lỗ hổng an ninh trong mạng Wi-Fi.

(4) Dùng phần mềm chuyên dụng để theo dõi các vụ xâm nhập.

https://tieulun.hopto.org

(5) Thay đổi password sau khi cho phép một máy tính mới truy nhập vào mạng.

(6) Vô hiệu hóa tự động đăng nhập: Đừng thiết lập chế độ tự động đăng nhập vào vùng Wi-Fi gần nhất.

(7) Lướt web có chọn lọc.

https://tieulun.hopto.org

https://tieulun.hopto.org

Phần III

Bảo mật khi truy cập Internet và sử dụng thư điện tử

https://tieulun.hopto.org

https://tieulun.hopto.org

Chương VI

NHỮNG CÀI ĐẶT CẦN THIẾT ĐỂ TĂNG TÍNH BẢO MẬT KHI TRUY CẬP INTERNET

1. Cập nhật các phiên bản Windows và Office mới

a. Tại sao phải cập nhật mới

Mỗi một phiên bản Windows hoặc Office mới ra đời đều tiềm ẩn những lỗi, đặc biệt là các lỗi bảo mật. Những kẻ tin tặc luôn tìm hiểu và tận dụng triệt để các lỗi này để xâm nhập trái phép vào hệ thống máy tính sử dụng các ứng dụng này với mục đích xấu.

Để tránh những tổn thất cho người sử dụng, hãng Microsoft thường xuyên tìm hiểu và tiếp thu những ý kiến đóng góp và đội ngũ chuyên gia của hãng luôn tìm cách khắc phục những thiếu sót đó. Các bản sửa lỗi của Windows và Office cũng như các phần mềm ứng dụng khác luôn được triển khai nhất là bổ sung thêm các chương trình tường lửa. Vì vậy, người sử dụng các phần mềm này nên thường xuyên cập nhật các phiên bản mới mà mình cài đặt trên máy tính, đặc biệt là Windows và Office.

https://tieulun.hopto.org

b. Cập nhật Windows

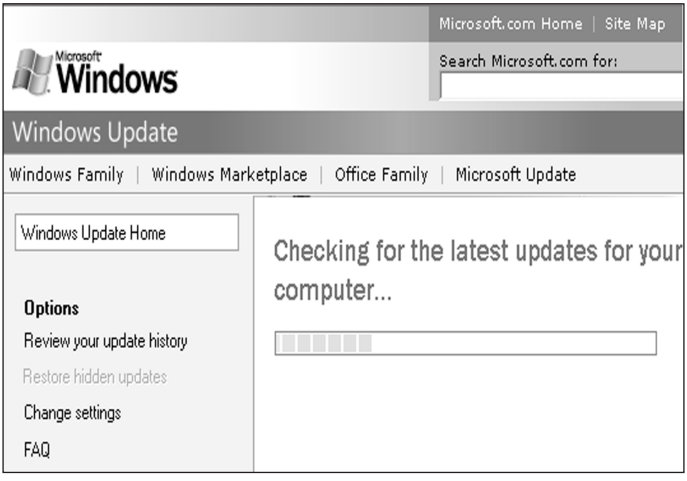
Để cập nhật phiên bản Windows mới, tiến hành các bước như sau:

- Kết nối vào Internet
- Trong khung Address nhập địa chỉ:

http://Windowsupdate.microsoft.com

Tùy theo phiên bản của Windows, hãy chọn nút Express: get hight-priority Update hay nút Express Install: Hight-priority Updates for your computer.

Windows Update Website sẽ quét máy tính của bạn để xác định các mảnh vá bảo mật bị bỏ sót.



Trong một số trường hợp, Windows có thể yêu cầu khởi động lại máy tính.

c. Cập nhật Office

Giống như Windows, phần mềm Microsoft Office như Word, Excel, PowerPoint phải được

https://tieulun.hopto.org

thường xuyên cập nhật với các bản sửa lỗi gần nhất. Cho dù bản Office của bạn mới hay cũ, bạn cũng nên cập nhật thường xuyên mỗi tháng một lần để nhận được sự hỗ trợ tốt nhất về bảo mật của nhà sản xuất. Các bước tiến hành như sau:

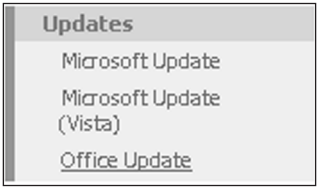
- Kết nối Internet
- Trong khung Address nhập địa chỉ:

http://office.microsoft.com

Khi này trang web cập nhật Office xuất hiện. Nhấn chuột vào nút Check for free updates (thường nằm ở góc trên bên phải của trang web).

Trang web Office Update sẽ quét máy tính để xác định những bổ sung bảo mật đang bỏ sót.

Nhấn chuột vào mục Office Update thường nằm ở bên trái của trang web.



2. Tối ưu hóa khả năng bảo mật của Windows

a. Giới thiệu chung

Là một hệ điều hành được ưa chuộng nhất

https://tieulun.hopto.org

hiện nay nên không có gì ngạc nhiên khi Windows XP đang bị biến thành một môi trường thi thố tài năng của những kẻ tin tặc trên thế giới. Và vì vậy, mỗi khi bạn nhận được các thông báo nào đó của Windows trên tivi hoặc báo chí thì cũng là lúc bạn phải củng cố lại hệ thống máy tính của mình.

Để hệ thống Windows ngày càng ổn định và an toàn hơn, năm 2003 Microsoft phát hành bản sửa lỗi Service Pack 1 tập trung khắc phục mọi sơ hở trong các phần mềm tiện ích đi kèm trong Windows. Bản Service Pack 2 phát hành vào cuối năm 2004 tập trung nâng cao mức độ an toàn và ổn định cho Windows khi kết nối vào Internet thông qua một số cải tiến, bổ sung như: nâng cấp phần mềm tường lửa có sẵn trong Windows; bổ sung chức năng kiểm soát cửa sổ pop-up cho trình duyệt Internet Explorer; tập trung các giao diện kiểm soát chế độ an toàn hệ thống vào một cửa sổ duy nhất có tên là Security Center trong Control Panel. Những tính năng mới này sẽ rất có tác dụng để người sử dụng yên tâm hơn trong môi trường Internet.

b. Cài đặt bức tường lửa

Để cài đặt bức tường lửa, các bạn tiến hành các bước như sau:

• Vào bảng chọn Start khi này một bảng chọn xuất hiện. Chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

https://tieulun.hopto.org

• Nhấn biểu tượng Security Center .

Hộp thoại Windows Sercurity xuất hiện như hình sau:

Chức năng Security Center (ở hình trên) thực chất là rà soát trạng thái hoạt động của các tiện ích bảo vệ hệ thống thông qua Security Center của Windows XP, là một giao diện tập trung để quản lý, theo dõi và cấu hình hoạt động tất cả các phần mềm bảo vệ hệ thống Windows XP như tường lửa (Windows Firewall hay Internet Connection Firewall), cập nhật Windows tự động (Automatic Updates) và cấu hình kết nối Internet. Ngoài ra, Security Center cũng rà soát

https://tieulun.hopto.org

xem hệ thống đã được cài đặt phần mềm chống virus máy tính nào không, tình trạng hoạt động hiện thời ra sao.

Khi một chức năng bảo vệ hệ thống nào đó bị vô hiệu hóa hay một vài chức năng nào đó bị tắt thì màu sắc của biểu tượng Security Center sẽ thay đổi cùng với dòng cảnh báo bằng văn bản hiển thị ở khay System của thanh Taskbar. Nhưng ngay cả khi biểu tượng hiện màu xanh (an toàn) thì cũng chưa chắc hệ thống đã được bảo vệ an toàn, ngược lại, khi hiện màu đỏ cũng không phải là hệ thống đang trong tình trạng nguy hiểm vì có thể do Security Center không nhận diện được các phần mềm bảo vệ khác đã được cài đặt trong máy tính. Làm thế nào để loại bỏ biểu tượng rắc rối này?

Firewall khi được áp dụng cho tất cả kết nối Internet sẽ rất tốt nếu bạn không dùng trình firewall nào khác. Và nếu bạn có cài trình chống virus mà Microsoft nhận diện được, bạn sẽ thấy đèn xanh ở vùng bảo vệ virus.

c. Tinh chỉnh tường lửa

Phần mềm tường lửa có sẵn trong Windows XP có tác dụng ngăn chặn các loại virus máy tính từ bên ngoài tìm cách xâm nhập vào hệ thống máy tính của bạn nhưng nó lại không ngăn chặn được sự liên lạc ra bên ngoài của các virus đã chui được vào trong máy tính của bạn. Thêm vào đó, phần mềm này cũng không có khả năng ngăn chặn

https://tieulun.hopto.org

các virus máy tính xâm nhập từ trình duyệt web, thư điện tử, chat... Vì vậy nên dùng các phần mềm tường lửa có đầy đủ các chức năng cần thiết được cung cấp bởi các nhà sản xuất đáng tin cậy. Sau khi cài đặt phần mềm tường lửa, nên thực hiện thủ tục vô hiệu hóa chức năng tường lửa của Windows như sau:

• Trong cửa sổ Security Center, nhấn chuột vào nút  . Khi này hộp thoại Windows Firewall xuất hiện như hình sau:

• Đánh dấu chọn tại mục Off (not recommended), cuối cùng nhấn nút OK.

Trong một số trường hợp, chức năng Security Center của Windows cũng có thể không nhận

https://tieulun.hopto.org

diện được phần mềm chống virus đang sử dụng và đưa ra những cảnh báo tương tự. Để loại bỏ thông báo này tiến hành như sau:

Mở hộp thoại Security Center, nhấn nút Recommendations... trong vùng Antivirus Protection. Khi này hộp thoại Recommendation xuất hiện như hình sau:

Đôi khi Windows không nhận diện được các phần mềm tường lửa của hãng thứ ba cài đặt trong hệ thống nên sẽ hiện cảnh báo về an toàn hệ thống ở vùng khay hệ thống của Taskbar.

Các bước tiến hành loại bỏ thông báo trên tiến hành như sau:

https://tieulun.hopto.org

- Mở hộp thoại Security Center, nhấn nút Recommendations... . Khi này hộp thoại Recommendation xuất hiện.

- Đánh dấu chọn I have an antivirus program that I'll monitor myself như hình sau.

- Nhấn nút OK .

d. Sử dụng chức năng Automatic Updates của Windows

Tính năng Automatic Updates sẽ tải về từ website của Microsoft và cài đặt các bảo mật quan trọng mỗi khi bạn kết nối Internet. Tính năng này được kích hoạt mặc định, trừ khi hủy bỏ chế độ này.

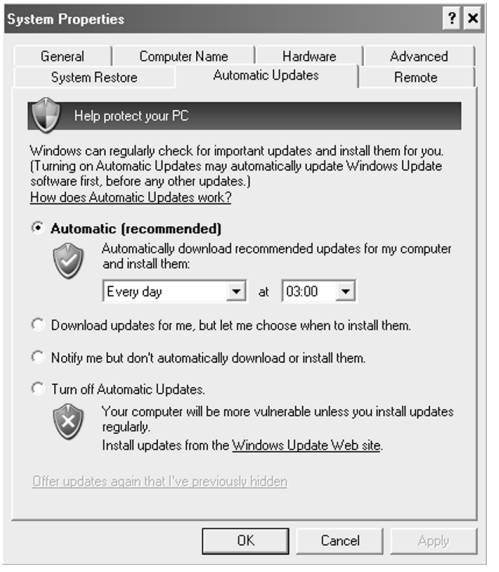
Để sử dụng chức năng Automatic Updates của Windows, tiến hành các bước như sau:

https://tieulun.hopto.org

- Nhấn nút Start của Windows, chọn Setting, chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

- Chọn mục System . Khi này hộp thoại System Properties xuất hiện.

- Chọn mục Automatic Updates. Hộp thoại System Properties có dạng như sau:



Ít có người nào mạo hiểm để máy tính của mình hoàn toàn tự do: tự do kết nối vào Internet, tự động tải về phần mềm, tự động cài đặt phần mềm.... vì làm như vậy vô hình trung đã để cho các phần mềm virus, gián điệp thường trú trong máy tính lợi dụng. Tuy nhiên, thống kê gần đây

https://tieulun.hopto.org

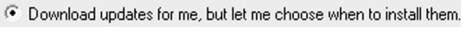
cho thấy thủ đoạn hoạt động của virus máy tính đã thay đổi, đa số virus xâm nhập vào máy tính và liên lạc với bên ngoài thông qua các lỗ hổng bảo mật của Windows hay trình duyệt. Vì vậy việc cập nhật kịp thời các phiên bản sửa lỗi cho Windows và trình duyệt là việc làm thiết thực. Hiện nay đa số các chương trình chống virus máy tính đều có sử dụng tính năng này và nhiều người sử dụng cũng đã khai thác tính năng Automatic Updates của Windows để máy tính của mình được cập nhật kịp thời.

Tuy nhiên, chế độ hoạt động mặc định của Automatic Updates chưa thật sự tối ưu, ví dụ như Automatic Updates tự động làm việc vào lúc 3 giờ sáng để cập nhật các phần mềm mới nhưng hiếm khi máy tính được bật vào giờ này. Hoặc có thể bạn muốn tự mình rà soát lại tất cả và quyết định cái nào cần cập nhật, cái nào không...

Thủ tục tinh chỉnh chế độ hoạt động của Automatic Updates tiến hành như sau:

• Trong hộp thoại System Properties chọn khung Automatic Updates

• Nhấn chọn nhãn Automatic (recommended) rồi chọn thời gian máy tính có thể tiến hành cập nhật.

• Nhấn nút 

để kiểm soát những gì máy tính tải về và cài đặt bổ sung.

https://tieulun.hopto.org

• Nếu kết nối Internet có tốc độ chậm không thích hợp để tải về các tập tin có dung lượng lớn thì nên chọn nút 

, máy tính sẽ thông báo có bản cập nhật mới phát hành để bạn tự tải về và cập nhật vào máy tính.

• Nhấn nút 

khi đã chọn xong.

3. Tạo và kiểm tra bức tường lửa, phần cứng, phần mềm

a. Bức tường lửa phần cứng

Đa số các thiết bị phần cứng (như modem ADSL để nối mạng Internet tốc độ cao) khi được cung cấp đều đi kèm với mật khẩu ngầm định là: "admin". Bạn nên cài đặt lại mật khẩu mới để ngăn chặn việc truy cập trái phép vào máy tính cũng như sử dụng thiết bị phần cứng vào mục đích xấu.

Thường xuyên cập nhật phần mềm điều khiển cho các thiết bị phần cứng để được hỗ trợ các tính năng bảo mật đã được hiệu chỉnh tránh được các lỗi về bảo mật của các phần mềm cũ. Để tải được các phần mềm mới, cần truy cập vào website của nhà sản xuất và tìm kiếm liên kết thường nằm trong mục Support của website đó.

b. Bức tường lửa phần mềm

Kiểm soát được quá trình phát sinh cửa sổ

https://tieulun.hopto.org

pop-up trong khi duyệt web là một tính năng cần thiết và khá hiệu quả để ngăn chặn việc cài lén chương trình bất hợp pháp hay sửa đổi cấu hình hệ thống nhằm ăn cắp thông tin. Trong khi nhiều trình duyệt web khác đã có tính năng này từ lâu thì cho đến nay trình duyệt IE của Microsoft lại không có.

Các tiện ích bảo vệ hệ thống hữu dụng Windows XP sẽ an toàn và ổn định hơn sau khi cài đặt phiên bản Service Pack 2, tuy nhiên các phần mềm bảo vệ hệ thống miễn phí sau sẽ giúp máy tính an toàn hơn nữa.

ZoneAlarm 5: Phần mềm tường lửa có sẵn trong Windows XP có nhược điểm là không kiểm soát được sự chuyển thông tin đi ra từ hệ thống máy tính, do vậy không đủ mạnh để bảo vệ thông tin cá nhân. Zone Alarm của hãng Zone Labs có khả năng bảo vệ an toàn hơn. Phiên bản miễn phí của sản phẩm này chỉ thiếu một vài chức năng bảo mật, còn chức năng tường lửa thì đầy đủ như phiên bản có trả tiền.

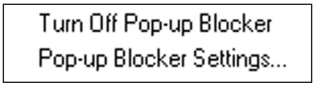
Spybot Search & Destroy 1.3: Phần mềm này ngăn chặn các chương trình gián điệp, quảng cáo xâm nhập hệ thống rất hiệu quả. Phiên bản mới nhất có nhiều cải tiến, sửa đổi quan trọng cho các chức năng như: Phát hiện phần mềm gián điệp theo thời gian thực, kiểm soát chức năng tự động cài đặt của trình duyệt IE, ngăn chặn phần mềm

https://tieulun.hopto.org

gián điệp thay đổi cấu hình của Windows... Bản cập nhật SP2 cho Windows XP đã bổ sung tính năng này cho IE và kích hoạt nó mặc định. Vì vậy, nếu như sau khi cài đặt bản SP2 bạn thấy hoạt động của trình duyệt IE không giống như trước, nhất là khi duyệt các địa chỉ web sử dụng kỹ thuật pop-up để thu thập thông tin từ người sử dụng, thì nên khai báo lại để IE không ngăn chặn pop-up đối với các địa chỉ này.

Để kiểm tra xem chức năng khóa cửa sổ pop-up có hoạt động không, tại trình duyệt Internet Explore tiến hành như sau:

• Vào bảng chọn Tools, chọn mục Pop-up Blocker. Khi này một bảng chọn phụ xuất hiện như hình sau:

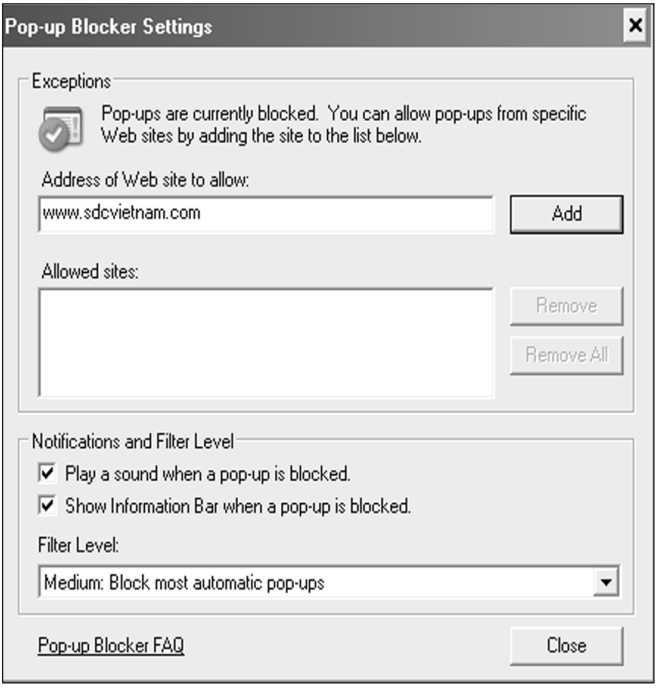


• Chọn mục Turn Off Pop-up Blocker.

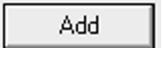
Nếu trình duyệt web hoạt động bình thường thì tiến hành thủ tục khai báo để IE không chặn cửa sổ pop-up đối với địa chỉ web bằng cách tiến hành như sau:

Tiến hành các thao tác như trên và trong hộp thoại phụ xuất hiện, chọn mục Pop-up Blocker Settings, khi này một hộp thoại xuất hiện như hình sau:

https://tieulun.hopto.org



• Trong khung 'Address of website to allow', nhập địa chỉ trang web cần thiết.

• Nhấn nút 

khi đã khai báo xong.

4. Tạo mức bảo mật cho Internet Explorer. Cài đặt bảo mật cho thư điện tử

a. Tạo mức bảo mật cho Internet Explorer

Để tăng độ an toàn khi sử dụng Internet Explorer, nên tạo một mức bảo mật theo yêu cầu như sau:

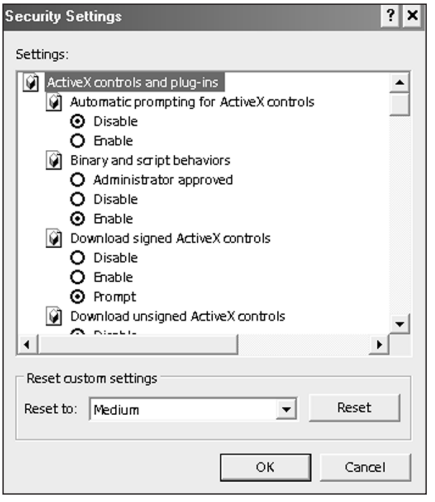
• Khởi động Internet Explorer. Chọn khung Tools.

https://tieulun.hopto.org

• Chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

• Chọn khung Security, nhấn chuột vào nút Custom Level....

Khi này hộp thoại Security Settings xuất hiện có dạng như hình sau:



• Nếu bạn đã cài Windows XP Service Pack 2 hãy cuộn xuống khi nhìn thấy:

• Chọn nút Enable như hình trên.

• Để bảo vệ tránh khỏi các nguy cơ có thể xảy ra, nên vô hiệu hóa toàn bộ các tính năng liên quan đến các kiểm soát ActiveX và JavaScrip.

https://tieulun.hopto.org

b. Vô hiệu hóa AutoComplete

Một số trang web (ví dụ như diễn đàn trao đổi chẳng hạn) yêu cầu bạn nhập mật khẩu và có một tính năng là AutoComplete lưu lại các mật khẩu này để bạn không phải nhập lại mỗi khi truy cập vào trang web đó. Đây là một chức năng thuận lợi cho người sử dụng. Nhưng chính tính năng này là một kẽ hở để những kẻ chuyên ăn cắp mật khẩu lợi dụng. Bởi vì nếu lướt qua được sự phòng thủ của máy tính họ sẽ có danh sách các mật khẩu của bạn.

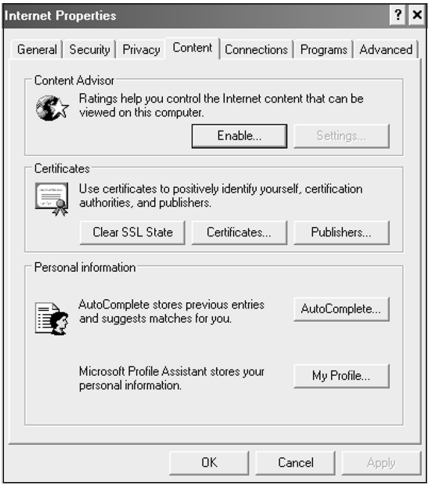
Để vô hiệu tính năng AutoComplete, tiến hành các bước như sau:

• Khởi động Internet Explorer.

• Chọn khung Tools.

• Chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

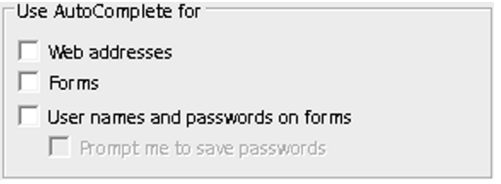
• Chọn khung Content.



https://tieulun.hopto.org

• Nhấn chuột vào nút AutoComplete... . Hộp thoại AutoComplete Settings xuất hiện.

• Xóa đánh dấu trong các ô như hình sau:



• Nhấn chuột vào các nút Clear Forms và Clear Passwords để xóa toàn bộ các mật khẩu và thông tin khác mà chức năng AutoComplete của Internet Explorer lưu trữ.

• Nhấn nút OK để khẳng định.

☞ *Xin các bạn lưu ý*: Trong Internet Explorer 7, hộp thoại Internet Properties có dạng như sau:

Chọn nút Settings trong vùng AutoComplete và khi này cũng thực hiện các thao tác như trong Internet Explorer 6.

https://tieulun.hopto.org

c. Khai báo các Website tin cậy

Khi thiết lập chế độ bảo mật cao (high) thì có thể một số trang web không hoạt động bình thường. Để tránh tình trạng này, nên yêu cầu Internet Explorer cho phép truy cập vào một số trang web theo khai báo được hiển thị bình thường. Các bước tiến hành như sau:

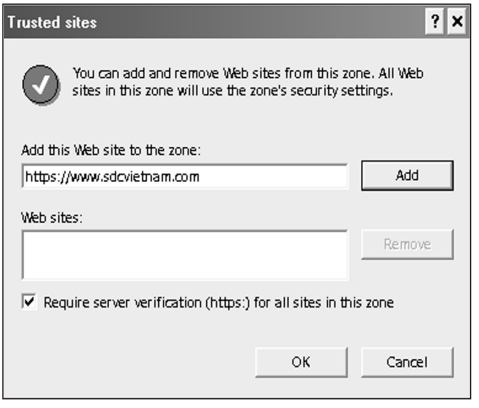
• Vào trình duyệt Internet Explorer

• Vào bảng chọn Tools, chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

• Chọn khung Security.

• Chọn biểu tượng 

• Nhấn chuột vào nút Sites... . Khi này hộp thoại Trusted sites xuất hiện như hình sau:



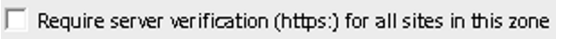
• Nhập địa chỉ trang web tin cậy vào khung Add this website to the zone và nhấn nút Add .

https://tieulun.hopto.org

☞ *Xin các bạn lưu ý*: Trong địa chỉ của trang web phải là https (có chữ "s" ở cuối). Trong trường hợp thiếu chữ "s", Internet Explorer thông báo lỗi:

• Quá trình tiếp tục cho các trang web tiếp theo.

