Để bạn an toàn trên mạng !

Phần lớn chúng ta đều rất hồn nhiên khi kết nối vào Internet. Chúng ta cảm thấy Internet quả là một kho dữ liệu vô tận về muôn mặt cuộc sống, và khi lướt qua các trang web chúng ta không khỏi trầm trồ về sự kỳ diệu, sự phi thường mà Internet mang lại cho cuộc sống của chúng ta. Nhưng chúng ta cũng phải hết sức cảnh giác. Internet, hiểu một cách hình tượng, cũng giống như xã hội loài người. Nghĩa là: nó cũng bao gồm tất cả những gì là tốt là xấu, là cao quí cũng như thấp hèm, là thật thà cũng như lừa đảo... Tuy nhiên chúng ta lại không thể sống mà không tham gia vào cộng đồng xã hội, không thể tiến hành cuộc cách mạnh khoa học công nghệ mà lại bỏ qua Internet. Chính vì vậy, bài viết này có tham vọng giúp các bạn tăng cường các biện pháp bảo vệ chính mình khi tham gia vào mạng toàn cầu Internet.

TẠO MẬT KHẨU (PASSWORD)

Đừng bao giờ tạo một mật khẩu (password) dễ dàng. Đừng bao giờ tự bằng lòng với mình và đừng bao giờ, chỉ vì để dễ nhớ mà dùng một hoặc hai password khi bạn đăng ký làm thành viên với nhiều địa chỉ (site) khác nhau. Nhớ đừng dùng những từ dễ đoán ra, hãy kết hợp các chữ cái, các biểu tượng và con số với nhau, và nhớ phải tạo password dài hơn 7 ký tự. Bạn không nên dùng ngày sinh, tên người yêu, con cái... hoặc đơn giản như ABCD1234. Hãy ghi nhớ password của mình nhưng không nên lưu trên máy tính. Bạn không nên dùng chức năng nhớ password và hãy chịu khó nhập password mỗi lần đăng nhập.

XÓA FILE TẠM CỦA TRÌNH DUYỆT (CACHE)

Bạn không nên giữ các file tạm (cache) mà trình duyệt lưu giữ. Các trình duyệt lưu giữ các thông tin về những trang mà bạn đã ghé thăm trong một thư mục đặc biệt trên ổ cứng. Chức năng này là một con dao hai lưỡi: một mặt nó nâng cao tốc duyệt web, mặt nó lại cho phép bất cứ ai tiếp cận được máy tính của bạn cũng có thể biết được bạn vừa làm gì. Cho nên, lời khuyên của tôi là bạn nên thường xuyên xóa cache.

Để làm được điều này trong Internet Explorer 5x và 6, bạn chọn Tools – Internet Options. Trong thẻ (tab) General, chọn Delete Cookies (IE6), Delete Files trong phần Temporary Internet Files. Trong thẻ Advance, dưới phần Security đánh dấu vào “Empty Temporary Internet Files folder when browser is closed”. Còn trong Nescape, bạn chọn Edit – Preperences. Trong cây thư mục, nhấn đúp vào Advanced để chọn Cache. Trong phần Cache, nhấn vào Clear Memory Cache, nhấn OK, rồi nhấn vào nút Clear Disk Cache.

VÔ HIỆU HÓA CHÍA SẺ FILE (FILE AND PRINTER SHARING)

Bạn hãy kiểm tra xem tính năng này có hoạt động không. Nếu bạn không dùng mạng LAN (mạng nội bộ) hoặc không có lý do dặc biệt nào để sử dụng tính năng này thì bạn hãy vô hiệu hóa nó. Tính năng File and Printer Sharing rất hữu hiệu trong một mạng nội bộ. Tuy nhiên, đây lại là một cánh cửa rộng mở cho tin tặc (hacker) thâm nhập vào máy tính của bạn.

Để loại bỏ tính năng này trong Win 9x, bạn chọn vào Control Panel, chọn biểu tượng Network rồi chọn thẻ Configuration – nhấn nút File and Print Sharing - rồi bỏ dấu kiểm trong cả 2 ô của hộp thoại nếu như chúng chưa bị loại bỏ. Trong WinXP (Win2000 cũng tương tự), bạn chọn Control Panel - Network and Internet Connections - Network Connections – Properties – Networking, và bỏ dấu kiểm khỏi ô “File and Printer Sharing for Microsoft Networks”.

KHÔNG GHI LẠI LỊCH SỬ (HISTORY)

Tốt hơn hết là bạn không nên để cho trình duyệt ghi lại những địa chỉ mà bạn đã ghé thăm. Nếu như bạn đang dùng chung một máy tính thì tính năng ghi lại lịch sử (History) này quả là rất phiền toái.

Để vô hiệu hóa tính năng này trong IE 5 & 6, bạn chọn Tools – Internet Options - thẻ General, nhấn Clear History. Từ đây, bạn cũng có thể thiết đặt lại tính năng History theo như ý muốn. Còn trong Nescape, bạn chọn Edit – Preperences. Trong cửa sổ Category, chọn Navigator và nhấn vào Clear History.

QUẢN LÝ COOKIES

Cookie là một chương trình nhỏ được lưu xuống ổ cứng của bạn giúp cho web site nhận ra bạn khi bạn ghé thăm những lần tiếp sau. Lợi dụng điều này, nhiều cookie đã được phát triển để theo dõi và ghi lại toàn bộ hoạt động của bạn khi bạn duyệt web. Nguyên tắc chung là không nên chấp nhận Cookie từ những nguồn không rõ danh tính.

Về cơ bản, Win98 lưu các cookie tại \Windows\Cookies. Win2000 lưu tại \Documents and Settings\....\Local Settings\Temporary Internet Files. Còn WinXP lưu tại \Documents and Settings\User...\Cookies. Nescape lưu các cookie trong một file text mang tên "cookies.txt". Bạn nên dùng chức năng Search hoặc Find của hệ điều hành (HĐH) để tìm và xóa file chứa cookie này. Tuy nhiên, không phải cookie nào cũng có hại. Đôi khi bạn cần giữ lại những cookie có ích và việc tìm – xóa các cookie một cách thủ công tỏ ra rất bất tiện.
Hiện nay, có một số chương trình quản lý cookie rất tốt, chỉ cần một hoặc hai thao tác là bạn có thể lựa chọn giữ lại những cookie có ích và xóa toàn bộ những cookie khác. Theo kinh nghiệm của mình, tôi thấy chương trình Super Cleaner (V2.26) làm rất tốt nhiệm vụ này. Ngoài ra, chương trình nhỏ này còn giúp bạn xóa History chỉ bằng một lần nhấn chuột

KHÔNG LIÊN LẠC KHI KHÔNG CẦN THIẾT

Đừng nó chuyện với người lạ khi bạn không có biện pháp bảo vệ nào. Tất nhiên, bạn luôn nghĩ mình an toàn khi liên lạc với những người bạn biết. Điều này không sai, nhưng những kẻ gửi thư rác (spammer) và các web site nguy hiểm lợi dụng kẽ hở này và dùng các phần mềm bí mật (hoặc công khai) để lấy địa chỉ e-mail của bạn thậm chí cả khi bạn cho rằng mình không hề để lộ địa chỉ e-mail.

Cách tốt nhất để tránh mối nguy hiểm này là không chạy các phần mềm trao đổi thông điệp ở chế độ nền. Khi không sử dụng những dịch vụ này, bạn hãy tắt hoặc thiết đặt sao cho bạn luôn ở chế độ ngoại tuyến. Nếu bạn đang sử dụng AOL Instant Messenger, hãy chọn My Aim – Edit Options – Edit Preferences – thẻ Privacy. Bạn cũng cần vô hiệu hóa tính năng tự động nhận file đính kèm. Trong MSN Messenger (hoặc Windows Messenger), chọn Tools – Options – Preferences - bỏ dấu kiểm khỏi 3 ô đầu tiên.

LƯỚT WEB MÀ KHÔNG ĐỂ NGƯỜI KHÁC BIẾT

Lời khuyên ở đây là hãy làm cho mình "ẩn danh" trên mạng. Nếu bạn muốn dấu danh tính của mình khi lướt trên web, hãy sử dụng một trong những dịch vụ ẩn danh vốn có rất nhiều trên Internet. Bạn đừng lo lắng về tính an toàn cả các dịch vụ loại này. Hầu hết, các dịch vụ ẩn danh đều làm việc theo một nguyên tắc giống nhau: Bạn đăng nhập vào web site cung cấp dịch vụ và từ đây bạn có thể đi gần như bất cứ đâu trên mạng mà bạn thích. Dịch vụ ẩn danh dấu đi địa chỉ IP thực sự của bạn, và thay vào đó là địa chỉ của chính dịch vụ này. Tuy nhiên tốc độ của các dịch vụ này không được thuyết phục lắm. Trang Safeweb.com hoặc phần mềm Proxomitron, Anonymity 4 Proxy là những ví dụ cụ thể về dịch vụ này.

XÂY DỰNG TƯỜNG LỬA (FIREWALL)

Thật là dại dột nếu chu du trên mạng mà không có một bức tường lửa (firewall) bảo vệ. Nếu bạn thường xuyên kết nói Internet thì điều đó có nghĩa là bạn phải luôn chuẩn bị để đối mặt với hacker.
Trước khi thâm nhập vào máy tính của bạn, các hacker thường phải làm một công việc gọi là "quét địa chỉ" bằng cách gửi tín hiệu (ping) đến các khối địa chỉ IP với mục đích tìm xem có địa chỉ nào trả lời không. Nếu có lời đáp, tức là máy của bạn đang trực tuyến, hacker sẽ chuyển sang bước thứ hai là quét các cổng thâm nhập vào máy tính. Nếu có một cổng bị phát hiện đang mở, hacker sẽ ngay lập tức đột nhập vào máy của bạn, và thậm chí nắm quyền điều khiển hoàn toàn hệ thống. Việc quét các cổng thâm nhập vào máy tính cũng giống như việc kẻ trộm điều tra xem cửa chính hay cửa sổ nhà bạn có bị khóa không.
Tiếp cận Internet với mà không có phương tiện bảo vệ như tường lửa cũng gống như một đấu sĩ ra trận mà không có giáp sắt. Các máy tính dùng Win9x luôn bị kêu ca về khả năng phòng bị yếu kém. Tuy nhiên, điều này đã được Micosoft khắc phục trong Win2000 và XP. Thậm chí, trong WinXP còn có một chương trình tường lửa cá nhân hoạt động cùng IE rất có hiệu quả.
Hiện nay, người sử dụng Internet có kinh nghiệm thường cài đặt các chương rình tường lửa cá nhân cho máy tính của mình như: BlackIce Defender, ConSeal PC Firewall, ZoneAlarm..., nhưng theo kinh nghiệm của tôi, bạn nên dùng BlackIce Defender. Chương trình tường lửa này rất dễ dùng, chỉ việc cài đặt là xong, mà hiệu quả lại rất cao. Các bạn dùng WinXP cũng có thể dùng chương trình này nhưng phải nâng cấp lên bản tương thích với WinXP.

PHÒNG CHỐNG VIRUS

Mặc dù cài đặt một chương trình phòng chống virus thường trực sẽ làm hao tổn phần nào tài nguyên hệ thống, song hiệu quả mà nó đem lại sẽ giúp bạn tránh được rất nhều nguy hiểm, thậm chí là cả việc đổ vỡ hệ thống. Máy tính của một người làm việc trên mạng không thể không có một chương trình phòng chống virus thường trực và được cập nhật thường xuyên.
Ở nước ta hiện nay, chương trình BKAV2002 cũng đang trên đường "hướng mạng" và làm việc khá tốt trên Windows. Ngoài ra, bạn rất nên quan tâm tới các chương trình có uy tín từ lâu như: Norton Antivirus, McAfee VirusScan... với rất nhiều tính năng bổ trợ.

CẨN TRỌNG VỚI JAVASCRIPT

Bạn phải luôn nhớ rằng càng nhiều thông tin cá nhân của bạn được tiết lộ, thì tính riêng tư của bạn cành dễ bị vi phạm. Mỗi khi bạn tham gia vào một diễn đàn, hay sử dụng một dịch vụ nào đó, bạn lại bị yêu cầu cung cấp rất nhiều thông tin cá nhân. Trong nhiều trường hợp bạn không thể không cung cấp nhưng cách tốt nhất là cung cấp càng ít càng tốt. Đối với những tùy chọn theo kiểu "optional" thì bạn nên bỏ qua. Đối với thông tin về số thẻ tín dụng, password... bạn không nên chọn chế độ tự động nhớ. Ngoài ra, bạn cũng nên có vài địa chỉ e-mail dùng dịch vụ Web Mail (hotmail hoặc yahoo) bởi vì nguy cơ địa chỉ e-mail của bạn bị tiết lộ cho các hãng quảng cáo hoặc spammer là rất cao. Hãy thận trọng khi dùng địa chỉ e-mail mà ISP như FPT hoặc VDC cung cấp cho bạn để tham gia các dịch vụ trên mạng. Theo tôi, nếu diễn đàn hoặc dịch vụ mà bạn tham gia không quá khắt khe về tính chính xác của thông tin cá nhân, thì bạn không nên cung cấp những thông tin thật về mình.

BẢO VỆ E-MAIL

Bạn nên mã hóa để bảo mật e-mail nếu như thông tin trong đó là bí mật. Nhà quản trị hệ thống mạng, hacker, hay bất cứ ai có tham vọng cũng có thể tiếp cận và đọc thư của bạn. Cho nên cách tốt nhất để tránh điều này là mã hóa e-mail. Ích lợi có được là chỉ bạn và người nhận đích thực có thể đọc được thư. Nếu bạn đang sử dụng Outlook Express, hãy chọn Tools – Options – Security - rồi chọn Restricted sites zone (More secure). Nếu bạn có OE6, hãy chọn thêm "Warn me whenever other applications try to send mail as me". Dưới thẻ Maintenence, bạn hãy thêm dấu kiểm vào "Empty messages from the 'Delete Items' folder on exit". Trong trường hợp bạn ít gửi

thư theo định dạng HTML, hãy vô hiệu hóa nó bằng cách chọn thẻ Send - chọn Plain text dưới Mail (News) Sending Format.

NGĂN CHẶN VIRUS LAN TRÀN QUA E-MAIL

Cách mà tôi sắp trình bày sau đây thoạt nghe có vẻ rất thủ công nhưng hiệu quả mang lại có thể phần nào giúp bạn ngăn virus hoặc sâu máy tính dùng sổ địa chỉ của bạn để gửi chính nó tới các địa chỉ e-mail khác. Trong Address Book, chọn New - New Contact (hoặc New Card trong Nescape). Trong ô First Name bạn hãy nhập "0000". Trong ô địa chỉ e-mail, bạn hãy bỏ trống hoặc nhập một địa chỉ vô hiệu theo kiểu email@123. Sau đó nhấn Add – OK. Trong trường hợp, virus hoặc sâu máy tính thâm nhập vào máy bạn theo ngả e-mail, nó lập tức duyệt sổ địa chỉ của bạn theo thứ tự bảng chữ cái và cố gắng gửi chính nó theo thứ tự này. Với tên người nhận đứng đầu bảng chữ cái và một địa chỉ e-mail không hợp lệ, thư cần gửi sẽ vẫn mằm trong hộp thư đi (Outbox) trên máy bạn và lập tức một thông báo về địa chỉ e-mail không hợp lệ xuất hiện. Nhờ đó bạn có đủ thời gian ngắt kết nối Internet và xóa tất cả các thư chờ gửi đi có nhiễm virus.
Ngoài ra, nếu bạn có một chương chống virus thường trực như Norton Antivirus chẳng hạn, bạn có thể thiết đặt để nó kiểm tra mọi thư gửi tới và gửi đi. Nhờ đó bạn có thể phát hiện ra các virus.

MÃ HÓA HỆ THỐNG MẠNG

Những công cụ dùng trên các máy chủ hoặc máy trạm hiện nay không có được mức độ an toàn cao như người dùng mong muốn. Bạn không nên sử dụng các chương trình như Telnet, POP, hoặc FTP nếu như password truyền qua Internet không có mức độ mã hóa cao hoặc thông tin của bạn là tối mật. Theo cách này, những thông tin "nhạy cảm" cũng không nên gửi qua e-mail. Bạn cũng cần chú ý thêm rằng bất cứ biện pháp mã hóa nào cũng đòi hỏi cả máy khách và máy chủ hỗ trợ mới có hiệu lực.

ĐỪNG QUÁ CẢ TIN

Bạn hãy cẩn thận với những chương trình tải xuống (download) từ Internet. Không nên cài đặt những phần mềm mà bạn lấy từ những địa chỉ chưa được kiểm chứng hoặc ít người biết đến. Ở những địa chỉ này, rất nhiều phần mềm được quảng cáo với những tính năng hấp dẫn lại chứa những "con ngựa thành Troy" (Trojan) cực kỳ nguy hiểm trong nó. Thời gian gần đây có nhiều người dùng Internet phàn nàn về những cú gọi điện thoại ra nước ngoài mà họ không hề thực hiện. Có nhiều lời giải thích cho vấn đề này, nhưng một trong những lý do cơ bản là bạn đã vô tình tải về máy mình một phần mềm có khả năng ngắt kết nối Internet hiện hành của bạn và thực hiện cuộc gọi tới một số điện thoại nước ngoài nào đó.
Bạn cũng cần phải lưu ý, có những trang web tỏ ra rất lịch sự khi cho bạn biết phần mềm của họ sẽ ngắt kết nối Internet hiện hành và thực hiện cuộc gọi ra nước ngoài từ máy của bạn. Sau đó, trang web loại này sẽ hỏi bạn có muốn download hay không bằng cách đưa ra tùy chọn YES (OK) hoặc NO (CANCEL). Tất nhiên, phần lớn người dùng sẽ chọn NO (CANCEL). Như vậy là trang web này đã giăng bẫy thành công. Bạn đều biết, thuộc tính của nút bấm YES hoặc NO không hề phụ thuộc vào chữ YES hay chữ NO. Chúng hoàn toàn có thể được tráo đổi cho nhau.
Ngay cả một web site có tiếng tăm cũng có thể bị hacker tấn công và thao túng. Cho nên, lời khuyên của tôi là đừng bao giờ tuyệt đối tin vào mọi thứ xuất hiện trên Internet.

CẬP NHẬT HỆ THỐNG THƯỜNG XUYÊN

Bạn nên thường xuyên cập nhật cho hệ thống của mình. Các bản sửa lỗi hay nâng cấp cho phần mềm hay HĐH là một điều mà bạn phải chấp nhận khi sử dụng Windows. Thậm chí, cả WinXP vừa mới ra lò hồi cuối tháng 10/2001 với tiếng tăm nổi như cồn, đã nhanh chóng được Microsoft đưa ra bản sửa lỗi đầu tiên!!! Những cái mà thuật ngữ chuyên môn gọi là lỗ hổng (hole) này thật không may phần lớn lại do hacker phát hiện ra. Nói nôn na, miếng vá chỉ xuất hiện khi xăm xe đã bị thủng. Thật là nguy hiểm! Do vậy cách tốt nhất để hạn chế thiệt hại trước những yếu kém của

phần mềm hay HĐH một cách kịp thời là đăng ký vào dịch vụ tin thư của những diễn đàn công nghệ thông tin đáng tin cậy.

DUYỆT WEB Ở CHẾ ĐỘ NGOẠI TUYẾN (OFFLINE) MỖI KHI CÓ THỂ

Tất nhiên chúng ta đều ngắt kết nối Internet mỗi khi không sử dụng. Tuy nhiên, để an toàn trước các virus dạng Trojan và Zombie, bạn cần phải tự tay tháo jack cắm mạng khỏi máy tính. Trong trường hợp máy chủ, bạn hãy loại bỏ những dịch vụ hệ thống (deamon) không cần thiết hoặc ít sử dụng. Bạn cần chú ý rằng khi mới cài HĐH, theo ngầm định, các dịch vụ hệ thống luôn chạy ở chế độ nền và hầu hết các hệ thống máy chủ đều không thông báo cho bạn điều này. Nếu bạn không dùng Win2000 hoặc XP làm máy chủ thì bạn hãy loại bỏ tính năng Indexing Service và Internet Information Services (ISS) vốn đã bị virus Code Red gây tai tiếng hồi cuối mùa hè vừa qua.

KIỂM TRA CÁC THIẾT ĐẶT CỦA INTERNET EXPLORER

Bạn chọn Tools – Internet Options –Security – Internet - Custom Level... và chọn mức độ an toàn thích hợp cho công việc của bạn. Trong nhiều trường hợp, bạn cần phải chọn chế độ vô hiệu hóa (Disable) tất cả các lựa chọn, hay ít nhất là chế độ "nhắc" (Prompt). Theo tôi, bạn nên chọn chế độ vô hiệu hóa tất cả ở mục Restricted Sites.

NGĂN CHẶN QUẢNG CÁO TỪ XA

Bạn hãy cài đặt một phần mền ngăn chặn từ xa các mẩu quảng cáo. Những chương trình loại này sẽ luôn giám sát quá trình ngao du trên mạng của bạn, ngăn chặn từ xa các mẩu quảng cáo (không cho tải về máy bạn) cũng như ngăn cản các ý đồ sử dụng cookies để giảm bớt khả năng bạn trở thành mục tiêu khai thác của các nhà quảng cáo trên Internet. Theo kinh nghiệm của tôi, các chương trình như Pop up Zero Pro , AtGuard, AdSubtract PRO, ZoneAlarm... làm khá tốt nhiệm vụ này.

HIỂN THỊ PHẦN MỞ RỘNG CỦA MỘT TẬP TIN

Nhìn thấy phần mở rộng của một tập tin sẽ giúp bạn tránh được việc chạy những chương trình như *. REG hay *. VBS mà bạn đã vô tình download xuống máy tính của mình. Những chương trình có phần mở rộng là REG hoặc VBS thường có tham vọng can thiệp vào Registry của Windows hoặc chính là các Trojan.

Giả sử, nhìn thấy một file mang tên "pretty_girl.jpg", bạn sẽ có thể vội vàng mở ra xem mà không biết thực chất nó là "pretty_girl.jpg.exe" hoặc "pretty_girl.jpg.vbs".

Để hiển thị phần mở rộng của file, bạn làm như sau: mở Windows Explorer, chọn Tools – Folder Options – View – Advanced Setting, bỏ dấu kiểm khỏi "Hide file extensions for known file types". Nếu bạn muốn mức độ an toàn cao hơn và không lo màn hình của mình quá chộn rộn, hãy chọn "Show hidden files and folders". Sau đó, bạn nhấn vào nút "Like Current Folder" hoặc "Apply to All Folders" (WinXP) rồi nhấn OK để làm cho những thay đổi này có hiệu lực ở tất cả các thư mục.

