AN NINH ĐIỆN TỬ VÀ BẢO VỆ ĐỜI TƯ

CHO NHỮNG NHÀ ĐẤU TRANH NHÂN QUYỀN

FrontLine
INTERNATIONAL FOUNDATION
FOR THE PROTECTION
OF HUMAN RIGHTS DEFENDERS

AN NINH ĐIỆN TỬ VÀ BẢO VỆ ĐỜI TƯ

CHO NHỮNG NHÀ ĐẤU TRANH NHÂN QUYỀN

Quyển sách này được viết tặng cho tất cả các nhà đấu tranh cho nhân quyền, còn đang tiếp tục công việc khó khăn và lương thiện của họ, cũng như trên Internet. Có người trong số này đang bị ngồi tù vì những sinh hoạt trên mạng của họ.

FrontLine
INTERNATIONAL FOUNDATION
FOR THE PROTECTION
OF HUMAN RIGHTS DEFENDERS

AN NINH ĐIỆN TỬ VÀ BẢO VỆ ĐỜI TƯ CHO NHỮNG NHÀ ĐẤU TRANH NHÂN QUYỀN

Tháng Hai 2007
cập nhật tháng Chín 2009

Dmitri Vitaliev

Front Line cám ơn sự giúp đỡ tài chánh từ Hội Irish Aid nhờ đó mà đề án này được thực hiện.
Trách nhiệm cho nội dung của tài liệu hoàn toàn thuộc về tác giả và Front Line.

LỜI CẢM TẠ

Front Line và Dimitri Vitaliev thành thật cám ơn quý vị và các tổ chức sau đây cho sự giúp đỡ vô giá trong việc tra cứu và viết tài liệu này:

- Phóng Viên Không Biên Giới www.rsf.org
- Bí Mật Quốc Tế www.privacyinternational.org
- Khởi Đầu OpenNet www.opennetinitiative.org
- Wikipedia www.wikipedia.org
- Trung tâm Berkman cho Internet và Xã hội ở trường Luật Harvard http://cyber.law.harvard.edu
- Tự do về Trao Đổi Diễn Đạt (IFEX) www.ifex.apc.org
- Hội Truyền Thông Tiến Bộ www.apc.org
- Hội Hòa Bình Quốc Tế www.pbi.org
- Hội Biên Giới Điện Tử www.eff.org
- Chương Trình An Ninh Cambridge www.cambridge-security.net
- Vùng Đất Riêng Tư www.privateterra.org

Rosemary Warner
Steven Murdoch
Ross Anderson
Elijah Zarwan
Julian Wolfson
Bert-Jaap Koops
Wojtek Bogusz
Mary Lawlor
Andrew Anderson

…và rất nhiều nhà đấu tranh nhân quyền từ nhiều quốc gia trên khắp thế giới gồm có Zimbabwe, Guatemala, Trung Quốc, Cuba, Tunisia, Saudi A rập, Ai Cập, Yemen, Kyrgyzstan, Nga, Belarus, Mễ Tây Cơ, vân vân, đã trả lời các câu hỏi, cung cấp lời chứng và bằng cớ, tạo nên ý tưởng và nội dung của cuốn sách này.

graphic design and illustrations Assi Kootstra

LỜI NÓI ĐẦU

Nhân Quyền được bảo đảm bởi luật pháp quốc tế, nhưng việc bảo đảm nhân quyền và thu thập những vi phạm nhân quyền có thể là một việc làm nguy hiểm ở nhiều quốc gia trên thế giới. Những Nhà Đấu Tranh cho Nhân Quyền thường là một lực lượng đứng giữa những người dân thường và sức mạnh vô biên của quốc gia. Họ là yếu tố cho sự phát triển các tiến trình và cơ chế dân chủ nhằm chấm dứt tình trạng dân lành bị ghép tội vô cớ, cũng như cổ võ và bảo vệ nhân quyền. Những Nhà Đấu Tranh cho Nhân Quyền thường phải đối diện với nhiều sách nhiễu, giam cầm, tra tấn, vu khống, mất việc làm, mất quyền tự do đi lại và khó khăn trong việc có được sự công nhận pháp lý cho những hội đoàn của họ. Ở một vài quốc gia họ thậm chí có thể bị giết chết hay bỗng dưng "mất tích".

Front Line được thành lập năm 2001 ở Dublin với mục đích chuyên biệt là bảo vệ những Nhà Đấu Tranh cho Nhân Quyền, những người hành động bất bạo động cho một hay tất cả những quyền được liệt kê trong bản Tuyên Ngôn Quốc Tế Nhân Quyền. Front Line đáp ứng những nhu cầu đưa ra bởi chính những nhà đấu tranh, gồm có bảo vệ, hoạt động mạng lưới (làm việc chung), huấn luyện và trao đổi về các vấn đề liên quan đến cơ chế các quốc gia của Liên Hiệp Quốc và các cơ quan khu vực khác.

Trọng tâm của Front Line là bảo vệ những nhà đấu tranh cho nhân quyền đang bi đe dọa, dù là trong tạm thời hay trong lâu dài bởi vì họ làm những việc nhân danh đồng bào của họ. Front Line thực hiện một chương trình tài trợ nhỏ để cung cấp cho nhu cầu an ninh của những nhà đấu tranh. Front Line phát động chiến dịch vận động chính giới nhân danh những nhà đấu tranh đang bị trực tiếp đe dọa. Trong những trường hợp khẩn cấp, Front Line có thể giúp đỡ nơi tạm trú.