• Để đưa vào danh sách các website không đảm bảo, tiến hành xóa nút đánh dấu ở ô



và nhập tên trang web bắt đầu bằng http:// và nhấn nút 

để bổ sung vào danh mục.

• Khi cần xóa một trang web khỏi danh mục, chọn tên trang web đó và nhấn nút 

.

d. Cài đặt bảo mật cho Outlook Express

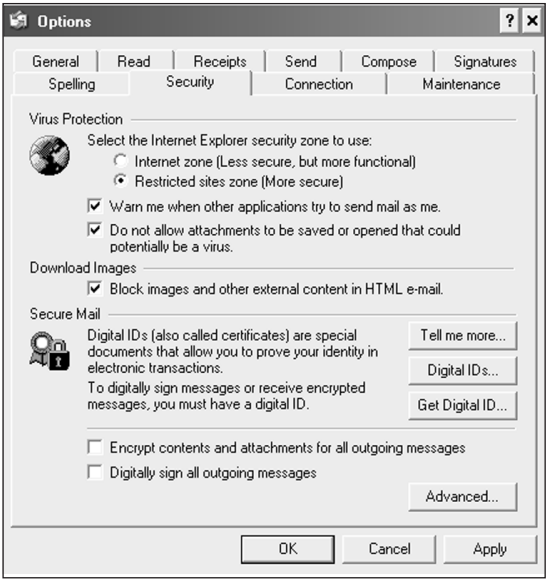
Bản Service Pack 2 của Windows cũng cung cấp thêm cho Outlook Express một chức năng bảo mật khá hấp dẫn. Một số chương trình virus máy tính nhúng trong thư điện tử kiểm tra xem máy tính có kết nối với Internet không bằng cách kiểm tra sự hiện diện của một hình nhỏ nhúng trong thư điện tử bằng ngôn ngữ HTML. Để loại bỏ thủ thuật này, mặc định Outlook Express cấm tải về hình nhúng trong thư điện tử. Vì vậy hình thức của thư điện tử trông sẽ rất xấu. Nếu muốn

https://tieulun.hopto.org

nó khôi phục lại hình dạng nguyên thủy ban đầu thì thực hiện thủ tục sau:

• Tại giao diện của Outlook Express, vào bảng chọn Tools, chọn mục Options. Khi này hộp thoại Options xuất hiện.

• Chọn khung Security. Hộp thoại Options có dạng như hình sau:



• Bỏ dấu chọn tại mục có nhãn Block images and other external content in HTML e-mail.

• Nhấn OK.

5. Xem xét những trình duyệt khác

Mặc dù trình duyệt Internet Explorer của Microsoft được sử dụng khá phổ biến (chiếm khoảng 85% tổng số người truy cập Internet)

https://tieulun.hopto.org

nhưng nó vẫn bị phê bình do những lỗi bảo mật. Microsoft đã nhanh chóng tìm ra các lỗi này và đưa ra các bản sửa lỗi, tăng thêm tính bảo mật, để ngăn chặn những kẻ xâm nhập bất hợp pháp.

Tuy nhiên, bạn cũng nên xem xét các trình duyệt khác, tất nhiên có những tính năng riêng, để phù hợp với công việc của bạn. Hiện nay có nhiều trình duyệt, chúng tôi giới thiệu hai trong số đó là Firefox và Opera.

a. Firefox

Firefox là một trình duyệt có độ bảo mật cao và chiếm rất ít bộ nhớ trong (RAM). Firefox truy cập web nhanh và có khả năng quản lý các cookies, hạn chế được các mẫu quảng cáo. Phần mềm gián điệp và phần mềm quảng cáo khó có thể tự động cài đặt trong Firefox khi truy cập vào website. Firefox không có phần hỗ trợ cho VBScript và ActiveX (hai công nghệ là lý do cho nhiều khe hở bảo mật trong Internet Explorer). Trình duyệt được tải miễn phí tại địa chỉ:

http://ww.molliza.org/product/firefox

b. Opera

Phiên bản miễn phí được tải từ địa chỉ:

http://www.opera.com

Trình duyệt này hạn chế các chương trình quảng cáo, tạo nhiều cửa sổ nhỏ trên màn hình.

https://tieulun.hopto.org

Opera hỗ trợ các tính năng chống phishing, hỗ trợ tính năng quản lý cookies đơn giản và thuận tiện. Trường thông tin bảo mật của Opera tự động được kích hoạt khi người sử dụng truy cập vào một trang web an toàn. Opera đưa ra các chỉ số an toàn của website và hiển thị thông số về người sở hữu chứng thực bảo mật của website đó. Bằng cách trên, người sử dụng có thể đánh giá được mức độ an toàn của website ngân hàng hoặc thanh toán trực tuyến để tránh được những kẻ lừa đảo hay tạo những website giả giống như website của ngân hàng và yêu cầu người truy cập điền số tài khoản và các thông tin cá nhân khác.

Opera cũng hỗ trợ ra lệnh bằng giọng nói - voice command (chỉ bằng tiếng Anh và trên hệ điều hành Windows XP).

6. Cài đặt tùy chọn cao cấp

a. Đối với với trình duyệt Internet Explorer

Có thể tăng cường khả năng bảo vệ cho Internet bằng cách sử dụng một vài tính năng cao cấp của Internet Explorer bằng cách như sau:

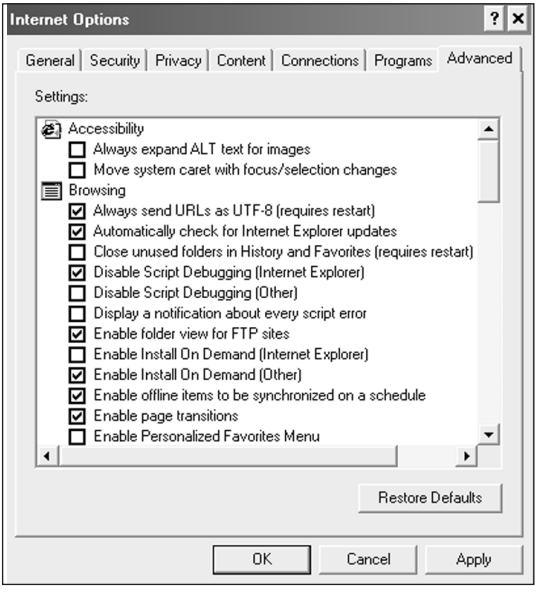
• Khởi động trình duyệt Internet Explorer.

• Vào bảng chọn Tools, chọn mục Internet Options.

• Chọn khung Advanced.

Khi này hộp thoại Internet Options trở thành như hình sau:

https://tieulun.hopto.org



• Chọn các nút của các ô như sau:

☑ Automatically check for Internet Explorer updates

☑ Check for publisher's certificate revocation

☑ Check for signatures on downloaded programs

☑ Do not save encrypted pages to disk

☑ Empty Temporary Internet Files folder when browser is closed

☑ Use SSL 2.0

☑ Use SSL 3.0

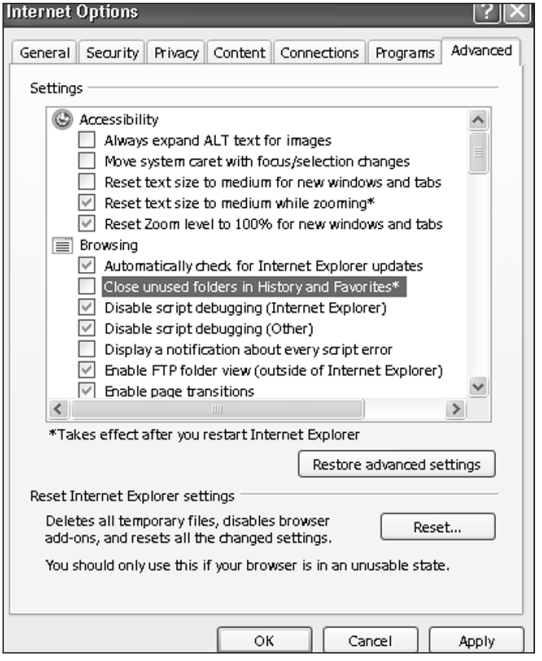
☑ Warn about invalid site certificates

• Xóa đánh dấu của các ô:

☐ Enable Install On Demand (Internet Explorer)
☐ Enable Install On Demand (Other)
☐ Use inline AutoComplete
☐ Enable Profile Assistant

https://tieulun.hopto.org

Xin các bạn lưu ý: Đối với Internet Explorer 7, hộp thoại khi thực hiện các thao tác như trên có hơi khác như hình sau:



Đối với các chức năng có dấu sao (*) ở cuối, bạn phải khởi động lại Internet Explorer mới có hiệu lực.

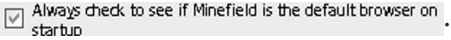
b. Đối với Firefox

Tương tự như Internet Explorer, Firefox cho phép bạn thiết lập các chế độ bảo mật để truy cập Internet an toàn hơn bằng các bước như sau:

• Khởi động Firefox.

• Vào bảng chọn Tools, chọn Options, khi này hộp thoại Options có dạng như hình sau:

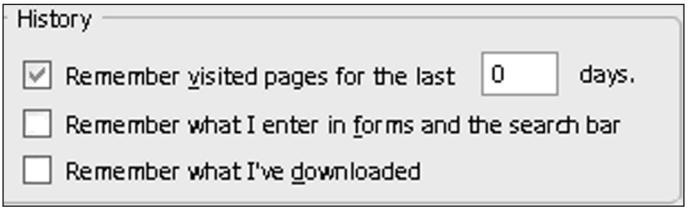
https://tieulun.hopto.org

• Chọn mục 

.

• Chọn biểu tượng 

, trong khung History, thay số 0 vào số 9 trong ô Remember visited pages for the last và xóa đánh dấu còn lại như hình sau:



https://tieulun.hopto.org

• Nhấn nút 

trong hộp thoại Options (khi chọn biểu tượng Privacy). Hộp thoại Exceptions - Cookies xuất hiện như hình sau:

• Nhập địa chỉ của một trang web vào khung Address of website.

• Nhấn chuột vào nút 

để xác định trang web trong cửa sổ Address of website không đặt cookies, ngược lại, khi nhấn nút 

, trang web luôn để lại cookies trong máy tính của bạn.

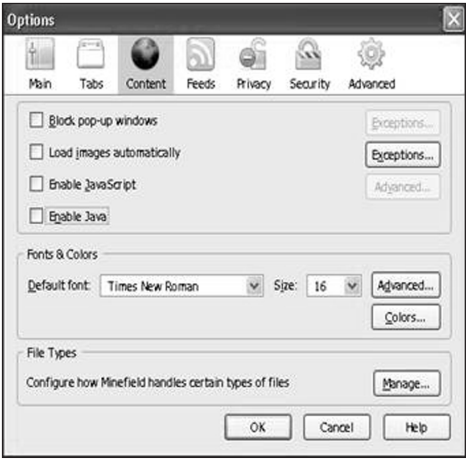
• Nhấn nút 

khi cài đặt xong.

• Trong hộp thoại Options, chọn biểu tượng 

. Khi này hộp thoại Options có dạng như hình sau:

https://tieulun.hopto.org

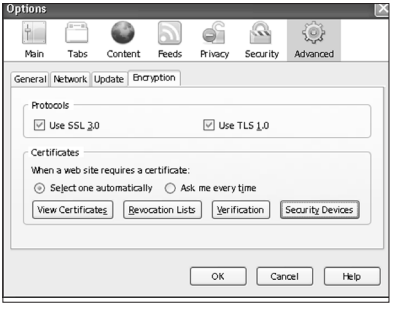


• Xóa đánh dấu trong các nút Block pop-up windows, Load images automatically, Enable JavaScript, Enable Java như hình trên.

• Trong hộp thoại Options, chọn biểu tượng Advanced, chọn khung Update.

• Đánh dấu chọn nút Minefield.

• Nhấn chuột vào khung Encryption, khi này hộp thoại Options có dạng như hình sau:



• Trong khung Protocols, đánh dấu vào các nút chọn như hình trên.

https://tieulun.hopto.org

Chương VII

TRUY CẬP WEB AN TOÀN

1. Kiểm tra hệ thống bảo mật trước khi truy cập Internet

a. Cập nhật Windows và Office

Bạn nên cập nhật lại Windows và Office để hệ thống có được phiên bản mới nhất với những hỗ trợ về bảo mật. Có thể cài đặt bằng tay hay thiết lập chế độ tự động. Thao tác này không nhất thiết phải thực hiện trước mỗi lần truy cập Internet nhưng cũng cần có kế hoạch thực hiện thường xuyên để tăng thêm tính bảo mật cho hệ thống.

b. Kiểm tra các bức tường lửa

Bức tường lửa (Firewall), bao gồm phần cứng và phần mềm đặc biệt quan trọng khi truy cập Internet. Bức tường lửa có thể lọc dữ liệu gõ vào máy tính, kiểm tra các cookie, cảnh báo khi có phần mềm gián điệp. Bức tường lửa thực sự là bức tường thành bảo vệ cho máy tính của bạn trước những nguy cơ tiềm ẩn trên Internet.

Việc cài đặt các bức tường lửa là một việc làm rất quan trọng, tuy nhiên trong một số trường hợp, hoạt động của chúng có thể không được ổn thỏa và kiểm tra sự hoạt động của chúng trước

https://tieulun.hopto.org

khi truy cập Internet là một việc làm cần thiết cho mọi người sử dụng.

2. Thận trọng khi truy cập Internet

a. Lựa chọn trang web khi truy cập

Cách tốt nhất để an toàn trên mạng Internet là lựa chọn các website mà bạn truy cập. Các website thương mại như cnn.com, amazon.com, các website có bản quyền trong nước được phép hoạt động... hầu như luôn an toàn. Các website này không có phần mềm gián điệp, phần mềm quảng cáo. Tuy nhiên cũng không thể khẳng định chắc chắn các trang web này không bị liên kết từ các trang web nguy hiểm khác. Nhìn chung các website có nguy cơ mất an toàn nhất là các website có nội dung đồi trụy, cờ bạc hay phim ảnh bất hợp pháp. Phần lớn các trang web này cài đặt các phần mềm quảng cáo, phần mềm gián điệp vào máy tính của người sử dụng để quảng cáo các sản phẩm của họ hoặc nhằm mục đích không tốt khác.

b. Kiểm tra khả năng bảo mật của website cần truy cập

☞ *Xin các bạn lưu ý*: Các thao tác sau chỉ dùng cho Internet Explorer 6.

Hầu hết các trang web thương mại điện tử đều có giấy chứng nhận chứng minh các giao dịch Internet của họ có khả năng bảo mật và an toàn

https://tieulun.hopto.org

cho người truy cập. Để kiểm tra, tiến hành theo các bước như sau:

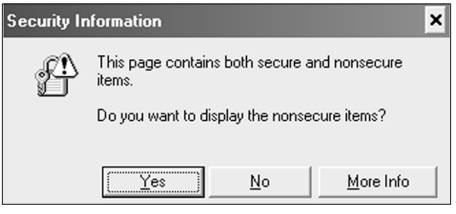
(1) *Bước 1*. Nếu ở phía dưới ở góc phải của màn hình xuất hiện biểu tượng Internet cùng với hình một chiếc khóa như hình sau:

Nhấn chuột vào chiếc khóa và tiến hành *Bước 3* dưới đây.

(2) *Bước 2*: Nếu không thấy biểu tượng là chiếc khóa như trên thì nhập vào khung Address của trình duyệt: https// tên trang web, thay cho việc nhập http:// như thông thường. Ví dụ với trang web: amazon.com thì nhập như sau:

• Nếu bạn được hướng dẫn đến một trang web có dạng http:// như bình thường thì trang web này không có phiên bản bảo mật sẵn có.

• Nếu trang web có bản bảo mật, sẽ xuất hiện một hộp thoại như hình sau:



(Trang này chứa cả hai hạng mục bảo mật và không bảo mật. Bạn có muốn hiển thị hạng mục không bảo mật?)

https://tieulun.hopto.org

• Nhấn chuột vào nút No.

• Nếu hệ thống đang sử dụng Internet Explorer, vào bảng chọn File, chọn mục Properties. Khi này hộp thoại Properties xuất hiện.

• Chọn nút Certificates.

(3) *Bước 3*. Khi này hộp thoại Certificate xuất hiện để bạn kiểm tra chứng nhận của trang web như hình sau:

☞ *Xin các bạn lưu ý*: Đối với Internet Explorer 7 có sự thay đổi khác có liên quan tới https vì vấn đề bảo mật là cách thức Internet Explorer đáp ứng khi gặp một trang web được mã hóa bởi https, nhưng cũng có chứa nội dung http.

https://tieulun.hopto.org

Khi Internet Explorer 6 gặp phải một trang như vậy, trình duyệt này sẽ hỏi người dùng xem họ có muốn hiển thị tất cả các mục được bảo mật cùng với các mục không được bảo mật hay không (như chúng tôi giới thiệu ở *Bước 2*). Vì phần lớn người dùng không hiểu biết sâu về các hậu quả có thể xảy ra do việc hiển thị các dữ liệu không an toàn trong một trang web bảo mật nên Internet Explorer 7 sẽ loại bỏ đi tùy chọn này và chỉ hiển thị nội dung an toàn trong các trang được truy cập thông qua https.

Đối với Firefox, bạn có thể kiểm tra một trang web có được bảo mật không bằng cách nhập địa chỉ: https://.

Ví dụ: https://amazom.com

3. Giảm bớt các mẫu quảng cáo, hạn chế cookie

a. Giảm bớt các mẫu quảng cáo

Để việc truy cập Internet được nhanh và an toàn hơn, bạn nên sử dụng một chương trình hạn chế các mẫu quảng cáo. Có thể sử dụng Google để tìm các bản miễn phí và cài vào hệ thống.

Những phiên bản mới nhất của các trình duyệt web phổ biến như Internet Explorer, Firefox, Opera đều hỗ trợ các chương trình hạn chế mẫu quảng cáo. Bạn nên thường xuyên cập nhật những phiên bản mới nhất để có được những

https://tieulun.hopto.org

hỗ trợ cần thiết. Nếu sử dụng Internet Explorer, bạn nên cập nhật Windows XP Service Pack 2 từ trang web cập nhật.

Một số công ty lớn trên thế giới cũng cung cấp các thanh công cụ miễn phí được cài đặt trong trình duyệt web và tăng cường khả năng tìm kiếm trên Internet.

Một số trang web và tên thanh công cụ hạn chế các trang web quảng cáo như sau:

- MSN Toolbar - http://Toolbar.msn.com
- Google Toolbar - http://Toolbar.google.com
- Yahoo! Toolbar - http://Toolbar.yahoo.com

b. Hạn chế các cookie

Để giảm bớt khả năng bị xâm nhập bởi những kẻ tiếp thị trên Internet, bạn nên kiểm tra các cookie trước khi truy cập Internet để tăng khả năng bảo mật của hệ thống. Nhìn chung, việc xóa bớt các cookie là điều nên thực hiện để tăng tính bảo mật cho hệ thống.

4. Thực hiện an toàn chương trình đáng ngờ

a. Chương trình đáng ngờ là gì?

Khi truy cập vào Internet, bạn sẽ tìm được vô vàn các ứng dụng rất cần thiết cho việc học tập và nghiên cứu như các chương trình chống virus, các ứng dụng của các thành viên trong diễn đàn, các sách điện tử, các phần mềm xử lý đồ họa, xử lý âm thanh...

https://tieulun.hopto.org

Tuy nhiên, trong nhiều trường hợp, bạn không thể chắc chắn về tính an toàn của phần mềm mà mình đã tải về để thực hiện (chạy chương trình), hay cài đặt vào hệ thống. Có thể thiết lập khả năng cài đặt "có hạn chế" cho bất kỳ phần mềm đáng ngờ nào bằng cách sử dụng một tính năng hữu ích trong Windows XP.

b. Thực hiện chương trình đáng ngờ

Đưa con trỏ đến mục của chương trình trong bảng chọn Program hoặc biểu tượng của chương trình trên màn hình Desktop, nhấn chuột phải. Khi này một bảng chọn phụ xuất hiện như hình sau:

☞ *Xin các bạn lưu ý*: trong vài trường hợp, bạn cần ấn và giữ phím <Shift> để thấy mục Run as khi mở bảng chọn.

Trong hộp thoại Run As, bạn chọn Current user và đảm bảo rằng tùy chọn Protect my computer and data from unauthorized program activity được đánh dấu như hình sau:

https://tieulun.hopto.org

Nhấn nút OK.

Khi được thực hiện chương trình (hoặc ứng dụng) trong chế độ này, chương trình có thể đọc các thông số cài đặt Registry, nhưng không thể thay đổi chúng. Ngoài ra, nếu đĩa cứng máy tính được định dạng theo NTFS thì chương trình này sẽ không thể thay đổi bất kỳ tệp nào gắn với tài khoản người dùng (profile) hiện tại, bao gồm các cookie và tập tin tạm của trình duyệt, màn hình nền và thư mục My Documents. Bên cạnh khả năng bảo vệ máy tính trước các chương trình nguy hại được thực hiện trong hệ thống thì tùy chọn này sẽ ngăn cản vài ứng dụng khi có nhu cầu lưu lại tệp vào những thư mục nêu trên. Do đó, chỉ nên áp dụng tùy chọn này cho các phần

https://tieulun.hopto.org

mềm với lai lịch không rõ ràng hay bạn chưa từng sử dụng.

Không những thế, khi bạn khởi động trình duyệt Internet Explorer với tùy chọn Run as, các website sẽ bị vô hiệu hóa khả năng ghi lại dữ liệu trên đĩa cứng nên máy tính cũng sẽ an toàn hơn. Cũng cần lưu ý, ở chế độ này, bạn không thể sử dụng IE để truy xuất đến bất kỳ website được bảo mật nào (bắt đầu bằng "https://"). Thậm chí một vài lệnh cũng sẽ không được thực hiện.

5. Các biện pháp an toàn khi tải dữ liệu từ Internet

Khi tải từ Internet và cài đặt vào máy tính một phần mềm mới không rõ nguồn gốc, nguy cơ máy tính bạn sẽ nhiễm virus hoặc spyware là rất cao. Bạn hãy ghi nhớ những điều sau đây để download một cách an toàn.

a. Chọn site download cẩn thận

Không phải tất cả các site đều có kiểm tra virus, spyware, có tính ổn định và có khả năng dùng được của phần mềm.

b. Đọc đánh giá chuyên nghiệp hay nhận xét của người dùng

Trước khi download, hãy tìm đọc đánh giá chuyên nghiệp hay nhận xét của người dùng. Các trang download tốt nhất đều có cung cấp thông tin nhận xét đánh giá của nhóm biên tập và cho

https://tieulun.hopto.org

phép người dùng gửi ý kiến về ưu, nhược điểm của phần mềm.

c. Có thật sự cần phần mềm đó không

Microsoft cung cấp rất nhiều tiện ích kèm theo mỗi phiên bản Windows, như tiện ích dò lỗi và sắp xếp đĩa cứng, tiện ích giám sát hệ thống, và chương trình sao lưu dữ liệu. Tại sao bạn lại phải mất công dùng thử phần mềm không rõ xuất xứ trong khi Windows có công cụ thực hiện cùng chức năng.

d. Kiểm tra xem tác giả hay hãng phần mềm có cung cấp hỗ trợ kỹ thuật không

Thường thì bạn sẽ tìm thấy địa chỉ website, địa chỉ email hay số điện thoại của tác giả hay hãng cung cấp phần mềm.

e. Đọc kỹ thỏa thuận sử dụng phần mềm và xem xét cẩn thận màn hình cài đặt

Đây là hai cách tốt nhất để xem chương trình miễn phí có kèm theo phần mềm gián điệp không. Nếu bạn không hiểu rõ thỏa ước, hãy kiểm tra ở spychecker.com, website này cung cấp cơ sở dữ liệu các chương trình download có kèm quảng cáo (adware) và gián điệp (spyware).

f. Gạt bỏ nguy cơ

Một khi bạn có vấn đề với phần mềm, hãy loại bỏ nó đừng do dự. Nếu chương trình không có chức năng gỡ bỏ cài đặt, hãy thử dùng Add or

https://tieulun.hopto.org

Remove của Windows hoặc các chương trình khác có tính năng tương tự.

g. Xóa các file DLL liên quan đến phần mềm gỡ bỏ

Hãy xóa sạch các file DLL rác và các mục ở bên trái của Windows Registry liên quan đến phần mềm đã gỡ bỏ. Người dùng có kiến thức có thể tự tin thực hiện việc này bằng cách thủ công, nhưng tốt hơn nên dùng chương trình đáng tin cậy để thực hiện.

h. Tìm xem phần mềm có chức năng gỡ bỏ không

Nếu bạn đã vô tình download phần mềm quảng cáo hay gián điệp, và giờ bạn muốn loại bỏ nó, hãy tìm xem phần mềm có chức năng gỡ bỏ cài đặt không và sử dụng tính năng này gỡ bỏ phần mềm khỏi hệ thống.

https://tieulun.hopto.org

Chương VIII

BẢO VỆ THÔNG TIN CÁ NHÂN KHI TRUY CẬP INTERNET

1. Cài đặt các mật khẩu

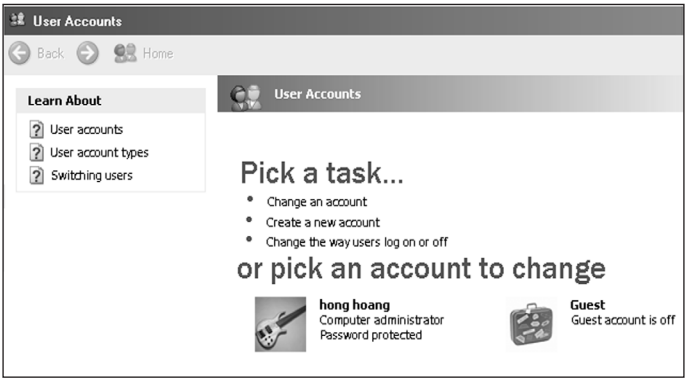
a. Cài đặt account và mật khẩu mới

Một điểm quan trọng trong việc bảo vệ máy tính không bị truy cập một cách trái phép là thiết lập mật khẩu cho các account. Để cài đặt một account mới, tiến hành các bước sau:

• Nhấn chuột vào nút Start của Windows.