VÔ HIỆU HÓA PERSONAL WEB SERVER

Nếu bạn đang sử dụng đầy đủ các tính năng của MS FrontPage, có khả năng chương trình MS Personal Web Server (PWS) đã được cài đặt trên máy của bạn. Chương trình này được cài đặt để khởi động cùng Windows và nó luôn mở cổng 80. Để thiết đặt lại PWS khởi động mỗi khi cần thiết, bạn hãy tạo một biểu tượng cho nó (trên desktop chẳng hạn). Rồi khởi động chương trình, chọn thẻ StartUp và bỏ dấu kiểm khỏi ô "Run the Web server automatically at start up". Làm như vậy sẽ tránh cho chương trình này phải luôn luôn hoạt động và cũng tiết kiệm được phần nào tài

nguyên hệ thống. Tất nhiên, mỗi khi có công việc gì liên quan tới FrontPage, bạn chỉ việc nhấn chuột lên biểu tượng PWS và chọn “Start” từ thẻ “StartUp”.

THAY ĐỔI THIẾT ĐẶT GHI NHẬN VỀ SỰ CỐ HỆ THỐNG

Khi Windows (2000 hoặc XP) gặp sự cố, hệ điều hành sẽ tạo ra một file gỡ rối (dump) và có thể tự khởi động lại hệ thống. Những kẻ có gắng đột nhập vào hệ thống của bạn có thể tìm thấy những thông tin vô cùng đáng giá như những password chẳng hạn trong file “dump” này. Bên cạnh đó, hacker cũng có thể gây xung đột cho hệ thống của bạn khiến máy tính phải khởi động lại, và chỉ chờ có vậy chúng sẽ cho chạy một Trojan khởi động hoặc giành quyền kiển soát tài khoản quản trị hệ thống.
Các hiểm họa nêu trên có thể được loaii bỏ khi bạn thực hiện các bước thiết đặt lại sau: Trong Win2000, hãy mở Control Panel, chọn System Properties - Advanced - Startup and Recovery, thay đổi tùy chọn ngầm định dưới thẻ "Write Debugging Information” thành “None” và bỏ dấu kiểm khỏi ô "Automatically reboot". Trong WinXP bạn cũng làm tương tự: Control Panel - Performance and Maintenance – System – Advanced – Startup and Recovery – Settings... Thực ra, bạn không thể đọc được file “dump” nhưng bạn cũng có thể khôi phục lại việc ghi các thông tin gỡ rối nếu như bạn thực sự cần có một file “dump” để gửi cho Microsoft.

NÂNG CAO CÁC THIẾT ĐẶT AN TOÀN KHÁC

- Trong Win2000, mở Control Panel - Users and Passwords – thẻ Advanced – trong mục Secure Boot Settings, chọn ô "Require users to press Ctrl-Alt-Delete before logging in". Động thái này sẽ chặn đứng việc các Trojan ăn cắp password.
- Nếu bạn sử dụng Netmeeting, bạn nên vô hiệu hóa tính năng “Remote Desktop Sharing”. Bạn hãy làm theo các bước sau: Trong Win2000 (hoặc Win9x), chọn Start – Programs – Accessories – Communicatons – NetMeeting –Tools - Remote desktop sharing", và bỏ dấu kiểm khỏi “Enable Remote desktop sharing on this computer”.-

Trong Win2000, mở Control Panel - Administrative Tools - Local Security Policy - Security Setting - Local Policies - Security Options, trong mục "Additional restrictions for anonymous connections" nhấn chuột phải chọn "No access without explicit anonymous permissions”. Một người dùng ẩn danh được Windows ngầm định thuộc nhóm “Everyone”. Mặc dù, nhóm người dùng “Everyone” đã bị hạn chế nhiều khả năng, nhưng làm như trên sẽ giúp ta có thêm một lớp bảo vệ nữa. Để tăng cường mức độ an toàn, Win2000 bổ xung thêm thiết đặt “no access” khiến cho nhóm người dùng “Everyone” hay bất cứ kết nối mạng nào khác cũng trở nên vô hiệu nếu không được phép.
- Để tránh việc bị rò rỉ tên tài khoản (người dùng thông thường và nhà quản trị), bạn hãy làm như hướng dẫn bên trên (cả Win2000 và XP) và chọn "Do not display last name in logon screen."
- Để tránh cho người dùng đăng nhập qua Internet truy xuất ổ CD-ROM và ổ đĩa mềm, bạn hãy làm như trên (cả Win2000 và XP) và chọn "Restrict CD-ROM access to locally logged-on user only"; "Restrict floppy access to locally logged-on user only”. Thông qua các thiết đặt mới này, bạn có thể tránh được việc hacker xóa hoặc lấy cắp thông tin, thậm chí là cài một virus boot (khởi động) lên đĩa mềm.
Bạn cũng nên vô hiệu hóa tính năng “Autorun” của ổ CD-ROM. Từ Win95, Microsoft đã cho phép ổ CD-ROM tự chạy nếu có dòng lệnh “autorun” trên đĩa. Tính năng này tỏ ra rất hay nhưng nó cũng bị những kẻ thâm nhập trái phép triệt để lợi dụng để kích hoạt những Trojan nguy hiểm cho dù bạn đã khóa màn hình. Trong Win9x, bạn mở Control Panel – System – System Properties – Device Manager - chọn ổ CD-ROM - nhấn chuột phải để mở Properties - chọn thẻ Settings và bỏ dấu kiểm khỏi ô “Auto Insert Notification” - nhấn OK để hoàn tất công việc. Trong WinXP, mở My Computer - nhấn chuột phải vào ổ CD-ROM - chọn Properties - chọn thẻ AutoPlay - chọn “Take no action”, rồi nhấn OK để hoàn tất công việc.

- Bạn cũng nên chọn "Restrict users from installing printer drivers" như cách làm ở trên (Win2000) để tránh việc người khác cài những trình điều khiển máy in mà bạn không mong muốn. Tuy nhiên, nếu muốn thêm hoặc bớt các trình điều khiển máy in, bạn phải vô hiệu hóa tùy chọn nêu trên.

- Cũng theo cách trên (Win2000), bạn hãy bỏ tùy chọn "Disable CTRL+ALT+DEL requirement for logon" để làm cho ô "Require users to press Ctrl-Alt-Delete before logging in" trong Users and Passwords không còn hiệu lực. Rất nhiều Trojan phải vô hiệu hóa hai tùy chọn trên trước khi có thể đánh cắp password.
- Cũng vào Administrative Tools - Local Security Policy - Local Policies - Security Options, bạn nên chọn "Clear virtual memory pagefile when system shuts down" trong Win2000 hoặc "Clear Virtual memory pagefile" trong WinXP. Như chúng ta đều biết, Windows dùng file "page" (Win2000, XP) hoặc "swap" (Win98) (tập tin hoán đổi) trên đĩa cứng như mộ bộ nhớ RAM thứ hai. Chọn "Clear virtual memory pagefile when system shuts down" không chỉ có ích trong một số trường hợp hy hữu như mất cắp ổ cứng hoặc máy xách tay, mà còn khiến cho hacker không thể đặt một phần tử cảm nhận nào đó trong file page để thu thập các password hoặc số thẻ tín dụng hay những thông tin quan trọng khác của bạn.
- Khi mua một máy tính dùng rồi, để tránh những rủi ro sau này, tốt nhất là bạn nên định dạng lại đĩa cứng và cài đặt sạch (clean) lại HĐH.

LỜI KẾT

Nếu như bạn áp dụng các lời khuyên nêu trên, đảm bảo rằng việc lướt trên Internet của bạn sẽ nhanh hơn, an toàn hơn, bí mật hơn và ít phiền toái hơn. Tuy nhiên, trên đây chỉ là những lời khuyên. Điều đó có nghĩa là bạn hoàn toàn có thể lựa chọn mức độ an toàn sao cho phù hợp với yêu cầu của mình. Ngoài ra việc khám phá thế giới máy tính và mạng sẽ đem lại cho bạn nhiều bất ngờ thú vị cũng như những hiểu biết quí báu giúp bạn vững bước hơn trên con đường hướng tới tương lai.

Chúc các bạn thành công!

Nguyễn Việt Khoa
Khoa Ngoại ngữ
Đại học Bách khoa Hà Nội
E-mail: vietkhoabk@hotmail.com

Hãy cẩn trọng khi lướt Web

Internet là một nơi nguy hiểm, đầy những kẻ đầu cơ trục lợi lúc nào cũng lăm le bán dữ liệu cá nhân của bạn cho những kẻ môi giới thông tin và cũng không thiếu những kẻ tội phạm chỉ trực đánh cắp số An sinh xã hội của bạn, dùng thẻ tín dụng của bạn để mua sắm.

Cho dù bạn đang mua sắm trên mạng hay đang chat với người thân, bạn cần phải thận trọng bảo vệ những thông tin cá nhân của mình. Để bảo vệ chính mình, bạn chỉ cần có nhận thức về những mối đe dọa tiềm tàng và biết cách phòng vệ. Bài viết này sẽ cung cấp cho bạn những kiến thức cần thiết để bảo vệ các thông tin cá nhân.

Giấu định danh
Trước khi làm điều gì đó trên mạng, bạn cần ghi nhớ những điều sau đây:
Một kẻ nào đó trên mạng có thể kiếm tiền bằng cách bán dữ liệu cá nhân của bạn.

Mỗi khi bạn lên mạng, bạn sẽ để lộ những thông tin mới, dù chỉ là chút ít, về những sở thích của bạn.
Một số nhà thu thập dữ liệu không thoả mãn với việc chờ đợi bạn đến với họ, và họ dùng nhiều thủ đoạn để đánh cắp được nhiều thông tin hơn về bạn.

Chúng ta có thể gọi những điều trên là Các quy tắc cơ bản về thông tin cá nhân, và các quy tắc này đúng với tất cả những người sử dụng Internet. Tên bạn và những thông tin về bạn sẽ được đem bán. Vì bạn chẳng được chia chút lợi nhuận nào, nên tốt nhất là hãy giữ kín các thông tin cá nhân cho riêng bạn. Nếu những thông tin đó lọt vào tay người khác, bạn sẽ không thể kiểm soát được việc người ta sẽ sử dụng chúng như thế nào.

Bảo vệ địa chỉ IP
Giống như số nhà và tên phố của bạn, địa chỉ IP của một máy tính cho người khác biết làm thế nào để có thể tìm thấy máy tính đó trên mạng. Định danh này gồm có bốn số, mỗi số có giá trị từ 0 đến 255, cách nhau bởi một dấu chấm (ví dụ 123.123.23.2). Mỗi Website và mỗi thiết bị điện tử kết nối Internet đều phải có một địa chỉ IP duy nhất; tại một thời điểm thì không thể có hai thiết bị nào có cùng địa chỉ IP.

Nếu những kẻ gửi spam hoặc là các hacker biết được địa chỉ IP của bạn, chúng có thể tấn công máy tính của bạn bằng các loại virus hay thậm chí còn xâm nhập trực tiếp vào bên trong để đánh cắp các dữ liệu cá nhân của bạn. Bạn có thể cài đặt các firewall phần cứng hoặc phần mềm và các chương trình diệt virus trên mỗi nút mạng của bạn, nhưng nếu có đủ thời gian và đủ tài nguyên máy tính, hacker vẫn có thể xâm nhập được vào hầu như là bất cứ máy tính nào.

Bạn nên bảo vệ địa chỉ IP của mình cẩn thận như là đối với tên và địa chỉ của bạn. Bản thân trình duyệt hay là Windows không cho phép bạn giấu địa chỉ IP, nhưng có một số phần mềm khác có thể giúp bạn giải quyết vấn đề này. Với giá 5 USD một tháng, phần mềm Freedom (có tại địa chỉ http://www.freedom.net/) của hãng Zero-Knowledge Systems sẽ giấu địa chỉ IP của bạn bằng cách gửi tất cả các dữ liệu của bạn qua mạng Zero-Knowledge.

Nếu bạn sử dụng một kết nối quay số, bạn sẽ ít gặp rủi ro hơn vì địa chỉ IP của bạn thay đổi theo mỗi phiên đăng nhập. Nhưng nếu bạn sử dụng kết nối liên tục, như là DSL hay cáp, bạn sẽ có một địa chỉ IP cố định. Một địa chỉ IP cố định khiến cho bạn rất dễ bị dò quét và tấn công. Nhưng nếu mỗi lần kết nối Internet bạn có một địa chỉ IP khác với lần trước (địa chỉ IP động) thì bạn có thể trở thành một mục tiêu di động đối với các hacker. Nếu bạn có ý thức về bí mật riêng tư, hãy đề nghị nhà cung cấp dịch vụ Internet cho bạn một địa chỉ IP động. Những kẻ xâm nhập sẽ gặp khó khăn hơn nhiều để tìm ra máy tính của bạn nếu như địa chỉ của bạn không cố định.

Cookies theo dõi bạn
Các Website còn sử dụng các công nghệ khác để theo dõi bạn và dò theo các chuyển động của bạn ở trên mạng. Cookie là những file dữ liệu nhỏ mà các Website bạn ghé thăm ghi vào ổ cứng máy tính để theo dõi đường đi của bạn trên Web hoặc ghi lại những sở thích của bạn. Hầu hết các cookies đều có mục đích tốt. Ví dụ, nếu bạn đăng ký để xem một Website cụ thể (chẳng hạn như là Thời báo New York trên Web), site này có thể ghi một cookie lên máy tính của bạn để giúp bạn sau đó không cần nhập username và password vào để truy cập site này. Có hai loại cookie: cookie vĩnh viễn (tồn tại trên máy tính của bạn kể cả sau khi bạn tắt máy), và cookie tạm thời (chỉ tồn tại trong một phiên làm việc nhất định và không được lưu trữ khi bạn tắt máy tính).

Mối đe doạ của các cookie không nằm trong những thông tin mà các cookie lưu giữ; ví dụ, cookie không cho phép các hacker tìm được đường truy cập vào các file riêng tư của bạn. Hầu hết các site ghi các cookie mỗi lần bạn nhấp chuột vào một liên kết mới trong site bạn đang thăm, và sau đó người ta có thể biết được là bạn đọc những trang nào và thời gian bạn đọc trang đó là bao lâu. Những thông tin như vậy có thể rất hữu ích cho các nhà kinh doanh – những người luôn khai thác các chi tiết về những thói quen và sở thích của bạn. Theo thời gian, những mẩu dữ liệu nhỏ bé này

có thể giúp cho các công ty xây dựng một hồ sơ về bạn, và họ có thể bán những thông tin này cho cung cấp nhà kinh doanh khác.Những "con bọ" Web còn lợi hại hơn

Nếu bạn thường xuyên xoá các cookie hoặc đặt cấu hình cho trình duyệt để không cho phép ghi cookie (xem hướng dẫn trong phần Chặn các ứng dụng nguy hiểm), các site sẽ không thể thu thập đủ dữ liệu để xây dựng hồ sơ về bạn. Đó là lý do vì sao mà một số công ty lại sử dụng các "con bọ" Web như một biện pháp dự phòng để theo dõi người sử dụng nếu như các cookie không hoạt động được. Con bọ Web hoạt động như sau: đó là những hình đồ hoạ nhỏ xíu, đôi khi chỉ có chiều cao và chiều rộng là một điểm ảnh, có màu sắc giống như màu nền của trang Web. Bất cứ khi nào bạn tới một site, site đó sẽ có địa chỉ IP của bạn trước khi bạn có thể tải bất kỳ file đồ hoạ nào trên Web (bao gồm cả con bọ Web), và khi có địa chỉ IP trên tay, máy chủ Web có thể ghi lại địa chỉ của bạn trong suốt phiên làm việc của bạn. Như vậy, ngay cả khi các cookie bị chặn, con bọ Web vẫn có thể bí mật theo dõi người sử dụng. Trong nhiều trường hợp, việc theo dõi như vậy có thể là để phục vụ cho mục đích tốt (ví dụ, một site muốn điều tra xem một trang Web nhất định nào đó có được nhiều người xem không), nhưng không phải lúc nào cũng như vậy. Các site thương mại có sử dụng banner quảng cáo phát hiện ra rằng bản thân các công ty quảng cáo, chẳng hạn như là DoubleClick, có thể sử dụng con bọ Web để theo dõi các luồng lưu thông trên những site đăng quảng cáo của họ. Vì vậy, con bọ Web có thể mở đường cho việc tạo ra hồ sơ về bạn, và còn có thể khiến cho bạn phải nhận spam (nếu như con bọ Web được nạp sau khi người sử dụng điền vào một đơn mua hàng trên Web).

Chặn các ứng dụng nguy hiểm
Các cookie vốn không phải là những thứ nguy hiểm, nhưng có nhiều file nhỏ cư trú trên ổ cứng của bạn (một ví dụ là các cookie nằm trong folder C:\Windows\Cookies nếu bạn sử dụng trình duyệt Internet Explorer) và chúng cho phép Website hoặc công ty mà đã đặt cookie ở đó nhận dạng được bạn thông qua một chuỗi số và chữ (được gọi là một định danh duy nhất). Ví dụ, các công ty như DoubleClick, Adbureau.net, hay LinkExchange (đều là những nhà quảng cáo trên các Website) có thể ghi một cookie lên ổ cứng của bạn trong khi bạn đang đọc một site (ví dụ như Amazon.com) và sau đó đọc cookie đó khi bạn tới một site khác được DoubleClick phục vụ (ví dụ như CNN.com). Đó là cách mà các công ty theo dõi bạn qua một hệ thống các site khác nhau.

Tống cổ các cookie
Thật may là trình duyệt của bạn có thể dễ dàng vô hiệu hoá các cookie: Trong trình duyệt Internet Explorer 5.x, nhấp chuột vào Tools > Internet Options, rồi chọn mục Security. Nhấp chuột vào biểu tượng Trái đất có dòng chữ ghi ở bên dưới là Internet, rồi nhấp chuột vào nút Custom Level ở gần đáy của cửa sổ. Trong cửa sổ Sercurity Settings mới được mở ra, kéo thanh cuộn xuống mục ghi là Cookies. Để ngăn không cho trình duyệt của bạn tự động ghi cookie lên máy tính, hãy chọn Disable hoặc Prompt trong mục "Allow cookies that are stored on your computer". Nói chung nếu bạn để chế độ cho phép ghi các cookie tạm thời (per-session) thì cũng không sao; thường thì đó là những cookie ghi nhớ các mặt hàng mà bạn đã chọn mua trong một cửa hàng trực tuyến.

Trong trình duyệt Netscape, nhấp chuột chọn Edit > Preferences và chọn mục Advanced trong ô bên phải. Tại đây, bạn có thể chọn chế độ chặn tất cả các cookie hoặc hoặc chế độ cho phép một site ghi cookie theo quyết định của bạn. Bạn nên chọn chế độ thứ hai và cho phép trình duyệt sử dụng cookie đối với một số site. Theo cách đó, bạn có thể thực hiện một biện pháp kiểm soát các thông tin của bạn, đồng thời vẫn có thể tận dụng được tính tiện lợi của cookie. Tuy nhiên, nếu bạn quá đa nghi, có thể bạn sẽ muốn ngăn chặn tất cả các cookie ngay cả khi việc làm đó cản trở bạn mua hàng một cách hiệu quả trên mạng.

Nếu bạn thực sự tò mò muốn tìm hiểu xem có bao nhiêu site đặt các cookie lên máy tính của bạn, hãy đánh dấu lựa chọn trong mục "Warn me before accepting a cookie", trình duyệt Navigator sẽ hiển thị một hộp thoại mỗi khi có một site định ghi cookie lên máy tính của bạn. (Trong trình duyệt Internet Explorer vẫn chưa có lựa chọn này). Bạn chỉ nên thử lựa chọn này trong một thời

gian ngắn, vì sẽ có rất nhiều hộp thoại hiện lên hỏi bạn có chấp nhận cookie trong quá trình bạn lướt Web, điều đó có thể sẽ khiến cho bạn phải khó chịu.

Hãy biết chọn lựa
Tuy nhiên, việc tắt chế độ cho phép ghi cookie một cách đơn giản có thể sẽ không giúp ích cho bạn. Internet Explorer không chặn các cookie được gửi tới các công ty quảng cáo khi đang cho phép các site mà bạn ghé thăm ghi cookie. Trình duyệt này chỉ có thể cho phép hoặc là chấp nhận tất cả các cookie hoặc là không chấp nhận bất cứ cookie nào. Việc xoá tất cả các cookie sẽ làm bạn mất một thuận lợi là có thể tiết kiệm thời gian trên những site tin tức có thể tuỳ biến như My Yahoo. Nếu bạn sử dụng IE và chỉ muốn cho phép một số site ghi cookie lên ổ cứng của bạn, hãy thử sử dụng phần mềm miễn phí CookieWall của hãng AnalogX. CookieWall chạy trong hệ thống, lặng lẽ giám sát file cookie trong từng phút và cho phép bạn lựa chọn những cookie nào được phép ghi lên ổ cứng. Khi chương trình này gặp một cookie, một hộp thoại sẽ xuất hiện hỏi bạn muốn làm gì với các cookie đến từ site này - rất tiện lợi trong những trường hợp chẳng hạn như bạn đăng ký sử dụng My Yahoo và không muốn phải nhập username mỗi khi bạn nạp trang Web.

Chống lại virus
Nếu bạn không có phần mềm diệt virus trên máy tính, hãy cài đặt một chương trình như vậy. Ngày nào máy tính của bạn không được bảo vệ phù hợp thì ngày đó máy tính có nguy cơ bị nhiễm virus và có thể làm cho máy tính khác cũng bị lây nhiễm. Các virus không chỉ xoá sạch ổ cứng của bạn; một số virus còn có khả năng đánh cắp toàn bộ sổ địa chỉ e-mail hoặc cài các chương trình "cửa sau" lên ổ cứng của bạn (chẳng hạn như Trojan SubSeven hoặc BackOffice) và sau đó các hacker có thể sử dụng chương trình này để xâm nhập vào máy tính của bạn. Với giá 20 USD, phần mềm eTrust Antivirus cung cấp khả năng chống virus khá tốt, nhất là bạn lại có thể dùng thử miễn phí eTrust Antivirus trong vòng hai tháng. Tuy nhiên, để có một chương trình diệt virus toàn diện hơn, bạn có thể muốn bỏ tiền ra mua Norton Anti Virus.