Front Line thực hiện việc sưu tầm và công bố các bản phúc trình về tình hình cụ thể của những nhà đấu tranh nhân quyền ở một số nước. Tổ chức cũng phổ biến những tài liệu tham khảo và thực hiện những chương trình huấn luyện nhân danh những nhà đấu tranh cho nhân quyền cũng như tạo điều kiện thuận lợi cho việc hoạt động mạng lưới và trao đổi (thông tin) giữa những nhà đấu tranh ở các nơi trên thế giới. Những dự án của Front Line thường được thực hiện trong khuôn khổ hợp tác với các tổ chức nhân quyền cấp quốc gia.

Front Line cổ võ sự hiểu biết về Bản Tuyên Ngôn Quốc Tế Nhân Quyền và đang hoạt động để bảo đảm rằng những nguyên tắc và tiêu chuẩn đưa ra trong Bản Tuyên Ngôn về Quyền và Trách Nhiệm của Những Cá Nhân, Nhóm và Tổ Chức và các Cơ Quan Xã Hội, để Cổ Võ và Bảo Vệ những Nhân Quyền Phổ Quát Được Công Nhận và các quyền Tự Do Căn Bản (được biết tới qua bản Tuyên Ngôn về Những Nhà Đấu Tranh Cho Nhân Quyền) được biết đến, được tôn trọng và được tuân thủ trên khắp thế giới.

Front Line có Vị Thế Pháp Lý Tư Vấn Đặc Biệt bên cạnh Hội Đồng Kinh Tế và Xã Hội của Liên Hiệp Quốc.

Để hỗ trợ cho việc làm này, Front Line tùy thuộc hoàn toàn vào sự đóng góp rộng lượng của những cá nhân và tổ chức.

Front Line đã may mắn, từ khi khởi đầu vào năm 2001, nhận được tài trợ từ nhiều nguồn khác nhau và ghi ơn những cống hiến và quyên góp trên căn bản cá nhân.

Front Line là một tổ chức nhân đạo, bất vụ lợi (số đăng ký CHY NO 14029), độc lập và không thiên vị.

Thân gửi quý bạn đang tranh đấu cho nhân quyền và xây đắp cho nền dân chủ Việt Nam

Thưa quý bạn,

Hiện nay chúng ta đang ước mong dân Việt Nam mình có được điều mà hàng trăm triệu người trên thế giới đã có từ hơn thế kỷ nay, đó là quyền tự do thông tin và trao đổi ý kiến. Người dân Việt Nam đã không có những quyền này vì đất nước chúng ta đã liên tiếp bị thực dân Pháp rồi độc tài cộng sản thống trị. May mắn là chúng ta sống trong kỷ nguyên tin học, nhờ phương tiện điện toán, chúng ta có thể vượt qua được những rào cản mà chế độ độc tài hôm nay đã dựng lên để kiểm soát người dân.

Là những người đấu tranh cho lẽ phải, chắc chắn nhiều bạn đã và đang gặp vấn đề với nhà cầm quyền. Khi một người bị gán cho tội chống đối chính quyền thì việc đầu tiên mà toán công an tới khám nhà sẽ làm là lục lọi trong máy điện toán của nạn nhân xem có chứa tài liệu gì phê phán chính quyền hoặc các thư liên lạc với những người bị chính quyền tình nghi. Do đó ta phải làm sao biết xóa bỏ trong máy điện toán của mình vết tích những thông tin hay tài liệu mà công an của chế độ có thể dùng làm lý cớ buộc tội. Tập tài liệu này sẽ chỉ cho bạn cách thực hiện điều này.

Làm sao trong máy điện toán của mình không chứa những bằng cớ để công an có thể buộc tội chỉ là một trong nhiều nhu cầu của người muốn tranh đấu cho dân chủ. Còn vô số nhu cầu khác mà cuốn sách này có thể giúp bạn, thí dụ như giữ tài liệu ở dạng người khác đọc không được. Đây là điều ngay như cả một người dân thường sống trong xã hội tự do đôi khi cũng cần tới, huống chi là người tranh đấu cho dân chủ dưới một chính thể độc tài.

Mối đe dọa thường xuyên cho anh chị em dân chủ là bị công an cài đặt vi rút vào máy. Mục đích của công an là kiểm soát các thông tin và tài liệu trong máy để tìm hiểu thêm về hoạt động và tổ chức của anh chị em dân chủ. Càng ngày họ càng áp dụng nhiều kỹ thuật tinh vi để theo dõi liên lạc của các anh chị em dân chủ qua mạng internet.

Bởi những lý do nêu trên, và còn vì nhiều lợi ích khác nữa, Đảng Việt Tân chúng tôi xin giới thiệu với quý bạn cuốn sách: "An Ninh Điện Tử và Bảo Vệ Đời Tư cho những Nhà Đấu Tranh Nhân Quyền" mà chúng tôi đã dịch sang Việt ngữ. Tập sách này do Dmitri Vitaliev thực hiện cho Front Line, một tổ chức phi chính phủ bảo vệ cho các nhà đấu tranh nhân quyền.

Mong rằng tài liệu này sẽ hữu ích cho quý bạn và được quý bạn tiếp tay phổ biến tới hết cả những ai đang tìm cách phát huy nhân quyền và xây dựng dân chủ cho Việt Nam.