• Chọn mục Settings, chọn Control Panel. Khi này hộp thoại Control Panel xuất hiện.

• Chọn biểu tượng User Accounts . Khi này hộp thoại User Accounts xuất hiện như hình sau:



https://tieulun.hopto.org

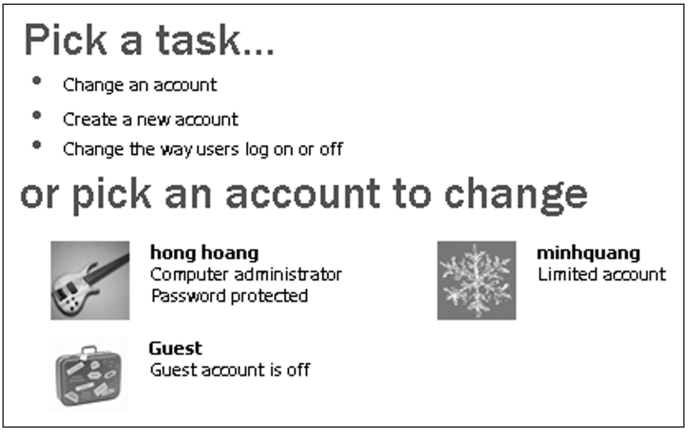
• Chọn mục [• Create a new account].

• Nhập tên account mới vào khung Type name for the new account như hình sau:

• Nhấn chuột vào nút [Next >].

• Trong khung Pick an account type, chọn dạng cho account: Computer administrator (quản trị máy) hoặc Limited (bị giới hạn). Giả sử chọn Limited.

• Nhấn nút [Create Account] khi khai báo xong. Khi này quay lại hộp thoại User Acccount và phía dưới hộp thoại này có dạng như hình sau:



• Nhấn chuột phải vào account mới tạo, hộp thoại User Account trở thành như hình sau:

https://tieulun.hopto.org

• Nhấn chuột vào nút Create a password Khi này một hộp thoại xuất hiện để bạn nhập mật khẩu cho account vừa được tạo. Khi nhập xong mật khẩu, nhấn chuột vào nút Create Password để khẳng định thiết lập mật khẩu cho account được tạo.

b. Sửa mật khẩu cho account. Xóa, thay đổi một số tham số cho account

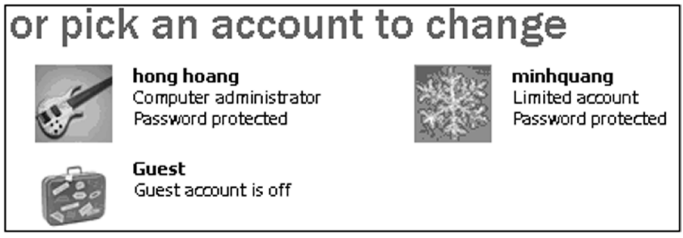
Có thể thực hiện bằng một trong hai cách sau:

➢ *Cách 1*:

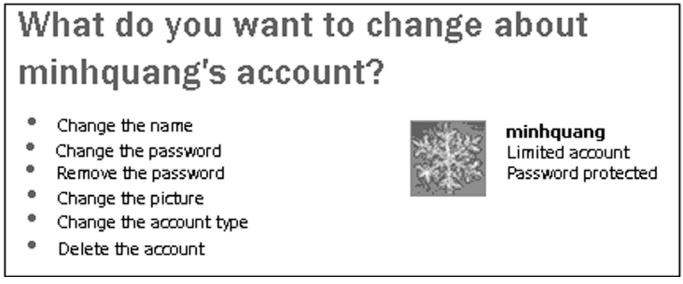
• Nhấn chuột vào nút Start của Windows, chọn mục Settings. Chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

• Chọn biểu tượng User Accounts. Khi này hộp thoại User Account xuất hiện, chọn mục Change an account Khi này danh sách các account xuất hiện như hình sau:

https://tieulun.hopto.org



• Nhấn chuột vào account cần sửa, ví dụ account minhquang. Khi này hộp thoại User Account xuất hiện có dạng như hình sau:



• Trong hộp thoại này, chọn mục Change the password. Một hộp thoại xuất hiện để thay đổi lại mật khẩu hoặc chọn các nút khác để thay đổi dạng mật khẩu, xóa mật khẩu (Remove password), xóa account (Delete the account)...

➢ *Cách 2*: Có thể thay đổi mật khẩu bằng các bước như sau:

• Nhấn chuột phải vào biểu tượng 

.

☞ *Xin các bạn lưu ý*: Nếu biểu tượng này không có sẵn trên màn hình, hãy nhấn nút Start của Windows để mở bảng chọn Start và nhấn chuột

https://tieulun.hopto.org

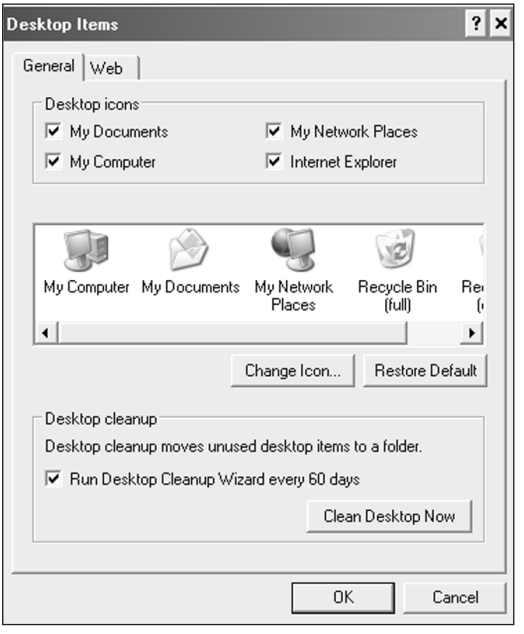
phải vào mục My Computer. Nếu thao tác như trên vẫn không tìm thấy mục My Computer, tiến hành như sau:

• Nhấn chuột phải vào khoảng trống trên màn hình. Khi này một hộp thoại xuất hiện. Chọn mục Properties. Khi này hộp thoại Properties xuất hiện.

• Chọn khung Desktop.

• Chọn nút Customize Desktop... ở phía dưới màn hình.

• Chọn khung General. Hộp thoại Desktop Items có dạng như hình sau:



• Nhấn chuột chọn nút My Computer và nhấn nút OK, khi này con trỏ trở về màn hình trước.

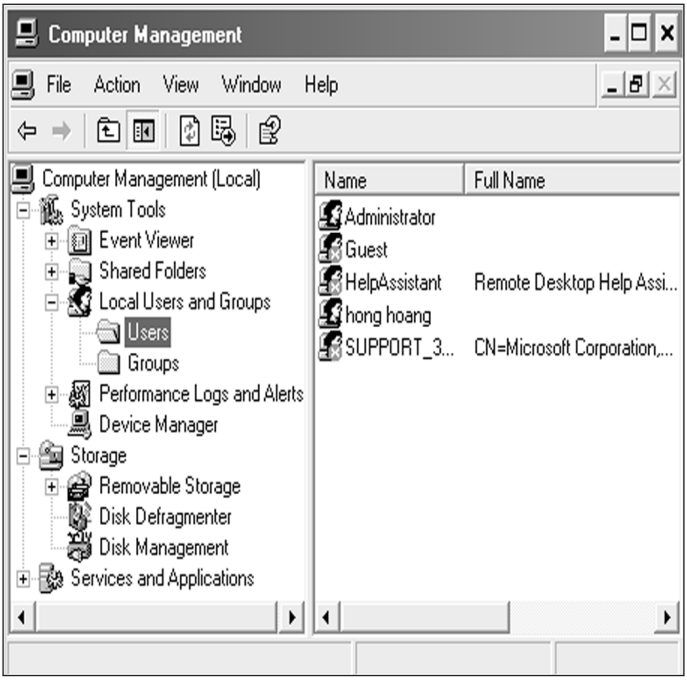
https://tieulun.hopto.org

• Nhấn chuột vào nút Apply. Khi này biểu tượng My Computer xuất hiện trên màn hình Desktop.

• Khi nhấn chuột phải vào biểu tượng My Computer, một hộp thoại xuất hiện, chọn Manage. Hộp thoại Computer Management xuất hiện.

• Tại cửa số bên trái, nhấn chuột vào mục Local User and Groups. Khi này phía dưới xuất hiện thêm hai mục: User và Group.

• Chọn mục User như hình sau:



• Bên phải cửa sổ xuất hiện các account, nhấn chuột phải vào account muốn thay đổi. Khi này một hộp thoại xuất hiện.

https://tieulun.hopto.org

• Chọn Set Password.

• Khi này một cửa sổ mới hiện ra và nhập mật khẩu mới cho account.

c. Yêu cầu nhập account và mật khẩu khi truy cập

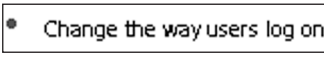
Màn hình Welcome là một chức năng mặc định trong Windows XP cho phép đăng nhập vào Windows bằng cách nhấn vào biểu tượng tương ứng với account của bạn. Để máy tính làm việc an toàn hơn với những người xâm nhập vào máy tính một cách bất hợp pháp, nên vô hiệu hóa màn hình này. Nghĩa là, mỗi người sử dụng trên máy phải gõ account của mình (cùng với mật khẩu) mới có thể truy cập vào máy. Việc làm này sẽ làm tăng tính bảo mật của máy vì những người không được phép sử dụng phải tìm cách lấy được cả account và mật khẩu tương ứng mới sử dụng được máy tính. Để thực hiện được công dụng trên, các bạn tiến hành các bước sau:

• Nhấn nút Start của Windows, chọn mục Settings.

• Chọn mục Control Panel.

• Chọn biểu tượng 

. Khi này hộp thoại User account xuất hiện.

• Chọn nút 

. Khi này hộp thoại có dạng như hình sau:

https://tieulun.hopto.org

• Trong hộp thoại trên, xóa đánh dấu trong nút ☐ **Use the Welcome screen.**

• Nhấn nút **Apply Options**.

d. Bảo vệ máy tính khi tạm thời không làm việc

Nếu bạn cần rời khỏi máy tính trong một thời gian ngắn, máy tính có thể bị một người khác truy cập trực tiếp hoặc gián tiếp qua Internet. Cách an toàn nhất để bảo vệ máy tính là ra khỏi máy tính bằng chức năng Log off của Windows. Thao tác này đòi hỏi phải thoát khỏi các chương trình ứng dụng với các tệp đang mở vì vậy trước khi thực hiện thao tác này, cần lưu các tệp đang mở.

Để thực hiện chức năng Log off của Windows, tiến hành các bước như sau:

• Nhấn chuột vào nút Start ở góc bên trái của Windows.

• Nhấn nút Log Off. Cửa sổ Log Off Windows xuất hiện.

• Nhấn chuột vào nút 

.

https://tieulun.hopto.org

e. Khóa Windows

Thay cho việc đóng các tệp và log off có thể tiến hành khóa Windows bằng cách như sau:

Nếu bàn phím có phím Windows (phím có lôgô như lá cờ của Microsoft):

• Nhấn tổ hợp phím Windows và L. Khi này màn hình Welcome xuất hiện (hay đến một hộp thoại).

• Để trở lại Windows, gõ lại mật khẩu (password) trong màn hình Welcome hay hộp thoại.

Nếu bàn phím không có phím Windows thì tiến hành như sau:

• Nhấn chuột vào nút Start nằm ở phía dưới bên trái màn hình. Khi này một bảng chọn xuất hiện.

• Nhấn chuột vào nút Log Off.

• Nhấn chuột vào nút 

trong hộp thoại Log Off.

Để trở lại Windows, nhấn chuột vào User name và gõ Password.

f. Cài đặt chương trình bảo vệ màn hình

Chương trình bảo vệ màn hình là một ứng dụng của Windows để người sử dụng cài đặt mật khẩu. Sau một thời gian xác định, nếu không nhấn một phím nào hoặc kích chuột thì một màn hình theo cài đặt xuất hiện và muốn trở lại màn hình làm việc thì phải nhập mật khẩu. Chức năng này giúp bạn bảo vệ được máy tính khỏi người khác truy cập khi không được phép và tăng thêm khả năng bảo mật của máy tính.

https://tieulun.hopto.org

Để thực hiện chức năng trên, tiến hành như sau:

• Vào hộp thoại Display Properties theo một trong hai cách sau:

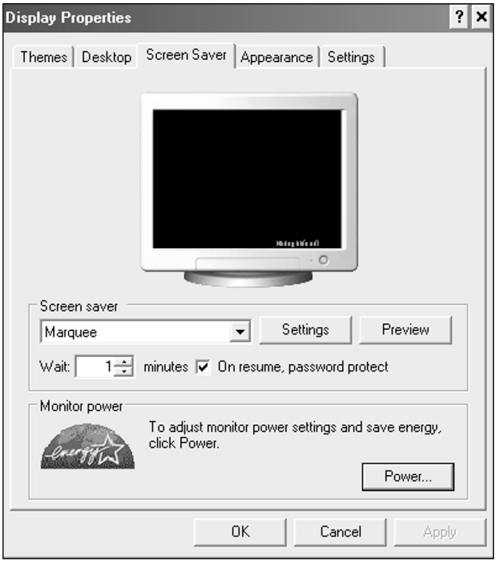
- Tại màn hình giao diện của Windows (desktop), nhấn chuột phải.

- Vào bảng chọn Start, chọn mục Control Panel, chọn biểu tượng 

.

• Sau khi thực hiện một trong hai cách trên, hộp thoại Display Properties xuất hiện.

Chọn khung Screen Saver. Hộp thoại có dạng như hình sau:



• Đặt thời gian chờ trong khung Wait.

• Chọn nút On resume, password protect. (Xin các bạn lưu ý: Đối với Windows XP Home Editor

https://tieulun.hopto.org

thì nút trên trong hộp thoại là: On resume, display Welcome screen).

• Nhấn chuột vào nút Apply .

g. Ngăn chặn sự xâm nhập chương trình bảo vệ màn hình

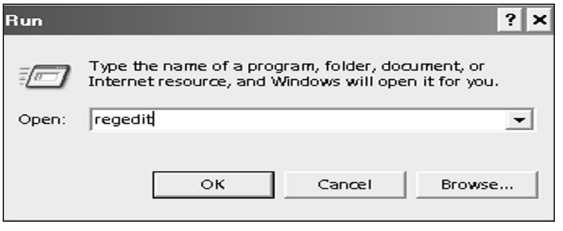
Windows XP Professional Edition tạo khả năng cho phép người sử dụng thiết lập chế độ: khi máy tính không làm việc trong một thời gian nào đó thì một chương trình bảo vệ màn hình sẽ thực hiện. Khi này phải trả lời mật khẩu thì mới vào làm việc tiếp được.

☞ *Xin các bạn lưu ý*: Chế độ này chỉ thực hiện khi bạn truy cập vào Windows bằng mật khẩu.

Vấn đề là ở chỗ, những kẻ xâm nhập vào máy tính có thể thực hiện một phương pháp phổ biến hiện nay là thay thế nó bằng một tệp có thể thi hành nhằm mục đích thay đổi mật khẩu và truy cập vào máy tính của bạn. Bạn cần ngăn chặn khả năng này của những kẻ xâm nhập bằng cách như sau:

• Nhấn chuột vào nút Start của Windows.

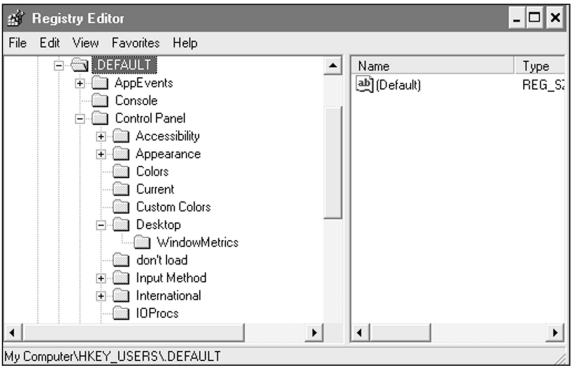
• Chọn mục Run, khi này bảng chọn Run xuất hiện. Nhập regedit vào khung Open của hộp thoại Run như hình sau:



https://tieulun.hopto.org

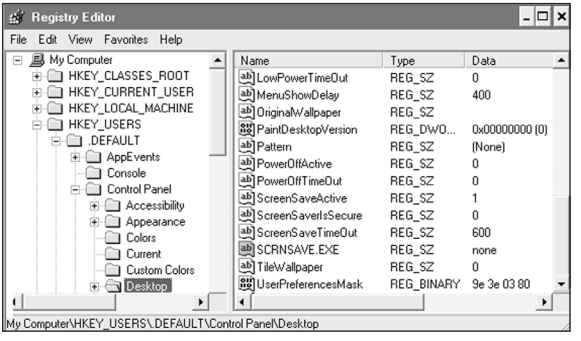
• Hộp thoại Registry Editor xuất hiện. Dùng thanh cuộn bên phải của hộp thoại, tìm và nhấn đúp vào nút HKEY_USER.

• Tìm và nhấn đúp lên mục DEFAULT. Khi này hộp thoại Registry Editor có dạng như hình sau:



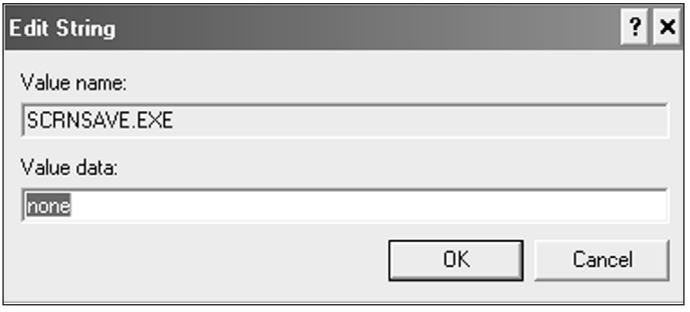
• Tìm và nhấn đúp chuột vào mục Control Panel. Khi này danh sách các mục xuất hiện phía dưới mục Control Panel.

• Tìm và nhấn chuột vào mục Desktop. Các mục tương ứng khi chọn mục Desktop xuất hiện trên cửa sổ bên trái như hình sau:



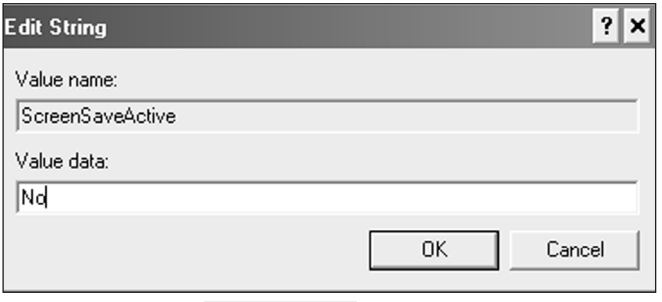
https://tieulun.hopto.org

• Tìm và nhấn chuột lên mục SCRNSAVE.EXE trên cửa sổ bên phải. Hộp thoại Edit String xuất hiện. Trong khung Value data, nhập từ none như hình sau:



• Nhấn nút OK. Khi này con trỏ trở về màn hình Registry Editor. Trên cửa sổ bên phải, dùng thanh cuộn, tìm và nhấn chuột vào mục ScreenSaveActive như hình sau:

• Hộp thoại Edit String xuất hiện. Trong khung Value data nhập: No như hình sau:



• Nhấn nút OK.

https://tieulun.hopto.org

• Nhấn nút  ở góc phải trên cùng để thoát ra khỏi Registry Editor.

h. Đổi tên account của người quản trị

Windows XP Professional chứa một mật khẩu của người quản trị có thể truy cập vào tất cả các vùng trong máy tính và vì vậy, account của người quản trị luôn là đối tượng của những kẻ muốn xâm nhập trái phép vào máy tính của bạn. Chính vì vậy, account và mật khẩu của người quản trị phải được bảo mật đặc biệt. Để đổi tên người quản trị (account), tiến hành các bước như sau:

• Nhấn chuột vào nút Start của Windows.

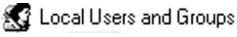
• Vào mục Settings, khi này một bảng chọn phụ xuất hiện. Chọn Control Panel. Khi này hộp thoại Control Panel xuất hiện.

• Chọn biểu tượng 

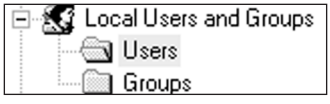
. Hộp thoại Administrative Tools xuất hiện.

• Chọn biểu tượng 

. Hộp thoại Computer Management xuất hiện.

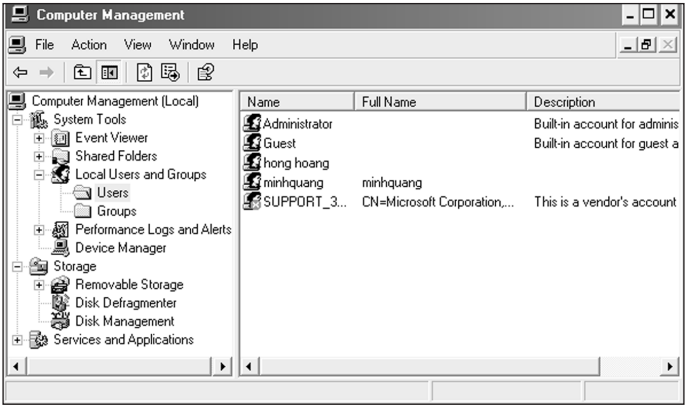
• Nhấn chuột vào biểu tượng 

để phía dưới xuất hiện thêm hai biểu tượng mới như hình trên.



• Khi này hộp thoại Computer Management có dạng như hình sau:

https://tieulun.hopto.org



• Tại cửa sổ bên phải, nhấn chuột phải vào biểu tượng Administrator. Một bảng chọn phụ xuất hiện. Chọn Rename.

• Nhập tên mới cho account người quản trị.

• Có thể tăng cường sự bảo mật bằng cách nhập mật khẩu mới cho người quản trị bằng cách nhấn chuột phải vào biểu tượng Administrator. Khi này một bảng chọn xuất hiện. Chọn mục Set Password. Một màn hình xuất hiện. Nhấn chuột vào nút Proceed. Khi này một màn hình Set Password for Administrator xuất hiện như hình sau:

https://tieulun.hopto.org

• Nhập mật khẩu mới vào hai ô phía trên và nhấn nút 

.

2. Một số vấn đề cần quan tâm khi đặt mật khẩu

a. Các mật khẩu cần tránh

Khi sử dụng máy tính, một loạt các mật khẩu cần thiết lập như để truy cập vào máy tính, mở hộp thư điện tử, truy cập vào một số trang web đòi hỏi có account và mật khẩu, thành viên của một số diễn đàn... và việc nhớ các mật khẩu đó quả thật cũng là một vấn đề cần quan tâm. Để không tốn nhiều thời gian nhớ mật khẩu, người sử dụng thường dùng những từ có liên quan như: tên thành viên trong gia đình, ngày tháng năm sinh của những người thân... và điều này rất dễ để những kẻ gian xâm nhập trái phép và bẻ khóa vì những từ này là đối tượng đầu tiên để chúng quan tâm. Nhìn chung, khi đặt mật khẩu nên tránh:

• Tên của bạn hay thành viên trong gia đình.

• Số nhà hay tên đường bạn đang cư trú.

• Các con số liên tiếp (Ví dụ như 1234 hay 5678).

• Các từ liên quan đến nghề nghiệp của bạn (Ví dụ như nếu bạn là kiến trúc sư thì không nên đặt Kientrucsu...).

• Các con số là ngày sinh của bạn hay người thân trong gia đình...

b. Nên sử dụng mật khẩu như thế nào

Mật khẩu càng phức tạp thì những kẻ ăn

https://tieulun.hopto.org

trộm mật khẩu càng khó có thể ăn trộm được bằng phương pháp thủ công là gõ vào các mật khẩu mà chúng dự đoán hoặc sử dụng các phần mềm ăn trộm mật khẩu. Mật khẩu nên có ít nhất là 6 ký tự và nên có các ký tự đặc biệt như @ # &.

Có thể sử dụng ký tự đầu của một đoạn văn hay tên một bài thơ mà bạn ưa thích và dễ nhớ để làm mật khẩu. Ví dụ: *Hỡi con sông đã tắm cả đời tôi*, để được mật khẩu hcsdtcdt.

Nhìn chung, với bất kỳ một phương pháp đặt mật khẩu thế nào thì việc bị mất cắp vẫn có thể xảy ra và việc thay đổi mật khẩu cần được thực hiện thường xuyên, nhất là sử dụng mật khẩu cho các dịch vụ trực tuyến, thư điện tử...