Bảo vệ kết nối
Nếu bạn sử dụng một kết nối tốc độ cao như DSL hay cáp, hãy suy nghĩ về việc tải xuống chương trình ZoneAlarm, firewall cá nhân miễn phí rất được ưa chuộng của CNET. Các firewall không chỉ ngăn không cho các ứng dụng nguy hiểm xâm nhập vào máy tính của bạn mà còn ngăn cản các những chương trình lạ trên máy tính của bạn kết nối với Internet mà bạn không hay biết. Những chương trình bí ẩn đó có thể là do một virus cài vào máy tính để đánh cắp những thông tin quan trọng của bạn.

Để biết được là kết nối của bạn an toàn tới mức nào, hãy tới site Shields Up của Steve Gibson và thử một cuộc kiểm tra miễn phí về khả năng bảo mật. Shields Up thực hiện nhiều thử nghiệm giống như của hacker để dò các lỗ hổng trên máy tính của bạn và cung cấp cho bạn một bản đánh giá về tình trạng bảo mật trên máy tính của bạn và những gì mà bạn cần làm (nếu có) để giảm số lỗ hổng trên máy tính. Cuộc kiểm tra của Gibson có thể cho bạn biết liệu có chương trình "cửa sau" nào đang chạy trên máy tính của bạn hay không nhưng không cho biết chương trình đó đã được sử dụng hay chưa. Nhưng một chút thông tin đó thôi cũng đã rất có ý nghĩa rồi. Nếu bạn biết máy tính của bạn có Trojan, bạn có thể hành động để xoá bỏ chương trình đó.

Chặn những kẻ gửi spam và bọn bất lương
Gần như mọi người sử dụng Internet đều coi e-mail là lý do cơ bản để lên mạng, nhưng khi nói đến e-mail quảng cáo (hay còn gọi là spam) thì spam còn gây khó chịu hơn là những tờ quảng cáo được treo vào cửa nhà bạn. Đó là vì người sử dụng Internet phải trả tiền cho băng thông và khoảng không gian đĩa mà spam chiếm chỗ. Những đống spam có thể làm giảm tốc độ tải e-mail của bạn. Thậm chí còn tồi tệ hơn: mỗi khi những kẻ gửi spam biết địa chỉ email của bạn, chúng có thể bán địa chỉ đó cho hàng chục kẻ gửi spam khác. Một trong những spam làm cho người sử dụng tức giận nhất là spam mời chào bạn mua tên và địa chỉ email của 5 triệu nạn nhân spam với giá chỉ có 40 USD.

Phòng ngừa spam
Những kẻ gửi spam làm thế nào để lấy được địa chỉ của bạn? Hầu hết những kẻ đó tạo được kho dữ liệu về các địa chỉ thông qua quá trình thu thập địa chỉ. Đó là quá trình sử dụng phần mềm quét các Website để tìm bất cứ văn bản nào có ký tự @, rồi ghi lại các địa chỉ đó vào trong cơ sở dữ liệu. Sau đó những kẻ này gửi spam của chúng tới các địa chỉ đó, hoặc bán hay trao đổi địa chỉ e-mail với những kẻ gửi spam khác.

Đâu là cách tốt nhất để ngăn cản những kẻ gửi spam theo dõi bạn? Hãy tránh sử dụng địa chỉ chính thức của bạn; thay vào đó hãy đăng ký một account e-mail miễn phí ở một site nào đó chẳng hạn như là Hotmail hay Yahoo, và sử dụng các địa chỉ này mỗi khi bạn gửi thông điệp tới những nơi công cộng hoặc đặt mua các sản phẩm trên Web.

Những kẻ gửi spam cũng thu thập các địa chỉ e-mail qua những thông điệp mà bạn gửi tới các nhóm tin Usenet và những nơi lưu trữ trên mạng của các danh sách thư mà bạn đăng ký. Đừng bao giờ nhập địa chỉ e-mail vào các chương trình học tin của bạn. Những kẻ gửi spam dễ dàng thu thập được địa chỉ e-mail trên các bảng tin, vì vậy, hãy sử dụng một account e-mail miễn phí để đăng ký và gửi lời đáp cho các bảng tin như vậy. Trong một số ít trường hợp, virus gửi nội dung sổ địa chỉ trong chương trình thư điện tử của bạn cho những kẻ gửi spam, bạn sẽ chẳng thể làm gì được, vì vậy tốt nhất là phải chạy chương trình diệt virus trong mọi lúc.

Che dấu thông tin về bạn
Tất nhiên, cách đơn giản nhất để ngăn chặn spam là giữ kín địa chỉ e-mail của bạn ngay từ đầu. Hãy chỉ tiết lộ địa chỉ đó cho những người bạn đáng tin cậy, gia đình và các đồng nghiệp của bạn. Đừng nhập địa chỉ chính thức của bạn vào các trang Web hoặc các mục lựa chọn của trình duyệt Usenet. Một số site có thể đọc được địa chỉ e-mail hoặc tên thật của bạn từ các mục lựa chọn này. Nói chung, khi một trình duyệt Web hoặc một chương trình đọc tin Usenet yêu cầu bạn nhập tên thật hoặc địa chỉ e-mail vào một hộp thoại, hãy để trống các trường đó và tiếp tục.

Khi những kẻ gửi spam nắm được địa chỉ e-mail của bạn, họ có thể sử dụng các e-mail HTML để lấy thêm các địa chỉ khác từ bạn. E-mail HTML trông khác với e-mail văn bản thuần tuý ở chỗ e-mail HTML có thể được định dạng với những kích cỡ font chữ khác nhau và có thể đặt cả các liên kết Web ngay vào trong phần nội dung của e-mail. Thật không may là những e-mail như vậy không chỉ làm bạn mất thời gian tải về mà chúng còn có thể chứa đựng những đoạn mã ẩn có thể gửi danh sách các địa chỉ e-mail trong cuốn sổ địa chỉ của bạn cho những người soạn ra các bức thư đó. Nhưng việc tắt chức năng xem e-mail HTML cũng rất đơn giản: chỉ cần tới hộp thoại các lựa chọn trong chương trình e-mail và bỏ chọn lựa xem thư dưới dạng HTML. (Ví dụ, trong các phiên bản mới của Eudora, bạn hãy nhấp chuột vào Tools > Options, rồi chọn Viewing Mail trong ô bên trái và bỏ dấu lựa chọn trong hộp Use Microsoft's Viewer).

Các công cụ khác, trong đó có phần mềm Script Defender miễn phí của hãng AnalogX có thể chặn các mã lệnh nguy hiểm trong e-mail của bạn trước khi các mã lệnh đó được kích hoạt. Cũng giống như CookieWall, Script Defender chạy trong hậu trường, chờ đợi cho đến khi phát hiện ra một mã lệnh nguy hiểm. Sau đó, chương trình này sẽ chặn không cho kích hoạt mã lệnh đó và thông báo cho bạn biết điều gì đã xảy ra.

Bảo vệ bằng cách mã hoá
Ngay cả khi bạn tuân thủ đầy đủ các nguyên tắc đã được nói đến trong các phần trước, bản thân nội dung các e-mail cũng vẫn không an toàn trước những cặp mắt tò mò; bất cứ kẻ nào chặn e-mail của bạn giữa máy tính gửi đi và máy tính đích đều có thể đọc các e-mail này. Trừ phi bạn mã hoá nội dung của các e-mail để chỉ có bạn và người bạn muốn gửi có thể đọc được chúng. Bạn có thể sử dụng một chương trình miễn phí như là PGPfreeware (có thể tải xuống từ địa chỉ home.cnet.com/downloads/0-3356727-100-4880518.html?tag=txt) để mã hoá e-mail của mình, nhưng cả bạn và người nhận đều phải cài đặt và cấu hình chương trình này trước đó. Một số ứng dụng khách e-mail cung cấp các chọn lựa mã hoá, nhưng các chương trình này yêu cầu bạn phải

mua một định danh (ID) kỹ thuật số từ một bên thứ ba. Ví dụ như, để mã hoá e-mail bằng Outlook, trước tiên bạn phải đăng ký với một công ty như VeriSign để mua một ID và phải trả lệ phí hàng năm.

Ngăn chặn những kẻ xâm nhập IM
E-mail không còn là cách nhanh nhất để liên lạc qua Internet. Các chương trình gửi tin nhắn (IM) như là ICQ, AOL Instant Messenger, và MSN Messenger là những chương trình cực kỳ phổ biến. Nhưng bạn phải trả giá cho sự tiện lợi của việc gửi tin nhắn: spam, spam và nhiều spam hơn, trừ phi bạn là người siêng năng.

Vấn đề: địa chỉ IP bị lộ
Mối đe doạ bảo mật nghiêm trọng nhất khi sử dụng các chương trình gửi tin nhắn là: ICQ cho phép những người trao đổi tin nhắn với bạn biết được địa chỉ IP của bạn. Nhiều chương trình gửi tin nhắn hoạt động bằng cách kết nối trực tiếp hai máy tính với nhau, và kết quả là máy tính này có thể xác định được địa chỉ IP của máy tính kia và ngược lại, nhưng ICQ sử dụng các kết nối trực tiếp gần như là trong mọi thứ. Mặc dù một hacker có ít kinh nghiệm có thể gặp khó khăn trong việc tìm ra địa chỉ IP của bạn, nhưng có rất nhiều công cụ miễn phí giúp cho hacker dễ dàng làm được điều đó. Những công cụ như vậy giám sát các kết nối mạng của Windows và thu thập được một danh sách tất cả các địa chỉ IP mà máy tính đó kết nối tới. (Thậm chí các lệnh DOS như là netstat cũng có thể hiển thị địa chỉ các máy tính khác khi kết nối).

Một khi mà các hacker nguy hiểm đã biết được địa chỉ IP của bạn, chúng có thể triển khai những cuộc tấn công nhằm vào máy tính của bạn để phá huỷ hệ thống hoặc làm chậm dịch vụ Internet của bạn, khiến cho bạn như đang "bò" trên mạng. Bằng cách sử dụng các chương trình miễn phí và rất dễ lấy, các hacker còn có thể làm tràn ngập máy tính của bạn với hàng đống dữ liệu tới mức kết nối Internet của bạn sẽ không thể gửi dữ liệu đi ra được; thường thì các chương trình này lợi dụng một lỗ hổng vốn có trong Windows và làm ngưng hoạt động của hệ điều hành.

Giải pháp: bảo vệ địa chỉ IP của bạn
Trong ICQ 2000 - nhấp chuột vào nút ICQ và chọn Security and Privacy. Chọn thanh General và hãy đảm bảo rằng hộp kiểm tra Web Aware không được đánh dấu. Hãy chọn thanh Direct Connection và chọn nút có ghi "Allow direct connection with any user upon your authorization" (cho phép kết nối trực tiếp với bất cứ người sử dụng nào nếu được bạn xác nhận". ICQ sẽ liệt kê một danh sách các thành phần của chương trình mà có thể cho phép những người khác nhìn thấy địa chỉ IP của bạn.

Trong AOL Instant Messenger - Trong cửa sổ AIM Preferences, hãy chọn thanh Privacy. Bỏ dấu chọn trong hộp ghi "Allow users to see how long I've been idle" và chọn nút "Nothing about me" trong mục "Allow users who know my email address to find..."

Trong MSN Messenger - Trong hộp thoại Options dưới thanh Preferences, không đánh dấu 3 lựa chọn dưới mục General.

Vấn đề: các log file (file ghi chép các hoạt động của máy tính) có thể bị lộ
Tất cả các chương trình gửi tin nhắn cho phép ghi lại các cuộc nói chuyện của bạn với người khác theo mặc định. Nhưng nếu như có hacker xâm nhập vào máy tính của bạn, chắc hẳn bạn sẽ không muốn lưu giữ những ghi chép về các cuộc nói chuyện của mình, và bạn có thể muốn xoá các log file.

Giải pháp: xoá các log file
Trong ICQ 2000 - Khi bạn cài ICQ, một chương trình có tên là dbconvert.exe cũng sẽ được đưa vào cùng thư mục với ICQ (theo mặc định là C:\Program files\ICQ). Để xoá các log file hiện có, hãy đóng chương trình ICQ và chạy dbconvert.exe. Hãy nhập tài khoản ICQ của bạn, chọn "No history (contact list only)" và nhấp nút Next. Sau khi chương trình này xoá cơ sở dữ liệu của các

log file, nhấp nút Next một lần nữa, rồi nhấp Done để đóng chương trình. Bạn cũng có thể không cho ICQ ghi lại các cuộc nói chuyện với những người nhất định trong danh sách liên lạc của bạn: nhấp chuột phải vào tên của một người trong danh sách liên lạc, chọn Alert/Accept Modes, mở thanh Accept, và đánh dấu vào hộp "Do not log event history". Nếu bạn muốn không cho phép ghi lại bất cứ cuộc nói chuyện nào, hãy nhấp chuột vào nút ICQ và chọn Preferences, chọn mục Events từ ô bên trái, và đánh dấu vào hộp "Do not log event history" rồi nhấp Apply.

Trong AOL Instant Messenger - Tất cả các file ghi chép của AIM nằm trong folder C:\Windows\AIM95\username-của-bạn. Chương trình này không ghi lại các cuộc nói chuyện (trừ phi bạn chon File > Save), nhưng vẫn lưu giữ một file chứa danh sách các bạn thân của bạn và những lần gửi file mà bạn đã thực hiện qua AIM. Hãy xoá các file trong folder đó.

Trong MSN Messenger - MSN Messenger không tự động ghi lại các cuộc trò chuyện, mặc dù bạn có thể ghi lại các dòng riêng lẻ bằng cách nhấp chuột vào File > Save. Sau đó bạn có thể xoá bất kỳ cuộc hội thoại nào mà bạn đã ghi lại bằng cách kéo biểu tượng của file đó vào Thùng rác.

Vấn đề: instant spam
Đôi khi, các chương trình gửi tin nhắn tạo ra một đống spam dưới dạng một chuỗi các thông điệp có nội dung là "forward me to everyone you know" hoặc là các liên kết tới các Website khiêu dâm. Các instant spam như vậy thường khiến cho người sử dụng khó chịu hơn là e-mail spam, bởi vì rất nhiều chương trình theo mặc định cảnh báo cho bạn bằng một biểu tượng nhấp nháy hoặc một âm thanh khi bạn nhận được bất kỳ một thông điệp nào, kể cả những thông điệp đáng ghét.

Giải pháp: chặn spam
Trong ICQ 2000 - Nhấp chuột vào nút ICQ và chọn Security And Privacy. Trong hộp thoại hiện ra, hãy chọn thanh Ignore và đánh dấu vào tất cả các hộp lựa chọn. Chọn "Users not on my contact list" từ menu thả xuống. Tiếp theo, chọn thanh General, rồi chọn nút "My authorization is required before users add me to their contact list" và nhấp chuột vào nút Save.

Trong AOL Instant Messenger - Để AOL Instant Messenger chặn các thông điệp đến từ những người không có trong danh sách các bạn thân của bạn, nhấp chuột vào My AIM > Edit Options> Edit Preferences. Hãy chọn thanh Privacy, sau đó chọn "Allow only users on my Buddy list".

Trong MSN Messenger - Nhấp chuột vào menu Tools và chọn Options. Chọn thanh Privacy, rồi đưa thêm các username mà bạn muốn nhận được các thông điệp từ đó hoặc chặn những người nhất định bằng cách chuyển các username của họ giữa hai trường sử dụng các nút mũi tên (nằm giữa hộp thoại).

Giữ an toàn cho các giao dịch tài chính
Cho dù bạn đang mua hàng tại các cuộc bán đấu giá trực tuyến hay đang kiểm tra số dư tài khoản ngân hàng, bạn vẫn có thể giữ kín được những dữ liệu tài chính của mình.

Người mua hàng trên mạng cần thận trọng
Nói chung, việc mua bán trên mạng ít gặp rủi ro. Đó là vì hầu hết các site bán hàng đều sử dụng một phương pháp mã hóa số thẻ tín dụng của bạn và những thông tin khác trong khi dữ liệu này được truyền từ máy tính của bạn tới máy chủ Web. Phương pháp đó được gọi là SSL (Secure Sockets Layer) và là một phương pháp an toàn tuyệt đối.

Có lẽ việc mua hàng bằng thẻ tín dụng là an toàn nhất. Khi bạn sử dụng thẻ tín dụng, bạn có quyền từ chối trả tiền nếu sản phẩm hoặc dịch vụ không đúng như mô tả hoặc hàng không được giao. Còn nếu như bạn trả bằng ngân phiếu hoặc lệnh chuyển tiền, vào lúc bạn phát hiện ra có vấn đề thì có thể tiền của bạn đã mất rồi.

Tuy nhiên, việc mua bán trên mạng cũng không phải là tuyệt đối an toàn. Bọn tội phạm đôi khi vẫn đánh cắp được những thông tin về thẻ tín dụng, địa chỉ và những số an sinh xã hội không được bảo vệ. Nhưng khi bạn đã biết được điều này thì bạn có thể đề phòng.

Mã hoá trình duyệt
Thông tin trong thẻ tín dụng của bạn rất dễ bị lộ khi được truyền qua mạng từ máy tính tới một cửa hàng trực tuyến. Các hacker có thể chặn các số thẻ tín dụng trên đường truyền bằng cách chạy các phần mềm gọi là sniffer trên các bộ định tuyến (bộ định tuyến hoạt động giống như là các đèn giao thông trên Internet). Các sniffer có thể nhìn thấy tất cả các byte bên trong một gói tin và tìm các từ khoá trong đó.

May thay, hầu hết các trình duyệt hiện nay đều hỗ trợ các Website mã hoá dữ liệu trong khi truyền. Trước khi bạn mua hàng, hãy tìm các site tuyên bố họ sử dụng phương pháp mã hoá SSL. Khi bạn vào vùng được bảo mật của một Website, bạn sẽ thấy một biểu tượng hình móc khoá nhỏ ở đáy cửa số trình duyệt; hãy luôn kiểm tra biểu tượng này có hay không mỗi khi bạn mua hàng trên mạng. Và nếu lúc thanh toán tiền cửa hàng trực tuyến đề nghị bạn cho lưu giữ thông tin trong thẻ tín dụng của bạn lên máy chủ, thì bạn hãy từ chối. Đôi khi các hacker xâm nhập vào các máy tính lưu trữ và đánh cắp các thông tin quan trọng của khách hàng.

Sử dụng phương pháp mã hoá mạnh nhất
Các phiên bản của trình duyệt Netscape từ Navigator 4.61 trở lên đều hỗ trợ phương pháp mã hoá SSL 128 bit. (phương pháp mã hoá mạnh nhất hiện nay). Hãy xem bạn đang sử dụng phiên bản nào của Netscape bằng cách nhấp chuột vào menu Help và chọn About.

Nếu bạn sử dụng bất cứ phiên bản nào của Internet Explorer cũ hơn phiên bản 5.5, bạn nên tải về chương trình Internet Explorer High Encryption Pack (chương trình mã hoá SSL 128 bit của Microsoft có tại đây). Internet Explorer phiên bản 5.5 và các phiên bản sau đó không đòi hỏi phải tải về chương trình trên. Tất cả các trình duyệt IE mới hiện nay đều đã hỗ trợ phương pháp mã hoá 128 bit. Bạn có thể xem mình đang sử dụng phiên bản nào bằng cách nhấp chuột vào menu Help trong IE và chọn About. Hãy để ý đến danh tiếng của cửa hàng mà bạn định mua.

Nếu bạn đang cân nhắc có nên mua hàng từ một cửa hàng trực tuyến nào đó hay không, trước tiên bạn nên tìm site BBBOnline (http://www.bbbonline.com/) của cơ quan Better Business Bureau để xem những người tiêu dùng khác có khiếu nại gì cửa hàng đó không. Đồng thời, bạn nên đọc chính sách bán hàng và chính sách về bí mật riêng tư để biết chắc rằng site này có ghi địa chỉ đường phố và số điện thoại của trụ sở chính hay không. (Nếu chỉ có địa chỉ e-mail thì không đủ; một địa chỉ đường phố thực có thể bảo đảm rằng bạn không làm ăn với một công ty ma). Các site được các tổ chức bảo vệ người tiêu dùng đánh giá cao thường cung cấp đường link tới site của tổ chức đó để người tiêu dùng kiểm tra các thông tin đánh giá.

Sử dụng thẻ tín dụng (không dùng thẻ ghi nợ) để mua hàng
Hầu hết các ngân hàng hiện nay đều cung cấp thẻ ghi nợ ATM cho những người có mở tài khoản tại ngân hàng. Vì các thẻ này có chức năng giống như là thẻ tín dụng nên bạn có thể sử dụng chúng để thực hiện hầu hết các cuộc mua bán trực tuyến. Tuy nhiên, nếu ai đó đánh cắp được số thẻ ghi nợ của bạn, hắn sẽ không chỉ làm cho số nợ của bạn tăng lên nhanh chóng mà còn có thể rút hết tiền trong tài khoản tiết kiệm của bạn. Tuy các ngân hàng cung cấp một chế độ hoàn trả lại tiền khi bị gian lận (với một khoản khấu trừ là 50 USD) đối với tất cả những người dùng thẻ, nhưng có thể phải mất một vài tháng mới nhận lại được tiền, vì thế tốt hơn hết là bạn nên tránh rủi ro này.

Thẻ tín dụng chỉ dùng một lần
Gần đây, các công ty trong ngành tín dụng (gồm cả American Express và Discover) đã nghĩ ra một cách để ngăn ngừa những gian lận về thẻ tín dụng: tạo ra số thẻ tín dụng chỉ dùng một lần. Để nhận được một số thẻ tín dụng chỉ dùng một lần, bạn chỉ cần đăng ký với công ty thẻ tín dụng của

mình. Sau đó, bất cứ lúc nào bạn muốn mua hàng trên Internet, bạn tới site của công ty thẻ tín dụng và điền giá trị của hàng mua vào một biểu mẫu trên Web. Công ty thẻ tín dụng của bạn sẽ cung cấp cho bạn một số thẻ tín dụng chỉ dùng một lần và bạn có thể sử dụng số này để mua món hàng đó.