Việt Nam Canh Tân Cách Mạng Đảng

NỘI DUNG

2

4

Như chúng ta biết, có những điều biết được được biết. Có những điều chúng ta biết là chúng ta biết. Chúng ta cũng biết có những cái không biết được biết. Như thế để nói lên rằng chúng ta biết có những điều chúng ta không biết. Nhưng cũng có những cái không được biết mà không ai biết, những cái chúng ta không biết là chúng ta không biết.

Donal Rumsfeld, Bộ Trưởng Quốc Phòng Hoa Kỳ, tháng Mười Hai 2003.

NHẬP ĐỀ

Các nhà đấu tranh cho nhân quyền đang ngày càng gia tăng xử dụng máy điện toán và mạng Internet trong công việc của họ. Mặc dầu tiếp cận với khoa học kỹ thuật vẫn là một vấn đề lớn trên thế giới, các phương tiện điện tử để lưu giữ và truyền đạt thông tin ngày càng phổ biến trong các tổ chức nhân quyền. Bằng nhiều cách, Internet đã nâng cao chất lượng công việc và sự an toàn cho những nhà đấu tranh nhân quyền: Internet gia tăng hiệu quả sứ mạng của họ, tạo dễ dàng cho sự tiếp cận thông tin và đẩy mạnh những trao đổi với những tổ chức bạn. Mặt khác, Internet đã tạo những vấn đề và những nhược điểm trước đây không được biết tới.

Tài liệu này không nhắm tới những thiên tài điện toán. Mục đích của nó là huấn luyện những người xử dụng máy điện toán một cách bình thường và cung cấp họ những giải pháp cho những vấn đề về bảo mật và an toàn trong môi trường điện toán hiện nay.

Chúng ta viết tài liệu, vẽ hình và thông tin với nhau trên máy điện toán và qua Internet. Những thảo chương để thực hiện những nhiệm vụ này đã được làm thật giản dị đến nỗi chúng ta không cần phải biết chính xác máy điện toán hoạt động như thế nào - miễn là chạy tốt. Như vậy, chúng ta xử dụng kỹ thuật học mà chúng ta không cần hiểu hết ngược lại, chúng ta lại bị lệ thuộc nặng nề vào nó. Là những người tiêu thụ trong kỷ nguyên kỹ thuật số, chúng ta muốn có một sản phẩm hoàn tất, mà không cần phải biết sản phẩm gồm có những bộ phận gì.

Nhưng chúng ta cần làm gì khi bị "sự cố" ? Khi máy điện toán của chúng ta bị hư hỏng và xóa sạch đi công trình nhiều năm làm việc cực nhọc? Khi emails của chúng ta không đến được người nhận hay khi chúng ta không thể lên được mạng? Chúng ta phản ứng như thế nào về chuyện virus phá hoại các máy điện toán trên thế giới, hay một email tưởng như đến từ một người bạn, yêu cầu mở một hồ sơ đính kèm? Những quyết định thiếu thông tin sẽ dẫn đến sự chọn lựa không hay, và sự lệ thuộc mù quáng vào khoa học kỹ thuật thường dẫn đến những lỗi lầm đắt giá.

Công việc của những nhà đấu tranh và những tổ chức nhân quyền thường dựa nhiều vào kỹ thuật. Kỹ thuật tạo dễ dàng cho việc thông tin và cho phép chúng ta lưu trữ và khai thác những lượng thông tin lớn một cách rẻ tiền và với một sức chứa tối thiểu. Kỹ thuật cho phép một tổ chức dù nhỏ bé, xa xôi cũng có thể có tiếng nói trên toàn thế giới và ngược lại. Một cuộc đàm thoại điện tử xảy ra trước đây vài năm có thể được nghe lại trong vài giây, và một cá nhân vi phạm nhân quyền, chẳng hạn, sẽ nhận được hàng ngàn email và fax phản đối đến từ khắp nơi trên thế giới. Nói tóm lại, máy điện toán và mạng Internet đã trở nên cần thiết và là những phần không thể tách rời của công việc nhân quyền.

Những vấn đề

Số lượng lớn thông tin được cất giữ dưới dạng điện tử và khả năng phân phối nó ra trên khắp thế giới đã tạo ra một trong những kỹ nghệ lớn nhất trong lịch sử loài người - kỹ nghệ thông tin. Trị giá hàng tỷ đô-la, nó tạo ra những lợi nhuận khổng lồ cho những người kiểm soát và điều hành cấu trúc quan trọng của nó. Khả năng điều khiển, theo dõi và giới hạn thông tin điện tử đã trở thành một sở thích, một công việc hay một chính sách cho nhiều cá nhân, công ty và các bộ phận trong chánh phủ. Cuộc chiến chống khủng bố đã cung cấp cho họ toàn quyền hành động để tiến hành giám sát và kiểm duyệt hệ thống Internet mà một thời được vận hành một cách tự do và rộng mở. Biện minh cho những việc làm này thường không được nêu lên và làm soi mòn nhân quyền và những quyền tự do căn bản.

Một số quốc gia trên thế giới đã đưa vào thành luật để biện minh và khuyến khích những hành vi trên đây nhằm gia tăng hơn nữa sự bức hại và đau khổ của những nhà đấu tranh Nhân Quyền và phá hoại công việc chính đáng của họ hầu hạn chế khả năng bảo vệ người khác của họ.

Hàng chục nhà đấu tranh Nhân Quyền và ký giả độc lập hiện đang ngồi tù vì họ đã tìm cách tán phát công trình của họ trên thế giới internet mà không có được những kiến thức tối thiểu để làm chuyện đó một cách an toàn.