3. Tạo đĩa cài đặt lại mật khẩu

Để tăng tính an toàn khi đặt mật khẩu, bạn có thể tạo một đĩa cài đặt lại mật khẩu nếu vì một lý do nào đó, mật khẩu bị mất. Các bước tiến hành như sau:

• Chuẩn bị một đĩa mềm trống.

• Nhấn chuột vào nút Start của Windows.

• Đưa con trỏ đến mục Settings, khi này một hộp thoại xuất hiện. Chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

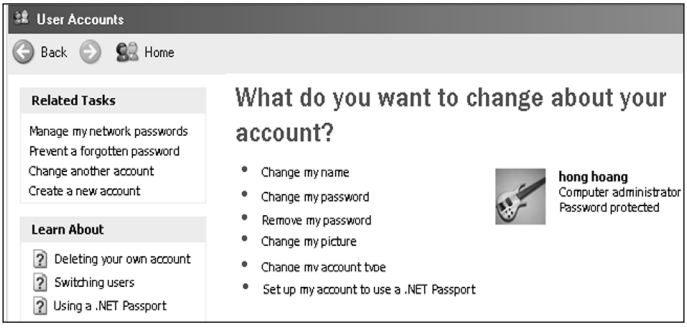
• Chọn biểu tượng 

. Khi này xuất hiện hộp thoại User Account.

https://tieulun.hopto.org

• Nếu Windows sử dụng account có những đặc quyền quản trị, tìm tiêu đề Pick an account to change và nhấn chuột vào tên của account ở dưới biểu tượng này, ngược lại hãy chuyển sang các bước tiếp theo.

• Nhấn chuột vào mục Prevent a forgotten password như hình sau:



• Hộp thoại Forgotten Password Wizard xuất hiện, nhấn nút Next >.

• Đưa đĩa mềm vào ổ đĩa A: và nhấn nút Next >.

• Nhập mật khẩu hiện tại vào khung Current user account password như ở hình sau:

https://tieulun.hopto.org

• Nhấn nút Next >. Máy tính bắt đầu tạo đĩa cài đặt lại mật khẩu. Khi quá trình tạo đĩa cài đặt kết thúc sẽ báo hiệu 100%, nhấn tiếp vào nút Next >.

• Nhấn chuột vào nút Finish để kết thúc. Lấy đĩa cài đặt ra khỏi máy, ghi tên vào nhãn đĩa và cất đĩa vào nơi an toàn.

Để cài đặt lại khi bị mất mật khẩu, tiến hành các thao tác như sau:

• Bật máy tính.

• Sau khi Windows XP tải xuống, hãy nhấn chuột vào tên user của bạn. Một hộp thoại xuất hiện.

• Trong khung Type Your Password, nhấn chuột vào khoảng trắng và không gõ từ nào. Nhấn phím Enter trên bàn phím.

• Nhấn chuột vào nút chấm hỏi (?) trên thông báo Did You Forget Password? để xem phần gợi ý mật khẩu.

• Nếu vẫn không nhớ mật khẩu, nhấn chuột vào mục: Use Your Password Reset Disk.

• Nhấn chuột vào nút Next >.

• Đưa đĩa cài đặt lại mật khẩu vào ổ đĩa mềm.

• Nhấn nút Next >.

• Trong khung Type a New Password, nhập mật khẩu mới.

• Trong khung Type the Password Again to Confirm, nhập lại mật khẩu mới một lần nữa.

• Trong khung Type a New Password Hint nhập một vài từ để giúp bạn nhớ lại mật khẩu mới.

https://tieulun.hopto.org

• Nhấn nút Next > và nhấn nút Finish. Khi này, máy tính quay lại màn hình đăng nhập Windows XP và sẽ nhập mật khẩu mới vào khung Type Your Password để vào làm việc với máy tính.

✍ *Xin các bạn lưu ý*:

Khi thực hiện các thao tác trên thì trên đĩa cài đặt lại mật khẩu đã tự cập nhật mật khẩu mới.

Không thể sử dụng đĩa cài đặt lại mật khẩu trên một máy tính khác ngay cả khi hai máy cùng user và mật khẩu.

4. Hủy bỏ một số chức năng không thật cần thiết

a. Vô hiệu hóa Guest account

Windows có một account mặc định là Guest. Mặc dù account này bị hạn chế một số chức năng truy nhập vào máy tính nhưng cũng tạo điều kiện cho những kẻ tin tặc một cơ hội. Để tăng cường tính bảo mật, nên vô hiệu hóa account này bằng các bước như sau:

• Nhấn chuột vào nút Start của Windows.

• Đưa con trỏ đến mục Settings. Khi này một hộp thoại xuất hiện. Chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

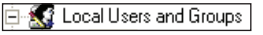
• Chọn biểu tượng 

. Hộp thoại Administrative Tools xuất hiện.

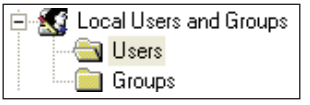
https://tieulun.hopto.org

• Chọn biểu tượng 

. Hộp thoại Computer Management xuất hiện.

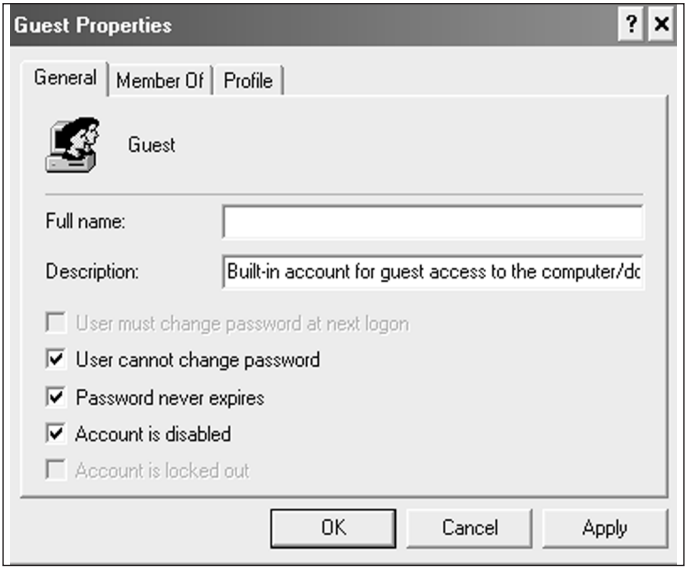
• Nhấn chuột vào biểu tượng 

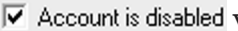
để phía dưới xuất hiện thêm hai biểu tượng mới như hình sau:



• Trên cửa sổ bên phải, nhấn chuột phải vào biểu tượng 

, chọn Properties. Khi này hộp thoại Guest Properties xuất hiện như hình sau:



• Đánh dấu nút 

và nhấn 

và nút 

.

☞ *Xin các bạn lưu ý*: Đối với Windows XP Home Edition tiến hành như sau:

https://tieulun.hopto.org

• Nhấn nút Start của Windows. Bảng chọn Start xuất hiện.

• Nhấn mục Control Panel xuất hiện trong bảng chọn Start, nếu không xuất hiện trong bảng chọn Start thì chọn Settings, và chọn Control Panel.

• Nhấn chuột vào biểu tượng User Account. Khi này một cửa sổ được mở ra.

• Nhấn chuột vào mục Change an Account.

• Nhấn chuột vào mục Guest account.

• Nhấn chuột vào Turn off the Guest account.

b. Vô hiệu hóa Remote Desktop

Windows XP Professional Edition có chức năng Remote Desktop nhằm cho phép bạn truy cập vào hệ thống của bạn từ vị trí bên ngoài. Ví dụ, khi bạn đi du lịch ở một nơi nào đó với một máy tính có kết nối Internet, bạn có thể truy cập vào máy tính đặt tại gia đình để lấy ra các thông tin cần thiết từ các tệp dữ liệu. Mặc dù đây là chức năng thuận tiện, Remote Desktop vẫn tiềm ẩn một nguy cơ mà những kẻ tin tặc có thể tận dụng để xem dữ liệu trên máy tính của bạn nếu có được thông tin đúng về account của Windows. Trong trường hợp không sử dụng chức năng này, bạn nên vô hiệu hóa bằng các bước như sau:

• Nhấn chuột phải vào biểu tượng My Computer trên màn hình. Nếu biểu tượng này không xuất hiện trên màn hình, hãy nhấn chuột

https://tieulun.hopto.org

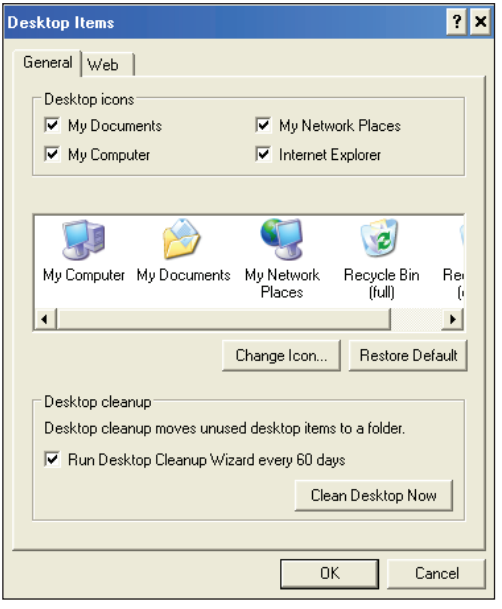
vào nút Start của Windows. Khi này bảng chọn Start xuất hiện. Trong bảng chọn này nếu cũng không tìm thấy biểu tượng My Computer thì tiến hành các bước như sau:

• Nhấn chuột phải vào khoảng trống trên màn hình. Khi này một hộp thoại xuất hiện. Chọn mục Properties. Khi này hộp thoại Properties xuất hiện.

• Chọn khung Desktop.

• Chọn nút Customize Desktop... ở phía dưới màn hình.

Chọn khung General. Hộp thoại Desktop Items có dạng như hình sau:



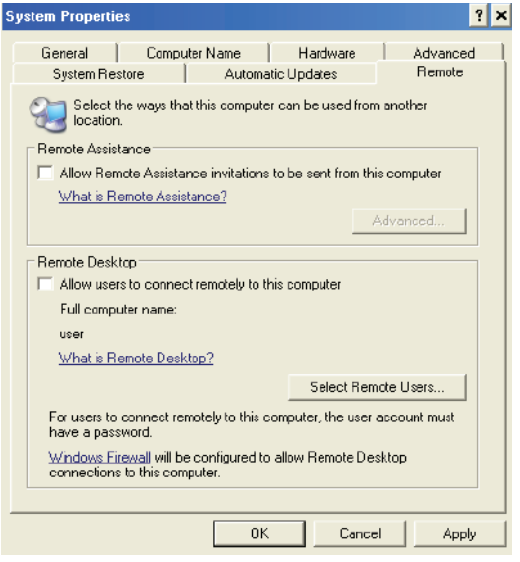
• Nhấn chuột chọn nút My Computer và nhấn nút OK, khi này con trỏ trở về màn hình trước.

https://tieulun.hopto.org

• Nhấn chuột vào nút Apply. Khi này biểu tượng My Computer xuất hiện trên màn hình Desktop.

• Chọn Properties. Khi này hộp thoại System Properties xuất hiện.

• Nhấn chuột vào khung Remote. Hộp thoại System Properties có dạng như hình sau:



• Bỏ đánh dấu trong ô Allow Remote Assistance invitations to be sent from this computer

• Nhấn nút OK và nút Apply.

c. Vô hiệu hóa Remote Assistance

Remote Assistance là chức năng của Windows XP cho phép bạn mời một người nào đó thông qua Internet kết nối với máy tính của bạn để sửa chữa và khắc phục một sự cố phần mềm nào đó. Với cách thức này, những kẻ truy cập trái phép

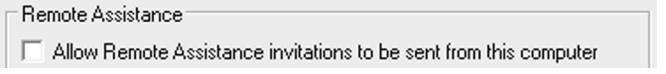
https://tieulun.hopto.org

có thể lợi dụng để cài đặt các phần mềm xấu để tấn công máy tính của bạn hoặc thực hiện những ý đồ không tốt. Trong trường hợp không cần đến tính năng này, có thể ngắt bỏ khỏi hệ thống của bạn (khi cần thì có thể thiết lập lại) bằng cách như sau:

• Nhấn chuột vào biểu tượng My Computer trên màn hình. Nếu biểu tượng này không có, xin vui lòng xem mục: *Vô hiệu hóa Remote Desktop*.

• Chọn Properties. Chọn khung Remote.

• Trong khung Remote Assistance, bỏ dấu chọn trong ô Allow Remote Assistance invitations to be sent from this computer như hình sau:



• Nhấn nút OK và nút Apply.

• Nếu bạn cần thiết lập lại chức năng trên thì chỉ việc chọn nút trong ô ở hình trên.

d. Không dùng chung tệp và máy in khi không cần thiết

Trong trường hợp máy tính của bạn không dùng chung các tệp hoặc máy in với một máy tính khác, nên ngắt bỏ chế độ này để tăng cường bảo mật cho hệ thống của bạn bằng cách như sau:

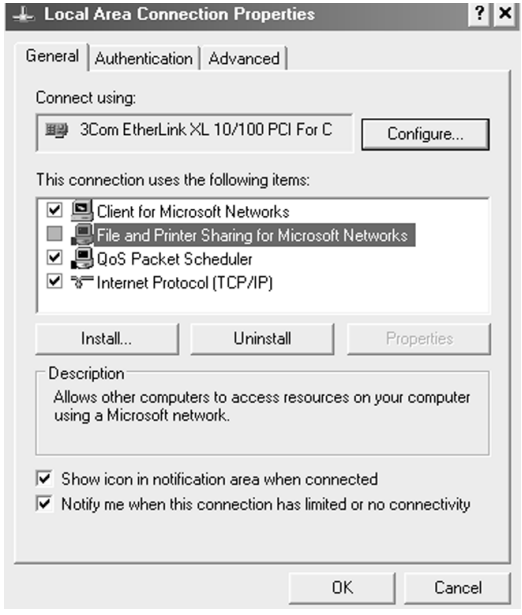
• Nhấn chuột vào nút Start của Windows.

• Đưa con trỏ đến mục Settings, khi này một bảng chọn xuất hiện. Chọn Control Panel.

https://tieulun.hopto.org

• Chọn biểu tượng 

.



• Nhấn đúp vào biểu tượng 

(tuỳ theo máy tính mà Card mạng có thể khác nhau). Khi này hộp thoại Local Area Connection Status xuất hiện.

• Nhấn chuột vào nút 

. Hộp thoại Local Area Connection Properties xuất hiện như hình trên.

• Bỏ chọn ô 

.

• Nhấn nút 

để quay về hộp thoại trước và nhấn nút 

để kết thúc.

e. Xóa tệp Pagefile

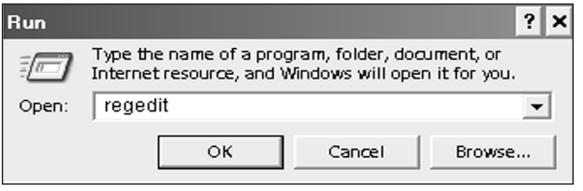
Pagefile là một tệp chứa rất nhiều thông tin

https://tieulun.hopto.org

về máy tính như các mật khẩu, tên user hoặc các đường dẫn tới các dữ liệu riêng khác. Đây là một kẽ hở để những người truy cập vào máy ngoài ý muốn có thể tìm thấy những thông tin bất lợi cho người sử dụng. Để ngăn dữ liệu không nén lại trong tệp Pagefile, có thể thiết lập chế độ để Windows xóa tệp này mỗi khi ra khỏi hệ thống bằng cách như sau:

• Nhấn chuột vào nút Start của Windows.

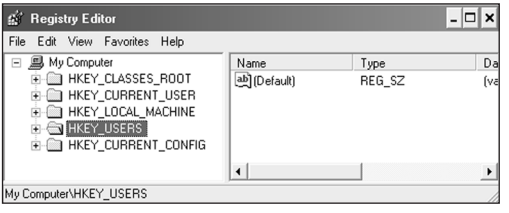
• Chọn Run. Khi này hộp thoại Run xuất hiện. Nhập regedit như hình sau:



• Nhấn nút OK. Khi này hộp thoại Registry Editor xuất hiện.

• Nếu mục HKEY nào có dấu trừ (-) ở bên trái (và phía dưới sẽ là các thư mục con khác) thì nhấn chuột để đóng thư mục này trở thành dấu cộng (+).

• Tiến hành tương tự cho các mục khác để hộp thoại chỉ còn xuất hiện 5 mục như hình sau:



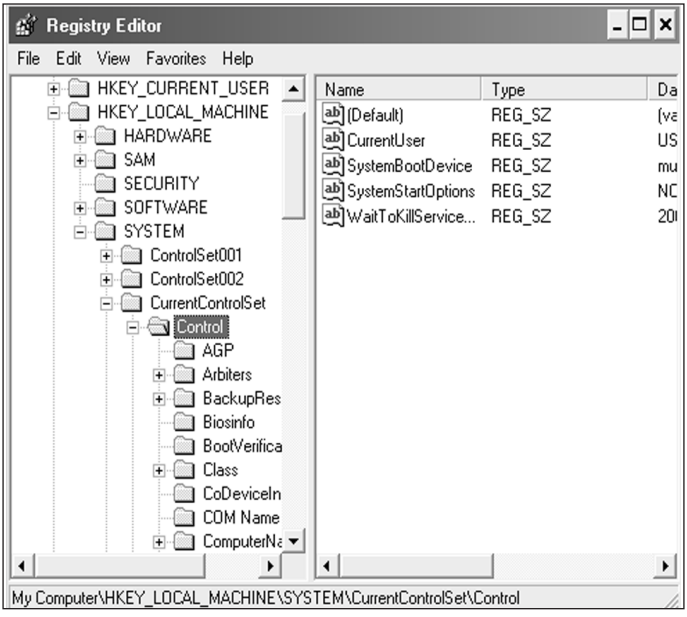
https://tieulun.hopto.org

• Nhấn chuột vào mục HKEY_LOCAL_MACHINE.

• Phía dưới mục này nhấn vào nút SYSTEM.

• Phía dưới mục SYSTEM nhấn chuột vào mục CurrentControlSet .

• Phía dưới CurrentControlSet, nhấn đúp vào mục Control. Một danh sách các khóa được hiển thị như hình sau:



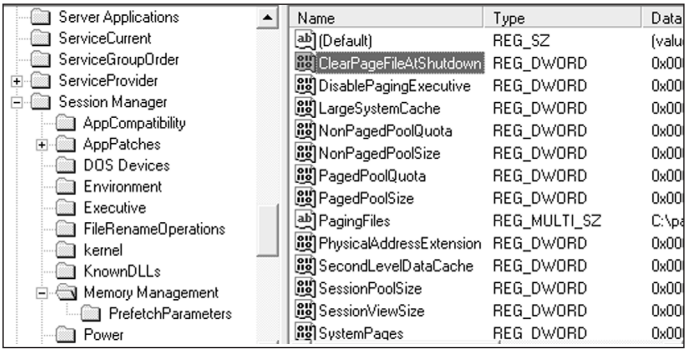
• Sử dụng thanh cuộn để xem các mục phía dưới trong cửa sổ bên trái.

• Nhấn đúp chuột vào mục Session Manager.

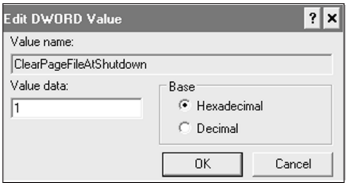
• Phía dưới mục Session Manager, nhấn chuột vào mục Memory Management.

• Tại cửa sổ bên phải nhấn đúp vào nút ClearPageFileAtShutdown như hình sau:

https://tieulun.hopto.org



• Khi này hộp thoại Edit DWORD Value xuất hiện như hình sau:



• Trong khung Value data, thay số 0 bằng số 1 như hình trên.

• Nhấn nút OK để khẳng định và thoát khỏi Registry Editor, nhấn chuột vào nút ✕ phía trên bên phải của hộp thoại.

f. Vô hiệu hóa Dump File

Khi Windows bị lỗi sẽ gửi thông tin đến một kho dữ liệu là Dump File. Tuy nhiên, trong Dump File cũng chứa các thông tin như mật khẩu... sẽ là nơi những kẻ truy nhập trái phép khai thác và sẽ ảnh hưởng đến tính bảo mật của máy tính. Để vô hiệu hóa chức năng này, tiến hành các bước như sau:

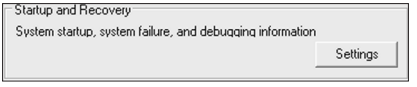
https://tieulun.hopto.org

• Nhấn chuột vào nút Start của Windows.

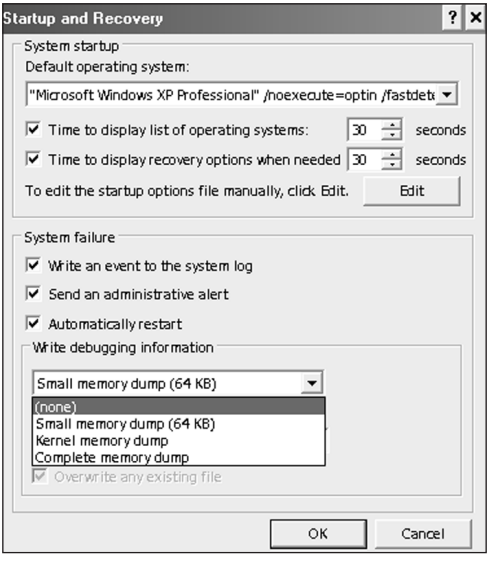
• Đưa con trỏ đến mục Settings. Khi này một hộp thoại xuất hiện. Chọn mục Control Panel. Nhấn chuột vào biểu tượng  **System** . Khi này hộp thoại System Properties xuất hiện.

• Nhấn chuột vào khung Advanced.

• Trong khung Startup and Recovery nhấn chuột vào nút Settings như hình sau:



Khi này hộp thoại Startup and Recovery xuất hiện như hình sau:



• Trong khung Write debugging information nhấn chuột vào mũi tên xuống để xuất hiện một bảng chọn và chọn mục (none) như hình trên.

• Nhấn nút OK để kết thúc.

https://tieulun.hopto.org

g. Vô hiệu hóa Simple File Sharing

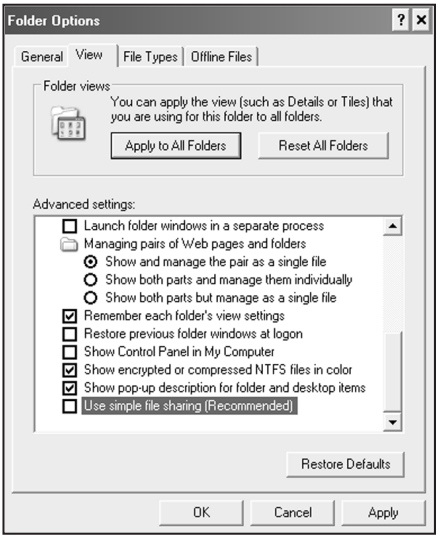
Simple File Sharing là một tính năng cho phép chia sẻ một thư mục lên mạng máy tính để mọi người có thể sử dụng chung. Nếu máy tính của bạn không nằm trên một mạng hoặc là một phần của mạng, bạn cũng nên ngắt chức năng này để tăng tính bảo mật trên máy tính. Các bước tiến hành như sau:

• Nhấn đúp vào biểu tượng My Computer. Nếu biểu tượng này không có, xin vui lòng xem mục: *Vô hiệu hóa Remote Desktop*.

• Chọn khung Tools, chọn mục Folder Options. Khi này hộp thoại Folder Options xuất hiện.

• Chọn khung View.

• Dùng thanh trượt tìm mục Use simple file sharing và xóa nút như hình sau:



• Nhấn nút Apply và nút OK.

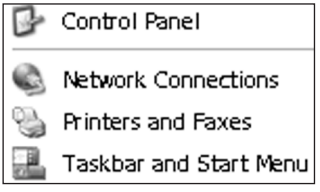
https://tieulun.hopto.org

h. Ngắt Web Server

Một số phiên bản của Windows có cài đặt sẵn chương trình Web Server. Nếu bạn sử dụng trong gia đình hoặc ở văn phòng và không sử dụng Web Server thì nên ngắt chức năng này để tăng thêm tính bảo mật cho máy tính. Để ngắt chức năng Web Server, tiến hành các bước như sau:

• Nhấn chuột vào nút Start của Windows. Khi này bảng chọn Start xuất hiện.

• Đưa con trỏ đến mục Settings. Khi này một bảng chọn xuất hiện như hình sau:



• Chọn mục Control Panel. Hộp thoại Control Panel xuất hiện.

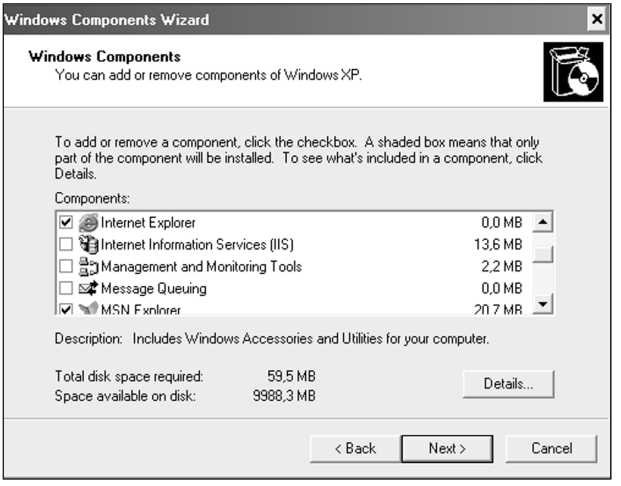
• Chọn biểu tượng 

. Hộp thoại Add or Remove Programs xuất hiện.