Tính an toàn của ngân hàng
Nếu bạn đang cân nhắc xem có nên sử dụng dịch vụ ngân hàng trực tuyến hay không, bạn sẽ phải đối mặt với nhiều vấn đề tương tự như khi mua hàng trực tuyến. Để giữ an toàn cho các thông tin tài khoản của bạn khi bạn gửi thông tin này từ máy tính tới ngân hàng, cần phải biết chắc rằng Website của ngân hàng đó sử dụng phương pháp mã hoá SSL 128 bit cho tất cả các giao dịch. Hãy tìm biểu tượng cái móc khoá, sau đó, trước khi bạn bắt đầu sử dụng tài khoản trực tuyến, hãy đảm bảo rằng phiên bản trình duyệt bạn đang sử dụng có hỗ trợ SSL.

Bạn cũng sẽ muốn chắc chắn rằng ngân hàng của bạn không bán tên, địa chỉ, số điện thoại, hoặc những thông tin cá nhân nhạy cảm khác của các khách hàng cho các hãng kinh doanh. Hãy đọc cẩn thận chính sách về bí mật riêng tư của ngân hàng để biết ngân hàng này chia sẻ thông tin với ai, và khi bạn đăng ký tài khoản, hãy đề nghị họ không đưa bạn vào bất cứ chương trình chia sẻ thông tin nào. Thường thì việc này sẽ được thực hiện thông qua một chọn lựa trong biểu mẫu Web.

Duy Anh-VASC Theo CNet News

Mười biện pháp bảo vệ khi dùng Email và Internet !

E-mail và Internet hiện nay được dùng như một phương tiện chính trong việc lan truyền vi-rút. Mười biện pháp dưới đây sẽ giúp các bạn bảo vệ được máy tính của mình:

1. Không mở bất kỳ file đính kèm được gởi từ một địa chỉ e-mail mà bạn không biết rõ hoặc không tin tưởng.

2. Không mở bất kỳ e-mail nào mà bạn cảm thấy nghi ngờ, thậm chí cả khi e-mail này được gởi từ bạn bè hoặc khách hàng của bạn. Hầu hết vi-rút được lan truyền qua đường e-mail. Do vậy, nếu bạn không chắc chắn về một e-mail nào thì hãy tìm cách xác nhận lại từ phía người gởi.

3. Không mở các file đính kèm các e-mail có tiêu đề hấp dẫn hoặc thu hút. Ví dụ như: “Look, my beautiful girl friend”, "Congratulations”, "SOS”... Nếu bạn muốn mở các file đính kèm này, hãy lưu chúng vào đĩa mềm hay một thư mục trên đĩa cứng và dùng chương trình diệt vi-rút được cập nhật mới nhất để kiểm tra.

4. Không mở các file đính kèm theo các e-mail có tên file liên quan đến sex hay các ngôi sao như “PORNO.EXE”, “PAMELA_NUDE.VBS”, “Britney Spears.scr”... Đây là **các thủ đoạn dùng để đánh lừa người dùng của những kẻ viết vi-rút.**

5. Xóa các e-mail không rõ hoặc không mong muốn. Đừng forward e-mail này cho bất kỳ ai hoặc reply lại cho người gởi. Những e-mail này thường là các spam e-mail. Mục đích của các spam e-mail chỉ để làm nghẽn đường truyền Internet.

6. Không copy vào đĩa cứng bất kỳ file nào mà bạn không biết rõ hoặc không tin tưởng về nguồn gốc xuất phát của nó.

7. Hãy cẩn thận khi tải các file từ Internet về đĩa cứng của máy tính. Dùng một chương trình diệt vi-rút được cập nhật thường xuyên để kiểm tra các file này. Nếu bạn nghi ngờ về một file chương

trình hoặc một e-mail thì đừng bao giờ mở nó ra hoặc tải về máy tính của mình. Cách tốt nhất trong trường hợp này là xóa chúng hoặc không tải về máy tính của bạn.

8. Dùng một chương trình diệt vi-rút tin cậy và được cập nhật thường xuyên như Norton Antivirus, McAffee, Trend Micro... Dùng các chương trình diệt vi-rút có thể chạy thường trú trong bộ nhớ để chúng có thể giám sát thường xuyên các hoạt động trên máy tính của bạn.

9. Nếu máy tính bạn có cài chương trình diệt vi-rút, hãy cập nhật chúng thường xuyên. Trung bình mỗi tháng có tới 500 vi-rút mới được phát hiện. Việc cập nhật thường xuyên này sẽ giúp cho máy tính của bạn trở nên miễn nhiễm trước các loại vi-rút mới.

10. Thực hiện việc sao lưu các dữ liệu quan trọng thường xuyên. Nếu chẳng may vi-rút xóa tất cả các dữ liệu trên máy tính của bạn thì vẫn còn có khả năng phục hồi các dữ liệu quan trọng này. Các bản sao lưu này nên được cất giữ tại một vị trí riêng biệt hoặc cất giữ trên máy tính khác.

Theo Báo Người Lao Động !
N.H. QUỐC (www.vnsecurity.net)

Mười cách thức bảo vệ bạn khi lướt Web !

Internet là một nơi đầy thú vị nhưng cũng đầy hiểm họa. Chúng tôi xin giới thiệu với các bạn 10 cách thức bảo vệ bạn khi lướt Web, giúp bạn bảo vệ được những thông tin bí mật và tránh được sự nhòm ngó của hacker.

1. Cài đặt phần mềm tường lửa gia đình và phần mềm chống virus
Hacker có thể lùng sục trong Internet để kiếm tìm các máy tính có lỗ hổng nhằm đánh cắp số thẻ tín dụng, các thông tin cá nhân và thực hiện các mưu đồ xấu xa khác. Phần mềm tường lửa gia đình như BlackICE Defender hoặc Zone Alarm có thể giúp bạn tránh được sự nhòm ngó của hacker. Bạn cũng nên cài đặt một phần mềm chống virus cho máy tính.

2. Cẩn thận khi gửi thông tin
Đừng gửi các thông tin nhạy cảm như địa chỉ nhà riêng, số điện thoại, tên và tuổi của bọn trẻ cho những người lạ mặt qua Internet. Hãy cẩn thận với những gì mà bạn đưa lên Website của mình. Nếu bạn muốn đưa một bức ảnh mình hoặc của gia đình lên mạng, bạn hãy chọn một site dịch vụ lưu ký mà cho phép thiết lập mật khẩu truy cập. Bạn nên nhớ rằng tất cả những gì bạn thảo luận tại các diễn đàn trực tuyến đều được ghi lại, và có thể dễ dàng tìm thấy.

3. Không tải xuống máy tính bất cứ thứ gì trừ phi bạn tin tưởng vào người gửi và nguồn gốc file gửi kèm
Những e-mail trông có vẻ không mấy nguy hại lại thường chứa các phần mềm gián điệp. Để được an toàn, không nên tải xuống máy tính bất cứ thứ gì trừ phi bạn biết người gửi, và tin tưởng rằng file gửi kèm sẽ không gây nguy hại cho máy tính của bạn.

4. Sử dụng một e-mail phụ
Khi bạn điền các thông tin vào một bản kê khai trên mạng, gửi thông điệp tới các nhóm thảo luận trực tuyến, hoặc cho người lạ địa chỉ e-mail của bạn, thì bạn hãy cho địa chỉ e-mail phụ mà bạn đã đăng ký từ các dịch vụ miễn phí như Hotmail hay Yahoo mail. Nếu địa chỉ e-mail này bị "bom thư", bạn có thể bỏ đi và sử dụng một địa chỉ e-mail khác. Bạn chỉ nên trao đổi địa chỉ e-mail chính với những người mà bạn thực sự tin tưởng.

5. Không để cho trình duyệt trở thành một kẻ ba hoa
Tên và địa chỉ e-mail của bạn có thể được nhúng trong trình duyệt. Một số Website có thể lấy các thông tin này từ trình duyệt của bạn và tạo một dữ liệu về bạn. Để ngăn không cho những thông

tin của bạn bị rò rỉ, bạn có thể vào thực đơn preferences của trình duyệt (Netscape) và xóa những thông tin này, hoặc thay thế bằng một cái tên và địa chỉ e-mail giả.

6. Chính sách bí mật cá nhân
Bạn hãy kiểm tra chính sách về bí mật cá nhân của Website mà bạn ghé thăm. Các Website thường giữ quyền chia sẻ dữ liệu về bạn với một bên thứ ba nào đó. Bạn hãy đọc phần Privacy Statement trên các Website.

7. Không chấp nhận các cookie không cần thiết
Bạn có thể muốn chấp nhận các cookie nằm trong máy tính vì các cookie thường giúp cho bạn mua hàng trực tuyến dễ dàng hơn do chúng nắm giữ thông tin về bạn. Nhưng bạn có thể tống khứ các cookie không cần thiết bằng cách thiết lập lại thực đơn preferences của trình duyệt (Netscape) hoặc sử dụng phần mềm tiện ích như Cookie Crusher.

8. Mã hoá các dữ liệu nhạy cảm
Trước khi gửi số thẻ tín dụng hoặc các thông tin tài chính khác qua Internet, bạn hãy đảm bảo rằng các thông tin đó đã được mã hóa để ngăn chặn sự nhòm ngó của hacker. Các Website đã được bảo mật thường cho bạn biết giao dịch đã được mã hóa, và trình duyệt của bạn thường hiển thị biểu tượng cái khoá để xác nhận rằng giao dịch đã được đảm bảo an toàn.

9. Sử dụng một ẩn danh
Bởi vì các Website thường lưu lại dữ liệu về bạn sau khi bạn ghé thăm, vì thế bạn có thể che giấu tên của mình bằng cách sử dụng một ẩn danh, chẳng hạn như sử dụng site ẩn danh http://www.anonymizer.com./ Site này sẽ mã hóa các địa chỉ Website mà bạn ghé thăm, vì thế Nhà cung cấp dịch vụ Internet của bạn sẽ không thể biết bạn đã truy cập vào site nào.

10. Xóa cache sau khi lướt Web
Máy tính của bạn có một phần gọi là memory cache, chuyên lưu giữ địa chỉ các Website mà bạn đã ghé thăm. Một người nào khác khi sử dụng máy tính của bạn có thể phát hiện ra các Website mà bạn đã truy cập. Bạn có thể xóa dấu vết bằng cách xóa cache. Hãy tìm đến thực đơn Preferences của trình duyệt Netscape hoặc thực đơn Tool/Internet Option của trình duyệt IE để xoá cache.

Và bạn hãy luôn nhớ rằng: dữ liệu mã hóa vẫn có thể bị bẻ khóa. Không dễ dàng phát hiện một phần mềm gián điệp trong máy tính của bạn.

Điều cuối cùng: nếu bạn có những dữ liệu cực kỳ quan trọng, thì đừng nên lưu trong một máy tính có kết nối Internet.

Đăng Khoa-VASC Theo Time !

Vô hiệu hóa những đoạn mã nguy hiểm trong Email !

Những đoạn mã nguy hiểm, ngụy trang dưới hình thức các siêu liên kết (hyperlink), là mầm mống chứa virus máy tính để nó có thể xuất hiện, thâm nhập và phát tán vào PC của bạn, gây ra hậu quả tai hại.

Những đoạn mã này thường có cách thức chung là được gửi đến cho nạn nhân thông qua các e-mail tưởng chừng vô hại. Một thủ thuật nhỏ có thể giúp bạn chủ động đề phòng và làm vô hiệu hóa chúng:

Trong cửa sổ trình duyệt Outlook Express, chọn Tools trên thanh công cụ, sau đó chọn Internet Options. Nhấp con trỏ chuột vào mục Security khi cửa sổ Options hiển thị ra với nhiều mục nhỏ. Trong phần Security, chọn Restricted Sites với biểu tượng giống như một tấm biển báo cấm giao thông (More Secure) sau đó nhấn Enter.

Tiếp theo, trong Control Panel cũng chọn Internet Options (với biểu tượng chiếc chìa khóa bên cạnh quả cầu màu xanh) bằng cách nhấp đúp chuột, và cũng chọn Security. Các biểu tượng cũng lần lượt trình bày như trong mục Security ở phần trên. Tiếp đến, chọn Restricted Sites với biểu tượng chiếc bảng cấm màu đỏ và bấm trỏ chuột vào đó. Bấm vào ô Custom Level ở dưới. Khi cửa sổ Security Settings xuất hiện, chọn Disable trong mục Active Scripting.

Hoàn thành tất cả những thao tác này, xem như bạn đã vô hiệu hóa chức năng Java Script chạy tự động và cũng có nghĩa là loại trừ được các nguy cơ xâm nhập phá hoại của những đoạn mã nguy hiểm (nếu có) khi bạn mở, kiểm tra và đọc e-mail.

Lưu ý: Để hoàn tất thủ tục này và lưu giữ nó, bấm trỏ chuột vào nút OK. Lúc này, màn hình sẽ xuất hiện hộp thoại hỏi bạn có nhất định muốn thay đổi Security Settings hay không, bạn chọn Yes.

(Theo Sài Gòn Giải Phóng)

Loại bỏ cookies với chức năng P3P trong IE !

Mục đích sinh ra cookie nhằm giúp người sử dụng truy cập thông tin được thuận tiện, người quản trị Web site có thêm thông tin để tối ưu hệ thống. Nhưng các thông tin trong cookie này sẽ gây phiền toái cho người sử dụng nếu như bị lọt vào tay các công ty nghiên cứu, thăm dò thị trường hay các công ty quảng cáo... vấn đề này liên quan đến việc bảo mật thông tin cá nhân trên Internet.

Tổ chức W3C (Tổ chức xây dựng các chuẩn Internet) hiện đang trong giai đoạn hoàn thiện bộ chuẩn P3P (Platform for Privacy Preferences, truy cập vào Web site của W3C - www.w3.org/P3P/ để có thông tin chi tiết hơn), bộ chuẩn này cho phép thực hiện tự động thoả ước bảo mật thông tin cá nhân giữa người sử dụng và công ty quản lý web site. Tuy bộ chuẩn P3P chưa hoàn tất nhưng hãng Microsoft đã nghiên cứu và áp dụng ngay bộ chuẩn này trong phiên bản trình duyệt IE6.

Chế độ bảo mật mặc định của trình IE6 sẽ loại bỏ tất cả các cookie được nhúng trong trang Web nếu như Web site quản lý không có thông tin chính sách bảo mật theo chuẩn P3P, ngoài ra nếu có một cookie nào đó đang tìm cách thu thập các thông tin cá nhân như họ tên người sử dụng, địa chỉ E-mail... thì trình duyệt sẽ cảnh báo cho người sử dụng biết.

Nếu như vẫn chưa hài lòng với những gì mà IE 6 đã cấu hình sẵn, chúng ta có thể tự mình xác định cấp độ thông tin cá nhân cho phép Web server ghi vào cookie. Thủ tục tiến hành : Chọn menu Tool.Internet Option.Privacy, rồi chọn cấp độ cung cấp thông tin phù hợp. Sau đó nhấn phím OK.

Hãy còn quá sớm để kết luận rằng P3P đủ hữu hiệu để quản lý thông tin cá nhân của người sử dụng và cũng chưa chắc chuẩn này sẽ được tất cả các nhà sản xuất trình duyệt hỗ trợ trong sản phẩm của mình. Ví dụ như trình duyệt Netscape Navigator đã có sẵn tính năng loại bỏ hoàn toàn tất cả các cookie khác, ngoại trừ cookie do chính Web site quản lý trang web. Với phiên bản Netscape Navigator 4.7, chọn menu Edit.Preferences.Advance rồi đánh dấu chọn tại mục Accept only cookies that ghet send back to the originating server. Với phiên bản Navigator 6.0 và bộ trình duyệt có mã nguồn mở Mozilla, chọn menu Edit.Preferences, trong mục Privacy and Security đánh dấu chọn tại mục Enable cookie for the originating web site only, rồi nhấn phím OK.

Theo PC World VN !

Đừng chia sẽ cookies với người lạ!

Nếu dùng Internet Explorer 5.5 hoặc 6.0, bạn nên "lấp" kẽ hở cho phép người ngoài ăn cắp cookie từ trình duyệt của bạn. Cookie là một đoạn dữ liệu mà website "dán" vào đĩa cứng để nhận biết khi nào bạn vào site đó lần sau. Hạn chế của Internet Explorer là để cho kẻ tấn công bất chính ăn cắp cookie trên máy tính của bạn.

Hầu hết các cookie không mang thông tin quan trọng, nhưng cũng có những site mua bán có thể ghi nhận dữ liệu "mật" (như mã số thẻ tín dụng" vào cookie của chúng. Bằng cách lừa bạn nhấn vào một liên kết đặc biệt trên website hoặc vào thông điệp e-mail HTML của kẻ tấn công, chúng có thể truy cập cookie của bạn.

Microsoft đã cho biết giải pháp xử lý vấn đề này. Bạn có thể tải tiện ích hoặc thực hiện vài thao tác để bảo vệ PC không bị mất cắp Cookie bằng cách vô hiệu hóa Active Scripting - một loại mã website dựa vào đó để thực hiện nhiều tính chức năng khác nhau. Lưu ý: URL có phần mở rộng .asp dùng Active Scripting; tên ngắn gọn tượng trưng cho "Active Server Pages". Nếu dùng tiện ích của Microsoft, Active Scripting sẽ tiếp tục công việc cho bạn.

Vào www.micrsoft.com/windows/ie/downloads/critical/q313675/default.asp để tải tiện ích này hoặc vào www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulettin/MS01-055/asp.

Theo PC World VN !

Chia sẽ file qua mạng Internet một cách an toàn !

File sharing là một chức năng cho phép những người dùng Windows chia sẻ file qua mạng. File sharing được hỗ trợ bởi giao thức riêng của Microsoft, gọi là NetBIOS.

Mặc dù chức năng chia sẻ này tỏ ra rất tiện lợi cho người sử dụng, nhưng nó cũng gây ra nhiều nguy hiểm về mặt bảo mật thông tin. Khá nhiều cuộc tấn công hoặc truy nhập trái phép qua mạng được thực hiện nhằm vào giao thức NetBIOS.

Có những trường hợp người sử dụng thậm chí chia sẻ toàn bộ đĩa cứng chứa nhiều thông tin quan trọng mà không hề đặt mật khẩu, hoặc đặt mật khẩu rất đơn giản khiến kẻ tấn công có thể truy nhập dữ liệu một cách dễ dàng.

Nguy hiểm tiềm tàng nữa là mặc dù NetBIOS vốn chỉ được thiết kế để hoạt động trong mạng cục bộ (LAN) nhưng lại có thể hoạt động trên nền TCP/IP vốn là giao thức cho phép truy nhập trên diện rộng. Điều này dẫn tới nguy cơ lớn cho những cá nhân truy nhập Internet: họ có thể vô tình phơi mình ra trước các cuộc tấn công nhằm vào dịch vụ NetBIOS. Trong trường hợp xấu nhất bất kỳ người nào trên Internet cũng có thể đọc, thậm chí ghi dữ liệu lên hệ thống của họ. Nhiều loại virus cũng hoạt động và thực hiện việc lây lan thông qua cách thức này.

Các tường lửa (firewall) thường được thiết kế để tự động chặn các truy nhập trái phép qua Internet vào các dữ liệu được chia sẻ qua NetBIOS. Tuy nhiên nếu không có lý do gì đặc biệt ta nên loại bỏ giao thức NetBIOS trên TCP/IP. Lời khuyên trên đặc biệt hữu ích với những người dùng đơn lẻ truy nhập Internet mà không có nhu cầu chia sẻ file: hầu hết những máy tính cá nhân, máy tính tại gia đình sử dụng để kết nối Internet đều có thể áp dụng mẹo này để nâng cao hơn nữa khả năng chống đột nhập.

Sau đây chúng tôi xin giới thiệu các bước nhằm tắt chức năng NetBIOS trên các phiên bản khác nhau của Windows.

Windows XP
Thực hiện lần lượt các bước sau:
* Chọn nút "Start"
* Chọn menu "Connect To"
(hoặc chọn menu "Settings", sau đó chọn "Network connections" nếu đang ở chế độ Classic mode)
* Kích chuột phải trên Network connection dùng để kết nối tới Internet (là kết nối modem nếu nối Internet qua modem)
* Kích chuột phải trên menu "Properties"
* Chọn trang "Networking"
* Chọn "Internet Protocol
(TCP/IP)"
* Chọn nút "Properties".
* Chọn nút "Advanced"
* Chọn trang "WINS"
* Chọn "Disable NetBIOS over TCP/IP"
* Chọn OK rồi đóng các cửa sổ còn lại để thoát ra

Windows 2000
Thực hiện lần lượt các bước sau:
* Mở "Control Panel"
* Chọn "Network and Dial-up
Connections"
* Kích chuột phải trên "Local Area Connection"
* Chọn "Properties"
* Chọn "Internet Protocol
(TCP/IP)"
* Chọn nút "Properties"
* Chọn nút "Advanced"
* Chọn trang "WINS"
* Chọn "Disable NetBIOS over TCP/IP"
* Chọn OK rồi đóng các cửa sổ còn lại để thoát ra

Windows 95, 98, ME
Thực hiện lần lượt các bước sau:
* Mở "Control Panel"
* Chọn "Network"
* Duyệt qua danh sách các thành phần trong trang Configuration để chọn cấu hình TCP/IP tương ứng với kết nối mạng hoặc Dialup adapter nối Internet.
* Chọn nút "Properties"
* Chọn trang "NetBIOS"
* Bỏ chọn lựa "Enable NetBIOS over TCP/IP"
* Chọn trang "Bindings"
* Bỏ chọn lựa "Client for
Microsoft Networks" và "File and printer sharing for Microsoft Networks"
* Chọn OK rồi đóng các cửa sổ còn lại để thoát ra. Sau đó khởi động lại máy tính.

Nguyễn Anh Quỳnh (I-today.com.vn)

Một máy tính 2 trình duyệt !

Internet Explorer hay Netscape Navigator? Cái nào hơn? Thế sao không dùng cả hai? Sau đây bạn sẽ biết cách làm cho chúng đi cùng với nhau .

Bạn có bao nhiêu trình duyệt trên máy? Nếu dùng Windows (có lẽ là vậy), bạn hẳn có ít nhất một trình duyệt là Internet Explorer. Nhưng rất có thể bạn còn có vài phiên bản của Netscape Navigator hoặc America Online ẩn đâu đó trên ổ đĩa cứng. Càng tốt! vẫn hay hơn nếu có nhiều cách đi vào Web.

Mỗi trình duyệt có ưu điểm riêng trong một số tác vụ nào đó trên Web. Chẳng hạn, Internet Explorer không phải bao giờ cũng hiển thị tiến trình tải xuống các tập tin (Navigator thì có), nhưng lại có thể in một trang Web với đầy đủ các frame được hiển thị (Navigator thì không).