Điều quan trọng phải nói ở đây là kỹ thuật nói chung đã chưa lan tới được khắp mọi nơi trên thế giới. Vẫn có hàng triệu người chưa bao giờ thấy được cái đèn điều hòa giao thông, nói chi đến máy điện toán. Khoảng cách vật chất giữa các quốc gia giàu và nghèo cũng thể hiện trên thế giới kỷ thuật điện tử và được biết như là "lằn ranh kỹ thuật điện tử". Những nhà đấu tranh nhân quyền ở bên phía nghèo của lằn ranh này nhận thấy cơ hội của họ với đến được cộng đồng thế giới giảm đi rất nhiều.

Tài liệu này nhằm giới thiệu thế giới phức tạp và tăng triển lâu dài của an ninh điện tử. Không những tài liệu này sẽ nâng cao kiến thức và sự hiểu biết về máy điện toán và Internet của bạn, mà sẽ còn cảnh giác bạn về những nguy cơ tiềm tàng khác nhau mà bạn có thể gặp phải trong môi trường điện tử và sẽ hướng dẫn bạn cách đối phó với những nguy cơ này.

Tài liệu này được viết cho những nhà đấu tranh nhân quyền, và vì vậy chú trọng vào những cách ngăn ngừa những việc giới hạn những quyền tự do được bảo đảm trên khắp thế giới. Ngoài những yếu tố về mặt lý thuyết, tài liệu cung cấp những giải pháp khả thi cho một số vấn đề về máy điện toán và an ninh Internet.

An Ninh như là một Phương Pháp

Đây không phải là một tài liệu chỉ có những câu trả lời!

Bạn hãy tưởng tượng bạn đến gặp một chuyên viên về an ninh để được chỉ cách đối phó với những đe dọa và sách nhiễu trong đời sống hàng ngày. Trước khi chỉ cách, chuyên viên có thể hỏi bạn một số câu hỏi, chẳng hạn như bản chất chính xác của những rủi ro và đe doạ mà bạn đang phải đối mặt. Đối với lãnh vực an ninh điện tử thì cũng tương tự như vậy. Không có câu trả lời tức khắc cho mọi vấn đề. Bạn có thể đã nhận thấy rằng 'các chuyên viên' cũng ít khi đưa ra những câu trả lời trực tiếp.

Tài liệu hướng dẫn về an ninh này giới thiệu với bạn nhiều bộ phận khác nhau của máy điện toán và sự vận hành của Internet (đặc biệt dành cho những nhà đấu tranh nhân quyền trong trường hợp này). Mục đích là để nâng cao kiến thức và gia tăng sự hiểu biết của bạn về những vấn đề an ninh điện tử và bảo mật điện toán. Thực chất, tài liệu có mục tiêu trình bày những lý thuyết, phương pháp và đem đến những câu trả lời về những yếu tố làm mất an toàn máy điện toán và những biện pháp đối phó.

Tóm lại, nội dung của tài liệu giúp bạn giải quyết và tăng cường sự an ninh điện tử của riêng bạn.

Hy vọng tài liệu này cũng sẽ giúp cho bạn quan tâm đúng mức về những đề mục nêu trên để bạn thực hiện việc tìm tòi cho riêng bạn một cách hứng khởi và để tiếp tục học hỏi.

Hướng dẫn cách thức xử dụng tài liệu này

Tài liệu này được chia làm bốn phần mà có thể được đọc không cần theo thứ tự. Độc giả không cần có bất cứ kinh nghiệm chuyên môn nào, tuy nhiên nếu có chút ít kiến thức về máy điện toán và sự điều hành Internet thì sẽ rất hữu ích. Những chương, chứa những thông tin có tính cách kỹ thuật hơn, được đánh dấu "Dành cho chuyên viên".

I. Phần đầu tiên nói về sự hiểu biết về những nhu cầu an ninh và nhược điểm của bạn. Phần này mô tả những yếu tố không kỹ thuật liên quan đến môi trường điện toán. Một phương pháp đồ họa những mối đe dọa, tạo ra bởi một hoàn cảnh đặc biệt, được trình bày nhằm giúp bạn quyết định những chiến lược cho việc thiết lập những giải pháp thuộc về bảo mật và an ninh.
II. Phần thứ nhì thiết lập một danh sách những yếu tố khác nhau liên hệ đến an ninh máy điện toán và Internet. Phần này giới thiệu đến độc giả sự vận hành của máy điện toán và hạ tầng cấu trúc Internet. Những phương pháp về bảo vệ thông tin, vượt qua sự kiểm duyệt Internet và bảo vệ chính bạn trước những sự tấn công đầy ác ý, sẽ được giải thích một cách chi tiết.
III. Phần thứ ba tóm tắt luật pháp trên thế giới để nhận diện ra những giới hạn và việc theo dõi lưu lượng thông tin và các hình thức trao đổi tin tức. Phần này cho thấy khuynh hướng đi xuống, gây ra bởi sự gia tăng khả năng giới hạn các quyền tự do diễn đạt, và truyền thông, ở nhiều quốc gia. Các trường hợp về những nhà đấu tranh cho nhân quyền hiện đang ở tù hay bị bức hại vì việc làm của họ qua Internet, được tường trình như là những thí dụ về các phương cách mà một số chính phủ đã đưa ra nhằm tăng cường cho những đạo luật này.
IV. Phần thứ Tư thảo ra những kịch bản có thể xảy ra cho những nhà đấu tranh nhân quyền và tổ chức của họ đối phó với những vấn đề về an ninh điện tử và đảm bảo sự liên tục cho công việc của họ. Những kịch bản này có liên hệ đến những khái niệm được trình bày trong suốt tài liệu và các giải pháp được dựa trên những hành động có thể thực hiện được.