• Tại cửa sổ bên trái, nhấn chuột vào nút:

• Khi này hộp thoại Windows Components Wizard xuất hiện. Dùng thanh cuộn tìm mục Internet Information Services (IIS) và xóa đánh dấu các mục trong hộp thoại như hình sau:

https://tieulun.hopto.org



• Nhấn chuột vào nút Next > và nút Finish.

i. Vô hiệu hóa VBScript

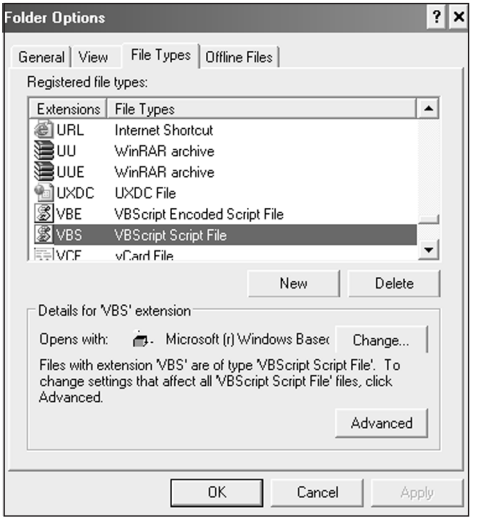
VBScripts - viết tắt của Visual Basic Scripts - là các tệp dạng text chứa mã chương trình có phần mở rộng dạng *.vbs. Những kẻ xâm nhập trái phép thường ẩn các virus hay các nguy hại trên Internet bên trong VBScripts và gán chúng vào các thư điện tử. Khi bạn mở tài liệu đính kèm, mã VBScripts được bung ra kèm theo các virus lây nhiễm vào máy tính của bạn. Để tăng cường khả năng bảo mật của máy tính, bạn nên vô hiệu hóa các VBScripts bằng các bước như sau:

• Nhấn đúp chuột vào biểu tượng My Computer trên màn hình. Nếu biểu tượng này không có, xin vui lòng xem mục: *Vô hiệu hóa Remote Desktop*. Khi này hộp thoại My Computer xuất hiện.

https://tieulun.hopto.org

• Vào bảng chọn Tools, chọn mục Folder Options. Khi này hộp thoại Folder Options xuất hiện.

• Chọn khung File Types. Dùng thanh trượt ở bên phải của cửa sổ tìm phần mở rộng với VBScript Script File như hình sau:



• Nhấn chuột vào nút Delete để xóa phần mở rộng VBS. Nhấn nút Yes khi Windows hỏi Are you sure you want to remove this extension? (bạn có chắc chắn muốn xóa phần mở rộng này không?).

Lặp lại các bước với các kiểu tệp sau:

+ JScript Script File (phần mở rộng JS)

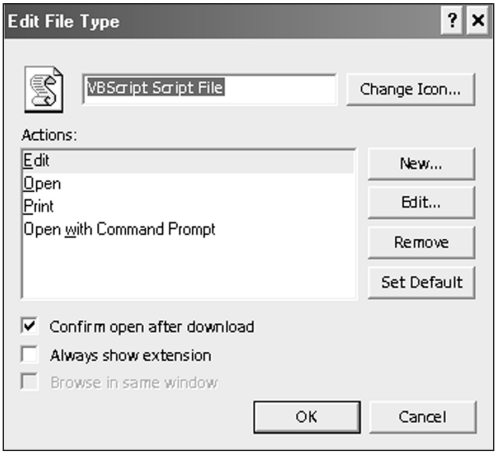
+ JScript Encoded Script File (phần mở rộng JSE)

+ VBScript Encoded Script File (phần mở rộng VBE)

+ Windows Script File (phần mở rộng WSF)

https://tieulun.hopto.org

☞ *Xin các bạn lưu ý*: Nếu vẫn muốn giữ nguyên khả năng chạy VBScript trong một thời điểm nào đó thì không nên xóa chúng mà chỉ ngăn chặn chúng không tự khởi động bằng cách như sau:

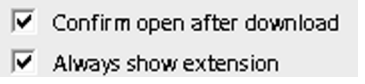


• Trong hộp thoại Folder Options nói trên, nhấn nút Advanced. Khi này một hộp thoại xuất hiện như hình trên.

• Trong khung Actions, nhấn chuột vào nút Edit (không nhấn đúp chuột).

• Nhấn nút Set Default.

• Chọn hai nút như hình sau:



• Nhấn nút OK để trở về hộp thoại Folder Options. Đóng hộp thoại này bằng cách nhấn nút Close.

j. Vô hiệu hóa Messenger

Các nhà thiết kế Windows tạo chức năng

https://tieulun.hopto.org

Messenger để các nhà quản lý mạng máy tính gửi các thông điệp đến các máy tính trong mạng. Chính tính năng này đã tạo nên một kẽ hở để các virus máy tính và các website quảng cáo thâm nhập vào máy tính của bạn.

Để ngắt Messenger các bạn tiến hành các bước như sau:

• Ngắt kết nối Internet để ngăn chặn virus hoặc các nguy cơ khác trên Internet thâm nhập vào máy tính trước khi vô hiệu hóa Messenger.

• Nhấn chuột vào nút Start của Windows.

• Đưa con trỏ đến mục Settings. Khi này một bảng chọn phụ xuất hiện.

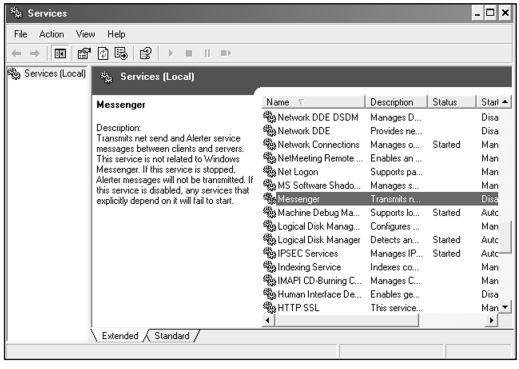
• Chọn mục Control Panel.

Nhấn chuột vào biểu tượng 

. Khi này hộp thoại Administrative xuất hiện.

Sử dụng thanh trượt, tìm và nhấn đúp chuột vào biểu tượng 

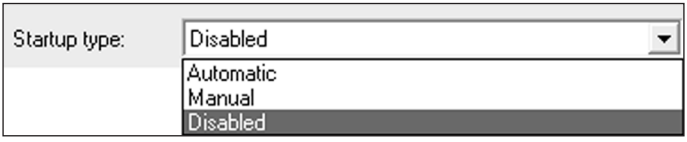
. Khi này hộp thoại Services xuất hiện. Sử dụng thanh trượt tìm mục Messenger như hình sau:



https://tieulun.hopto.org

• Nhấn đúp chuột vào mục Messenger. Hộp thoại Messenger Properties xuất hiện.

• Ở giữa cửa sổ, nhấn chuột vào mũi tên xuống và chọn Disabled như hình sau:



5. Ngăn chặn các phần mềm gián điệp

a. Thiết lập chế độ tự động

Một phương pháp khác để ngăn chặn các mẫu quảng cáo trên Internet không mong muốn và các trang web nguy hiểm là hiệu chỉnh một Windows file có tên là hosts. Để thiết lập chế độ tự động hiệu chỉnh, quản lý các hosts file, phải cập nhật các chương trình phần mềm chống trang web gián điệp như Spy Sweeper hay Spybot Search and Destroy. Bạn cần cập nhật thường xuyên vì các chương trình này luôn bổ sung thêm danh sách các trang web có chương trình quảng cáo hoặc trang web gián điệp để việc ngăn chặn có hiệu quả.

b. Cài đặt bằng tay

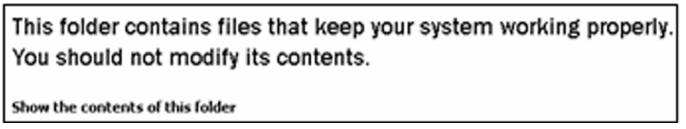
Cho dù bạn có sử dụng chương trình chống phần mềm gián điệp để hiệu chỉnh hosts file hay không, bạn cũng nên hiệu chỉnh nó bằng tay. Các bước tiến hành như sau:

https://tieulun.hopto.org

Nhấn đúp vào biểu tượng My Computer trên màn hình. Nếu biểu tượng này không có, xin vui lòng xem mục: *Vô hiệu hóa Remote Desktop*.

• Nhấn đúp chuột vào ổ đĩa C: (nếu Windows được cài đặt vào ổ đĩa khác thì nhấn đúp chuột vào ổ đĩa này).

• Nhấn chuột vào thư mục Windows. Thông báo như hình sau xuất hiện:



(Thư mục này chứa các tệp giúp hệ thống của bạn hoạt động chính xác. Bạn không nên hiệu chỉnh nội dung của nó).

• Nhấn chuột vào **Show the contents of this folder**. Khi này các thư mục và các tệp xuất hiện trong cửa sổ Windows.

• Nhấn chuột vào thư mục System32.

• Nhấn chuột vào thư mục Drivers.

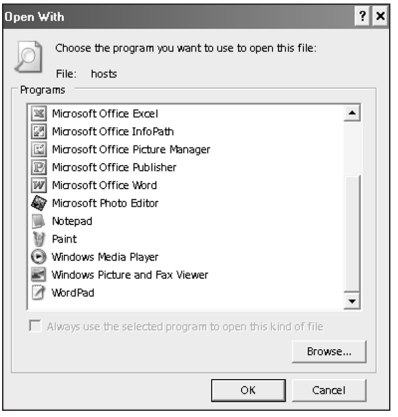
• Nhấn chuột vào thư mục Etc.

• Tìm một tệp có tên là hosts. Nếu chỉ có một tệp này, tiến hành ở bước tiếp theo. (Nếu có nhiều hơn một tệp hosts, tiến hành như sau: Nhấn chuột phải vào tệp hosts đầu tiên. Chọn Properties. Khi này một cửa sổ xuất hiện. Chọn khung General. Nếu xuất hiện: Bên cạnh tiêu đề Type of File sẽ là File và bên cạnh tiêu đề Description sẽ là hosts thì đã chọn tệp hosts chính xác và nhấn nút OK).

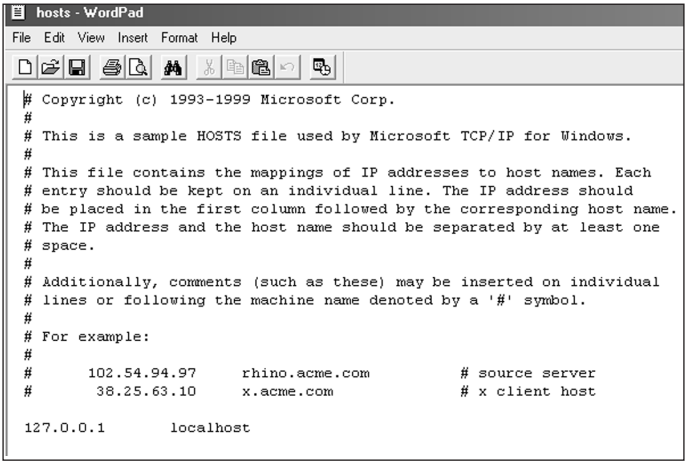
https://tieulun.hopto.org

• Nhấn chuột phải vào tệp hosts. Khi này một hộp thoại xuất hiện.

• Chọn mục Open. Hộp thoại Open with xuất hiện. Dùng thanh trượt tìm mục WordPad như hình sau:



• Nhấn chuột vào mục WordPad. Chương trình WordPad sẽ hiển thị nội dung của tệp hosts như hình sau:



https://tieulun.hopto.org

• Bên dưới cùng tạo một dòng trống bắt đầu bằng 127.0.0.1 tiếp theo là một khoảng trống và sau đó là tên trang web cần ngăn chặn.

Ví dụ: Để ngăn chặn một trang web có tên là www.xxx.com thì nhập vào trong tệp trên với nội dung như sau:

127.0.0.1 www.xxx.com

• Khi đã thực hiện xong việc hiệu chỉnh tệp hosts, vào bảng chọn file, chọn mục Save.

• Để thoát khỏi chương trình WordPad, nhấn chuột vào nút ✕ bên trái màn hình soạn thảo hoặc vào bảng chọn File, chọn mục Exit.

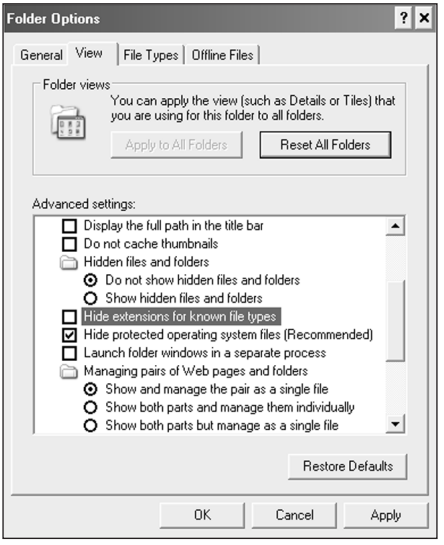
6. Một số thiết lập khác ngăn chặn virus

a. Không ẩn các phần mở rộng file

Windows tự động ẩn các phần mở rộng cho các tệp thường sử dụng hàng ngày. Đây là kẽ hở để nhiều virus ẩn vào trong các site tận cùng với hai phần mở rộng khác nhau: Một phần mở rộng an toàn và theo sau một phần mở rộng nguy hiểm. Ví dụ như: BX.txt.vbt. Do người sử dụng máy tính chỉ nhìn thấy phần mở rộng đầu tiên nên cho rằng đây là tệp an toàn và mở tệp. Tệp này sẽ bung ra các virus và gây ảnh hưởng đến hoạt động của máy tính.

Để thiết lập chế độ hiển thị tất cả các phần mở rộng của các tệp giúp người sử dụng có thể phát hiện virus và các nguy cơ khác có thể ẩn nấp trong đó, các bạn tiến hành các bước như sau:

https://tieulun.hopto.org



• Nhấn chuột vào nút Start của Windows, đưa con trỏ đến mục Settings. Khi này một bảng chọn xuất hiện.

• Chọn mục Control Panel. Khi này hộp thoại Control Panel xuất hiện.

• Nhấn chuột vào biểu tượng 

. Khi này hộp thoại Folder Options xuất hiện. Chọn khung View.

• Sử dụng thanh trượt bên phải để tìm mục Hide extensions for known file types như hình trên.

• Xóa nút đánh dấu trong mục này.

• Nhấn chuột vào nút OK và nút Apply.

b. Không ẩn các phần mở rộng đặc biệt

Mặc dù thực hiện các bước để hiện các phần mở rộng các tệp thông dụng, nhưng vẫn có một

https://tieulun.hopto.org

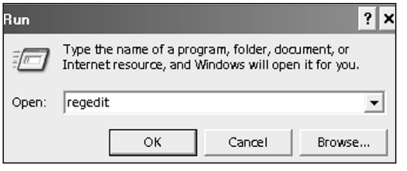
số phần mở rộng đặc biệt mà Windows vẫn cho ẩn, chẳng hạn như.shs,.lnk... Điều này tạo cơ hội cho kẻ xâm nhập trái phép cài virus đánh lừa người sử dụng.

Để thiết lập chế độ hiển thị phần mở rộng đặc biệt, tiến hành các bước như sau:

• Nhấn chuột vào nút Start của Windows.

• Chọn mục Run. Khi này hộp thoại Run xuất hiện.

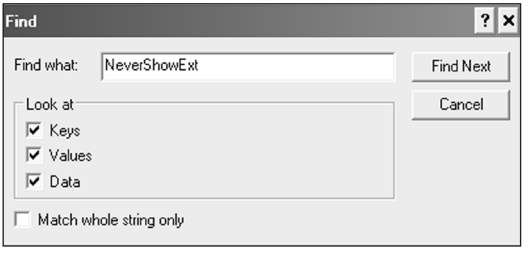
• Trong khung Open của hộp thoại Run, nhập regedit như hình sau:



• Nhấn nút OK. Hộp thoại Registry Editor xuất hiện.

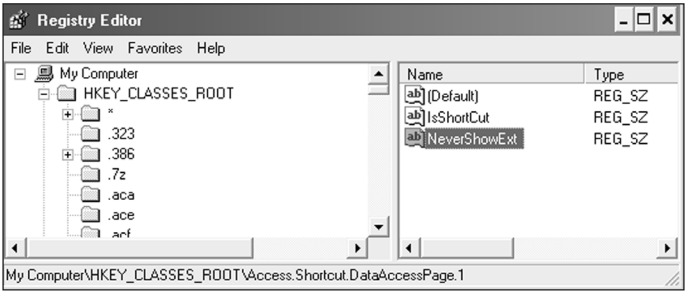
• Vào bảng chọn Edit, chọn mục Find. Khi này hộp thoại Find xuất hiện.

• Trong khung Find what nhập: NeverShowExt và nhấn nút Find Next như hình sau:



• Sau một khoảng thời gian bạn sẽ thấy một mục có tên là NeverShowExt ở bên cửa sổ bên phải của hộp thoại Registry Editor như hình sau:

https://tieulun.hopto.org



• Nhấn chuột vào mục NeverShowExt và nhấn phím Delete hoặc nhấn chuột phải vào mục này và chọn Delete để xoá.

• Nhấn phím F3 để tìm mục NeverShowExt tiếp theo và xóa cho đến khi hết.

• Khi đã xóa xong các mục NeverShowExt, vào bảng chọn File, chọn mục Exit hoặc nhấn chuột vào nút ☒ bên trái của hộp thoại để kết thúc.

7. Cookie máy tính

a. Cookie máy tính là gì?

Cookie máy tính là những tệp nhỏ lưu trữ thông tin mà người sử dụng truy cập và thực hiện trên Internet. Những cookie có ích giúp bạn quản lý được các địa chỉ Internet thường sử dụng, các mật khẩu truy cập vào các trang web và thật là thuận lợi khi không phải nhớ hoặc phải gõ lại những thông tin này. Khi truy cập vào các trang web thương mại điện tử để mua sắm, cookie theo dõi các mặt hàng mà bạn mua sắm. Tập hợp các cookie lại với nhau sẽ giúp bạn quản lý được toàn bộ các công việc thường thực hiện khi truy cập

https://tieulun.hopto.org

vào Internet như: Tin tức mới nhất, sự kiện thể thao, dự báo thời tiết... thay cho việc tìm từng mục trên các trang web riêng rẽ.

Tuy nhiên, cookie cũng tạo điều kiện cho những người quảng cáo và tiếp thị theo dõi các website mà bạn thường truy cập và xem nội dung. Họ đánh giá được nhu cầu, sở thích của bạn và đưa ra các chương trình quảng cáo nằm ngoài ý muốn của bạn.

Thực tế cho thấy, các trình duyệt như Internet Explorer, Firefox, Opera và nhiều trình duyệt khác có khả năng ghi lại chính xác tất cả hoạt động lướt web của người sử dụng một cách đáng kinh ngạc và không chỉ là những thông tin được hiển thị trong cửa sổ History. Việc xóa sạch mọi thông tin trong bộ nhớ trình duyệt (cache) và danh sách website đã truy xuất (history) không những bảo vệ sự riêng tư của người dùng, mà còn cải thiện khả năng hoạt động của máy tính nhờ giải phóng thêm không gian đĩa cứng.

Nhiều website đã nhúng các tập tin văn bản nhỏ (dùng để lưu thông tin về người dùng) vào máy tính khi bạn ghé thăm các website này. Về nguyên tắc, cookie không phải là mối đe dọa đến sự riêng tư của người dùng. Những tập tin này thường chỉ trao đổi thông tin với vài website nhất định. Những nội dung nhạy cảm trong cookie (như thông tin đăng nhập và mật khẩu) thường được mã hóa. Tuy nhiên, trong một số trường hợp sẽ gây ra những tác hại cần quan tâm. Và bất kỳ

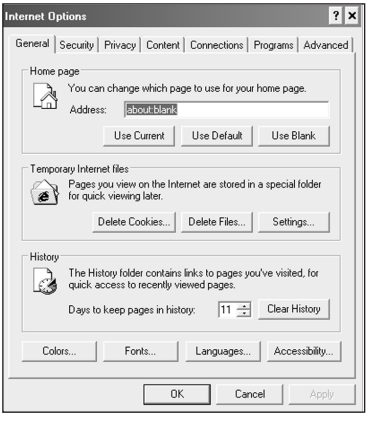
https://tieulun.hopto.org

ai truy cập vào máy tính của bạn không chỉ có thể nhìn thấy các website nào đang lưu cookie vào hệ thống mà còn là nội dung của các cookie không được mã hóa.

Cookie của các hãng thứ ba thường tiềm ẩn những mối đe dọa lớn hơn đối với sự riêng tư của người dùng. Cookie dạng này thường có nguồn gốc từ các dịch vụ quảng cáo và họ có thể sử dụng chúng để theo dõi những website bạn thường truy xuất và sau đó cung cấp những quảng cáo có liên quan đến vấn đề mà bạn quan tâm. Các chương trình chống phần mềm gián điệp thường có khả năng phát hiện và loại bỏ các cookie nhóm 3 này, nhưng bạn cũng có thể cài đặt trình duyệt để ngăn không cho chúng xâm nhập vào máy tính.

b. Kiểm soát cookie trong Internet Explorer

Vào bảng chọn Tools, chọn Internet Options. Khi này hộp thoại Internet Options xuất hiện như hình sau:

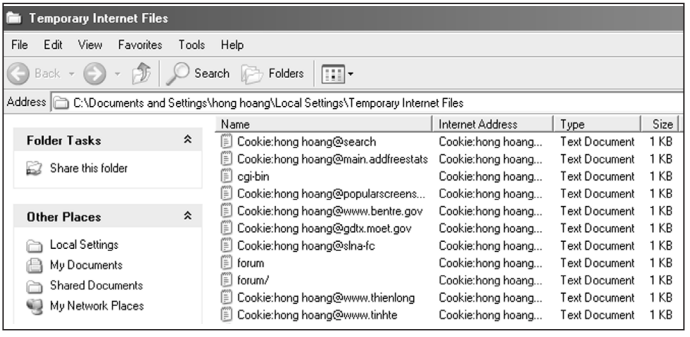


https://tieulun.hopto.org

Chọn khung General, chọn nút Settings... . Khi này hộp thoại Settings xuất hiện.

☞ *Xin các bạn lưu ý*: Có điểm khác về thao tác trong Internet Explorer 7. Chúng tôi sẽ giới thiệu ở cuối mục này.

Trong hộp thoại Settings, chọn mục View Files... . Khi này cửa sổ Temporary Internet Files xuất hiện có dạng như hình sau:



Để chỉ xem cookie, nhấn chuột vào cột Name, rồi sau đó cuộn đến các tập tin có tên bắt đầu bằng chữ "Cookie". Để xóa một cookie, bạn chỉ cần nhấn phải chuột cookie đó và nhấn phím Delete. Sau khi thực hiện xong, đóng cửa sổ thư mục này lại.

Nếu muốn xóa toàn bộ cookie trong máy, tiến hành như sau:

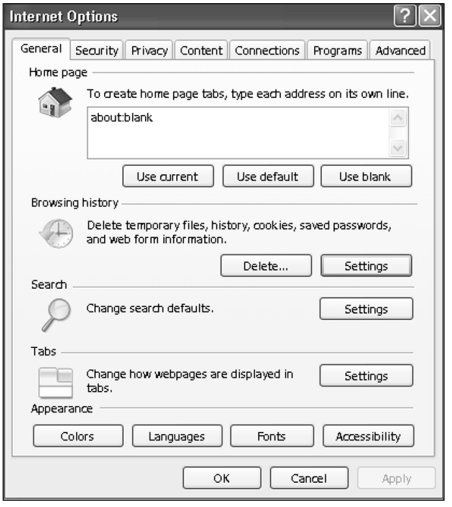
• Vào bảng chọn Tools, chọn mục Internet Options, chọn khung General.

• Nhấn nút Delete Cookies... .

☞ *Xin các bạn lưu ý*: Trong Internet Explorer 7, khi vào bảng chọn Tools, chọn mục

https://tieulun.hopto.org

Interrnet Options và chọn khung General, hộp thoại Internet Options trong trường hợp này có dạng như hình sau:



• Nhấn chuột vào nút Settings trong vùng Browsing history. Khi này hộp thoại Temporary Internet Files and History Settings xuất hiện. Trong hộp thoại này xuất hiện thư mục lưu các cookies như hình sau:

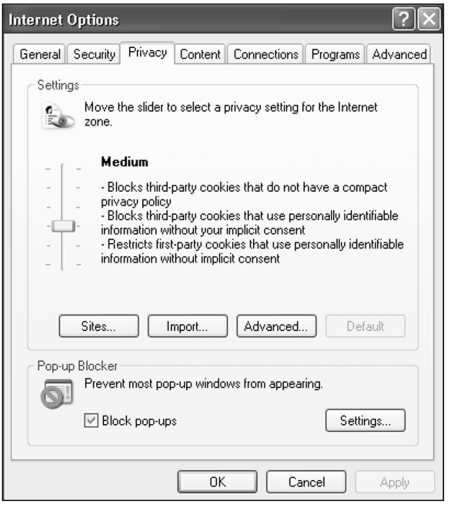
• Có thể chuyển các cookies sang một vị trí khác bằng cách nhấn chuột vào nút Move folder... . Khi này hộp thoại Browse for Folder xuất hiện để chọn ổ đĩa và thư mục cần lưu các cookies.

https://tieulun.hopto.org

Nhấn nút OK khi đã chọn được thư mục cần lưu cookies. Nếu cần xóa các cookies, nhấn chuột vào nút Delete...