Bạn có thể thích giao diện của trình duyệt này nhưng lại ưng ý hơn với chương trình e-mail của trình duyệt kia. Một số site tuyên bố họ đã tối ưu hóa cho trình duyệt này hay trình duyệt kia, thế là bạn băn khoăn không biết liệu mình có bỏ lỡ một vài tính năng tuyệt hảo nào đó bởi dùng không đúng trình duyệt (xem "Các site có được tối ưu hóa cho trình duyệt của bạn?").

Và nếu bạn là người tạo trang Web thì xem trước trang Web đó trong cả hai trình duyệt sẽ hay hơn nhiều, vì mỗi trình duyệt đều có những "tật" riêng mà bạn phải biết để chữa.

Nhưng các trình duyệt cũng có phần giống lũ trẻ, tối ngày cãi nhau. Cái nào cũng muốn bạn chỉ chú ý tới nó thôi và chẳng muốn chia sẻ gì hết (bookmark hay danh mục địa chỉ chẳng hạn).

Nhưng bạn có thể huấn luyện cho chúng chơi với nhau, thậm chí còn giúp nhau nữa. Chúng tôi sẽ cho bạn lời khuyên về các phiên bản 3.x và 4.x của Internet Explorer và Netscape Navigator, làm cách nào cho cả hai làm việc tốt hơn, dù sát cánh bên nhau hay riêng rẽ từng cái một.

Bạn cũng sẽ có một danh mục các phím tắt thường dùng của cả hai trình duyệt, hoặc những cú nhấn chuột phải rất tiện lợi, và chúng tôi mách nước bạn phải làm gì nếu chẳng may đường kết nối bị tắc nghẽn.

Các trình duyệt kình địch nhau

Lấy Internet Explorer làm mặc định. Bất cứ khi nào cài đặt một trình duyệt Web, nó đều yêu cầu bạn cho nó làm mặc định và nhắc đi nhắc lại cho tới khi bạn quyết định mới thôi. Thế lỡ sau khi dùng trình duyệt nào đó một thời gian, bạn lại muốn chuyển mặc định sang trình khác thì sao?

Bạn có thể đổi ý như vậy, nhưng làm việc này với Internet Explorer dễ hơn bất cứ phiên bản nào của Navigator. Trong IE 3.x và 4.x, chọn View.Internet Options, nhấn vào mục Programs, đánh dấu vào ô dưới cùng "Internet Explorer should check to see whether it is the default browser (Internet Explorer cần kiểm tra xem nó có phải là trình duyệt mặc định không)",

Sau đó nhấn OK. Đóng rồi lại mở Internet Explorer, trình duyệt Microsoft sẽ lại yêu cầu bạn cho nó làm trình duyệt mặc định.

Cho Navigator cầm lái. Đổi mặc định trong Navigator 3.x và 4.x thì rắc rối hơn đôi chút. Theo các bước như đã nói ở trên, nhưng xóa hộp kiểm tra "Internet Explorer should check to see whether it is the default browser".

Nếu bạn gặp may, khi khởi động lại Navigator bạn sẽ được yêu cầu chọn trình duyệt mặc định, nhưng tốt nhất đừng mong vào chuyện đó.

Nếu Navigator ỳ ra, bạn sẽ phải cần đến một trình văn bản như Notepad của Windows 95 hay 98 để sửa lại tập tin prefs.js. Thoát khỏi Navigator, nhấn Start.Programs .Accessories.Notepad.

Khi Notepad đã mở, nhấn File.Open. Nhấn phím mũi tên kế bên "Files of Type" rồi chọn All Files (*.*). File prefs.js nằm trong C:\Program Files\Netscape\Users \yourname, trong đó yourname là tên người dùng (user name) của bạn trong Windows.

Mở tập tin đó rồi tìm dòng 'user_Pref ("browser.wfe .ignore_def _check", true):. Cẩn thận đổi từ "true" thành "false". Lưu, sau đó thoát rồi khởi động lại Navigator. Hộp thoại yêu cầu chọn mặc định lại xuất hiện, lúc này bạn có thể cho Navigator lên "chiếu trên".

Chia sẻ dữ liệu

Sao lưu Bookmark/Favorite. Bạn đã bỏ ra thì giờ quý báu để thu thập các URL. Giờ, trước khi thử bất cứ mẹo nào, hãy tự vệ bằng cách sao lưu các Bookmark và Favorite.

Không quan trọng bạn đang dùng trình duyệt nào, cách dễ nhất để làm việc này là mở Windows Explorer, nhấn <Ctrl> và kéo một bản sao của tập tin bookmark.htm trong Navigator (trong cùng thư mục với prefs.js) hoặc thư mục Favorites của Internet Explorer (nó phải nằm trong thư mục Windows) sang đĩa mềm hay một vùng khác trên ổ đĩa cứng.

Đưa Navigator Bookmark vào Favorites của Internet Explorer. Nhờ đưa các Bookmark của Navigator vào danh mục Favorite của Internet Explorer, bạn sẽ có thể truy cập ngay lập tức mọi Bookmark từ trong Internet Explorer. Việc này cũng đơn giản như thêm một đường tắt vào tập tin bookmark.htm. Về sau, mỗi khi bạn thêm một Bookmark mới, nó sẽ được tự động bổ sung vào Favorites.

Trong IE 3.x và 4.x, chọn File.Open, chọn Browse, đặt "Files of type" thành All Files, rồi tìm đến tập tin bookmark.htm trong mục "Look in". Tìm thấy xong thì nhấn kép vào tập tin này để đưa nó vào hộp thoại Open. Nhấn OK, IE sẽ hiển thị Bookmark của Navigator như những liên kết . Trên menu của IE, nhấn Favorites.Add to Favorites, đặt tên cho liên kết dẫn đến Navigator Bookmarks, sau đó nhấn OK. Ô là là! Bây giờ bạn đã có thể nhấn vào các Bookmark của Navigator như bất kỳ Favorite nào trong Internet Explorer.

Chuyển Favorite của Internet Explorer thành Bookmark của Navigator. Netscape không cho bạn dễ dàng chuyển Favorite thành Bookmark. Giải pháp rẻ tiền nhất là IE Import and Export Favorites Tool (công cụ xuất nhập Favorite) của Microsoft, miễn phí (www .microsoft.com/msdownload/ieplatform/favtool/favtool.asp). Tiện ích này chỉ có 50KB, nhưng có thể nhập Bookmark thành Favorite và ngược lại lưu Favorite thành Bookmark.

Nhưng hãy coi chừng: khi đưa các Favorite của IE vào Navigator, tiện ích này sẽ xóa luôn và thế chỗ tập tin bookmark ban đầu; do đó, nếu muốn cả hai đều song song tồn tại, trước tiên bạn phải nhập các Bookmark vào Internet Explorer (dùng thủ thuật đã nêu trên), sau đó mới thay tập tin Bookmark bằng các Favorite đã hợp nhất.

QuikLink Explorer của hãng QuikLink (www.quiklinks.com/explorer) là một giải pháp tốt và lại đơn giản hơn. Nó nhập các Bookmark từ Navigator, IE, Opera và Mosaic vào một cơ sở dữ liệu bookmark tập trung.

Khi lưu bookmark trong cơ sở dữ liệu này, bạn sẽ mặc nhiên truy cập được bookmark đó từ bất cứ trình duyệt nào trong số kể trên. Hiện có một phiên bản QuikLink miễn phí cho phép tổ chức các bookmark trong một trình duyệt, nhưng với nhiều trình duyệt, bạn sẽ phải mua phiên bản Standard giá 20 USD.

Chuyển sổ địa chỉ. Trong quá trình cài đặt, cả Netscape và Internet Explorer đều nhập sổ địa chỉ (Address Book) từ các trình duyệt khác (và từ các phiên bản trước của cùng một trình duyệt).

Nhưng nếu bạn muốn cài đặt xong xuôi rồi mới nhập sổ địa chỉ thì sao? Trong Internet Explorer 3.x, chọn Go.Read Mail để mở Internet Mail; sau đó nhấn File.Import rồi chọn các tập tin thích hợp.

Muốn nhập sổ địa chỉ hoặc e-mail từ một chương trình khác vào IE 4.x, bạn mở Outlook Express, nhấn File.Import, kế đó chọn Address Book hoặc Messages.

Chọn xong thì nhấn Import. Nếu dùng Navigator 3.x, bạn phải dùng tiện ích của hãng thứ ba như E-mail Address Book Conversions của InterGuru, giá 20 USD (www.interguru.com/mailconv.htm), một chương trình dùng để chuyển qua lại các tập tin sổ địa chỉ của Eudora, Outlook Express, cũng như Netscape Messenger và Mail.

Nếu dùng Navigator 4.x thì dễ hơn: bạn chỉ cần mở Messenger, sau đó là Address Book bằng cách chọn Communicator.Address Book. Nhấn File.Import. Sau đó bạn có thể nhập tập tin địa chỉ từ Eudora Outlook Express hoặc bất cứ sổ địa chỉ nào dưới dạng LDIF hoặc text. Netscape khác nhiều thông tin trực tuyến về việc chuyển IE 3.x và 4.x sang Commu-nicator; hãy tìm địa chỉ help .netscape.com/kb/client/970709-1.html.

Các site có được tối ưu hóa cho trình duyệt của bạn?

Cả Netscape lẫn Microsoft đều đòi hỏi một số Web site nhất định phải tối ưu hóa cho trình duyệt của họ. Vậy liệu bạn có đang bỏ mất một số tính năng mới hữu ích vì không dùng đúng trình duyệt không?

Sau khi tìm kiếm các site đã tối ưu hóa, người ta phát hiện rằng một số site chỉ làm việc với Internet Explorer mà thôi, chẳng hạn site Investor của Microsoft (hình bên), hoặc một chiếc xe buýt nhà trường vui nhộn chở Mickey cùng bè bạn băng qua trang chủ của Disney.

Ngoài những cái nêu trên thì vài điểm khác biệt được tìm thấy chỉ là "râu ria" mà thôi; đồng thời, người ta không thấy một site nào có những tính năng dành riêng cho Navigator. Vậy bạn chẳng việc gì phải phân vân không biết chọn trình duyệt nào, bởi dù chọn bên nào bạn cũng không mất mát gì lắm.

Nâng cao hiệu năng

Bỏ bớt hình ảnh. Có lẽ trước đây, bạn từng nghe nói chuyện này, nhưng điều có ích thì dù lặp lại vẫn không thừa. Nếu mục đích chính của bạn là tải xuống càng nhanh càng tốt, bạn cần cố gắng loại bỏ các hình đồ họa, âm thanh và hình ảnh động, và thiết lập mặc định chỉ tải xuống văn bản (text-only loading) cho trình duyệt.

Nếu bạn dùng IE 3.x, nhấnView.Options, chọn General rồi xóa hộp kiểm tra Show Pictures. Nếu bạn dùng IE 4.x, chọn View.Internet Options .Advanced, sau đó xóa tất cả các ô kiểm tra trong phần Multimedia. Trong Navigator 3.x, chọn Options rồi xóa ô kiểm tra Auto Load Images.

Trong Navigator 4.x, nhấn Edit .Preferences, chọn Advanced, sau đó xóa ô Automatically load images. Nhưng rốt cuộc bạn vẫn thật sự muốn có hình ảnh? Đừng lo. Chỉ cần nhấn chuột phải vào biểu tượng hình ảnh rồi nhấn Show Picture (trong IE 3.x và 4.x), Load Image (trong Navigator 3.x) hoặc Show Image (trong Navigator 4.x).

Hoàn thiện hình ảnh. Power Toys for IE 4.x của Microsoft (www.microsoft.com/ie/ie40/powertoys/default.htm) có hàng loạt tiện ích thông minh để kiểm

soát đồ họa trên Web. Nếu bạn đã ngấy tận cổ việc chuyển đổi giữa chế độ văn bản và chế độ đồ họa, hãy thử dùng Image Toggler. Tiện ích này nằm trên thanh công cụ Link (kết nối) của IE 4.x; bạn chỉ cần nhấn chuột để tải xuống hoặc bỏ qua các hình ảnh.

Với một Power Toy khác là Zoom In/Zoom Out, bạn chỉ cần nhấn chuột phải là có thể phóng đại những hình đồ họa bé xíu. Với Web Search, bạn nhấn chuột phải nếu muốn đưa những từ khóa vào công cụ truy tìm mặc định, kết quả hiệu nghiệm ngay.

Một quan hệ ổn định hơn. Bất cứ sự cố nào trên trình duyệt đều có thể làm Windows trở nên bất ổn. Hậu quả thật khôn lường: nhẹ thì một ứng dụng nào đó bị "nóng lạnh", nặng thì màn hình màu xanh của Microsoft hoàn toàn chết cứng. Trong Navigator, bạn có thể nhấn <Ctrl>-<Alt>-<Delete> để gọi hộp thoại Close Program, nhưng việc này lại có thể làm cho những chương trình đang mở khác cũng trục trặc theo bởi hiệu ứng "đôminô". Cách tốt nhất là "ngậm đắng nuốt cay" khởi động lại. Riêng IE 4.x cho bạn một giải pháp khác:

Trước khi bị sự cố, hãy nhấn View .Internet Options.Advanced, kế đó đánh dấu vào hộp Browse in a new process (hình 1). Nhờ thao tác này, hệ thống sẽ mở một phiên bản IE riêng biệt chứ không nạp IE vào cùng một cửa sổ mở sẵn cho Windows. Nhờ vậy mà trong trường hợp IE 4.x lỡ có đụng núi băng lần nữa, nó sẽ không kéo Windows cùng chìm theo.

Duyệt nhanh hơn. Bằng cách đổi hai thông số trong Registry gọi là MTU (Maximum Transmission Units) trong Windows 95, tốc độ duyệt trong cả Navigator lẫn Internet Explorer sẽ tăng lên trông thấy. Nếu bạn ngần ngại lo bị mắc kẹt trong mớ bòng bong của Registry, có thể mua một tiện ích của hãng thứ ba, giá 10 USD để làm giúp bạn: MTUSpeed (www.mjs.unet .com/mike.htm).

Thu nhỏ tập tin dữ liệu. Mỗi lần bạn thăm một Web site, Internet Explorer lưu History (tức thông tin theo dõi những lần truy cập của bạn) và thông tin về cache trong những tập tin có đuôi .dat. Càng lưu nhiều, các tập tin đó lại càng phình to hơn.

Mặc dù Microsoft không ưa chuyện này, nhưng xóa các folder Cache và/hoặc History trong IE 3.x và 4.x không phải bao giờ cũng làm các tập tin đó trở lại kích thước mặc định ban đầu là 8KB, 16KB hoặc 32KB. Bạn có thể tự mình xem bằng cách mở dấu nhắc DOS (chọn Start .Programs.MS-DOS prompt) rồi tìm đến thư mục lưu cache và history (cd c:\windows\tempor~ hoặc cd c:\windows\history), sau đó tìm các tập tin có đuôi .dat. Nếu mở các tập tin đó, bạn sẽ thấy tất cả các URL mà bạn "đã xóa".

Vấn đề ở đây là gì? Không phải chỉ có đơn thuần là các tập tin có đuôi .dat này sẽ giúp những kẻ thóc mách theo dõi bạn đã đi đến đâu trên Web, mà Internet Explorer sẽ bắt đầu chạy chậm khi các tập tin này phình lên cỡ 200 KB. Và khi chúng đạt đến 500 KB, chương trình bắt đầu trục trặc. Một giải pháp là xóa cả hai tập tin, nhưng bạn phải làm việc đó trong DOS chứ không phải Windows. Nhấn Start.Shut Down.Restart in MS-DOS mode. Tại dấu nhắc C:\>, gõ deltree c:\windows\history, kế đó nhấn <Enter> (trong IE 4.x, đường dẫn là c:\windows \profiles\yourname\history). Kế đó đánh deltree c:\windows \tempoAạ1 rồi nhấn <Enter> (Việc làm này có thể mất 15 phút nếu các tập tin .dat quá lớn). Khi bạn mở trình duyệt lần sau, hệ thống sẽ tạo lại cả hai tập tin .dat này, nhưng là hai tập tin trống.

Có một cách hay hơn, nhưng tốn tiền. Bạn có thể xử lý kích cỡ tập tin và thường xuyên triệt tiêu mọi dữ liệu về cá nhân trong cache, history và các tập tin .dat bằng cách dùng chương trình TweakIE 2.0, giá 15USD (www.wizsys.com/tweakie.html). Với tính năng quét IE (IESweep), công cụ này sẽ xóa các folder cache và history rồi tái lập lại các tập tin .dat về kích thước trống. Tiện ích này cũng cảnh báo bạn khi các tập tin .dat đã trở nên đủ lớn có thể ảnh hưởng đến hiệu năng của trình duyệt.

Viết lại History. Navigator cũng duy trì một history (danh mục lưu) các site bạn thăm gần đây nhất, tuy rằng việc này không làm chậm tốc độ hệ thống. Nếu không muốn cho ai khác biết bạn đã đến những đâu, bạn phải xóa nó đi. Với Navigator 3.x, mỗi lần tắt chương trình thì history tự động bị xóa. Còn trong Navigator 4.x, bạn chọn Edit .Preferences, chọn Navigator rồi nhấn Clear History. Phiền là ở chỗ tập tin History của Netscape, cũng như các tập tin .dat của IE, đều lưu lại thông tin.

Muốn xóa hẳn dấu vết những chuyến du ngoạn trên Internet, bạn chỉ còn cách xóa tập tin này. Thoát Navigator, mở Windows Explorer rồi nhấn F3. Khi cửa sổ "Find: All Files" xuất hiện, bạn tìm tập tin netscape.hst, thường nằm ở C:\Program Files\Netscape \Communicator\Users\tên bạn. Nhấn chuột phải rồi chọn Delete.

Dùng chung cache. Nếu chạy Navigator 3.x và 4.x trên cùng một máy tính, và nếu bạn muốn thiết kế trang Web, bạn có thể tăng tốc cả hai trình duyệt và tiết kiệm không gian đĩa cứng bằng cách buộc chúng dùng chung một cache. Trong Navigator 4.x, nhấn Edit .Preferences, nhấn dấu cộng kế bên Advanced để mở rộng nó rồi nhấn Cache. Trong hộp Disk Cache Folder, gõ vào vị trí tập tin cache của Navigator 3.x (thường là c:\program files\netscape \navigator\cache). Trong Navigator 3.x, nhấn Options .Network Preferences, và trên mục Cache trong hộp Disk Cache Directory, gõ vào vị trí tập tin cache của Navigator 4.x (thường là c:\program files\netscape \users\tên bạn\cache).

Định hướng dễ dàng

Từ Windows 98 sang Web. Thậm chí dù không dùng IE 4.x hay Navigator, bạn vẫn có thể nhảy từ desktop của Windows lên Web bằng cách tạo một Address Bar (thanh địa chỉ) trong thanh tác vụ của Windows 98. Muốn mở Address Bar, bạn nhấn phím phải vào thanh tác vụ rồi chọn Toolbars, kế đó chọn Address.

Để tiết kiệm "mặt bằng" quý báu của thanh tác vụ, bạn có thể thu hẹp đến tối thiểu mọi cửa sổ mở bằng cách nhấnAddress Bar, kế đó, khi con trỏ chuột đổi thành mũi tên bốn đầu, bạn kéo thanh địa chỉ lên đầu desktop. Gõ URL bạn muốn vào thanh địa chỉ rồi nhấn <Enter>, thế là trình duyệt mặc định sẽ được tự động nạp.

Chuyển Bookmark/Favorite thành trang chủ. Bằng cách chuyển các tập tin bookmark thành trang chủ, bạn chỉ cần nhấn chuột một cái là đã vào ngay được site ưa thích nhất. Trong Navigator 3.x, nhấn Options, chọn General Preferences, kế đó dưới Browser Start With, thay địa chỉ URL bằng đường dẫn đến tập tin bookmark.htm của bạn. Trong Navigator 4.x, chọn Edit .Preferences, dưới Category chọn Navigator. Dưới "Navigator starts with", cần bảo đảm rằng nút Home Page đã được chọn (hình 2), và thay địa chỉ URL trong hộp Location bằng đường dẫn đến tập tin bookmark.htm của bạn (thường là c:\Program Files\Netscape \Users\tên bạn). Nhấn OK để đóng hộp thoại và lưu các thông số này. Thoát rồi khởi động lại Navigator, sau đó thì tha hồ đi đâu trên Web tùy ý.

Tuy nhiên, bạn không thể chuyển Favorites trong IE thành trang chủ IE, nhưng thay vào đó bạn có thể dùng các bookmark của Navigator. Mở IE 3.x hoặc 4.x, nhấn File.Open, nhấn Browse, sau đó tìm tập tin bookmark.htm của Navigator. Nhấn Open, sau đó nhấn OK. Khi các bookmark của Navigator hiển thị, nhấn View.Options, kế đó nhấn Navigation (đối với IE 3.x) hoặc Internet Options và nhãn General (đối với IE 4.x). Trong vùng Startup, nhấn Use Current rồi nhấn OK. Vậy là mỗi khi IE được tải thì Bookmark của Navigator cũng được nạp theo.

Chuyển Bookmark/Favorite thành nút bấm (button). Bạn có đặc biệt thích hai, ba site nào đó và ngày nào cũng thăm chúng không? Thay vì phải săn lùng nhiều thư mục để tìm các site đó, bạn có thể chuyển chúng thành nút trên thanh công cụ, để chỉ cần nhấn chuột là bạn truy cập được ngay. Cả IE 4.x lẫn Navigator 4.x đều có thêm một thanh công cụ mà bạn có thể mở ra đóng lại từ menu

View. Bạn có thể đặt từ sáu đến tám site lên từng thanh công cụ; nếu nhiều hơn thì thanh công cụ sẽ quá cồng kềnh và không chiều theo ý bạn nữa.

Muốn hiển thị Link Toolbar trong IE 4.x, nhấn View.Toolbars .Links. Trong IE 3.x, nhấn View.Options.General, sau đó đánh dấu hộp Links. Trên menu, nhấn Favorites rồi kéo bất cứ URL hoặc thư mục nào vào thanh công cụ Links.

Muốn mở Personal Toolbar trong Navigator 4.x, bạn nhấn View.Show Personal Toolbar (nếu Personal Toolbar đã hiển thị rồi, trên menu sẽ là Hide Personal Toolbar. Nhấn <Ctrl>-B để hiệu chỉnh các bookmark, sau đó kéo bookmark và "thả" lên thanh công cụ. Nhấn kép để kích hoạt thanh công cụ này.