Theo sau những bài tập, bạn sẽ thấy phần phụ lục, nhằm để cung cấp cho bạn bối cảnh chi tiết của máy điện toán (máy điện toán) và Internet, cũng như những giải thích sâu sắc về một số những đề mục an ninh. Phần cuối tài liệu, có phần Thuật Ngữ giải thích nhiều danh từ kỹ thuật và xa lạ được dùng trong quyển sách này.

Cuốn sách này có thể được dùng chung với cuốn Digital Security Toolkit (http://security.ngoinabox.org) – một bộ sưu tập các chương trình miễn phí bao gồm các dụng cụ (tools) và tài liệu chỉ dẫn những phương kế cần thiết để đạt được mức bảo mật và an ninh tốt hơn trên máy điện toán của bạn và trên Internet. Toàn bộ đồ nghề có sẵn bằng nhiều thứ tiếng như Anh, Pháp, Tây Ban Nha, Nga, và Á Rập. Toàn bộ phần mềm được trình bày trong tài liệu này có thể được tìm thấy một phần hoặc toàn phần trong cuốn Digital Security Toolkit, hoặc có thể tải xuống miễn phí từ Internet.

Một vài khái niệm và kỹ thuật học, được mô tả và giảng dạy trong tài liệu này, được xem là như bất hợp pháp tại nhiều quốc gia trên thế giới. Xin bạn thận trọng lưu ý đến hệ thống luật pháp địa phương của bạn để có quyết định sáng suốt để sở hữu và xử dụng quyển sách này.

1.1 AN NINH VÀ KHÔNG AN NINH

Tất cả các máy điện toán và Internet đều dồn về việc tìm kiếm thông tin, cất giữ và trao đổi. Do đó đề mục về an ninh trong lãnh vực điện toán liên hệ đến an ninh thông tin. Chúng ta cần hoạt động trong một môi trường nơi mà thông tin của chúng ta không bị đánh cắp, làm hư, bị phá hoại hay bị hạn chế. Trên lý thuyết, Internet cung cấp cho mọi người một cơ hội bình đẳng để truy cập và tán phát thông tin. Tuy nhiên, như có nhiều biến cố cho thấy, điều này không phải lúc nào cũng xảy ra. Các chính phủ và công ty lớn nhận ra tầm quan trọng và giá trị của việc kiểm soát lưu lượng thông tin, và việc quyết định khi nào thì có thể hạn chế khả năng xử dụng hệ thống này. Sự an ninh về thông tin trở nên phức tạp hơn nữa bởi những cá nhân xấu tạo ra virus và đột nhập vào hệ thống điện toán, thường không có mục đích nào khác hơn là gây hư hại.

Sự rối loạn còn được gia tăng bởi số lượng dồi dào của phần mềm, phần cứng và các thiết bị điện tử được chế ra để làm cho việc lưu trữ và trao đổi thông tin dễ dàng hơn. Một máy điện toán trung bình ngày nay chứa hàng triệu thảo chương phức tạp và hàng trăm cơ phận. Chúng có thể chạy bậy và làm tổn hại hệ thống ở bất cứ lúc nào. Người xử dụng phải đắm mình trong những khái niệm và kỹ thuật học, dường như bị tách ra xa với thế giới thật. Vấn đề an ninh cho máy điện toán của bạn là gánh nặng ưu tiên và nhiều nhất trên vai bạn và cần một sự hiểu biết về hệ thống của nó làm việc như thế nào.

Kết quả của cuộc chạy đua thu hoạch lợi nhuận từ Internet là sự xuất hiện của nhiều dịch vụ và cơ quan tài chánh. Ngày nay bạn có thể đặt vé máy bay, mua một cuốn sách, chuyển ngân, chơi xì phé, mua sắm và quảng cáo trên Internet. Chúng ta đã gia tăng khả năng của chúng ta trong việc giải quyết được nhiều công việc nhanh chóng hơn. Tuy nhiên, chúng ta cũng đã tạo ra vô số lưu lượng thông tin mới, và với những khái niệm mới về sự không an ninh, chúng ta chưa biết được làm thế nào để đối phó. Các công ty tiếp thị đang tích lũy hồ sơ của khách hàng trên Internet, với hy vọng biến kinh nghiệm truy cập của bạn thành một việc đi mua sắm thường xuyên. Thông tin cá nhân, bị thâu thập bởi những dịch vụ cung cấp Internet, chánh phủ và các công ty lớn, sau đó được bán cho những công ty khai thác thông tin, mà mục đích là tích trữ càng nhiều chi tiết càng tốt về đời sống cá nhân và các thói quen của bạn. Những thông tin này sau đó được dùng trong các thăm dò, cải tiến sản phẩm hay các cập nhật về an ninh quốc gia.

Dường như sự hỗn loạn đã lan rộng trong mục tiêu kiểm soát thế giới điện toán. Không có gì chắc chắn cả và mọi việc đều có thể xảy ra. Đa số chúng ta đều muốn viết một hồ sơ hay gởi đi một email, mà không phải cân nhắc hậu quả của sự mất an ninh. Rủi thay, điều này không thể được trong môi trường điện toán. Để là một tác nhân có được sự tự tin trong cái kỷ nguyên mới mẻ này của xa lộ thông tin và kỹ thuật điện tử đang phát triển, bạn cần phải biết đầy đủ về cái mạnh và yếu của bạn. Bạn phải có kiến thức và năng khiếu để tồn tại và phát triển với các khuynh hướng luôn thay đổi này.