• Chọn nút View files. Khi này hộp thoại Temporary Internet Files xuất hiện. Các cookies được hiển thị trong hộp thoại này.

Trong Internet Explorer 6, nếu chỉ muốn ngăn chặn các cookie thuộc nhóm 3, hãy chọn khung Privacy trong hộp thoại Internet Options. Trong khung Settings:



Di chuyển thanh trượt đến một mức giá trị phù hợp. Ví dụ, giá trị Medium High cho phép lướt web một cách bình thường mà không bị gián đoạn do IE yêu cầu bạn trả lời có chấp nhận cookie của một website cụ thể nào đó hay không.

Để kết thúc, nhấn nút OK. Cần lưu ý rằng, cookie được thiết lập bởi các website mà bạn

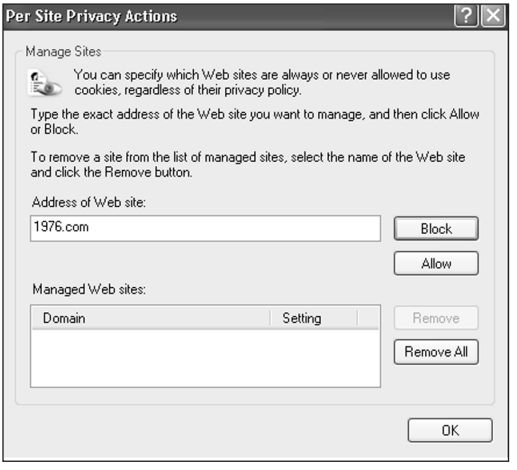
https://tieulun.hopto.org

muốn sử dụng cookie cũng sẽ tự động biến mất khi bạn xóa toàn bộ cookie trong IE.

Ngoài ra, có thể bổ sung địa chỉ các website có cookie mà bạn luôn muốn ngăn chặn hay cho phép xâm nhập vào máy tính bằng cách như sau:

• Nhấn chuột vào nút Sites... trong hộp thoại trên.

• Khi này hộp thoại Per Site Privacy Actions xuất hiện như hình sau:



• Nhập tên trang web vào khung Address of Website. Nhấn chuột vào nút Block để ngăn chặn không cho tạo cookie hoặc nhấn nút Allow để cho phép trang web nhập trong ô Address of Website được tạo các cookie.

Khi này tên trang web trên được đưa vào khung Managed Websites.

• Trong trường hợp muốn xóa một trang web trong khung Managed Websites, nhấn chuột vào

https://tieulun.hopto.org

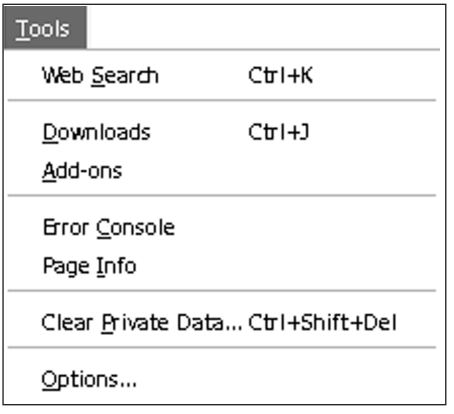
trang web đó và nhấn nút Remove. Khi cần xóa toàn bộ các trang web trong khung Managed Websites, nhấn nút Remove All.

• Nhấn nút OK để kết thúc.

c. Kiểm soát cookie trong Firefox

Trình duyệt mã nguồn mở của Mozilla Foundation được trang bị một tính năng Clear Private Data rất tiện lợi, giúp người dùng xóa nhanh tất cả thông tin cá nhân được lưu trong trình duyệt bằng cách:

• Vào bảng chọn Tools. Khi này bảng chọn Tools có dạng như hình sau:



• Chọn mục Clear Private Data hoặc thay thao tác trên bằng nhấn tổ hợp phím Ctrl+Shift+Del.

Firefox cũng cho phép bạn kiểm soát cookie bằng cách như sau:

• Vào bảng chọn Tools, chọn Options. Khi này hộp thoại Options xuất hiện.

https://tieulun.hopto.org

• Để xem, xóa các cookie, nhấn chuột vào nút Show Cookies... . Khi này hộp thoại có dạng như hình sau:

• Trong khung Site, nhấn chuột vào cookies cần xóa hoặc tìm trong khung Search.

• Nhấn chuột vào nút Remove Cookie để xóa cookie đã chọn hoặc nhấn chuột vào nút Remove All Cookies để xóa toàn bộ các cookie.

• Nhấn chuột vào nút Close để quay về hộp thoại Options.

Trong hộp thoại Options, có thể thiết lập các chế độ ngăn không cho tạo cookie hoặc cho phép tạo cookie đối với từng trang web bằng cách như sau:

• Nhấn chuột vào nút Exceptions... . Khi này hộp thoại xuất hiện như hình sau:

https://tieulun.hopto.org

• Trong khung Address of website, nhập tên trang web.

• Nhấn nút Block nếu muốn ngăn không cho tạo cookie hoặc nút Allow để cho phép tạo cookie.

• Trong trường hợp muốn xóa một trang web ra khỏi danh sách (ngăn không cho tạo hoặc cho tạo cookie) nhấn chuột vào nút Remove Site. Khi muốn xóa toàn bộ các trang web trong danh sách, nhấn nút Remove All Sites .

• Nhấn chuột vào nút Close để đóng hộp thoại lại.

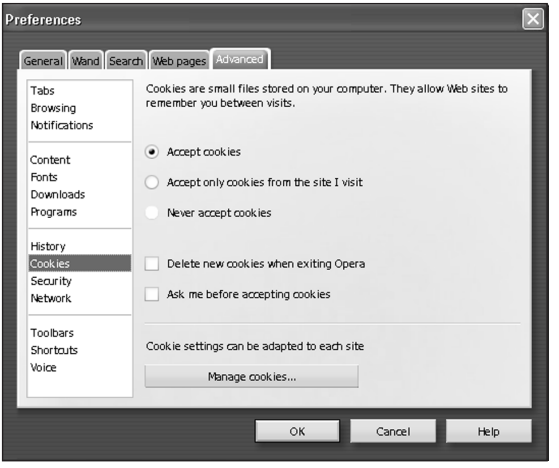
d. Kiểm soát cookie trong Opera

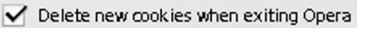
Trình duyệt này cho phép người dùng dễ dàng xóa mọi dấu vết quá trình lướt web. Giống với Firefox và IE, Opera cho phép bạn kiểm soát từng cookie bằng cách như sau:

• Vào bảng chọn Tools, chọn mục Preference. Hộp thoại Preferences xuất hiện.

https://tieulun.hopto.org

• Chọn khung Advanced. Chọn Cookies trên cửa sổ bên trái. Khi này hộp thoại Preferences có dạng như hình sau:

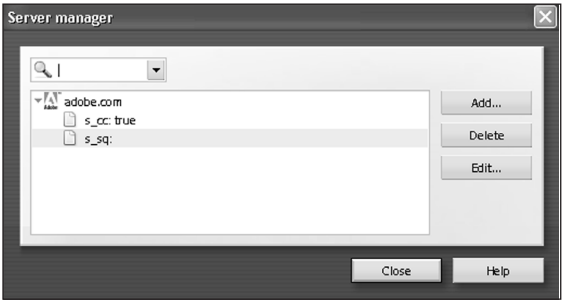


• Đánh dấu lên mục 

để không cho phép trình duyệt lưu lại cookie mới do các website tạo ra trong quá trình làm việc, do vậy tránh được tình trạng các mạng quảng cáo theo dõi hoạt động trên mạng của bạn.

• Để xóa từng cookie riêng lẻ, nhấn nút 

trong hộp thoại Preferences. Hộp thoại Server manager xuất hiện như hình sau:



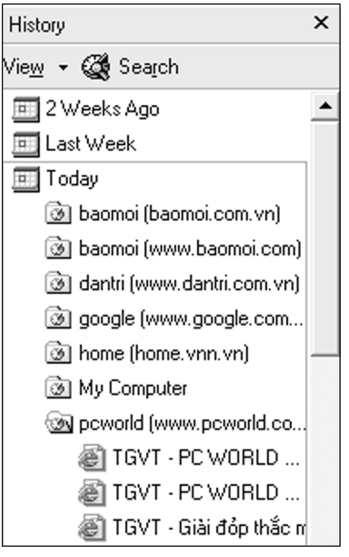
https://tieulun.hopto.org

• Sử dụng dòng tìm kiếm ở phía trên hay duyệt qua cửa sổ thư mục để tìm cookie mong muốn. Cũng giống trong Firefox, phải nhấn chuột lên từng biểu tượng thư mục của website để hiển thị tất cả cookie bên trong, có thể sửa đổi, xóa, cũng như tạo mới chúng bằng cách chọn nút phía bên phải của hộp thoại.

8. Xóa mọi dấu vết

Internet Explorer luôn theo dõi các quá trình tải các tệp tin về máy tính cũng như danh sách các trang web đã truy xuất (history). Bạn nên thực hiện theo các bước sau đây để xóa sạch mọi dấu vết đó.

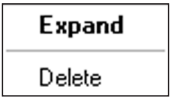
• Ấn tổ hợp phím tắt <Ctrl> + H, cửa sổ History trình duyệt có dạng như hình sau:



https://tieulun.hopto.org

• Trong khung này sẽ liệt kê tất cả website đã truy cập theo thứ tự thời gian và tên trang web.

Khi nhấn chuột phải lên một website, một bảng chọn phụ xuất hiện như hình sau:



• Để xóa tất cả trang web này, chọn Delete.

• Để hiển thị tất cả trang web bên trong chọn Expand và nhấn chuột phải lên một trang web và chọn Delete để xóa nó khỏi history của Internet Explorer.

Ngoài ra, có thể nhanh chóng dọn sạch History bằng cách vào bảng chọn Tools, chọn mục Internet Options, rồi nhấn nút Clear History.

9. Bảo vệ mật khẩu

Bất kỳ trình duyệt nào cũng có thể lưu lại và tự động điền thông tin cá nhân của người dùng vào các biểu mẫu trên web. Sau đây là cách thức giúp bạn cải biến, phục hồi, hoặc xóa bỏ các dữ liệu đó.

Tính năng AutoComplete của IE có khả năng giúp bạn tự động đăng nhập vào một website bằng cách ghi lại những gì bạn đã nhập vào các biểu mẫu lúc trước đây ở chính website này. Để kích hoạt tính năng AutoComplete, tiến hành như sau:

• Vào bảng chọn Tools.

https://tieulun.hopto.org

• Chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

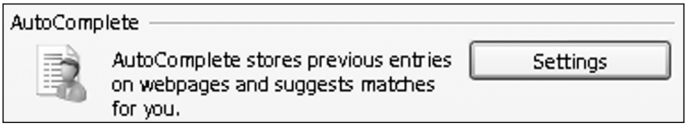
• Chọn khung Content.

• Chọn nút AutoComplete... . Khi này hộp thoại AutoComplete Settings xuất hiện như hình sau:

• Chọn các mục muốn AutoComplete kiểm soát hoặc nhấn Clear Forms hay Clear Passwords để xóa những biểu mẫu và thông tin đăng nhập được lưu trước đây.

• Nhấn OK khi khai báo xong.

☞ *Xin các bạn lưu ý*: Trong Internet Explorer 7, để mở hộp thoại AutoComplete Settings như trên chọn nút Settings trong vùng AutoComplete như hình sau:



https://tieulun.hopto.org

10. Cản trở những kẻ ăn trộm thông tin cá nhân

Khác với những vật dụng khác, những thông tin cá nhân có thể bị ăn trộm mà không cần đến vũ lực. Một sơ suất của người sử dụng có thể mang đến những hậu quả đáng tiếc. Chính do những đơn giản hóa trong quá trình truy cập Internet mà môi trường này đang là một sân chơi rất hấp dẫn của những kẻ chuyên ăn trộm tài khoản cá nhân trên mạng. Chúng ăn trộm tài khoản của người sử dụng để mua sắm hoặc rút tiền nhằm vào mục đích khác. Chúng còn sử dụng những thông tin ăn trộm được vào các mục đích xấu như gửi đi những bức thư với nội dung không lành mạnh, thậm chí đăng ký vào các dịch vụ bất hợp pháp.

a. Tạo các mật khẩu khác nhau

Một người sử dụng mạng Internet chắc chắn sẽ có nhiều account cho việc giao dịch trực tuyến như giao dịch với ngân hàng, kiểm tra cước điện thoại di động, mua sắm qua mạng và nhiều thứ khác nữa. Nhiều người sử dụng chung một account và mật khẩu để thuận tiện cho việc quản lý đã gây nên những rủi ro đáng tiếc vì nếu kẻ trộm khám phá được account và mật khẩu đó, chúng hoàn toàn có thể làm chủ được các account còn lại. Hãy tự bảo vệ mình bằng cách tạo ra cho mỗi một website một mật khẩu và chúng được ghi

https://tieulun.hopto.org

nhớ bằng cách viết vào một quyển sổ và cất vào một vị trí cần thiết. Việc ghi các mật khẩu vào máy tính cũng mất an toàn trừ trường hợp chúng được mã hóa vì việc máy tính bị thâm nhập bất hợp pháp, mất mát hoặc phải sửa chữa ngoài ý muốn rất có thể xảy ra.

b. Bảo vệ các thông tin cá nhân

Hãy thận trọng với các thông tin cá nhân khi phải khai báo trên Internet. Khi những thông tin đã được tiết lộ, bạn không thể biết được những ai có thể tình cờ thấy được và họ sử dụng chúng như thế nào. Với các thông tin như địa chỉ, số điện thoại, nơi công tác, địa chỉ email...nhìn chung không nên kê khai. Trường hợp các website đó bắt buộc phải khai báo, hãy ghi một thông tin giả nào đó, trừ trường hợp các website dành cho thương mại điện tử và bạn đã cân nhắc kỹ. Thậm chí, bạn cần sử dụng một hộp thư phụ để nhận các thông tin từ các trang web mà bạn không thật cảm thấy an toàn.

Công nghệ thông tin ở nước ta đang phát triển mạnh mẽ, một ngày nào đó không xa, các dịch vụ đăng ký trực tuyến sẽ phát triển, các thông tin cá nhân như số thẻ tài khoản, sổ bảo hiểm xã hội... sẽ trở thành đối tượng để kẻ trộm đầu tư thời gian khai thác và sử dụng với mục đích xấu. Hãy thận trọng với các trang web yêu cầu đăng ký sở thích cá nhân, bao nhiêu người trong gia đình, bạn bao nhiêu tuổi... vì rất có thể

https://tieulun.hopto.org

bạn sẽ nhận được vô vàn các thư điện tử không mong muốn từ những sơ suất rất nhỏ này.

c. Tránh truy cập tự động. Đăng xuất ra khỏi website

Một số trang web cho phép bạn đưa user name và mật khẩu và ghi nhớ lại để các lần truy cập sau không phải nhập lại. Thuận tiện này lại là cơ hội cho kẻ trộm ăn cắp mật khẩu để truy cập vào các trang web và sẽ gây ra những tổn thất. Việc tránh truy cập tự động vào các trang web có thể là bất tiện vì mất thời gian nhập các thông tin, nhớ account và mật khẩu nhưng sẽ tăng cường tính bảo mật cho các thông tin cá nhân của bạn.

Trước khi thoát khỏi một trang web có sử dụng account như diễn đàn trao đổi, thư điện tử, dịch vụ trực tuyến... hãy thoát khỏi trang web bằng cách đăng xuất khi chọn các nút Log Off, Log Out, Đăng xuất... tùy theo từng trang web và bạn cần tìm hiểu cụ thể khi sử dụng các web này. Với cách thức như trên, Internet sẽ đóng phiên làm việc và lần truy cập vào trang web lần tiếp theo sẽ phải nhập lại user name và mật khẩu cho dù đó là bạn hay một người khác. Một hộp thư điện tử được mở và không đăng xuất, một người khác có thể mở máy và truy cập vào trang web (như Yahoo! chẳng hạn) và đương nhiên các thông tin của bạn trong hộp thư được mở ra. Nếu ra khỏi trang web của một diễn đàn trao đổi mà

https://tieulun.hopto.org

không đăng xuất, người khác có thể sử dụng phím Back để quay lại diễn đàn với account của bạn. Điều gì sẽ xảy ra nếu họ đưa ra các thông tin bất lợi cho bạn. Và còn nhiều trang web như thương mại điện tử... sẽ gây cho bạn những thiệt hại khi không đăng xuất nếu ra khỏi trang web.

d. Không lưu tự động số thẻ tín dụng. Kiểm tra thẻ tín dụng thường xuyên

Một số trang web thương mại điện tử cho phép bạn lưu trữ số thẻ tín dụng của bạn trong cơ sở dữ liệu của chúng để thực hiện các lần giao dịch tiếp theo. Chức năng này giúp cho các thao tác sẽ nhanh và thuận tiện hơn nhưng cũng là kẽ hở cho những kẻ ăn trộm thực hiện được hành vi của mình. Hãy bảo vệ thông tin của bạn bằng cách luôn từ chối tính năng lưu số thẻ tín dụng tự động.

Cho dù bạn đã thực hiện rất nhiều biện pháp bảo mật, nhưng hãy thận trọng, kẻ trộm vẫn rình rập xung quanh và việc mất trộm vẫn có thể xảy ra. Hãy thường xuyên kiểm tra thẻ tín dụng để kịp thời phát hiện, tránh những hậu quả nghiêm trọng.

e. Bảo vệ các thông tin lưu trữ

Khi sử dụng một máy tính, nhất là máy tính có kết nối với Internet, ở văn phòng hay ở gia đình, bạn cũng sẽ có rất nhiều thông tin cần phải lưu trữ: các đĩa CD/DVD dữ liệu, sổ ghi account,

https://tieulun.hopto.org

mật khẩu của Windows và các trang web, thư điện tử, địa chỉ các trang web cần quan tâm... Điều gì sẽ xảy ra khi các thông tin này bị kẻ trộm khám phá, bị mất (do quên), các đĩa CD/DVD bị hỏng... Thật là khó xử khi một trang web cần quan tâm để lấy các thông tin cần thiết không truy cập được do không nhớ user name và mật khẩu thậm chí quên cả tên trang web, hộp thư không mở được, không nhớ được hộp thư của các đối tác... và vô vàn các vấn đề khác nữa có thể xảy ra nếu các thông tin cá nhân không được lưu trữ cẩn thận.

Hãy đặt các đĩa CD/DVD và sổ lưu trữ các thông tin cá nhân vào một vị trí an toàn và chúng phải được bảo vệ tránh những rủi ro như mất mát, thậm chí cả mưa gió và hỏa hoạn.

11. Một số điều cần lưu ý khi sử dụng Internet nơi công cộng

a. Giới thiệu chung

Trong nhiều trường hợp, bạn không thể về nhà để lấy những thông tin cần thiết và sử dụng máy tính công cộng như trong thư viện, quán cà phê Internet, điểm truy cập Internet... đều rất có thể xảy ra vì nhanh chóng, rẻ và tiện lợi. Nhưng sử dụng những máy tính này có thực sự an toàn hay không vì đây không phải máy tính riêng của bạn với các cách thức bảo mật đã được thiết lập!

https://tieulun.hopto.org

An toàn với máy tính công cộng phụ thuộc rất lớn vào cách sử dụng của người dùng. Xin các bạn lưu ý một số vấn đề mà chúng tôi sẽ giới thiệu ở các mục dưới đây.

b. Sử dụng phần mềm chống spyware

Hãy sử dụng các phần mềm chống gián điệp để quét máy tính công cộng trước khi sử dụng. Đây là thao tác cần thiết để các thông tin cá nhân của bạn không bị các phần mềm gián điệp đánh cắp và được sử dụng với mục đích xấu.

c. Không lưu lại những thông tin đăng nhập

Thay vì đóng cửa sổ trình duyệt hay gõ vào địa chỉ trang web khác, bạn hãy thoát khỏi (log out) trang web bằng nhấn vào nút hoặc liên kết log out trên trang web. Điều này hạn chế khả năng người sử dụng khác có thể truy cập vào các thông tin trong trang web mà bạn vừa ghé thăm. Rất nhiều chương trình, đặc biệt là các trình nhắn tin như Yahoo! Messenger, MSN,... có tính năng tự động đăng nhập (log in) để lưu lại tên người sử dụng và mật khẩu, giúp người sử dụng không phải gõ lại tên người dùng và mật khẩu. Tính năng này chỉ hữu ích khi sử dụng trên máy tính của riêng bạn, chúng sẽ rất nguy hiểm khi sử dụng ở những máy tính công cộng. Hãy vô hiệu hóa chức năng này mỗi khi sử dụng máy tính công cộng.

https://tieulun.hopto.org

d. Bảo vệ mật khẩu

Các trình duyệt cũng có khả năng ghi nhớ mật khẩu. Trước khi truy cập, nếu đang sử dụng Internet Explorer, vào bảng chọn Tools, chọn mục Internet Options, chọn khung Content, vào AutoComplete và bỏ chọn toàn bộ các mục đánh dấu trong hộp thoại AutoComplete Settings. Nhấn chuột vào các nút Clear Forms và Clear Passwords để xóa toàn bộ mật khẩu và các dữ liệu.

Những chương trình theo dõi thao tác bàn phím có thể ghi lại mật khẩu của bạn một cách đơn giản. Nhưng chúng không thể ghi lại được nếu bạn sử dụng các thao tác sao chép và dán từng chữ cái vào trong mật khẩu. Ví dụ: nếu mật khẩu là "km#6@" hãy sao chép từ một trang nào đó từng ký tự 'k', 'm', '#', '6', '@' và dán vào trường mật khẩu. Tuy có hơi phiền phức nhưng lại an toàn hơn.

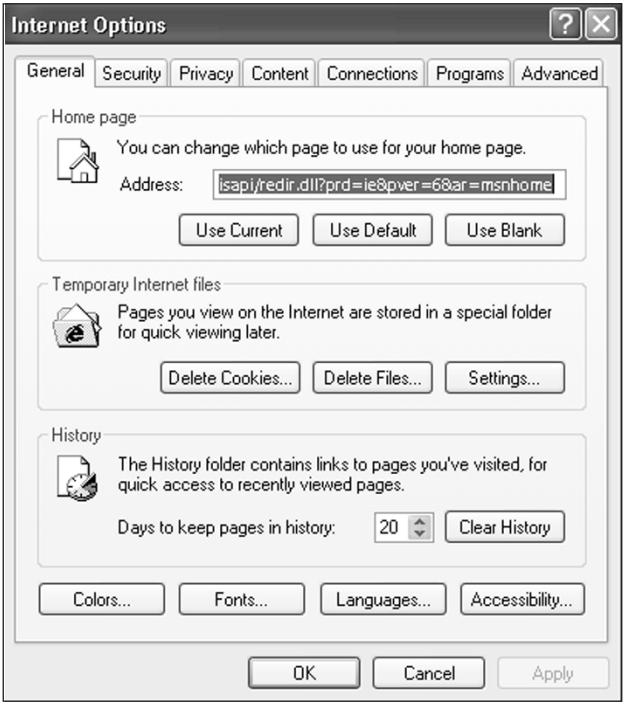
e. Xóa mọi dấu vết

Sau khi sử dụng máy tính công cộng, hãy xóa bỏ mọi tập tin đệm và danh sách History của Internet Explorer. Để xóa các tập tin tạm và History trong IE bạn hãy thực hiện như sau:

• Trong Internet Explorer, vào bảng chọn Tools, chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

• Chọn khung General. Hộp thoại Internet Options có dạng như hình sau:

https://tieulun.hopto.org



• Trong khung Temporary Internet files, nhấn chuột vào nút Delete Cookies..., và nút Delete Files....

• Trong khung History, nhấn nút Clear History.

• Nhấn nút OK.

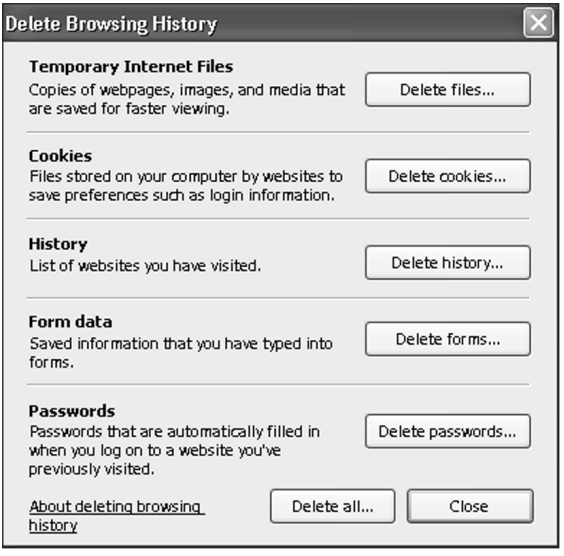
☞ *Xin các bạn lưu ý*: Trong Internet Explorer 7 để xóa các cookies và history, tiến hành như sau:

• Vào bảng chọn Tools, chọn Internet Options. Khi này hộp thoại Internet Options xuất hiện. Chọn khung General.