Xem các Favorite dưới dạng thu nhỏ (thumbnail). Bạn đã lướt Web hàng mấy tiếng đồng hồ, tích cóp hàng mớ favorite trên IE 4.x, thế rồi bỗng bạn nhận ra mình cần tải xuống một bức ảnh có thấy trước đó nhưng đã bỏ qua. Thay vì phải nhấn dồn dập vào nút Back (trở lại) hoặc đỏ mắt tìm trong danh mục lưu (History), bạn có thể xem trước các site ưa thích dưới dạng thu nhỏ (thumbnail) mà không phải truy cập chúng, với điều kiện bạn chưa xóa cache và chưa thoát khỏi Active Desktop.

Từ Windows Explorer, nhấn Favorites.Organize Favorites, sau đó nhấn chuột phải vào thư mục mà bạn muốn xem trước. Từ menu xuất hiện, chọn Properties, đánh dấu ô Enable thumbnail view, nhấn OK rồi đóng hộp thoại Organize Favorites. Giờ bạn mở thư mục đó trong Windows Explorer, nhấn chuột phải vào khoảng trống trong cửa sổ rồi chọn View .Thumbnail. Nó đây rồi! Từ nay trở đi, muốn xem thư mục và thư mục con nào, bạn chỉ cần lặp lại quy trình này; hiển nhiên bạn không có cách nào xem tất cả cùng một lúc được.

Quay lại hoặc tiến nhanh. Cần quay lui (hoặc tiến tới) sáu trang trong lúc bạn đang rất vội ư? Chẳng việc gì phải nhấn liên tục nút Back hay Forward. Trong IE 4.x, chỉ cần nhấn vào mũi tên hướng xuống nằm bên phải nút Back hoặc Forward, bạn đã có danh mục các site mới thăm gần đây nhất. Trong Navigator 4.x, bạn có thể nhấn rồi giữ nguyên nút Back hoặc Forward là đã có danh mục tương tự, sau đó chọn site bạn cần.

Tìm kiếm nhanh. Bạn có biết trình duyệt của bạn cũng là một công cụ truy tìm rất dễ sử dụng không? Trong thanh Address của IE 3.x và IE 4.x, bạn gõ "go" hoặc "find" hoặc "?" theo sau là một dấu cách (space) và từ hoặc câu mà bạn muốn xác định, IE sẽ truy tìm Yahoo. Trong Navigator 4.x, bạn cần gõ vào thanh định vị thêm vài ba chữ nữa rồi nhấn Enter.

Nếu muốn tìm kiếm với một từ mà thôi, bạn gõ một dấu cộng và một dấu cách trước từ đó (nếu chỉ gõ một từ duy nhất mà không có dấu cộng, trình duyệt sẽ cho rằng bạn muốn vào Web site đó và tự động chêm "www." vào trước và ".com" vào sau từ đó). Navigator 4.x tìm đến công cụ tìm kiếm mặc định của Netcenter. Navigator 4.5 thì có một tính năng rất hay gọi là What's Related nâng cao khả năng tìm kiếm bằng cách đưa bạn đến nội dung liên quan có chứa từ khóa đó.

Tìm đến tận site cụ thể. Navigator 4.5 còn tiến xa hơn một bước trong việc tìm kiếm từ thanh công cụ Location. Tính năng mới Internet Keyword có thể truy tìm đến một site cụ thể. Các từ khóa được so trùng với một cơ sở dữ liệu gồm các thương hiệu, cho nên nếu bạn gõ "America Airlines" chẳng hạn, chương trình sẽ đưa bạn đến thẳng Web site của hãng hàng không Hoa Kỳ. Nếu Navigator không tìm thấy cái bạn tìm trong cơ sở dữ liệu Netcenter, nó sẽ đi đến chỉ mục Excite-Netscape Web tại Netcenter của Netscape để tìm ở đó.

Cất kỹ mật khẩu. E-mail, nối mạng qua điện thoại, kết nối LAN, và giờ đến lượt Web site - hầu như ngày nay tất tật mọi thứ đều đòi mật khẩu, và nhớ cho hết từng ấy mật khẩu thì quả là đau đầu.

Một số site sẵn sàng nhớ mật khẩu giùm bạn, nhưng không phải bao giờ chúng cũng làm được như thế. Hiển nhiên, bạn có thể viết các mật khẩu ra giấy hoặc chép chúng vào một tập tin PIM hoặc xử lý văn bản, nhưng giải pháp tốt nhất là lưu chúng trong Bookmark của Navigator 3.x hay 4.x. Nhấn <Ctrl>-B để mở menu Bookmark, kế đó nhấn chuột phải vào Bookmark cho site đang yêu cầu mật khẩu rồi chọn Properties. Hộp thoại Bookmark Properties sẽ xuất hiện; bạn có thể nhập mật khẩu hay những thông tin khác vào hộp Description (hình 3).

Dĩ nhiên, bất cứ ai đọc được mánh này (hay nhìn trộm vào hộp thoại Properties) đều có thể thấy mật khẩu. Nếu vấn đề bảo mật thực sự là hệ trọng đối với bạn, hãy thử một tiện ích loại như Password Memorizer của The Limit Software, giá 15 USD (www.limitsoft.com).

Trần Tiễn Cao Đăng
US PC World 11/1998

Những vệ sĩ trên Internet !

Bạn phải thừa nhận rằng trên máy tính của bạn đang có những file mà bạn không muốn bất cứ ai thấy: bản đánh giá năng lực nhân viên, số liệu bán hàng trong tháng, thậm chí là thư tỏ tình của một cô đồng nghiệp. Nghĩ kỹ mà xem, có thể bạn cũng có nhiều e-mail cần giữ kín nữa đó. Các thói quen của bạn khi lướt trên Web cũng vậy; thích đến site nào và xem những thứ gì là chuyện riêng của bạn chứ chẳng của ai khác, đúng không nào?

Thật không may, giữ cho mình được riêng tư thật chẳng dễ gì trong thời đại kỹ thuật số. Cho dù kẻ trộm không ăn cắp các file khỏi máy bạn, thông tin về bạn vẫn cứ rò rỉ ra ngoài mỗi khi bạn lướt trên Web. Bài "Bảo vệ sự riêng tư trên Net" trong số trước (PCWorld VN 10/1998, trang 99) đã mách một số cách bảo mật các file và hoạt động của bạn trên Web.

Trong bài này, bạn sẽ biết được những sản phẩm nào là tốt nhất cho việc triển khai kế hoạch bảo mật mới. PCW US đã thử nghiệm 28 sản phẩm bao gồm các tiện ích chống cookie (xem định nghĩa về cookie trang 66 và trong phần thuật ngữ trang 69), chống mail vớ vẩn và mã hóa thông điệp, cũng như vài công cụ bảo mật khác. Đây là những sản phẩm giúp bạn loại bỏ mọi kẻ thóc mách, tại nhà hay ở văn phòng. Nhiều thứ trong số đó chẳng có giá trị gì, nhưng bạn cũng có thể tìm được trong mỗi loại ít nhất một sản phẩm đáng để cài đặt.

Một số sản phẩm khác đang báo trước khuynh hướng ngày càng tăng trong công nghệ bảo mật: đó là sinh trắc học (biometrics). Những thiết bị này kiểm tra các số đo sinh lý học như vân tay và mống mắt của bạn rồi mới quyết định cho bạn truy cập dữ liệu hay không (xem bài "Chỉ mình bạn mà thôi" - trang 45 cũng trong số này). Trong phần "Chính cơ thể bạn là mật khẩu: tương lai của bảo mật là khoa sinh trắc học" - trang 75, bạn thấy rằng các sản phẩm bảo mật bằng sinh trắc học mới nhất trên thị trường làm việc rất tốt. Bởi vậy, hãy chuẩn bị ngay bây giờ máy tính của bạn tiếp nhận công nghệ mới này.

Đừng quá tin vào những phần mềm dùng chung (shareware)

Nhiều tiện ích bảo mật, đặc biệt là các phần mềm dùng chung (shareware) và miễn phí (free-ware) rẻ tiền, đều đáng ngờ về giá trị sử dụng. Chẳng hạn, hầu hết tiện ích chống cookie dùng thử đều chẳng bổ sung được bao nhiêu ngoài những gì Navigator và Internet Explorer xưa nay vẫn cung cấp. Nhưng có hai ngoại lệ, đó là Cookie Pal của Kookaburra Software và Anonymous Cookie của Luckman Interactive. Nhờ các sản phẩm này, bạn sẽ có thể né tránh mọi cookie (như các cookie mách lẻo mà hầu hết Web site lưu vào ổ cứng để quản lý các thói quen của bạn khi lướt trên Web).

Cũng nên coi chừng cả các tiện ích chống spam (mail vớ vẩn). Nhiều sản phẩm loại này chẳng tiệt trừ các e-mail vớ vẩn tốt hơn so với các bộ lọc cài đặt sẵn trong trình duyệt hoặc của các ISP vẫn làm. Thực tế là trong tám sản phẩm thử nghiệm, chỉ có SpamScan - sản phẩm của Webstar Image bán chạy nhất (giá 23 USD) là dễ dùng và thật sự nhổ phăng mọi e-mail vớ vẩn mà thôi.

Dù hầu hết chương trình mã hóa e-mail đều làm việc khá, PGP for Personal Privacy (40 USD, của Network Associates) vẫn tốt hơn cả trong số bốn sản phẩm xem thử. Nó tương thích với nhiều chương trình e-mail nhất và làm cho e-mail không thể đọc được với bất cứ ai ngoại trừ người nhận e-mail đó.

Nếu biết rằng dữ liệu trên máy của bạn là bất khả xâm phạm đối với kẻ thóc mách, hẳn bạn sẽ ngủ ngon hơn phải không? Thế thì có lẽ đã đến lúc nạp thêm một chương trình mã hóa file vào máy. Các gói phần mềm này "chuyển hệ" từng file, từng thư mục, thậm chí toàn bộ ổ cứng. Sản phẩm hạng nhất theo đánh giá SecureWin của Secure-Win Technologies giá 50USD, có thể mã hóa và làm được nhiều thứ nữa.

Bảo mật cho công ty

Bảo vệ dữ liệu của riêng bạn là một chuyện; nhưng nếu phải bảo mật dữ liệu của toàn bộ công ty thì sao? Hãy uống hai viên aspirin rồi đọc phần "Bảo mật tại nơi làm việc sau hàng rào kẽm gai" - trang 71, ở đó sẽ có hướng dẫn cách triển khai một kế hoạch bảo mật cho cả công ty.

Cuối cùng, nếu bạn chóng mặt bởi mớ bòng bong những thuật ngữ về bảo mật, hãy chốt lại với phần thuật ngữ trong bài.

Các phần mềm trị "Cookies"!

Bạn có thường nhận cookie từ người lạ không ? Có lẽ không, trừ khi lướt trên Web. Sau mỗi lần bạn thăm, hầu hết các site đều âm thầm tải (download) rất nhiều cookie - là những chuỗi văn bản ghi nhận các thói quen và sở thích của bạn trên Web - xuống một file trên đĩa cứng của bạn. Nhiều người dùng máy tính rất phẫn nộ với sự xâm phạm vô hình đó nếu như họ biết được.

Mặc cho cái thói xâm lấn ngang nhiên đó, hầu hết các loại cookie đều có ích. *Visitor Cookie theo dõi mọi lần bạn đến thăm một site nào đó, nhờ vậy bạn truy xuất trang đó nhanh hơn khi trở lại lần sau. Preference Cookie lưu trữ chi tiết những thông số bạn đã cài đặt cho hình ảnh hay dữ liệu trên trang đó, để khi mở lần sau, trang Web đó sẽ xuất hiện đúng ý bạn.* Còn cookie gọi là Shopping Basket ghi nhận những gì bạn mua từ catalog trực tuyến.

Nhưng cookie "theo dõi" (tracking cookie) mới là thứ khó nuốt. Được dùng chủ yếu bởi những tiêu đề quảng cáo xuất hiện trên các trang Web (thậm chí bạn chẳng cần phải nhấn vào mục quảng cáo đó), cookie theo dõi duy trì một danh sách tức thời (running list) những site bạn vừa ghé thăm. Bất cứ Web site nào mà bạn phải cung cấp thông tin về mình mới được phép đăng nhập đều có thể truy cập sau đó vào file cookie theo dõi, ghi nhận các site ưa thích và địa chỉ e-mail của bạn (bằng cách đối chiếu số ID của cookie với dữ liệu đăng nhập của bạn) rồi lấy thông tin đó mà mua đi bán lại với kẻ khác.

Với Cookie Pal, bạn nhận được thông báo lưu ý khi một Web site gửi cho bạn cookie.

Cả Netscape lẫn Internet Explorer đều cho bạn phong tỏa các cookie, hoặc tất cả hoặc từng cái một. Netscape 4.0 cũng cho phép bạn cách ly từng cookie theo dõi - cookie từ các nhà quảng cáo - để loại bỏ bằng cách chọn thông số "Accept only cookies that get sent back to the originating server (chỉ chấp nhận những cookie có thể gửi trở lại máy chủ xuất phát)". Với hầu hết người dùng, chừng đó tùy chọn cũng vừa đủ để kiểm soát cookie. Nhưng nếu bạn chẳng muốn trông cậy

vào các công cụ chống cookie cài sẵn trong trình duyệt thì sao? Hay nếu bạn không thích phải hì hụi lội qua hàng tá lời nhắc về cookie mỗi lần lướt trên Web? Dù sao, bạn không thể cấm hoàn toàn mọi thứ cookie, bởi vì nhiều site, chẳng hạn The New York Times (www.nyt.com) đòi bạn phải chấp nhận một cookie thì mới cho phép truy cập.

Chính ở đây, sản phẩm ngăn chặn cookie thứ ba có thể rất hữu ích. Nhiều tiện ích chuyên dụng kiểu này hoạt động như những bộ biên tập cung cấp giao diện thân thiện để thanh lọc file cookie của bạn. Tiện ích tốt nhất trong số đó có thể được cấu hình để tự động chấp nhận chỉ các cookie đến từ một số site nhất định, nhờ đó bạn không bao giờ phải nhấn vào hộp thoại yêu cầu chấp nhận nữa. Qua kiểm tra bảy công cụ quản lý cookie, thì hầu hết trong số đó chẳng đáng cho bạn quan tâm. Tuy vậy, hai chương trình Cookie Pal 1.2 của Kookaburra Software và Anonymous Cookie của Luckman Interactive có thể bổ sung vài tính năng hữu dụng vào trình duyệt của bạn.

COOKIE PAL 1.2

Một trong số ít các công cụ ngăn chặn cookie hữu ích nhất. Cookie Pal 1.2 nằm trong khay Windows của bạn và tự động kích hoạt ở chế độ nền bất cứ khi nào bạn vào Web. Hộp thoại kiểu tab của nó hiển thị những cookie mà bạn nhận được và cho bạn xóa từng cái một. Không như các chương trình khác, nó còn cho phép tạo những bộ lọc (filter) để chấp nhận hoặc khước từ cookie từ một số site cụ thể, cũng như xem cookie được tải xuống trong tác vụ duyệt hiện hành để bạn có thể xóa ngay lập tức. Nó lại còn kêu một tiếng "mmmm" rất dễ thương mỗi khi bạn chấp nhận một cookie. Cookie Pal 1.2: 290KB, 15 USD; Kookaburra Software; www .kburra.com, cplsetup.exe

ANONYMOUS COOKIE

Anonymous Cookie có ít tính năng hơn Cookie Pal, nhưng bù lại nó miễn phí. Với Internet Explorer, nó có thể khước từ những cookie từ các nhà quảng cáo. Anonymous Cookie hoạt động bằng cách "lừa" các site rằng nó đã chấp nhận cookie khi lưu chúng vào bộ nhớ. Kết quả là bạn có thể thoải mái vào các site xưa nay vẫn đòi bạn chấp nhận cookie rồi mới cho bạn vào, mà sau đó không phải xóa các file không mời mà đến. Anonymous Cookie; 1,4MB, miễn phí; Luckman Interactive; www .luckman.com, setupac_b2 .exe

COOKIE CRUSHER 1.6

Cookie Crusher 1.6 sử dụng nhiều tính năng hệt như sản phẩm cùng giá là Cookie Pal để chặn cookie, nhưng lại chẳng tinh nhanh được như thế. Không giống Cookie Pal, Cookie Crusher nháy sáng các hộp thoại trên màn hình rồi mới tự động đóng lại, chỉ làm ngắt quãng một cách không cần thiết (và gây bực mình). Cookie Crusher 1.6; 865KB; 15 USD, dùng chung; The Limit Software; www .thelimitsoft .com, cookie.exe

SpamScan 97 cho phép bạn chấp nhận hoặc từ chối các loại e-mail khác nhau một cách tự động thông qua trình setup wizard đơn giản.

IECLEAN 4.2 và NSCLEAN 4.10

IEClean 4.2 (cho Internet Explorer) và NSClean 4.10 (cho Navigator) là những bộ biên tập cache trình duyệt và cookie đắt tiền. Bạn cứ mua các sản phẩm này nếu muốn triệt tiêu dấu vết của mình trên Web bằng cách xóa có chọn lọc các bằng chứng bạn đã đến những đâu. Bằng không, hãy để tiền mua những thứ khác. IEClean 4.2; 934KB; 40 USD, dùng chung; ied32301 .exe; NSClean 4.10; 1MB; 40 USD dùng chung; cả hai đều của Privacy Software; IEClean 4.2; 934KB; 40 USD, dùng chung; ied32301.exe; NSClean 4.10; 1MB; 40 USD dùng chung; cả hai đều của Privacy Software; www.nsclean.com.

COOKIE CRUNCHER 2.11

Bạn chớ bận tâm đến Cookie Cruncher 2.11. Nó chỉ biết có mỗi một việc là cho bạn xem và theo dõi cookie từ ổ cứng, đó là nếu bạn cho nó chạy được (rất khó khởi động được nó). Thà cứ dùng trình quản lý file Explorer và Notepad còn hơn. Cookie Cruncher 2.11; 880KB; miễn phí; RBA Software; www .rbaworld.com, cook211.zip

BUZOF 1.4.4

Mục đích duy nhất của Buzof 1.4.4 là loại bỏ các hộp thoại pop-up, kể cả các cửa sổ yêu cầu chấp nhận cookie. Tốt hơn bạn hãy tìm một tiện ích cho phép chỉ chấp nhận một số loại cookie chọn lọc mà thôi, như là Cookie Pal (chọn lựa số một của chúng tôi). Buzof 1.4.4; 310KB; 15 USD dùng chung; Basta Computing; www.basta.com, setup buzof.exe

ANTI-COOKIE 1.0 BETA

Tuy mệnh danh là beta (bản thử), Anti-Cookie 1.0 Beta là sản phẩm hoàn chỉnh, thế nhưng về hiệu năng thì đáng ngờ hơn cả một bản tiền-alpha. Chẳng làm cách nào cho nó chạy với Netscape Navigator 4.05 được cả. Anti-Cookie 1.0 Beta; 2.9MB; 10USD dùng chung; 2Dudes.com, www .2dudes.com, cookie10.zip.

Hãy nói "không" với spam!

Mail vớ vẩn, tiếng Anh (chính xác là tiếng Anh-Mỹ, ND) là spam, nhại theo mẫu quảng cáo "thịt vai lợn băm" trứ danh của nhà Hormel, là những e-mail bạn không mong muốn, không mời mà đến.

Làm cách nào các spammer (tức nhà quảng cáo cố tình quấy rầy bạn bằng những mail quảng cáo vớ vẩn đó) tìm ra bạn? Bạn để lại địa chỉ e-mail của mình ở nhiều nơi, nhiều đến ngạc nhiên là khác. Chẳng hạn, nếu bạn đăng nhập vào một Website, đến lượt mình site đó có thể gửi mail cho bạn về các sản phẩm và dịch vụ mới nhất, hoặc bán địa chỉ của bạn cho một công ty tiếp thị (một số site cho bạn tùy chọn không nhận các mail quảng cáo, nhưng bạn rất dễ bỏ qua hộp tùy chọn nhỏ xíu đó trong khi đăng nhập vào site).

Nếu đã phát ốm với các mail vớ vẩn, hãy đánh lại chúng. Một số khách hàng và phần mềm e-mail (như Eudora, Outlook và America Online - AOL) có cả những bộ lọc đặc biệt chuyên trị mail vớ vẩn, nhưng các ứng dụng thứ ba thì có khả năng tùy biến nhiều hơn. Hầu hết bộ lọc của khách hàng (client) kết hợp những từ hay dùng nhất trong tiêu đề của các mail vớ vẩn (như "tự do", "làm giàu chớp nhoáng", "XXX", "sex"...) kèm theo địa chỉ các spammer khét tiếng. Một phần mềm trị spam tốt còn có thể tăng cường sự bảo mật này bằng cách cho phép bổ sung thông tin. Chẳng hạn, một số sản phẩm cho bạn tùy ý lập danh mục các địa chỉ cần phong tỏa hoặc được phép của riêng bạn.

SecureWin hỗ trợ việc mã hoá tập tin, folder và đĩa, cũng như đưa ra nhiều đặc tính hữu ích và độc đáo.

Khi thử nghiệm, người ta thiết lập một account e-mail giả, cài đặt riêng rẽ tám chương trình lọc mail rồi gửi đến địa chỉ của chính nơi thử nghiệm mười thông điệp vớ vẩn điển hình (kiểu như "Bạn có cần nhiều tiền hơn không ?"). Kết quả cho thấy nhiều tiện ích lọc mail thuộc loại add-on (thêm vào) đều vô hiệu, và hầu hết chúng không thể hoạt động trên những chương trình e-mail riêng không thuộc chuẩn Internet, chẳng hạn AOL và Lotus Notes. Tuy nhiên, có hai chương trình rất hay, đó là SpamScan97 của Webster Image và Spam Buster 1.4 của Contact Plus.

SPAM SCAN97

Spam Scan97 loại bỏ dễ dàng các mail vớ vẩn. Nó tóm cổ từng thông điệp ba láp được gửi tới. Đây là chương trình trị spam dễ thiết lập và sử dụng nhất. Spam Scan97 cho bạn một danh mục các từ khóa (keywords, tức các từ hay dùng nhất) trong các mail vớ vẩn cũng như các domain "cấm", và bạn có thể bổ sung những địa chỉ ưa thích hoặc "địa chỉ cấm" và "từ cấm" của riêng bạn vào đó. Thế lỡ mình cấm cửa luôn những thông điệp đường đường chính chính thì sao? Bạn có thể lập những bộ lọc để chỉ định khi nào thì khước từ thẳng thừng một thông điệp còn khi nào cho phép ngoại lệ. Spam Scan97; 2,19MB; 23 USD dùng chung; Webster Image; webster-image .com; scan97.zip.