CÁC PHƯƠNG PHÁP VÀ KHUYNH HƯỚNG CỦA SỰ THEO DÕI, KIỂM DUYỆT VÀ TẤN CÔNG ĐIỆN TỬ

1.1

Quyền riêng tư là một vấn đề tranh cãi trong thế giới tân thời này. Có phải bất cứ ai cũng có quyền truy cập vào thông tin cá nhân của chúng ta không? Sau biến cố 9/11 ở Hoa Kỳ, đa số các chính phủ dường như đều nghĩ rằng họ phải có khả năng theo dõi và truy cập những sự truyền thông điện toán của chúng ta. Rất nhiều quốc gia đã làm ra luật lệ và đưa vào phương tiện kỹ thuật nhằm nâng cao khả năng theo dõi của họ lên đến những mức độ tinh vi chưa từng thấy. Ví dụ, dự án ECHELON là một hệ thống theo dõi toàn cầu, có thể ghi lại và khai thác các cuộc trao đổi điện thoại, Internet và qua vệ tinh.

Tháng Năm 2001, Uỷ Ban Lâm Thời của Quốc Hội Âu Châu về Hệ thống Kiểm Lưu Echelon (thành lập tháng Bảy 2000) đưa ra một báo cáo kết luận rằng "sự hiện hữu của một hệ thống toàn cầu cho việc theo dõi và thu lượm các cuộc trao đổi tin tức là một điều không còn phải nghi ngờ gì nữa." Theo Ủy Ban, hệ thống Echelon (được tường trình là điều hành bởi Hoa Kỳ với sự hợp tác của Anh, Gia Nã Đại, Úc và Tân Tây Lan) được thiết lập vào thời kỳ đầu tiên của cuộc Chiến Tranh Lạnh cho việc thu lượm tình báo và đã phát triển thành một mạng lưới gồm những trạm kiểm lưu trên khắp thế giới. Mục đích tiên khởi của nó, theo như bản tường trình, là theo dõi và thu lượm các trao đổi thông tin thương mại và tư nhân, không thuộc lãnh vực tình báo quân sự.[1]

►**ECHELON** trạm ngăn chặn ở Menwith Hill, Anh. *Source: www.greaterthings.com/Word-Number/Organizations/Echelon*

Quyền về tự do ngôn luận và thông tin cũng đã bị tấn công và đàn áp trên Internet. Khả năng truy cập thông tin từ bất cứ điểm nối Internet nào trên trái đất, bất kể thông tin được lưu trữ ở đâu đã dẫn đến kết quả là nhiều chính phủ - chưa sẵn sàng trong việc cung cấp loại tự do này cho công dân của họ – đã đua nhau giới hạn sự tự do truy cập. Việc những nguồn tài nguyên khổng lồ đã được đổ vào để phát triển những hệ thống kiểm duyệt cấp quốc gia, đặc biệt nhằm ngăn cản thông tin Internet, xem ra có vẽ không thích hợp hay có thể gây tổn hại đến luật pháp quốc gia địa phương và 'tinh thần dân tộc'.

Ở Trung quốc, một hệ thống được biết như là "Bức Tường Lửa Vĩ Đại" dẫn mọi mạch nối quốc tế qua những máy phục vụ của nhà nước ở những cổng nối mạng chính thức, nơi các viên chức Bộ Công An nhận diện những người sử dụng và nội dung trao đổi, ấn định các quyền hạn, và theo dõi sát sự lưu thông trên mạng vào và ra khỏi nước. Trong một buổi hội thảo về kỹ nghệ an ninh năm 2001, chính phủ Trung Quốc đã tuyên bố sẽ tiến hành một dự án nối tiếp thật vĩ đại mang tên là "Khiên Vàng" . Thay vì chỉ lệ thuộc vào hệ thống Intranet quốc gia, tách rời ra khỏi hệ thống Internet toàn cầu bằng một bức tường lửa kiên cố hiện đại, Trung quốc sẽ thiết lập hệ thống tình báo giám sát vào ngay trong mạng, để có khả năng "thấy", "nghe" và "suy nghĩ". Còn sự thanh lọc nội dung sẽ được chuyển từ cấp quốc gia xuống đến hàng triệu máy điện toán (thông tin điện toán và truyền thông ở nơi công cộng và tư gia dân chúng). Kỹ thuật của Khiên Vàng vô cùng phức tạp và phần lớn dựa trên những nghiên cứu bởi những hãng kỹ thuật điện tử Tây Phương, bao gồm Nortel Networks, Sun Microsystems, Cisco và những hãng điện tử khác.[2]

1
http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf

2
Sự Riêng Tư Quốc Tế -- Báo Cáo về Sự Riêng Tư và Nhân Quyền năm 2004 – Mối Đe Dọa cho Sự Riêng Tư

Những hệ thống thanh lọc này làm suy yếu đi khả năng xử dụng Internet và vượt qua những biên cương địa lý của chúng ta để tìm hiểu và trao đổi thông tin. Chúng cũng vi phạm nhiều điều khoản trong bản Tuyên Ngôn Quốc Tề Nhân Quyền bảo đảm quyền bảo mật riêng tư và tự do ngôn luận của mọi người. Điều có ý nghĩa đặc biệt là những hệ thống này chỉ phát triển sau khi có sự tăng trưởng về khả năng của Internet như là phương tiện trao đổi thông tin toàn cầu. Những hệ thống kiểm soát này không nằm trong những sáng kiến nguyên thủy của sự phát triển của Internet.