• Trong vùng Browsing history, chọn nút Delete....

Khi này hộp thoại Delete Browsing History xuất hiện như hình sau:

https://tieulun.hopto.org



Nhấn chuột vào các nút Delete files..., Delete cookies... và Delete history.... Bạn có thể xóa toàn bộ các vấn đề liên quan đến History khi nhấn nút Delete all....

f. Không hiển thị những thông tin nhạy cảm trên màn hình

Đừng để máy tính hiển thị những thông tin quan trọng, như: thông tin cá nhân, mã số tài khoản ngân hàng, mã số thẻ tín dụng... Khi có việc cần phải đi ra ngoài một chút, bạn hãy đóng toàn bộ các cửa sổ chương trình, thoát khỏi các cửa sổ có chứa những thông tin nhạy cảm.

g. Đừng quá tin tưởng vào khả năng mã hóa

Hiện nay, có rất nhiều phần mềm mã hóa trên thị trường. Chúng có thể được sử dụng để mã hóa các email. Tuy nhiên, các phần mềm này chỉ mã hóa các thư sau khi đã sẵn sàng để gửi

https://tieulun.hopto.org

thư. Điều này quả thực là khá muộn màng nếu như một phần mềm ghi chép mọi thao tác bàn phím đã được cài đặt vào trong máy (keylogger). Chúng sẽ ghi lại toàn bộ mật khẩu và nội dung thư được viết ra và gửi về dưới dạng email cho những kẻ cài đặt keylogger mà người sử dụng máy tính không hề hay biết. Những công cụ mà chúng sử dụng sẽ vô hiệu hóa, và lấy cắp được thông tin của bạn dễ dàng ngay khi bạn đã xóa mọi dữ liệu liên quan. Vì vậy, để thực sự an toàn, hãy tránh gõ vào số thẻ tín dụng bất cứ những thông tin tài chính hoặc các thông tin nhạy cảm vào trong máy tính công cộng.

h. Hãy chú ý xung quanh

Bởi vì có rất nhiều thông tin nói rằng những hacker có thể sử dụng những phương tiện kỹ thuật số nào đó để theo dõi người sử dụng nhằm ăn cắp mật khẩu, do đó chúng ta cũng không nên sao lãng những kiểu tấn công cổ điển này. Hãy quan sát kỹ xung quanh và chú ý tới những người ngồi bên cạnh mỗi khi nhập mật khẩu.

i. Phải thật thận trọng khi sao chép dữ liệu về máy tính của mình

Máy tính ở nơi công cộng thường được sử dụng với cường độ lớn hơn một máy tính ở gia đình trong khi đó ý thức bảo mật lại không cao. Khả năng bị nhiễm virus hoặc các hiểm họa khác là rất lớn. Trong trường hợp không thật cần thiết, không nên chép dữ liệu từ các máy này về máy tính của bạn.

https://tieulun.hopto.org

Chương IX

BẢO VỆ DỮ LIỆU KHI TRUY CẬP INTERNET

1. Kiểm tra hệ thống trước khi truy cập

Trong *Chương VIII*: *Bảo vệ thông tin cá nhân khi truy cập Internet*, chúng tôi đã giới thiệu các thiết lập cần thiết để bảo vệ thông tin cá nhân của bạn khi truy cập Internet. Tuy nhiên, trong quá trình sử dụng, các thiết lập này có thể đã bị thay đổi do bạn vô tình hay người khác cố ý. Trường hợp đặc biệt nguy hiểm cũng có thể xảy ra khi máy tính của bạn đã bị những kẻ xâm nhập đánh cắp được thông tin truy cập và đang ngồi từ xa để sử dụng máy của bạn. Nhìn chung, bạn nên kiểm tra lại các thông tin có tính chất nhạy cảm như: user name, mật khẩu truy cập Windows và các thiết lập bảo mật khác. Kiểm tra sự hoạt động của các bức tường lửa bao gồm bức tường lửa phần cứng và bức tường lửa phần mềm, đặc biệt là bức tường lửa của Widows đã được hỗ trợ với nhiều tính năng quan trọng. Bạn cũng nên thường xuyên cập nhật các bản sửa lỗi phiên bản mới của Windows, Office để tận dụng các hỗ trợ cho tính năng bảo mật của hệ thống.

https://tieulun.hopto.org

2. Kiểm tra việc dùng chung dữ liệu

Nếu máy tính của bạn dùng ở văn phòng không chung dữ liệu với các máy khác trên mạng và đặc biệt nếu ở gia đình chỉ sử dụng một máy tính thì tốt nhất là bạn nên vô hiệu hóa việc dùng chung dữ liệu (tệp và thư mục) và các thiết bị ngoại vi khác. Đây là một biện pháp cần thiết để tránh những kẻ xâm nhập trên Internet ăn trộm những thông tin trên máy tính của bạn.

3. Những vấn đề cần quan tâm khi xóa dữ liệu

a. Bản chất của việc xóa dữ liệu

Khi bạn xóa một tệp hay thư mục nào đó trên đĩa, thực chất lệnh này chỉ đánh dấu "đã xóa" trong Directory Entry và những thông tin liên quan trong File Allocation Table - FAT (với phân vùng định dạng FAT/FAT32) hoặc đánh dấu "xoá" trong Master File Table - MFT Entry (với phân vùng định dạng NTFS). Hay nói cách khác, lệnh này chỉ xóa tên của tệp hay thư mục này trên đĩa. Lúc này, các vùng (cluster) chứa dữ liệu của tập tin xem như trống và được tính là dung lượng chưa dùng đến của đĩa cứng mặc dù dữ liệu vẫn tồn tại. Khi dữ liệu mới được ghi vào, và nếu việc ghi dữ liệu mới trùng vào vị trí của dữ liệu cũ thì dữ liệu cũ thực sự bị xóa đi và ghi đè bằng dữ liệu mới. Bạn không thể "nhìn" thấy được những dữ

https://tieulun.hopto.org

liệu bị đánh dấu xóa nhưng những phần mềm cứu dữ liệu vẫn nhìn thấy chúng khi quét qua bề mặt đĩa. Vì vậy chúng ta mới cần đến những phần mềm này trong việc khôi phục dữ liệu. Các bạn có thể hình dung một cách tương đối (chỉ để dễ tưởng tượng mà thôi) như trong thư viện có một tủ gồm các thẻ để ghi tên sách (và các tham số khác). Mỗi một tên sách trong thẻ sẽ ghi địa chỉ để cuốn sách đó. Khi hủy một cuốn sách, người ta chỉ loại bỏ thẻ của cuốn sách đó trong tủ, còn cuốn sách vẫn nằm ở một vị trí nào đó. Khi kiểm tra dung lượng của kho, người ta tra từng thẻ trong tủ, tương ứng với bao nhiêu vị trí đặt và dung lượng (các bạn cứ tưởng tượng là cuốn sách có ghi thể tích chiếm chỗ). Như vậy, vị trí đặt cuốn sách bị hủy được coi là trống vì không có thẻ tương ứng với nó. Khi nhập cuốn sách mới vào kho, người ta cũng tra từng thẻ và chừa ra vị trí đặt các cuốn sách tương ứng với từng thẻ đó và tìm vị trí trống (như chúng tôi đã nói, vị trí cuốn sách bị hủy được coi là trống vì không có thẻ trong tủ) và để sách vào theo một nguyên tắc nào đó (từ ngoài vào trong chẳng hạn). Nếu việc đặt sách mới trùng với vị trí cuốn sách đã hủy thì khi này cuốn sách cũ mới bị hủy hoàn toàn còn nếu không, nó vẫn tồn tại trong kho.

b. Một số lưu ý khi cần khôi phục tệp bị xóa

Bạn có thể sử dụng bất cứ phần mềm nào phù hợp với khả năng tìm kiếm của mình để cứu

https://tieulun.hopto.org

dữ liệu, tuy nhiên chúng tôi xin lưu ý một vài điểm sau.

+ Một số phần mềm cho dùng thử và chỉ yêu cầu người dùng nhập số đăng ký (license key) khi sao lưu những dữ liệu cần khôi phục. Vì vậy, bạn hãy tận dụng tính năng này thử qua một vài phần mềm để tìm ra phần mềm thích hợp nhất với loại dữ liệu mình cần khôi phục.

+ Một số phần mềm cho phép tạo đĩa khởi động và làm việc trong chế độ MS-DOS. Tuy nhiên, bạn sẽ khó khăn hơn trong việc chọn lựa những dữ liệu cần khôi phục. Nếu có thể, hãy cài đặt phần mềm cứu dữ liệu trên một hệ thống khác và gắn ổ đĩa cần khôi phục vào khi đã sẵn sàng. Bạn sẽ dễ dàng làm việc hơn với những tập tin theo cấu trúc cây thư mục, xem qua nội dung những tập tin có thể khôi phục trước khi mua license key. Lưu ý: đừng lo lắng khi hệ điều hành không nhận ra đĩa cứng cần khôi phục, phần mềm khôi phục sẽ làm việc này tốt hơn nếu trong BIOS Setup vẫn nhận dạng được ổ cứng này.

+ Khi cần khôi phục lại dữ liệu bị xóa, tránh những thao tác ghi dữ liệu lên đĩa cứng cần khôi phục. Sau khi xóa, vị trí những cluster của tập tin không được bảo vệ, sẵn sàng cho việc ghi đè dữ liệu mới. Cả khi người dùng không tạo ra những tệp mới, hoạt động của hệ điều hành cũng ảnh hưởng đến dữ liệu đã xóa khi tạo ra những tập tin nhật ký (log) ghi lại hoạt động của hệ thống.

https://tieulun.hopto.org

Ngoài ra, việc truy cập Internet sẽ tải về khá nhiều tập tin tạm cũng được ghi trên đĩa cứng. Tốt nhất bạn nên ngừng ngay việc sử dụng ổ cứng này, chỉ gắn nó vào một hệ thống khác sau khi đã chuẩn bị sẵn sàng cho việc cứu dữ liệu.

+ Đừng chậm trễ khi cứu dữ liệu. Hãy hành động thật nhanh khi nhận thấy sai lầm của mình, bạn sẽ có nhiều cơ hội lấy lại được dữ liệu đã xóa mất. Ngoài ra, khả năng khôi phục phụ thuộc vào loại dữ liệu. Nếu là những tập tin hình, bạn có thể lấy lại được 9 trên 10 hình. Tuy nhiên, nếu là cơ sở dữ liệu (database), bảng biểu... dù lấy lại được 90% nhưng có thể chúng vẫn không sử dụng được vì cấu trúc dữ liệu bị phá vỡ, mà không mở được các tệp này - Một đĩa cứng hỏng nếu BIOS hay tiện ích quản lý đĩa cứng không thể nhận dạng được. Ổ cứng hỏng thường có những hiện tượng lạ như không nghe tiếng môtơ quay, phát ra những tiếng động lách cách khi hoạt động... Đây là những hỏng hóc vật lý của bo mạch điều khiển, đầu đọc, môtơ, đĩa từ... Hãy cố gắng tạo bản sao ảnh của đĩa cứng với Norton Ghost, Drive Image hoặc tính năng tương tự của một số phần mềm cứu dữ liệu. Khi đĩa cứng gặp sự cố, bạn có thể lấy lại dữ liệu từ bản sao ảnh của đĩa cứng.

+ Nếu dữ liệu thực sự rất quan trọng, bạn nên đem ổ cứng đến những dịch vụ cứu dữ liệu có uy tín để kiểm tra, đừng thao tác trên đĩa cứng vì sẽ ảnh hưởng đến khả năng khôi phục dữ liệu

https://tieulun.hopto.org

hoặc làm tình hình thêm nghiêm trọng. Và dĩ nhiên, cái giá phải trả cho việc này sẽ không rẻ chút nào. Tuy nhiên, bạn đừng trông chờ nhiều vào việc cứu dữ liệu khi ổ cứng hỏng vì việc này không phải lúc nào cũng thành công.

Dữ liệu đã bị xóa của bạn có thể được khôi phục bởi một phần mềm thích hợp. Đây là một tin tốt lành nếu bạn không may xóa nhầm một tệp nhưng lại là một điều tồi tệ nếu máy tính của bạn bị mất, mang đi sửa chữa ở những nơi không thật an toàn, mang đi tặng hoặc bán.

Hãy thận trọng, nếu máy tính của bạn không được xóa bỏ dữ liệu một cách an toàn bằng những biện pháp thích hợp.

c. Xóa dữ liệu một cách an toàn

Để xóa dữ liệu một cách an toàn mà người khác không khôi phục lại được, bạn phải sử dụng một chương trình xóa đặc biệt. Hầu như hãng nào viết chương trình khôi phục dữ liệu bị xóa (một cách bình thường) đều viết chương trình xóa dữ liệu.

Các bạn có thể tham khảo ở hai trang web:

• Active@ KillDisk (http://www.killdisk.com/), miễn phí

• DataEraser (http://www.ontrack.com/dataeraser/)

d. An toàn dữ liệu khi bán, tặng và vứt bỏ máy tính

Như chúng tôi đã giới thiệu ở phần trên, khi

https://tieulun.hopto.org

một số tệp bị xóa và đã loại bỏ chúng ra khỏi Recycle Bin thì vẫn có thể khôi phục lại được thông tin trong các tệp đó. Chính vì vậy, bạn hãy thận trọng khi đem đi bán, hoặc cho hay tặng máy tính, nhất là khi trong máy tính chứa nhiều thông tin cần phải bảo mật.

Cần sao chép dữ liệu có trong máy tính đem bán hay tặng sang một máy tính mới hoặc vào các thiết bị lưu trữ và xóa dữ liệu trong máy tính bằng các chương trình xóa chuyên dụng. Để thông tin được bảo mật cao hơn, bạn nên cài đặt lại Windows sau khi xóa xong dữ liệu để loại bỏ hoàn toàn các thông tin có thể còn lưu trên hệ thống.

Nếu muốn vứt bỏ máy tính hoặc ổ cứng, biện pháp an toàn nhất là phá hủy ổ cứng về mặt vật lý. Tuy nhiên, bạn cũng cần lưu ý rằng, một ổ đĩa cứng bị hỏng không đồng nghĩa với việc dữ liệu không thể khôi phục được. Bằng những phần mềm chuyên dụng người ta vẫn soi và lấy ra được từng phần dữ liệu trên ổ đĩa. Tốt nhất, trong trường hợp này là phá hủy ổ cứng ở mức độ cao nhất.

Đối với các đĩa mềm, CD/DVD chứa các thông tin quan trọng khi vứt bỏ cũng cần được xử lý ở mức độ cần thiết. Tốt nhất là tiêu hủy chúng thành các mảnh nhỏ.

4. Sao lưu dự phòng dữ liệu

a. Tại sao phải sao lưu dự phòng dữ liệu

Đĩa cứng cũng như bất kỳ một thiết bị nào

https://tieulun.hopto.org

khác được sản xuất và sử dụng có thời hạn nhất định, nghĩa là không phải là vô hạn. Ngoài ra còn một loạt các nguyên nhân khác như: sự cố về điện, những hỏng hóc do độ ẩm cao... và cũng rất có thể một bộ phận cơ hay điện của ổ cứng bị hỏng khi chưa đạt được thời gian như dự định kéo theo cả ổ cứng cùng với vô số dữ liệu bên trong không lấy ra được để phục vụ công việc cần thiết. Cũng không loại trừ các mối hiểm họa khác như mưa bão, lũ lụt, biến động của thời tiết có thể khiến dữ liệu của bạn bỗng chốc không còn sử dụng được. Cũng cần phải nói thêm rằng, không chỉ những sự cố về phần cứng mà một hiểm họa rất lớn đang tiềm ẩn: đó là virus máy tính. Không thể loại trừ khả năng bỗng nhiên máy tính không làm việc, ổ cứng bị mất hết dữ liệu hoặc dữ liệu không mở ra được.

Ngoài ra, sự truy cập vào máy tính của người khác với sự vô tình hay cố ý cũng có thể làm mất, hỏng dữ liệu trên máy tính. Cũng có thể dữ liệu bị mất mà kẻ lấy cắp đã sử dụng các thông tin lấy được với mục đích xấu như sử dụng các user name, mật khẩu để thực hiện các hành động phạm pháp trong khi bạn không có các thông tin cần thiết để vô hiệu hóa hành động của kẻ cắp kịp thời. Thật là tai hại khi kẻ trộm xuyên tạc những dữ liệu lấy được và đưa ra với danh nghĩa của bạn, trong khi bạn không có bản gốc để bảo vệ mình.

https://tieulun.hopto.org

Cũng không loại trừ khả năng do một chút sơ suất, bạn đã xóa nhầm đi những thông tin quan trọng và cần phải có bản dự phòng để lấy lại các dữ liệu đó.

Tóm lại, việc sao lưu dữ liệu là một vấn đề rất cần thiết cho người sử dụng máy tính không phải chỉ ở cơ quan mà đối với tất cả những ai sử dụng máy tính, kể cả máy tính đơn lẻ tại gia đình.

Việc sau lưu dữ liệu phụ thuộc vào mức độ sử dụng của mỗi người và tầm quan trọng của dữ liệu đó mà không nhất thiết theo một công thức nào. Với các dữ liệu quan trọng, bạn nên sao lưu thường xuyên khi có cập nhật mới sang các thiết bị lưu dự phòng mà chúng tôi sẽ giới thiệu ở mục sau. Thậm chí, với các tài liệu đặc biệt quan trọng, có thể bạn nên sao lưu sang ba, bốn vị trí khác để đề phòng những sự cố xảy ra. Tuy nhiên, cũng cần phải khẳng định rằng, đừng để việc sao lưu dữ liệu chiếm một khoảng thời gian quá lớn làm ảnh hưởng đến công việc hằng ngày. Bạn nên xây dựng cho mình một kế hoạch sao lưu dự phòng các dữ liệu một cách hợp lý, đáp ứng mục đích sử dụng của bạn.

b. Các thiết bị sử dụng khi sao lưu dự phòng

Không có một thiết bị sao lưu dữ liệu nào là tuyệt đối hoàn hảo xét cả về góc độ an toàn dữ liệu và kinh tế. Việc sử dụng thiết bị còn theo thói quen và sở thích của người sử dụng.

https://tieulun.hopto.org

Ổ cứng ngoài

Đây là một ổ cứng máy tính bình thường được đặt trong một hộp cứng nhằm mục đích tránh các tác động nhẹ như va chạm... Ổ cứng ngoài được nối với máy tính qua cổng USB.

Ưu điểm của thiết bị này là lưu trữ được một dung lượng lớn, dễ di chuyển và có thể sử dụng được với nhiều máy tính. Nhưng loại này có nhược điểm là kích thước lớn, dễ bị người khác truy nhập và giá thành cao.

Ổ cứng bên trong

Loại ổ cứng này được lắp trực tiếp vào máy tính nên thường có giá thành rẻ hơn ổ cứng ngoài cùng tham số và cũng lưu trữ được dung lượng lớn dữ liệu. Tuy nhiên nó cũng dễ bị truy cập trái phép và trong trường hợp rủi ro như tăng điện đột ngột (và không có bộ điều chỉnh điện áp), mưa bão hoặc bị mất mát máy tính, bị phá hoại... thì cũng bị mất luôn cùng với dữ liệu chính.

Các loại đĩa CD/DVD

Để sử dụng ghi dữ liệu lên các loại đĩa này cần có đầu ghi vì loại CD-ROM thông thường chỉ có thể đọc được dữ liệu. Các đĩa thuộc nhóm này có nhiều loại. Theo số lần ghi thì chia thành: loại ghi một lần (CD-R) và loại ghi nhiều lần (CD-RW). Theo dung lượng ghi thì chia theo: Đĩa CD ghi được 650MB đến 700MB dữ liệu; Đĩa DVD có thể lưu trữ được tới 4,7GB dữ liệu và lại được chia thành nhiều loại.

https://tieulun.hopto.org

Ổ USB

Đây là các thiết bị hiện nay đang được sử dụng rộng rãi do kích thước nhỏ, thời gian ghi, xóa nhanh và giá thành cũng hợp lý. Các loại ổ này được cắm qua cổng USB và đối với các máy sử dụng hệ điều hành thông dụng hiện nay là Windows XP đều có thể tự nhận được nên không cần phải cài driver khi sử dụng. Dung lượng của các ổ loại này là 128MB; 256MB; 512MB; 1GB; 2GB... và ngày càng được nâng cao thêm về dung lượng. Nhìn chung, với ổ loại này chỉ nên sao lưu tạm thời hoặc chuyển dữ liệu đến một vị trí khác mà không nên lưu các dữ liệu có tính ổn định như một năm sau mới sử dụng. Cũng do dễ sử dụng nên tính bảo mật của loại này không cao.

Các ổ băng từ

Thiết bị loại này thường chỉ được sử dụng trong các lĩnh vực đòi hỏi phải lưu được dữ liệu với dung lượng lớn tới hàng trăm GB.

Sử dụng song song hai ổ cứng

Đây là một biện pháp đưa dữ liệu vào hai ổ cứng có trong một máy tính. RAID (viết tắt của Redundant Array of Independent Disks) là tạo trong máy hai ổ đĩa giống hệt nhau cả từ hệ điều hành đến các chương trình, các tệp và được cài đặt theo cách như nhau. Đây là cách thức hiệu quả nhưng phức tạp đòi hỏi bạn phải là người có am hiểu về kỹ thuật. Ngoài ra còn đòi hỏi bo mạch chủ của máy tính phải tương thích với RAID.

https://tieulun.hopto.org

Nếu chưa có được một trong các thiết bị lưu dự phòng ở trên, bạn cũng nên lưu những dữ liệu quan trọng sang một thư mục khác trên đĩa cứng của máy tính để sử dụng trong trường hợp cần thiết. Việc làm này đơn giản, không phải đầu tư thêm thiết bị nhưng sẽ rất hiệu quả khi dữ liệu bị mất do xóa nhầm, bị người khác cố tình làm hỏng hoặc sửa đổi nhưng không biết có bản lưu dự phòng trên cùng đĩa, bị người khác vô tình hay cố ý sửa đổi và bạn muốn lấy lại bản gốc...

c. Bảo vệ dữ liệu lưu dự phòng

Dữ liệu khi đã được lưu dự phòng thì cần phải được bảo vệ tránh để mất mát hoặc rơi vào tay của những kẻ chuyên rình mò thông tin của bạn. Vì như vậy, vô hình trung, bạn đã tiếp tay cho hành động của họ. Vì là dữ liệu dự phòng, bạn cũng cần tính đến những khả năng như mất cắp, chập điện hay mưa bão ảnh hưởng đến vị trí đặt thiết bị có dữ liệu chính (máy tính đang làm việc)... thì dữ liệu lưu dự phòng vẫn không bị tác động đến.

https://tieulun.hopto.org

https://tieulun.hopto.org

Phần IV

Sử dụng Internet an toàn cho trẻ em

https://tieulun.hopto.org

https://tieulun.hopto.org

Chương X

NHỮNG NGUY CƠ TIỀM ẨN KHI TRẺ EM TRUY CẬP INTERNET

1. Những cơ hội và nguy cơ tiềm ẩn của Internet đối với trẻ em

a. Những cơ hội của trẻ em trước sự bùng nổ của Internet

Ngày nay, thế hệ trẻ đang lớn lên cùng với sự phát triển của máy tính và mạng thông tin toàn cầu Internet. Điều này giúp trẻ em sớm được học tập, vui chơi, giải trí trong một điều kiện môi trường hoàn toàn mới mẻ. Chúng có thể ngồi ở nhà tham gia các diễn đàn để thu được nhiều điều bổ ích. Trẻ em không phải xin phép bố mẹ đến nhà bạn bè để cùng làm bài tập nhưng vẫn có thể trao đổi được những ý tưởng hay để giải một bài toán khó qua việc chat trên mạng. Chúng thu nhận được các kiến thức sâu rộng qua các buổi học qua mạng Internet, tìm hiểu được tình hình chính trị, xã hội mà không phải mua báo. Với việc truy cập vào Internet, trẻ em có thể học ngoại ngữ với những phương pháp trắc nghiệm tiên tiến và hiện đại...

Ngay từ lớp một, nhiều em đã được bố mẹ trang bị máy tính ở nhà để nối vào mạng học

https://tieulun.hopto.org

tập, trao đổi thư từ và chơi trò chơi điện tử. Trên lớp, các học sinh được các thầy cô giảng một số môn bằng giáo trình điện tử. Vì vậy, kiến thức về máy tính, về mạng Internet... được các em quan tâm và ứng dụng thành thạo. Nhờ đó, kiến thức về xã hội, các môn học phổ thông, trong đó có môn ngoại ngữ, đặc biệt là tiếng Anh của các em được nâng cao.

Rất nhiều em đã có trang web và đó là một thế giới riêng để các em sáng tạo, thiết kế đồ họa cho giao diện và trình bày những chính kiến và kinh nghiệm học tập của mình. Các em đã trở nên năng động, thông minh và tự tin hơn.

Thông qua Internet, nhiều trẻ em đã nhận thức được những vấn đề xã hội mang tầm quốc tế, làm quen với những kỹ thuật công nghệ hiện đại mà chính cha mẹ chúng có thể chưa biết.

Không thể phủ nhận đươợc là công nghệ thông tin cùng mạng tin học toàn cầu đã và đang mở ra những điều mới mẻ về thế giới khoa học, kiến thức cần thiết cho cuộc sống. Mạng thông tin toàn cầu đã và đang mang lại cho trẻ em nhiều cơ hội mới.