SPAM BUSTER 1.4

Cũng như Spam Scan97, Spam Buster kiên quyết chặn đứng mọi e-mail linh tinh. Nó có thể quét các thông điệp e-mail trước khi bạn mở chương trình mail, hoặc bạn cũng có thể mở mail ngay trong Spam Buster sau khi nó đã xóa sạch các thông điệp không mong muốn. Spam Buster dựa trên một danh mục chừng 15.000 địa chỉ chuyên gửi mail vớ vẩn mà bạn có thể điều chỉnh bằng các thông số của chính bạn cũng như có thể cập nhật miễn phí qua Website của công ty (sau khi bạn đăng nhập). Tuy nhiên, người mới dùng có thể gặp khó khăn trong việc tìm một số chức năng trong giao diện khá rối rắm của Spam Buster. Spam Buster 1.4; 1.1MB; 20 USD; dùng chung; Contact Plus; www .contactplus.com; spam-bu32.zip

MAILJAIL 2.3

Là tiện ích bổ sung cho Eudora và Microsoft Outlook 97, MailJail cũng tóm được tất cả thông điệp vớ vẩn, nhưng nó thận trọng quá mức cần thiết. Thay vì tự động xóa các thông điệp ngờ là quảng cáo vớ vẩn, nó lại lưu các mail này vào một thư mục riêng để sau đó bạn phải duyệt lại và xóa từng cái một. Mặc dù cách này bảo đảm chỉ mail nào đáng xóa thì mới bị xóa, nhưng lại mất quá nhiều thời gian. MailJail 2.3; 20 USD dùng chung; Omron Advanced Systems; www .mailjail.com

SPAMKILLER 1.6

Phải lấy làm buồn mà nói rằng SpamKiller 1.6 chẳng tàn nhẫn như tên của nó (killer, kẻ giết người, kẻ tàn sát). Nó sử dụng những quy tắc có sẵn (và những quy tắc bạn thêm vào) để quyết định sẽ đánh dấu các thông điệp để xóa sau hoặc xóa lập tức. Nhưng SpamKiller hiếm khi bóp cò ngay cả với các mail vớ vẩn hiển nhiên nhất. Trong số mười thông điệp thử nghiệm, nó tóm được có ba, mà cũng chỉ đánh dấu thôi. Spam-Killer 1.6; 1,7 MB; 30 USD dùng chung; www.spamkiller.com; sk161.exe

SPAM EXTERMINATOR 3.2

Spam Exterminator 3.2 lớn tiếng rằng có một danh mục đồ sộ địa chỉ các nhà quảng cáo linh tinh (spammer) - tới 17.500 cái - chưa kể bạn còn có thể có nhiều hơn nhờ thường xuyên cập nhật

từ Web. Thế nhưng nó chỉ tóm được ba trong mười mail thử nghiệm, thật quá tệ. Nhưng chưa hết: thiết lập Spam Exterminator rất tốn thì giờ bởi có quá nhiều nút và tab. Spam Exterminator 3.2; 1,5MB; 28USD dùng chung; Unisyn Software; www.unisyn .com, sxsetup.exe

SPAMMERSLAMMER

SpammerSlammer không tự động xóa các thông điệp vớ vẩn. Thậm chí nó chẳng thèm giam mấy thông điệp đó lại nữa! Thay vào đó, nó gắn vào mỗi thông điệp một cái nhãn để tùy bạn quyết định diệt ngay hay để đọc kỹ lại đã. Hơn nữa, Spammer-Slammer chỉ bắt được mỗi hai trong số mười mail thử nghiệm. SpammerSlammer; 1.4 KB; miễn phí; Now Internet Tools; www.spammerslammer.com., spammerslammer.exe.

EFILTER 2.0

Khi thử cài đặt lần đầu, EFilter 2.0 suýt nữa quậy nát máy tính thử nghiệm. Còn khi thử lần thứ hai, nó đưa ra một thông điệp lỗi kỳ bí. Rốt cuộc, cũng khởi động được, nó lại cho qua hết chín trong số mười thông điệp ba láp. Giá cả thì khỏi bàn. EFilter 2.0; 2,64 MB; miễn phí (bản Pro 12 USD); TSW; www.eflash.com., filt262 .exe

SPAM HATER

Spam Hater có thể phát hiện spam, nhưng chuyển ý kiến thành hành động lại chẳng tốt cho lắm. Thật ra, nó hoàn toàn chẳng phong tỏa các mail vớ vẩn, đúng hơn nó chỉ phân tích các tiêu đề thông điệp sau đó gửi mail than phiền vào địa chỉ hồi đáp đã chỉ định. Thế nhưng hồi đáp spam - thậm chí còn mở chúng - chỉ có nghĩa là xác nhận địa chỉ e-mail của bạn và bật đèn xanh cho nhà quảng cáo chuyên quấy rầy cứ thế tiếp tục quấy rầy bạn. Spam Hater; 806KB; miễn phí; Net Services; www.cix.co.uk/net-services/spam/spam_hater .htm, spamh .exe.

Khuất phục những kẽ nghe lén trên net !

Mỗi ngày có hàng triệu người sử dụng e-mail để chia sẻ thông tin cá nhân - nào lương lậu, nào mật khẩu, ca cẩm về ông xếp - mà không nhận thức mối nguy cho quyền riêng tư của họ. Bất kỳ ai thao túng được e-mail của bạn - từ người quản lý máy chủ cho đến một tay quậy (hacker) - đều có thể đọc nó. Bạn làm sao tự vệ đây? Một chương trình mã hóa e-mail sẽ giấu thông điệp của bạn khỏi những con mắt cú vọ bằng cách "chuyển hệ" văn bản thường thành một mớ mật ngữ rắc rối mà chỉ người nhận e-mail mới giải mã được.

Nếu công ty bạn tiến hành kinh doanh trên Internet, có lẽ bạn cũng nên ký mọi e-mail của mình bằng chữ ký số. Một chữ ký số sẽ bảo đảm cho người nhận rằng thông điệp này là của chính bạn chứ không ai khác, hoàn toàn loại trừ khả năng một tên lừa đảo hay tội phạm có thể mạo danh bằng cách làm giả địa chỉ e-mail của bạn. Một thông điệp có chữ ký số cũng có tác dụng ràng buộc pháp lý như hợp đồng được ký bằng tay vậy.

Bạn có thể dùng một chương trình e-mail với quy cách mã hóa S/MIME (Secure Multipurpose Internet Mail Extensions) để mã hóa và ký bằng số các thông điệp; nhưng có qua có lại: bạn phải trả một khoản lệ phí cho S/MIME để mua bộ khóa thường trực cho chính mình. Và trong những lần triển khai trước đây, S/MIME không phải bao giờ cũng làm việc tốt. Nói đơn giản là e-mail được mã hóa với S/MIME bằng một số phiên bản của Netscape Messenger không phải bao giờ cũng có thể giải mã bằng các phiên bản của Microsoft Outlook chẳng hạn. Dù hiện nay, Netscape và Microsoft tuyên bố S/MIME có thể làm việc một cách hoàn hảo giữa các phiên bản ứng dụng mới nhất của họ, bạn vẫn có thể sẽ có rắc rối với S/MIME nếu gặp những chương trình e-mail cũ hơn.

Những biểu tượng đơn giản của PGP for Personal Privacy cho phép bạn nhanh chóng thực hiện mã hóa e-mail và kiểm chứng.

Để bảo vệ e-mail của bạn trước những kẻ thóc mách, hãy mua một chương trình mã hóa thứ ba. Khác với trình duyệt có những khóa giải mã riêng nên bạn không cần phải mua từ bên thứ ba nào nữa. Một lợi điểm khác: nếu bạn và người bạn gửi e-mail có cùng phần mềm mã hóa, thậm chí bạn chẳng cần dùng cùng một chương trình e-mail với người đó nữa.

Các tiện ích độc lập còn ăn đứt chương trình mã hóa e-mail cài sẵn trong trình duyệt nhờ hiệu quả bảo mật cao hơn. Các chuyên gia mã hóa tuyên bố rằng e-mail được tạo bằng bộ mã hóa 40-bit (là thứ mà trình duyệt cung cấp) có thể bị tháo tung bởi một phòng vi tính trường trung học trong vòng vài tiếng đồng hồ. Cũng theo các chuyên gia đó, phải "đến ngày tận thế" may ra một phòng vi tính trường trung học mới có thể bẻ khóa một file được mã hóa nhờ các khóa 128-bit. Tất cả các gói phần mềm được kể ở đây đều cung cấp bộ mã hóa ít nhất 40-bit. Nhưng vài cái trong đó - kể cả PGP for Personal Privacy: sản phẩm hay nhất - có thể mã hóa e-mail bằng các khóa dài đến 4096 bit, một mức độ toán học phức tạp đến mức làm cho e-mail thực sự không thể phá vỡ nổi.

PGP for Personal Privacy có thể làm việc với bất cứ chương trình và loại ứng dụng e-mail nào khác, thêm một lý do tại sao so với các phần mềm mã hóa khác, nó bán đắt như tôm tươi. Bạn chỉ cần chọn rồi sao chép đoạn văn bản muốn mã hóa. PGP là tùy chọn mã hóa tốt nhất để dùng với AOL hoặc trong một hệ thống e-mail văn phòng như Lotus Notes. Còn các tiện ích khác chỉ làm việc với những phần mềm e-mail dựa trên Simple Mail Transfer Protocol for Internet e-mail (giao thức chuyển mail đơn giản đối với e-mail trên Internet).

PGP FOR PERSONAL PRIVACY

Để giữ kín thông tin điện tử của bạn, lựa chọn hàng đầu là PGP For Personal Privacy. Trong bốn chương trình thử nghiệm, nó dễ cài đặt và sử dụng nhất. Hơn nữa lại miễn phí nếu không dùng vào mục đích kinh doanh (để sử dụng trong kinh doanh, bạn phải trả 40 USD cho Network Associates). Giống như các gói phần mềm khác đã nói ở đây, PGP cũng dùng phương thức mã hóa bằng khóa công cộng/khóa cá nhân (xem phần thuật ngữ). Muốn gửi e-mail riêng cho một người dùng PGP khác, bạn phải có khóa công cộng của người đó. Nếu có (người ta thường kèm thêm khóa công cộng của mình vào cuối thông điệp e-mail), bạn có thể sao và dán nó vào cửa sổ PGPKeys. Chương trình PGPKeys cũng cho bạn truy tìm những máy chủ đặc biệt trên Internet có chứa các khóa công cộng của bất cứ người nào gửi tới. Khi tìm thấy khóa công cộng cần thiết, bạn chỉ cần chọn nó từ danh mục rồi nhấn nút Add.

PGP làm việc với bất cứ chương trình nào. Việc mã hóa thật quá dễ: chỉ cần đánh dấu (highlight) văn bản, sao chép rồi nhấn vào biểu tượng PGP trên khay hệ thống. PGP sẽ mã hóa hoặc ký bằng chữ ký số bất cứ văn bản nào trên clipboard. PGP for Personal Privacy; 40 USD (cho tổ chức kinh doanh); Network Associates; www.nai .com.

RPK INVISIMAIL

Nếu bạn dùng Eudora của Qualcomm, Outlook hay Exchange của Microsoft hoặc Messenger của Netscape, RPK InvisiMail là một tùy chọn mã hóa đáng cho bạn để mắt tới. RPK InvisiMail quản lý tất cả thông điệp e-mail đến và đi của bạn, mã hóa và giải mã chúng trong nháy mắt. Mọi việc đều tự động: RPK InvisiMail duy trì một danh mục tức thời khóa công cộng của những người dùng InvisiMail khác bằng cách quét tiêu đề từng thông điệp gửi đến. Sau này, khi bạn gửi thông điệp đến cùng địa chỉ đó, chương trình sẽ mã hóa e-mail bằng khóa công cộng thích hợp. Đến lượt mình, RPK InvisiMail chèn khóa công cộng của bạn vào tiêu đề các thông điệp gửi đi. Và trên hết, chương trình này không gây lộn xộn cho hệ thống của bạn (như Mailguardian, sẽ bàn dưới đây). RPK InvisiMail; miễn phí; Invisi-Mail, www .invisimail.com.

MAILGUARDIAN

Mailguardian cũng bảo vệ những chương trình e-mail hệt như InvisiMail. Nhưng có họa là điên mới bỏ InvisiMail mà chọn Mailguardian. Mailguardian xem chừng không ổn định bằng (đã mấy lần nó phá hỏng Eudora), lại đắt tiền (69 USD, trong khi InvisiMail và PGP miễn phí); và mã hóa chậm hơn; dữ liệu nghèo nàn hơn. Mailguardian; 69 USD; Vanguara Security Technologies; www .vguard.com.

WORLDSECURE CLIENT

WorldSecure Client tích hợp khá trơn tru với Eudora, Outlook và nhiều ứng dụng e-mail khác nữa. Nó vận hành cũng tương tự các chương trình kia, nghĩa là tự động nhận diện khóa của những người khác kèm trong thông điệp gửi đến cho bạn và mã hóa văn bản một thông điệp e-mail gửi tới ai đó trong cơ sở dữ liệu. Tuy nhiên, ứng dụng này gây khó chịu với hộp thoại "OK to continue" (có tiếp tục không?) liên tục bất tận trong khi bạn thao tác trên mail. WorldSecure Client; 90 USD; www.worldtalk .com.

Khóa kỹ file và folder của bạn !

Đã bao nhiêu lần bạn đi ăn trưa mà vẫn để máy chạy? Hay đã bao nhiêu lần bạn rời văn phòng vào chiều thứ sáu mà không khóa cửa? Thậm chí dù bạn khóa kỹ máy lại, một ai đó vẫn có thể đọc hay sao chép những file quan trọng của bạn. Nếu bạn lo rằng những kẻ lạ mặt có thể đột nhập vào máy của mình, một chương trình mã hóa file có thể giúp bạn ăn ngon ngủ yên.

Cũng như các chương trình mã hóa e-mail, phần mềm mã hóa file bảo vệ các thông tin nhạy cảm bằng cách "chuyển hệ" nó sao cho thậm chí một tên ăn cắp đĩa cứng trang bị bằng công cụ phục hồi file cũng không đọc nổi. Người ta đã xem thử tám phần mềm mã hóa và giải mã từng file, từng thư mục hay toàn bộ đĩa cứng. Món tốt nhất theo đánh giá là Secure Win của SecureWin Technologies, một bộ công cụ hùng hậu để mã hóa và những tính năng bảo mật khác nữa.

SECURE WIN

Bạn không thể kiếm ra phần mềm nào khác với khả năng bảo mật dữ liệu hoàn hảo hơn với cùng một giá tiền như Secure Win. Nó cung cấp nhiều công cụ, từ những thư mục mã hóa dễ sử dụng cho đến chữ ký số, thậm chí những tính năng xóa dữ liệu hệt như trong phim trinh thám vậy. Cũng như Norton Yours Eyes Only của Symantec và Security 98 của Encore Software, Secure Win cho bạn tạo những thư mục mã hóa đặc biệt trong Windows Explorer. Chỉ cần kéo file mà bạn muốn mã hóa vào thư mục đó, thế là nội dung của file sẽ tự động được mã hóa. Nếu là kẻ đa nghi cỡ Tào Tháo, bạn sẽ rất hài lòng với Secure Delete. Là công cụ điện tử tương đương với máy hủy hồ sơ, Secure Delete ghi đè lên các file đã xóa bằng những số 0 liên tục khiến cho công cụ phục hồi file không thể nào đọc được. Tính năng thông dụng nhất của Secure Win là Self Destruct: Bạn chỉ cần ấn định tiêu chuẩn (chẳng hạn nhập sai mật khẩu 10 lần trong cùng một dòng), chương trình sẽ tự động xóa những file chỉ định nếu một kẻ đột nhập khởi hoạt được nó. Hẳn không cần nói thêm rằng bạn cần sao dự phòng các file được bảo mật bằng cách này. Secure Win; 50USD; Secure Win Technologies; www. *securewin.com.*

SECURPC 2.0

SecurPC đem lại nhiều tính năng tinh vi cho người dùng có đẳng cấp, nhưng ngay cả lính mới cũng có thể học dùng rất nhanh. Trong những khả năng hữu ích nhất của nó có tính năng chuyển các file đã mã hóa thành những vi chương trình (miniprogram) tự giải mã, một đặc tính rất tiện lợi nếu bạn muốn chia sẻ các file này với người khác. Nhược điểm duy nhất: người nhận phải dùng một mật khẩu do bạn cung cấp để truy xuất nội dung, do vậy gọi là bảo mật nhưng về khía cạnh

nào đó lại có nguy cơ để lộ khóa giải mật. SecurPC 2.0; 59 USD; Security Dynamics; www.securid .com.

SECURITY 98

Nếu bạn cần tiện ích mã hóa đơn giản mà lại không có chương trình chống virus nào, Security 98 sẽ là một giải pháp tốt. Nó là một trong những gói phần mềm rẻ tiền nhất và lại có thể chống virus, tính năng tưởng sẽ gặp trong Norton Your Eyes Only của Symantec. Tuy nhiên, nếu đã cài đặt một ứng dụng chống virus khác trong máy, nó có thể xung đột với chương trình cài sẵn của Security 98. Security 98; 39USD; Encore Software; www.encoresoftware .com.

DATASAFE ENCRYPTION

DataSafe Encryption là chương trình căn bản dễ sử dụng có cùng tính năng như SecurPC: nó có thể tạo những file tự giải mã, do đó là một lựa chọn khó bỏ qua nếu bạn muốn chia sẻ các file đã mã hóa với người khác (muốn giải mã các file, người nhận chỉ cần một mật khẩu). DataSafe cũng có thể nén file, nhưng nó làm việc này quá chậm. DataSafe Encryption; 40 USD; Nova Store; www.novastor.com.

ENTRUST/SOLO

Bạn muốn cho một số người trong công ty được quyền truy cập một file tối mật nhưng sau đó theo dõi xem họ sửa gì trong đó? Entrust/Solo là thứ duy nhất trong các chương trình giới thiệu ở đây làm được việc này. Nó tạo nhiều mật khẩu sao cho có thể kiểm soát mọi hành vi của nhiều người dùng khi cùng mở một file mã hóa (một file trên mạng chẳng hạn).

Đây là một trong hai chương trình (cùng với Secure Win) cho bạn ký tên vào file mã hóa bằng chữ ký số. Entrust/Solo; 49USD; Entrust Technologies; www.entrust.com.

NORTON YOUR EYES ONLY 4.1

Do có quá nhiều giao diện và thiết kế hơi thiên về kỹ thuật, Norton Your Eyes Only giống một lô phụ tùng bay thành đội hình hơn là máy bay lắp ráp hoàn chỉnh. Vì thế nó trông thật rối rắm, nhưng đâu chỉ có vậy, hầu hết tính năng của nó - như thư mục mã hóa nhanh, máy hủy giấy, giám sát việc sửa đổi file mã hóa - cũng chính là những tính năng bạn có thể gặp ở các chương trình khác chỉ rẻ bằng phân nửa. Norton Your Eyes Only; 75 USD; Symantec; www.symantec.com.

KREMLIN ENCRYPTION SECURITY SUITE 2.21

So với một ứng dụng mã hóa file thì Kremlin Encryption Security Suite 2.21 khá rẻ, nhưng ngoài mã hóa file ra nó chỉ biết mỗi việc nén file, trong khi bạn có thể làm việc này bằng một tiện ích miễn phí, chẳng hạn PKZip. Bạn bỏ ra thêm 15USD mua Secure Win thì hơn, vì ngoài nén file Secure Win còn nhiều tính năng khác nữa. Kremlin Encryption Security Suite 2.21; 35 USD; Mach5 Software; www.mach5.com/kremlin.

ENCRYPT-IT

Encrypt-It đắt nhất so với mọi chương trình khác ở đây. Ngoài mã hóa, Encrypt-It biết hủy dữ liệu bằng một công cụ giống như Secure Delete; nhưng các tính năng của nó cũng chỉ có thế. Encrypt-It; 89USD; Mae Dae Enterprises; www.maedae .com.

Trần Tiễn Cao Đăng
PC World US 9/1998

Thuật ngữ !

Dưới đây là các thuật ngữ bạn cần biết để cập nhật với ngôn ngữ dùng trong vấn đề bảo mật thường rất bí hiểm và rắc rối.

AUTHENTICATE (xác minh): kiểm chứng xem người đang tìm cách gửi thông điệp hay truy cập dữ liệu có đúng là người mà anh ta (chị ta) tự xưng không.

authorize (trao quyền): cho hoặc không cho phép ai đó truy cập dữ liệu hay hệ thống. Triển khai kiểm soát việc trao quyền thường là bước đầu tiên và cơ bản nhất trong một hệ thống bảo mật.

BIOMETRICS (sinh trắc học): là việc sử dụng các đặc điểm sinh lý như dấu tay hoặc nét mặt để xác minh một người dùng.

CIPHERTEXT (văn bản mã hóa): là nội dung một thông điệp hoặc file đã được mã hóa, không thể đọc được.

COOKIE: là một nhóm văn bản mà Website đặt vào một file trên đĩa cứng của bạn sau khi bạn thăm site đó. Cookie dùng để nhận diện khi bạn truy cập site đó lần sau.

DECRYPT (giải mã): là chuyển văn bản từ dạng mã hóa sang dạng thông thường có thể đọc được.

DIGITAL CERTIFICATE (chứng minh thư kỹ thuật số): là dữ liệu (thường là văn bản) được một người dùng để mã hóa hoặc ký vào thông điệp gửi cho người khác. Còn gọi là khóa công cộng (public key), gồm có tên người dùng, địa chỉ e-mail và một khóa mã hóa.

DIGITAL SIGNATURE (chữ ký số): là dữ liệu bằng văn bản - thường được thêm vào phần chính của một thông điệp e-mail - mà người nhận có thể dùng để xác minh (authenticate) người gửi có đúng là người có tên đó không.

ENCRYPT (mã hóa): là chuyển dữ liệu thành mã riêng.

FIREWALL (bức tường lửa): là một máy tính với phần mềm đi kèm, dùng để ngăn chặn người ngoài truy cập trái phép vào một mạng máy tính riêng.