Những kỹ thuật giám sát và theo dõi đã được chuyển từ những nhân viên tình báo xuống đến các hệ thống phần cứng và mềm, được điều hành bởi các công ty tư nhân và các cơ quan chính phủ. Việc đặt máy nghe lén điện thoại và việc mở thư đã được thay thế bởi kỹ thuật có thể theo dõi mọi người và mọi việc cùng một lúc. Sự phổ biến đại chúng của Internet và sự hội nhập của nó vào đời sống hàng ngày đã khiến việc đó có thể thực hiện được. Trước đây, người nào đó bị coi là nguy hiểm cho nền an ninh quốc gia thì mới bị theo dỏi. Ngày nay, tất cả chúng ta đều bị tình nghi vì là kết quả của hệ thống theo dõi và thanh lọc mà chính phủ chúng ta thiết lập trên hệ thống Internet. Kỹ thuật ngày nay thường không phân biệt được những người sử dụng vì nó chỉ chờ từ khóa (key word) nào đó xuất hiện trong email của chúng ta hay khi chúng ta truy cập trên Internet, và khi bấm những từ khóa đó, nó sẽ báo động cho toán giám sát hoặc có thể chặn đứng thông tin của chúng ta.

Sự tranh luận về việc kiểm soát Internet và lưu lượng thông tin cho những mục đích chống khủng bố nằm ngoài khuôn khổ tài liệu này. Tuy nhiên, phải nói rằng những hành động như vậy đã làm giới hạn quyền tự do ngôn luận, tự do lập hội và quyền bảo vệ đời tư trên khắp thế giới, vi phạm trực tiếp bản Tuyên Ngôn Quốc Tế Nhân Quyền. Các chính phủ đã thiết lập các hệ thống để theo dõi công dân của họ ở mức độ vượt xa hơn những biện pháp phòng chống khủng bố. Thông tin về nhân quyền, tự do báo chí, tôn giáo, khuyng hướng tình dục, tư tưởng và các phong trào chính trị, chỉ đưa ra một vài thí dụ, đã được bố trí để số đông không thể tiếp cận được.

> *"Theo tường trình, Chính phủ Uzbekistan đã ra lệnh dịch vụ cung cấp Internet của quốc gia chặn mạng www.neweurasia.net, nơi đón nhận một mạng lưới nhật ký điện tử cho khu vực Trung Á và Caucasus. Sự quyết định của chính phủ chặn mọi truy cập trên cả nước vào www.neweurasia.net được xem là lần đầu tiên có sự kiểm duyệt một trang nhật ký điện tử ở Trung Á..."*[3]

3
http://www.newseurasia.net
Ngày 6 tháng 7 2006

Những cuộc tấn công điện toán và những thí dụ về chiến tranh điện toán đã làm gia tăng kiến thức về những nhược điểm mà những tổ chức điều hành mạng và lệ thuộc vào các dịch vụ Internet đang phải đối diện. Những cuộc tấn công điện toán vào hạ tầng cấu trúc Internet về giáo dục và tài chánh của Estonia vào năm 2007 và trong cuộc xung đột giữa Nga và Georgia năm 2008 cho thấy nhu cầu phải bảo vệ biên giới điện toán của một quốc gia hay một cơ quan. Các mạng của các tổ chức nhân quyền đã bị ngăn chặn không truy cập được bởi những cuộc tấn công có tổ chức của cái gọi là Sự Từ Chối Dịch Vụ Phân Chia - Distributed Denial of Service (DDOS), nhằm sửa đổi nội dung và hủy bỏ dữ kiện.

NHỮNG ĐE DỌA ĐẶC BIỆT MÀ CÁC NHÀ ĐẤU TRANH CHO NHÂN QUYỀN PHẢI ĐỐI PHÓ

Những nhà đấu tranh cho nhân quyền thường là những đối tượng bị theo dõi và kiểm duyệt ngay trên chính đất nước của họ. Quyền tự do ngôn luận của những người này thường xuyên bị giám sát, kiểm duyệt và đàn áp. Khi quyết định tiếp tục việc làm của mình, họ thường phải gánh chịu những hình phạt nặng nề. Đối với những cá nhân này, thế giới điện tử vừa là một lợi điểm vừa là một mối họa. Một mặt vận tốc thông tin nhanh chóng đã giúp họ đến gần hơn với những người đồng nghiệp trên khắp thế giới, và những thông tin về vi phạm nhân quyền được truyền bá rộng rãi chỉ sau vài giây vài phút. Quần chúng đang thông tin, vận động qua mạng Internet, và nhiều chiến dịch về xã hội cũng được dem lên mạng. Điểm bất lợi đối với việc xử dụng rộng rãi máy điện toán và mạng Internet liên quan đến sự lệ thuộc quá nhiều vào các kỹ thuật tinh vi và mối đe dọa gia tăng nhắm vào các đối tượng của sự theo dõi điện tử và các cuộc tấn công. Trong khi đó, những người bảo vệ nhân quyền tại các quốc gia nghèo không có đủ điều kiện để có máy điện toán, và kết nối vào mạng Internet thì bị bỏ rơi lại bên ngoài các quan tâm mang tính chất quốc tế - một thí dụ khác điển hình cho sự mất quân bình gây ra bởi hố sâu điện tử.