Theo nhiều chuyên gia tin học nhận định: "Trẻ em là thế hệ tiếp thu công nghệ thông tin dễ dàng hơn người lớn. Chúng lớn lên cùng với sự phát triển của công nghệ chứ không phải học lại từ đầu như người lớn".

https://tieulun.hopto.org

Tuy nhiên, giới trẻ và các bậc phụ huynh cùng đứng trước một mối lo ngại lớn: Những hiểm họa tiềm ẩn khi trẻ em sử dụng mạng Internet.

b. Những hiểm họa tiềm ẩn khi trẻ em sử dụng mạng Internet

Thật đáng lo ngại khi vào mạng Internet ngày nay, nguy cơ tiếp xúc với các trang web bạo lực, khiêu dâm đồi trụy là rất lớn. Theo một thống kê gần đây cho thấy: trên mạng Internet chỉ có khoảng hơn 3 triệu trang web về chính trị nhưng có tới gần 20 triệu trang web có liên quan đến sex, hơn 3 triệu trang liên quan đến rượu... Ngoài ra còn có hàng trăm, nghìn trang web liên quan đến các trò chơi bạo lực, chém giết, bắn súng, bom và khủng bố cùng nhiều trang web về truyện tiếu lâm thô tục, bàn luận những chuyện bậy bạ rất dễ kích thích tính tò mò của trẻ em. Hàng trăm, hàng triệu trang web cung cấp phim ảnh bất hợp pháp với nội dung không lành mạnh. Nguy cơ trẻ em đi lạc vào các trang web đó là rất lớn và thường xuyên.

Ngày càng nhiều bậc cha mẹ phàn nàn vì các cô cậu học trò dành quá nhiều thời gian cho việc chơi trò chơi điện tử trực tuyến. Tuy chưa có minh chứng cụ thể nào về mối liên hệ giữa các trò chơi bạo lực trên Internet với tỉ lệ bạo lực trong giới thanh thiếu niên đang ngày càng gia tăng, nhưng nếu để trẻ em tiếp xúc nhiều với

https://tieulun.hopto.org

bạo lực sẽ bị mất dần cảm xúc trước bạo lực. Rất nhiều trẻ em có những hành vi hung bạo đối với bạn bè, người thân trong gia đình mà bản thân chúng lại vẫn nghĩ là đang trong trò chơi trên mạng. Những gia đình nối mạng Internet nếu không có sự quản lý chặt chẽ cùng với việc áp dụng các công nghệ cần thiết để định hướng cho trẻ em sử dụng Internet một cách hiệu quả và an toàn sẽ có thể gây ra những hậu quả đáng tiếc.

Nhiều bậc cha mẹ đang thật sự lo ngại về công nghệ thông tin ảo trên mạng. Công nghệ này làm cho con người ngày càng xa rời với thực tế, đối với trẻ em thì loại hình công nghệ này còn nguy hiểm hơn nhiều. Hành vi và tính cách của trẻ em cũng thay đổi khi lọt vào một thế giới ảo, không tình cảm. Khi lang thang trên mạng, trẻ em còn có thể gặp phải các vấn đề liên quan đến sự mất an toàn của bản thân và gia đình. Bằng hệ thống thư điện tử, không ít trẻ em bị dụ dỗ cung cấp các thông tin về bản thân, cha mẹ, bè bạn.

Trên mạng hoặc qua thư điện tử, nhiều lá thư quấy rối tình dục, kích động sẽ trở nên nguy hiểm khi rơi vào tay trẻ em. Ngoài ra không loại trừ khả năng kết bạn qua Internet, những cuộc hẹn hò, dụ dỗ tham gia vào các băng đảng xấu, tổ chức hành vi tống tiền, bắt cóc.

Công nghệ thông tin tác động mạnh mẽ đến đời sống của trẻ em, thậm chí thay đổi cả cuộc sống của các em. Nhiều em khi sử dụng máy tính nhiều,

https://tieulun.hopto.org

học và chơi với máy tính, trò chuyện nhiều với máy tính nên đã ngại tiếp xúc, chạy nhảy với bè bạn, ngại tiếp xúc với xã hội.

Nhiều giáo viên phàn nàn rằng có những học sinh ở bậc tiểu học không chịu tập viết vì "đã có máy tính viết hộ". Nhiều học sinh phổ thông cơ sở, phổ thông trung học, thậm chí cả học sinh tiểu học, đã nộp bài tập ở nhà cho thầy cô bằng văn bản được in từ máy tính. Nhiều học sinh còn tải phim, truyện trên mạng rồi sao chép sang đĩa để tặng bè bạn ở trường.

Hiện có quá nhiều điểm cung cấp dịch vụ Internet công cộng. Những lời mời chào hấp dẫn như kết bạn qua mạng, trò chuyện qua mạng, truy cập Internet giá rẻ với giá cước cực kỳ hấp dẫn, cấu hình máy tính mạnh, game online với những trò chơi quyến rũ... đã và đang thu hút giới trẻ. Nhiều thanh thiếu niên đã tìm mọi cách để có tiền đến với các dịch vụ Internet công cộng. Quả thực, Internet có mặt tốt và cũng có mặt xấu.

2. Trách nhiệm của người lớn

Trong bối cảnh phát triển mạnh mẽ Internet, các bậc làm cha mẹ hãy cảnh giác khi cho con em mình tiếp xúc với mặt xấu của Internet. Vì vậy, người lớn, bao gồm: gia đình (bố, mẹ, ông bà..), nhà trường (thầy, cô) và xã hội (các đoàn thể)

https://tieulun.hopto.org

cần phải quan tâm hơn, giáo dục, quản lý chặt chẽ hơn, cần quan tâm đến các trang web có lợi cho sự phát triển của trẻ em, tạo cho các em có một môi trường tốt trên Internet phục vụ cho việc học tập, tìm hiểu văn hóa, xã hội có hiệu quả.

Việc tìm hiểu và ngăn chặn các hiểm họa từ Internet bằng các biện pháp kỹ thuật và công nghệ mà chúng tôi đã giới thiệu ở một số chương trong cuốn sách này là rất cần thiết. Tuy nhiên, như chúng tôi đã giới thiệu ở trên, các em rất am hiểu về máy tính và mạng Internet. Vì vậy nếu không có định hướng tốt, thì chính các em sẽ loại bỏ các biện pháp phòng ngừa bằng công nghệ để được tự do tiếp xúc với tất cả những gì Internet mang lại, bao gồm cả mặt tốt và mặt xấu của nó. Vấn đề là giúp các em phân biệt được những mặt tích cực của Internet để biến nó thành công cụ hữu ích cho sự phát triển của bản thân, thấy được những nguy cơ tiềm ẩn của Internet, tìm cách khắc phục hoặc lảng tránh nó và biết cách tự bảo vệ mình.

https://tieulun.hopto.org

Chương XI

SỬ DỤNG INTERNET AN TOÀN CHO TRẺ EM

1. Cài đặt hệ thống

a. Tạo các account riêng biệt

Nên tạo một account riêng cho con cái của bạn và account này không cho phép được sửa các tham số hệ thống, cài đặt phần cứng hay phần mềm mới. Các bước tiến hành như sau:

• Nhấn chuột vào nút Start của Windows.

• Vào mục chọn Settings, chọn Control Panel. Khi này hộp thoại Control Panel xuất hiện.

• Nhấn chuột vào biểu tượng 

. Hộp thoại User Account xuất hiện.

• Chọn mục • Create a new account .

• Nhập tên account trong ô Type a name for the new account. Ví dụ: VanTrinh.

• Nhấn chuột vào nút Next >.

• Nhấn nút Limited như hình sau:

• Nhấn nút Create Account.

https://tieulun.hopto.org

b. Kiểm tra các trang web được cập nhật hằng ngày

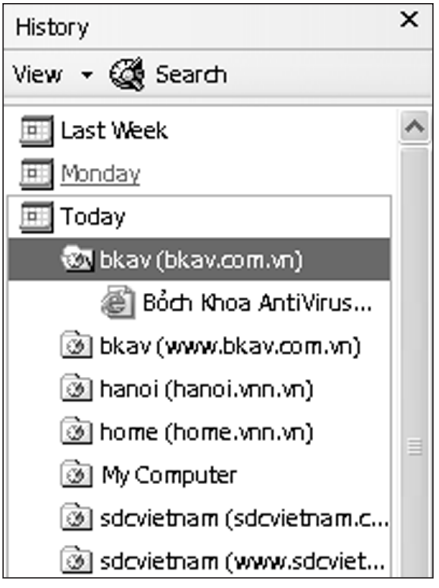
Kiểm tra những trang web nào con cái bạn hay truy cập bằng cách xem lại Internet History như sau:

(1) Đối với Internet Explorer

• Khởi động Internet Explorer.

• Nhấn chuột vào biểu tượng 

. Khi này một danh sách các trang web được truy cập trong tuần xuất hiện ở cửa sổ bên trái.

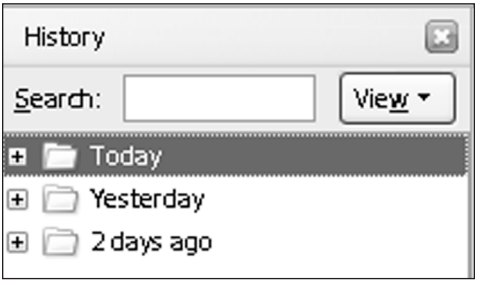


(2) Đối với Firefox

• Khởi động Firefox.

• Vào bảng chọn History. Khi này ở bên trái màn hình xuất hiện cửa sổ History như hình sau:

https://tieulun.hopto.org



• Chọn thời gian cần xem, ví dụ Today, danh sách các trang web truy cập trong ngày sẽ xuất hiện. Có thể nhấn chuột vào từng trang để kiểm tra nội dung.

• Nhập một đoạn văn bản để lọc các trang web theo một chỉ tiêu nào đó trong khung Search.

2. Cài đặt hạn chế

a. Cài đặt hạn chế các website và nội dung

Để ngăn chặn trẻ em truy cập các trang web có nội dung không phù hợp, có thể cài đặt các phần mềm chọn lọc nội dung hoặc sử dụng chức năng Content Advisor của Internet Explorer.

Các bước tiến hành như sau:

• Khởi động Internet Explorer.

• Vào bảng chọn Tools, chọn mục Internet Options. Khi này hộp thoại Internet Options xuất hiện.

• Chọn khung Content.

• Nhấn chuột vào nút Enable... . Hộp thoại Internet Options trở thành như hình sau:

https://tieulun.hopto.org

• Trong khung Select a category to view the rating levels có bốn hạng mục: Language, Nudity, Sex và Violence. Bạn có thể hạn chế Internet Explorer không truy cập nội dung trong các hạng mục này bằng cách sử dụng các thanh trượt. Giả sử chọn Sex, và kéo thanh trượt sang trái, bạn sẽ tăng cường bảo vệ ngăn truy cập vào các trang web có nội dung là Sex.

☞ *Xin các bạn lưu ý*: Khi mức độ gia tăng, nghĩa là thanh trượt được kéo sang bên phải thì mức độ bảo vệ giảm xuống. Trong Internet Explorer 7, nhấn nút Settings.

b. Thiết lập danh mục các trang web không được truy cập

Trong hộp thoại Content Advisor, nhấn chuột vào khung Approved Sites. Bạn có thể khai báo danh sách các trang web mà con cái bạn *không được*

https://tieulun.hopto.org

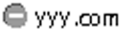
truy cập bằng cách nhập tên trang web trong khung Allow this Website và nhấn nút Never và các trang web *được truy cập* bằng cách nhấn nút Always. Nếu muốn xóa một trang web khỏi danh sách các trang web bị cấm truy cập, chọn trang web này và nhấn nút Remove. Kết quả, bạn được một danh sách các trang web được phép truy cập và không được truy cập như hình sau:

Bạn có thể khai báo một loạt các trang web bị cấm truy cập. Trong trường hợp này, không xét tới mức độ truy cập và nhấn nút Apply khi đã khai báo xong danh sách các trang web bị cấm truy cập.

Khi này trang web bị ngăn không được phép truy cập xuất hiện trong khung List of approved

https://tieulun.hopto.org

and disappoved Website và có dạng một biển cấm như sau:



Các trang web được phép truy cập được đánh dấu có dạng như sau: .

c. Cài đặt mật khẩu để truy cập hạn chế

☞ *Xin các bạn lưu ý*: Các thao tác dưới đây chỉ áp dụng khi bạn lần đầu tiên tạo mật khẩu trong trình duyệt. Việc xóa hoàn toàn hoặc sửa lại mật khẩu chúng tôi sẽ giới thiệu ở mục sau.

Để cài đặt mật khẩu cho các trang web các bạn tiến hành như sau:

• Khởi động Internet Explorer.

• Vào bảng chọn Tools, chọn Internet Options. Khi này hộp thoại Internet Options xuất hiện. Chọn khung Content. Nhấn nút Enable... .

☞ (*Xin các bạn lưu ý*: Trong Internet Explorer 7 nhấn nút Settings trong vùng Content Advisor).

• Hộp thoại Content Advisor xuất hiện. Chọn khung General. Khi này hộp thoại Content Advisor có dạng như hình sau:

https://tieulun.hopto.org

☞ *Xin các bạn chú ý*: Hai nút trong khung User options có ý nghĩa khác nhau. Bạn hãy chọn nút ☑ Supervisor can type a password to allow users to view restricted content. Đây là chức năng ngầm định.

• Nhấn chuột vào nút Create Password... . Khi này hộp thoại Create Supervisor Password xuất hiện. Nhập mật khẩu vào khung Password và nhập lại mật khẩu này vào khung Confirm password. Nhập một lời gợi ý vào khung Hint như hình sau:

• Nhấn nút OK . Khi này con trỏ trở lại hộp thoại Content Advisor.

• Nhấn nút Settings... .

Như vậy, bạn đã tạo được mật khẩu để truy cập vào các trang web. Với cách thiết lập như trên thì các khả năng sau sẽ xảy ra:

(1) Các trang web được phép truy cập, ví dụ như trang ✓ home.vnn.vn trong hộp thoại trên, được truy cập bình thường.

https://tieulun.hopto.org

(2) Khi truy cập vào các trang bị cấm truy cập hoặc không có trong danh mục được truy cập sẽ xuất hiện một hộp thoại như hình sau:

Bạn phải nhập mật khẩu đã thiết lập mới truy cập vào được trang web.

d. Sửa đổi mật khẩu để truy cập hạn chế

Mật khẩu để truy cập vào một số trang web bị hạn chế có thể được sửa đổi bằng các bước như sau:

• Khởi động Internet Explorer.

• Vào bảng chọn Tools, chọn Internet Options. Khi này hộp thoại Internet Options xuất hiện.

• Chọn khung Content.

• Chọn nút Settings... . Khi này một hộp thoại xuất hiện và bạn phải trả lời mật khẩu đã thiết lập như hình sau:

https://tieulun.hopto.org

• Nhấn nút OK. Khi này con trỏ trở về hộp thoại Content Advisor. Chọn khung General và nhấn nút Change Password... Hộp thoại Change Supervisor Password xuất hiện. Nhập mật khẩu cũ vào khung Old password. Nhập mật khẩu mới vào khung New password và khung Confirm new password. Nhập một lời nhắc nhở về mật khẩu ở khung Enter a hint for your new password như hình sau:

• Nhấn nút OK.

https://tieulun.hopto.org

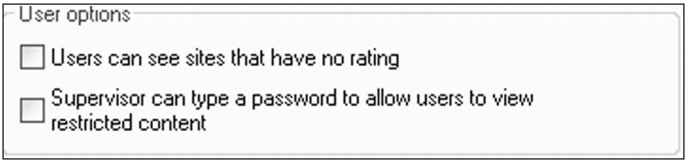
☞ *Xin các bạn lưu ý*: Sau khi cài đặt các tham số và mật khẩu, các bạn nên ra khỏi Internet Explorer và khởi động lại. Khi đã cài đặt chế độ Content Addvisor và trong hộp thoại Internet Options khi chọn khung Content và trong vùng Content Advisor xuất hiện nút Disable... thì chế độ này đang ở chế độ mở (On), ngược lại, nếu xuất hiện nút Enable... thì đang ngắt chế độ. Để chuyển đổi giữa mở và ngắt Content Advisor, bạn cần phải trả lời đúng mật khẩu.

e. Thiết lập chế độ ngăn truy cập tuyệt đối

Để ngăn truy cập tuyệt đối vào các trang web cấm truy cập, ví dụ như trang yyy.com trong hộp thoại Content Advisor nói trên, và các trang web không nằm trong danh mục được truy cập, kể cả có mật khẩu tiến hành như sau:

• Khởi động Internet Explorer, chọn mục Options. Khi này hộp thoại Internet Options xuất hiện. Chọn khung Content. Chọn nút Settings... . Trả lời đúng mật khẩu để vào hộp thoại Content Advisor.

• Chọn khung General. Trong khung User Options bỏ nút đánh dấu trong mục thứ hai như hình sau:



https://tieulun.hopto.org

Khi truy cập vào một trang web không được khai báo được phép truy cập, ví dụ như trang www.sdcvietnam.com, bạn không thể vào được và trình duyệt thông báo.

☞ *Xin các bạn chú ý*: Nếu trong vùng User options ở trên chọn nút 

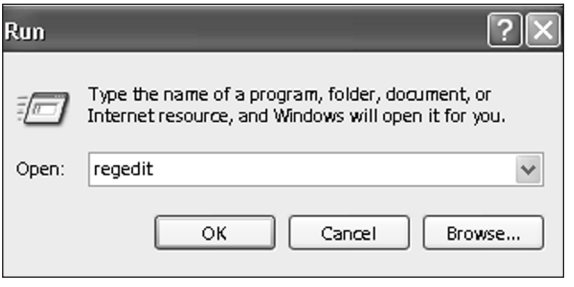
thì tất cả mọi trang web đều được truy cập bình thường.

f. Xóa mật khẩu của Content Advisor

Để tăng tính bảo mật cao, người sử dụng không thể xóa được mật khẩu trong hộp thoại Content Advisor mà phải xóa trong cấu hình của Windows bằng cách như sau:

• Nhấn chuột vào nút Start của Windows, chọn mục Run.

• Nhập regedit như hình sau:



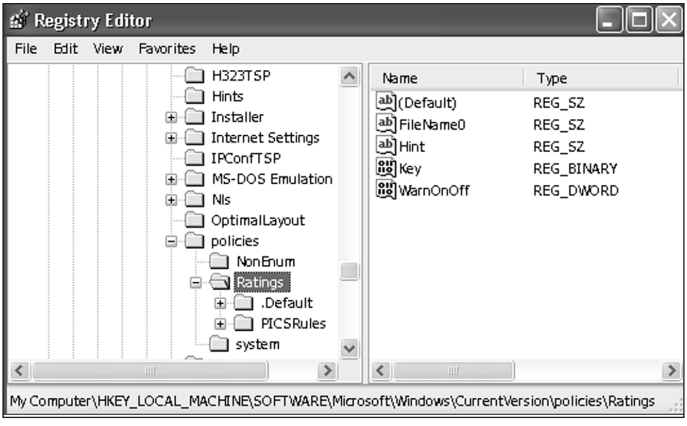
https://tieulun.hopto.org

• Nhấn nút OK. Khi này hộp thoại Registry Editor xuất hiện.

• Chọn mục HKEY_LOCAL_MACHINE. Trong mục này, tìm và chọn SOFTWARE. Trong các mục nằm phía dưới thuộc mục này, chọn Microsoft, chọn tiếp các mục con thuộc các mục lớn theo thứ tự sau:

Windows\CurrentVersion\Policies\Ratings

Kết quả được hộp thoại như hình sau: (các bạn chú ý đường dẫn phía dưới hộp thoại).



• Nhấn chuột phải vào mục Key REG_BINARY bên phải của hộp thoại, một bảng chọn xuất hiện, chọn mục Delete. Khi này hộp thoại Confirm Delete Value xuất hiện.

• Chọn nút Yes.

https://tieulun.hopto.org

PHỤ LỤC

Các trang web cần quan tâm để sử dụng Internet an toàn và hiệu quả

1. Các trang web tìm kiếm

www.google.com.vn

www.yahoo.com

2. Cập nhật bản sửa lỗi của Windows và Microsoft Office

www.microsoft.com

3. Các trang web có phần mềm chống virus nước ngoài

• Phần mềm miễn phí Active Virus Shield

http://www.activevirusshield.com/antivirus/freeav/index.adp

• Phần mềm Microsoft Windows AntiSpyware

www.microsoft.com/downloads

• Quét virus trực tuyến miễn phí

▪ Avast:

http://onlinescan.avast.com/

▪ Kaspersky:

http://www.kaspersky.com/virusscanner

https://tieulun.hopto.org

▪ Symantec:

http://security.symantec.com/default.asp?productid=symhome&langid=ie&venid=sym

▪ TrendMicro:

http://housecall.trendmicro.com/

▪ Quét spyware trực tuyến

http://www.trendmicro.com/spyware-scan

• ClamWin

http://www.clamwin.com/

• Các trang web cung cấp phần mềm chống virus miễn phí

http://www.pandasoftware.com/activescan/com/activescan_principal.htm

http://www.kaspersky.com/scanforvirus

http://www.ravantivirus.com/scan/

4. Các trang web tải các phần mềm chống virus trong nước

Bkav: www.bkav.com.vn

D32: www.echip.com.vn/echiproot/html/d32.html

5. Các trang web của Việt Nam về công nghệ thông tin

• Tạp chí PCWORLD

http://www.pcwolrd.com.vn/

• VnExpress

http://vnexpress.net/Vietnam/Vi-tinh/

• VDC

http://www.vnmedia.vn/ShowCat.asp?CatId=30

• Công ty FPT

http://www.fpt.vn/

https://tieulun.hopto.org

• Vietnamnet

http://vietnamnet.vn/vi-tinh/

6. Danh sách các trang web của một số trường đại học có chuyên mục và diễn đàn trao đổi về công nghệ thông tin, trong đó có bảo mật cho máy tính

• Trường Đại học quốc gia Hà Nội

http://www.vnu.edu.vn

• Trường Đại học dân lập Hải Phòng

http://www.hpu.edu.vn

• Đại học mở Hà Nội

http://www.fithou.edu.vn/

• Trường Đại học Phương Đông.

http://www.phuongdong.edu.vn

• Đại học Sư phạm Hải Phòng

http://www.dhhp.edu.vn

• Đại học Sư phạm Thái Nguyên

http://www.dhsptn.edu.vn

• Đại học Thăng Long

http://www.dhthanglong.com

• Học viện Công nghệ bưu chính viễn thông

http://www.e-ptit.edu.vn

• Học viện Mạng Cisco Bách khoa

http://www.ciscobachkhoa.com

• Học viện Ngân hàng

http://www.hvnh.edu.vn

• Khoa Công nghệ thông tin - Trường Đại học Sư phạm Hà Nội

http://cntt.dhsphn.edu.vn

https://tieulun.hopto.org

• Trường Đại học Nông nghiệp I Hà Nội
http://www.hau1.edu.vn
• Đại học Cần Thơ
http://www.ctu.edu.vn
• Đại học Công nghiệp thành phố Hồ Chí Minh
http://www.hui.edu.vn
• Đại học Quốc gia thành phố Hồ Chí Minh
http://www.vnuhcm.edu.vn
• Trường Đại học Khoa học tự nhiên thành phố Hồ Chí Minh
http://www.hcmuns.edu.vn

7. Các trang web tải trình duyệt Internet

• Internet Explorer
http://www.microsoft.com/Windows/ie/ie7/default.mspx
• Trình duyệt Opera
http://www.opera.com
• Firefox
http://ww.molliza.org/product/firefox
• Netscape
http://browser.netscape.com/ns8/download/default.jsp

https://tieulun.hopto.org

MỤC LỤC

https://tieulun.hopto.org

https://tieulun.hopto.org

https://tieulun.hopto.org

https://tieulun.hopto.org

https://tieulun.hopto.org

https://tieulun.hopto.org

Chịu trách nhiệm xuất bản
TS. NGUYỄN DUY HÙNG
Chịu trách nhiệm nội dung
ThS. NGUYỄN VĂN TRỌNG
ThS. LÊ TỬ GIANG

Biên tập nội dung: LÊ MINH HOÀI
TRẦN LAN KHANH
Trình bày bìa: DƯƠNG THÁI SƠN
Chế bản: LÊ MINH ĐỨC
Sửa bản in: PHÒNG BIÊN TẬP KỸ THUẬT
Đọc sách mẫu: LÊ MINH HOÀI

https://tieulun.hopto.org

https://tieulun.hopto.org

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA - SỰ THẬT
12/86 phố Duy Tân, Cầu Giấy - Hà Nội ĐT: 080.49221, Fax: 080.49222,
E-mail: nxbctqg@hn.vnn.vn, website: www.nxbctqg.org.vn

TÌM ĐỌC

- LUẬT VIỄN THÔNG NĂM 2009
VÀ VĂN BẢN HƯỚNG DẪN THI HÀNH

- LUẬT TẦN SỐ VÔ TUYẾN ĐIỆN

TS. Lê Minh Toàn
- HƯỚNG DẪN SOẠN THẢO VĂN BẢN TRONG
LĨNH VỰC THÔNG TIN VÀ TRUYỀN THÔNG

https://tieulun.hopto.org