PASSWORD (mật khẩu): là một loạt chữ số, chữ cái hoặc cả hai, có tính riêng biệt và đơn nhất, cho phép người dùng truy cập dữ liệu. Một mật khẩu dài được gọi là mật ngữ (passphrase).

PRIVATE KEY (khóa cá nhân): là một tệp dữ liệu gắn liền với một cá nhân duy nhất, dùng để giải mã các thông điệp được mã hóa trước đó bằng khóa công cộng (public key) cũng của người đó.

PUBLIC KEY (khóa công cộng): là tệp dữ liệu gắn liền với một người cụ thể, nhưng các cá nhân khác có thể dùng để gửi thông điệp mã hóa cho người đó. Bởi khóa công cộng không chứa những thành phần cần thiết để giải mã thông điệp, ta có thể cung cấp chúng cho người khác mà không ngại gì.

SPAM (mail vớ vẩn): là một e-mail dấm dẳng, nhũng nhiễu, không mời mà đến, thường do các nhà quảng cáo gửi tới.

Bảo mật tại nơi làm việc sau hàng rào kẽm gai !

Đọc những chuyện trên báo chí gần đây, một công ty có thể cho rằng không ai gây hại đến an toàn dữ liệu của họ hơn một gã thích chu du trên Web nào đó. Các hacker (tay quậy) quả thật là mối đe dọa về bảo mật đối với công ty, nhưng nhìn tổng thể đó chỉ là những nhân vật phụ mà thôi. Nếu công việc của bạn là bảo vệ cho hệ thống của công ty luôn bất khả xâm phạm, dưới đây là năm bước cần tiến hành để có thể bảo mật tối đa hệ thống của bạn.

1. Lập chính sách

Ưu tiên số một phải là thiết lập chính sách bảo mật cụ thể. Ngoài những nội dung khác, chính sách này phải xác định mục tiêu bảo mật của công ty là gì. Thông thường, các mục tiêu đó gồm ngăn chặn ăn cắp thiết bị, tiết lộ thông tin mật và bảo đảm hoạt động liên tục. Nhu cầu bảo mật của một ngân hàng chẳng hạn rất khác so với nhu cầu bảo mật của một công ty chuyên về công cụ truy tìm trên Web.

2. Bảo vệ máy tính của bạn

Đề phòng việc mất một bộ RAM hay con chip CPU đắt tiền là mối lo chính của các doanh nghiệp có nhiều máy tính. Những máy tính đặt ở nơi nhiều kẻ ra vào đặc biệt dễ bị chiếu cố vì sự giám sát khi có khi không, nhưng bạn có thể giảm bớt phần nào rủi ro nếu dùng các khóa và nhãn ID.

Hầu hết máy tính xách tay đều có rãnh khóa ở panel sau dùng để khóa bằng cáp. Để cắt được cáp của công ty Kensington Microsaver, kẻ cắp sẽ không thể không làm hỏng nặng chính cái máy (và thế là máy chẳng còn giá trị gì trên thị trường nữa).

STOP (Security Tracking of Office Property) bán những nhãn dính (sticker) (bán lẻ 25USD/chiếc, nếu mua nhiều thì 8,25USD/chiếc); các nhãn dính này gồm một mã số ID và một số điện thoại để gọi trong trường hợp tìm thấy máy tính bị thất lạc hoặc ăn cắp). Bạn dán nhãn dính này vào máy tính; nếu có ai gỡ ra, nó sẽ để lại một "vết xăm" trên máy không thể nào xoá nổi. Kensington MicroSaver; 25-50USD bán trong cửa hàng; Kensington; www .kensington.com; * Stop Plates: 8,25 đến 25USD theo list; STOP; www .stoptheft.com.

3. Kiểm soát truy cập máy chủ

Sau khi bảo đảm bọn ăn cắp không thể rớ tới máy tính của bạn, cần tập trung vào bảo vệ dữ liệu chứa trong các máy tính đó.

Công cụ hữu ích để bảo vệ mạng là SecurID, một máy tính vừa đúng bằng chiếc thẻ tín dụng có màn hình tinh thể lỏng. Cứ mỗi phút, một mã số khác nhau lại "phóng ra" (pop-up) trên màn hình "thẻ" này. Muốn truy cập máy chủ, người dùng phải nhập tên người dùng và mật khẩu chuẩn cũng như nhập đúng mã SecurID. SecurID; giá thay đổi; Security Dynamics; www.securid.com.

4. Mã hóa dữ liệu quan trọng

ý tưởng "mã hóa" thường gợi nhớ về hoạt động tình báo thời chiến tranh lạnh, với những điệp viên bí mật khoác măngtô kín mít. Nhưng trong thực tế doanh nghiệp, việc mã hóa dữ liệu có thể bảo vệ công ty trước nguy cơ thông tin bị tuồn ra ngoài một cách trái phép.

Cũng như với e-mail và file, bạn có thể bảo vệ thông tin mật trên một máy chủ Web bằng cách mã hóa. Nếu công ty bạn chạy intranet và phần mềm Web server có thể mã hóa dữ liệu, bạn hãy đổi mọi URL thành https: thay vì http: - việc này sẽ khởi hoạt chương trình mã hóa cài sẵn trong

các trình duyệt Web và bảo đảm rằng bất cứ dữ liệu nào gửi từ máy chủ sang trình duyệt và ngược lại đều không thể đọc được đối với người ngoài.

5. Phát triển hệ thống sao lưu

Mọi hệ thống phức tạp chẳng sớm thì muộn rồi cũng hỏng; do đó bạn nên sao lưu dự phòng hệ thống mạng cũng như dữ liệu. Tháng Năm vừa qua, khách hàng của PageNet mất dịch vụ nhắn tin (paging) trong suốt bốn ngày khi vệ tinh Galaxy IV bị hỏng trên quỹ đạo. Ngược lại, khách hàng của Sky Tel, đối thủ lớn nhất của PageNet, vẫn được phục vụ thông suốt. Lý do: Sky Tel có hệ thống dự phòng thừa sức vận hành không lúc nào ngừng nghỉ.

Một lĩnh vực người ta hay khinh thường trong bảo vệ dữ liệu là nguồn điện của tòa nhà. Nếu mất điện trong vòng 10 giây, công ty bạn sẽ mất bao nhiêu dữ liệu? Không chỉ mua một UPS cho mỗi máy chủ, bạn phải bảo đảm mỗi người trong công ty đều có một cái. Hầu hết nhân viên đều rất lơ là trong việc sao lưu thường xuyên các file trong ổ cứng của mình.

Cách tốt nhất với công ty lớn để phòng tránh sự cố hệ thống toàn công ty là xây dựng hệ thống dự phòng tại một địa điểm khác. Địa điểm đó phải có máy tính đủ mạnh, dung lượng đĩa lớn và được nối kết mạng để có thể thay thế mạng chính. Mạng dự phòng này phải được trao đổi dữ liệu thường xuyên với file server sao cho các file trong mạng dự phòng luôn được cập nhật kịp thời để khi cần có thể chuyển ngay qua mạng dự phòng.

Chính cơ thể bạn là mật khẩu !
Tương lai của bảo mật sinh trắc học !

Chắc rồi sẽ đến ngày máy tính nhìn thẳng vào mắt bạn - theo nghĩa đen - để biết bạn là ai. Cũng như cảnh sát dùng dấu tay để kiểm chứng nhân thân một người, các nhà sản xuất máy tính đang sử dụng sinh trắc học (biometrics) - một khoa học đo lường các đặc tính sinh lý như mống mắt, dấu tay, nét mặt, thậm chí thiết diện DNA - để bảo mật hệ thống tốt hơn.

Các bộ phận cơ thể

Bảo mật bằng sinh trắc là thế nào? Đặc điểm sinh lý của bạn - màu của mống mắt chẳng hạn - được ghi nhận bằng một bộ đọc (reader) rồi lưu vào cơ sở dữ liệu. Để nhận diện, hệ thống sẽ đối chiếu đặc tính sinh lý của người xin truy cập với dữ liệu lưu trữ này. Nếu xác minh được rằng bạn đúng là người được xưng tên, nó sẽ cho phép truy cập.

Có lẽ không may rằng không phải bộ phận nào trên cơ thể ta cũng có thể phục vụ cho mục đích này. Để làm ký hiệu sinh trắc, bộ phận cơ thể đó phải đo được một cách chính xác và là độc nhất không lẫn với ai, không thay đổi theo thời gian - trọng lượng của bạn chẳng hạn thì chẳng giúp được gì. Và một số ký hiệu sinh trắc có độ tin cậy cao hơn, một số khác đáng ngờ hơn, có thể sai lệch theo chiều dương (nghĩa là cứ tưởng đúng nhân dạng nhưng lại cho qua một kẻ mạo danh), hoặc chiều âm (tức là cấm cửa mặc dù kẻ tự xưng A quả là anh (chị) A thật). Giọng nói cho độ tin cậy cao, có thể nhận diện đúng trong 90 đến 99% trường hợp. Những ai ủng hộ các hệ thống nhận diện theo dấu tay bảo rằng chúng không thể lầm, thế nhưng vân tay người ta có thể bị mòn bởi chính công việc họ làm là gõ trên bàn phím. Nhận diện qua khuôn mặt thì đặc biệt mới và hãy còn "chập chờn". Một sản phẩm nhận diện qua khuôn mặt là Facelt PC 3.0 của Visionic (giá 100USD) trước sau như một đều không nhận ra người thử nghiệm.

Dẫu vậy, việc sử dụng sinh trắc ngày càng trở nên phổ biến. Trên thị trường hiện có những sản phẩm giá từ 300 đến 5000 USD, nhưng tương lai sẽ xuất hiện những sản phẩm vừa túi tiền bạn hơn. VeriVoice Internet Security System chẳng hạn, dùng microphone và card âm thanh chuẩn của máy bạn, cộng với một nối kết trình duyệt để nhận diện qua giọng nói trên Web. Trong một lần thử nghiệm, công nghệ này hoạt động suôn sẻ, tuy vậy cả quá trình đăng nhập lẫn giao diện

người dùng vẫn cần hoàn thiện thêm. Trong khi đó Digital Persona (www .digitalpersona .com) lại tung ra U.are.U giá từ 150 đến 190USD, một phần mềm bao gồm bộ đọc dấu tay cắm vào cổng USB (xem hình) và phần mềm hỗ trợ. Khi thử nghiệm một trong các phiên bản mẫu của sản phẩm này, Digital Persona tỏ ra dễ thiết lập và dễ sử dụng, nhưng quan trọng nhất là độ tin cậy cao. Facelt PC 3.0; 100USD; Visionics; www .facelt.com * VeriVoice Internet Security System; giá tùy theo số người dùng; VeriVoice * U.are.U; từ 150 đến 190USD (tùy theo ứng dụng được dùng); Digital Persona; www.digital persona.com.

Tiếp xúc bằng mắt

Một trong những công nghệ sinh trắc hứa hẹn nhất - nhưng cũng rắc rối nhất - hiện nay là đo kích cỡ và màu sắc tròng mắt của bạn. Là sản phẩm của IriScan, hệ thống này tạo một thiết diện (profile) chi tiết cho từng nhãn cầu mà nó quét. Công ty tuyên bố mức độ tin cậy của sản phẩm này vượt qua bất cứ hệ thống sinh trắc nào khác. Mặc dù nếu để sử dụng cho cá nhân thì còn quá đắt, công nghệ này đang ngày càng xuất hiện nhiều trong các công ty trên khắp thế giới (để thay cho số căn cước cá nhân trong máy rút tiền tự động và thu tiền xe trong phương tiện chuyên chở công cộng chẳng hạn).

Nhiều người cho rằng công nghệ bảo mật bằng sinh trắc là quá "viễn tưởng" và có phần "lấn lướt" tự do thông tin - thật mỉa mai, nếu xét rằng công nghệ đó được phát minh là nhằm ngăn chặn tình trạng xâm phạm thông tin. Việc các công ty bảo mật bằng sinh trắc đều trơ trơ trước những mối lo này cũng đáng lo không kém. Thế nhưng công nghệ này thực tế chẳng lấn lướt ai, cũng chẳng hại gì cho sức khỏe. Do đó, dường như người ta lo lắng về khía cạnh đạo đức chứ không phải khía cạnh sinh lý. Người ta có thực sự muốn cứ mỗi lần mua hàng lại phải in dấu tay không? Dù vậy, ắt hẳn công nghệ này sẽ ngày càng hiện diện nhiều hơn trong tương lai gần.

Kỹ thuật quyét lén !

Nếu máy tính của bạn thường xuyên kết nối tới Internet, máy của bạn có thể sẽ bị tấn công. Đó là thực tế. Nhưng tất cả các cuộc tấn công đều có một nguyên tắc, một trình tự chung không thể thay đổi được. Để ngăn chặn buộc bạn phải hiểu nó. Bài viết này sẽ đề cập đến các thông tin căn bản của kỹ thuật quét lén: nó là gì, nó hoạt động như thế nào?

Quét một hệ thống, hoặc một mạng là kỹ thuật được sử dụng để tìm ra dịch vụ nào trên hệ thống đang hoạt động. Có 2 nhóm người thường xuyên làm việc này. Nhóm thứ nhất là các người quản trị hệ thống, họ sử dụng kỹ thuật này để giám sát các dịch vụ trên mạng. Nhóm thứ hai là các hacker, cracker, họ sử dụng kỹ thuật này để xác định các lỗ hổng của hệ thống và dựa vào lỗ hổng đó để tấn công. Tuy nhiên cách thứ hai không được mọi người ủng hộ.

Có thể ví việc quét hệ thống để xác định các dịch vụ đang hoạt động như việc xem xét một toà nhà có bao nhiêu cổng đang mở. Nhưng thay vì các cổng vật lý, với máy tính đây là các cổng như Web server, mail Server, Telnet, FRP RPC... Các phần mềm có thể làm được việc này được gọi là các phần mềm quét cổng (Port scanner).

Trên thực tế hacker, cracker được chia làm nhiều mức khác nhau. Mức cao nhất là những người biết được điểm yếu của từng hệ thống và viết ra các công cụ để khai thác lỗ hổng này. Ngược lại mức thấp nhất là những kẻ chỉ biết sử dụng công cụ để tấn công mà không biết các công cụ này hoạt động như thế nào - nhóm này được biết đến với tên "Script Kiddie".

Một vấn đề khó khăn cho các Hacker và Cracker là hệ thống có thể ghi chép (log) tất cả các kết nối mà họ tạo ra. Hầu hết các Hacker, Cracker có kỹ thuật thấp lại không nhận ra rằng họ đã để lại dấu vết khi quét hệ thống đối phương. Nhưng cũng có rất nhiều cách khác nhau để tránh để lại dấu vết.

Ví dụ: các Hacker, Cracker bậc thấp thường mượn một máy trên mạng và tiến hành quét từ xa đến máy đích. Khi đó dấu vết để lại không chỉ trực tiếp đến máy các Hacker và Cracker mà chỉ vào máy của một nạn nhân "đóng thế" nào đó.

Một kỹ thuật tránh để lại dấu vết khi thăm dò hệ thống khác thường được sử dụng là kỹ thuật quét lén. Để hiểu về kỹ thuật này, trước hết bạn phải có những hiểu biết cơ bản về các gói tin trên giao thức TCP/IP làm việc thư thế nào? Bình thường các gói tin đi trên mạng đều có một phần được gọi là TCP header. Nó thường chứa số thứ tự gói tin Sequence Number), địa chỉ IP máy nhận, địa chỉ IP máy gửi, cờ và một số phần khác.

Trong bài viết này chúng ta chỉ tìm hiểu về 3 cờ chính có liên quan đến kỹ thuật quét lén là SYN, ACK, FIN. Để hiểu về chức năng của từng cờ, chúng ta cùng xét về sự bắt tay giữa hai máy trao đổi thông tin với nhau trên mạng. Với các phiên làm việc thông thường khi 2 máy tính muốn trao đổi thông tin với nhau thì máy muốn lấy thông tin phải đưa yêu cầu thiết lập kết nối đến máy còn lại. Để làm việc này máy muốn lấy thông tin gửi gói dữ liệu SYN đến máy đích. Nếu máy đích chấp nhận yêu cầu nó sẽ gửi lại gói tin SYN và gói ACK để báo hiệu cho máy yêu cầu biết rằng chấp nhận kết nối.

Khi nhận được gói tin SYN máy yêu cầu cũng phải gửi trả lại một gói ACK với số thứ tự tương ứng để khẳng định với máy phép kết nối. Sau đó các gói dữ liệu bắt đầu được gửi đi. Khi kết thúc phiên làm việc thủ tục bắt tay lại xảy ra nhưng lần này là các khung tín hiệu FIN (Finish) báo kết thúc.

Để kết thúc phiên làm việc máy phục vụ phải gửi khung tín hiệu FIN cho máy yêu cầu. Khi nhận được khung này, máy yêu cầu hiểu rằng bên gửi báo hết phiên làm việc và nó gửi lại khung FIN cho máy phục vụ báo rằng chấp nhận kết thúc phiên làm việc.

Như vậy có 2 điểm yếu trong thủ tục bắt tay giữa 2 máy mà các trình quét lén đã khai thác để tránh việc để lại dấu vết trên máy trạm.

Điểm yếu thứ nhất là khi máy yêu cầu không gửi khung tín hiệu ACK cho máy phục vụ để báo bắt đầu phiên làm việc. Khi đó phiên làm việc được gọi với thuật ngữ "mở một nửa" (half-open) bởi chỉ có một bên hiểu rằng kết nối đã được thiết lập và như vậy nếu máy yêu cầu không gửi tín hiệu ACK sang cho máy phục vụ thì kết nối sẽ không bao giờ được tạo. Máy phục vụ sẽ không có khả năng ghi lại dấu vết của kết nối này (bởi kết nối trên thực tế không được tạo ra) nhưng máy yêu cầu lại có thể xác định được cổng này trên máy phục vụ đang mở thông qua tín hiệu ACK mà máy phục vụ gửi đến.

Một điểm yếu thứ hai mà các phần mềm quét lén lợi dụng vào là tín hiệu FIN. Khi 2 máy trao đổi tín hiệu FIN để báo kết thúc nếu máy yêu cầu dữ liệu đã nhận được tín hiệu báo kết thúc từ máy phục vụ mà không gửi lại một khung FIN với số thứ tự tương ứng (Sequence Number) thì phiên làm việc giữa 2 máy sẽ không kết thúc và như vậy việc ghi lại dấu vết của cuộc kết nối này sẽ không được tiến hành.

Như vậy mặc dù dựa vào hai khung tín hiệu khác nhau các Hacker, Cracker đã khai thác được đầy đủ các thông tin bên ngoài của một máy đích trên mạng. Tuy nhiên, khi viết bài viết này tác giả không có ý chỉ đường cho các Hacker, Cracker lý thuyết tấn công vào một hệ thống mà chỉ có ý định mang đến cho các nhà quản trị mạng tương lai và những bạn yêu thích CNTT, những lý thuyết cơ bản nhất về kỹ thuật quét lén nhằm củng cố và giám sát mạng của mình ngày một hiệu quả hơn.

Một trong những phần mềm giám sát mạng sử dụng kỹ thuật này là NMAP (Network Mapper) đây là một phần mềm rất nổi tiếng, có tốc độ quét nhanh nhất trong nhóm các phần mềm giám sát dịch vụ mạng phiên bản mới nhất hiện nay là 2.0.5 có thể tải về từ http://www.nessus.org/

Dưới đây là links mà bạn có thể download phần mềm này .

Nessus is made up of two parts : a server and a client. The server (nessusd) is actually in charge of the attacks, whereas the client is just a frontend designed to collect the results. As of today, there is only one version of the server which works on POSIX systems (Solaris, FreeBSD, GNU/Linux and others), and there are multiple clients : one which works with GTK (the Gimp ToolKit, see the GTK website, others have been written for Win32.

The server is not an option. It performs the security checks.

Package name	**Description**	**Comment**
Nessus 1.2	The previous stable version, for Unix-compatible systems only	Avoid using it and install 2.0 instead
Nessus 2.0	The current stable version, for Unix-compatible systems only	This is the brand new version of Nessus
NessusWX	A native Win32 *client*	Note that you will need to install nessusd on a Unix server for this software to be of any use to you !

(Theo Tin học và Đời sống)

Chat trong mạng nội bộ của Window XP- 2000 !

Trong Windows 2000/XP có 1 chương trình nhỏ gọn dùng để chat trong mạng nội bộ nhưng nếu không nói ra thì… ít ai biết vì chẳng hiểu sao Microsoft lại không tạo biểu tượng mặc định cho chương trình này trong nhóm Communication.

Để muốn sử dụng chương trình này bạn làm theo các bước dưới đây.

Bước 1:

Tạo biểu tượng cho chương trình bằng cách chạy Explorer --> mở thư mục Windows/System32 tìm file Winchat.exe --> bấm và giữ phím phải chuột trên file rồi kéo ra màn hình Desktop --> nhả phím chuột rồi chọn lịnh Create Shortcut Here.

Nếu muốn chương trình chạy thường trú mỗi khi khởi động Windows bạn bấm phím phải chuột lên nút Start rồi chọn lịnh Explorer All Users trong menu rút gọn.

Mở Start Menu/Programs/Startup --> Bấm phím phải chuột trong cửa sổ liệt kê nội dung nhóm Startup, chọn lịnh New/Shortcut --> Bấm nút Browse và chỉ đến file Winchat.exe

Bước 2: Các máy đang chạy Winchat trong cùng 1 mạng nội bộ có thể chát với nhau, nếu muốn chat với máy nào bạn bấm chuột nút Dial trong thanh công cụ hay dùnh lịnh Dial trong menu Conversation.

Biểu tượng chat trong máy được gọi sẽ chớp sáng và phát âm thanh, nếu người được gọi chấp nhận trả lời sẽ bấm nút Answers rồi hai bên trao đổi thông điệp với nhau.

Nửa cửa sổ bên trên là thông điệp gởi, nửa cửa sổ bên dưới là thông điệp nhận.

Bạn có thể mở nhiều cửa sổ chat để chat cùng lúc với nhiều người, khi không muốn chat với ai bạn bấm nút Hangs up trong cửa sổ tương ứng để ngắt.

Chú ý: Nếu bạn đóng chương trình, không ai có thể chat với bạn.

Bước 3: Bạn mở menu Options để xác lập font chữ tiếng Việt, màu nền cho cửa sổ, cách xếp đặt cửa sổ (trên dưới hay song song).

Phạm hồng Phước .