Trong nhiều năm qua, các nhà đấu tranh cho Nhân Quyền đã học hỏi nhằm có thể tự điều hành môi trường của họ và đã khai triển những phương cách nhằm tự bảo vệ mình và ngăn ngừa các cuộc tấn công trên mạng. Họ nắm vững hệ thống pháp lý của quốc gia, mở ra nhiều mạng xã hội thân hữu và chọn quyết định dựa trên sự nhận thức hàng ngày của mình. Tuy nhiên, máy điện toán và đặc biệt là mạng Internet đã tạo nên một thế giới hoàn toàn mới, để khám phá và tìm hiểu. Việc thiếu sự quan tâm hay khả năng học hỏi giới hạn về lãnh vực an toàn điện tử đã dẫn tới nhiều vụ bắt giữ, tấn công cũng như những mâu thuẫn trong cộng đồng đấu tranh cho nhân quyền. An toàn điện tử và các lãnh vực cá nhân trên môi trường điện từ đã không những trở thành một lãnh vực quan trọng để hiểu biết và tham gia mà còn là một trận thế mới trong cuộc đấu tranh cho và vì nhân quyền.

Emails không đến được nơi nhận, đường dây nối vào mạng Internet lúc tắt, lúc chạy một cách bất thường, máy điện toán bị tịch thu và sự xâm nhập của virus làm tổn hại những công trình của hàng năm trời làm việc. Những vấn đề này đã xảy ra thông thường đến mức đã trở nên rất quen thuộc. Một hiện tượng quen thuộc khác nữa là mức độ quan tâm ngày càng gia tăng của những người có khả năng đăng tải thông tin trên mạng. Những giới chức có thẩm quyền luôn truy tìm những trang web mới trên Internet, cũng như các blog và diễn đàn –và một khi đã phát hiện những trường hợp đăng tải thông tin "không vừa ý" sẽ đưa ra các biện pháp "trừng phạt" nhanh chóng một khi những tài liệu đến từ một nhà đấu tranh cho nhân quyền bị khám phá. Điển hình là trường hợp của Mohamed Abbou, người đã phải gánh chịu 3 năm rưỡi tù ở Tunisia vì đã đăng tải một bài báo so sánh trại tù giam ở Tunisian với Abu Ghraib.[4] Tại Trung Quốc, hàng chục nhà báo đã bị bỏ tù vì những hoạt động trên mạng Internet của họ.[5]

Những người đấu tranh cho nhân quyền cần phải bảo vệ những hoạt động của họ bằng cách học hỏi thêm về kỹ thuật và những khái niệm về an toàn điện toán, và những hoạt động trên Internet. Những nỗ lực này sẽ giúp họ có khả năng tự bảo vệ và quảng bá, một cách hữu hiệu hơn, những quyền con người mà họ muốn bảo vệ.

4
Front Line
http://www.frontlinedefenders.org/news/2081

5
Ký giả không biên giới
http://www.rsf.org
February 2007.

1.2 Ý THỨC AN TOÀN THÔNG TIN

TÓM TẮT

1. Hãy tự hỏi mình, một người lạ mặt có thể dễ dàng chiếm đoạt được quyền vào văn phòng và nơi làm việc của bạn hay không?
2. Hãy ý thức được rằng việc sử dụng máy điện toán trong một quán café công cộng không an toàn bằng việc sử dụng máy tại nhà.
3. Dữ kiện được lưu giữ trong máy điện toán của bạn cần được bảo mật bằng nhiều tầng lớp tiếp cận khác nhau: sự an toàn của chính chiếc máy điện toán, nơi bạn đặt máy điện toán như căn phòng của bạn hoặc tòa nhà nơi bạn làm việc.
4. Biết rõ vị trí trong máy những dữ kiện đang có và mọi bản sao chép để lưu trữ.
5. Không sử dung mật mã trống không hoặc để lộ cho người khác biết.
6. Hãy thật cảnh giác khi mở email và đồng thời tắt chức năng duyệt trước (preview) được gài sẵn trong chương trình email.
7. Hạn chế tối đa cơ hội cho những người khác có thể vào máy điện toán của bạn sau khi bạn rời máy.

Nội dung của chương này sẽ đề cập tới những phương pháp không kỹ thuật nhằm gia tăng mức an toàn cho những thông tin liên lạc của bạn. Hãy cảnh giác đến môi trường chung quanh và như vậy có thể giúp bạn nhận diện ra các đe dọa tiềm tàng, đó là bước đầu trong kế hoạch an ninh thông tin của bạn. Bạn cần nắm vững môi trường hoạt động và có sẵn một phương pháp hợp lý nhằm giải quyết những sự cố ngoài ý muốn liên quan tới an toàn thông tin.

Đa số những sự cố có liên quan đến việc làm và đời sống của các nhà đấu tranh cho nhân quyền đều liên hệ đến bạo lực va sự xâm nhập vào môi trường làm hoạt động của họ. Bất luận là bạn đang làm việc tại văn phòng hay đem máy điện toán xách tay ra khỏi nhà, hay truy cập Internet tại quán café Internet, bạn nên luôn luôn ý thức được khả năng và giới hạn của mình. Sau đây là danh sách những câu hỏi mà bạn cần có câu trả lời. Cho mỗi một câu hỏi, hãy tưởng tượng đến tình huống tệ nhất có thể xảy đến và hãy suy nghĩ cách thức ứng phó.

Môi trường văn phòng

a. Người lạ có thể đột nhập một cách dễ dàng vào văn phòng của bạn mà không cần xin phép bạn hay không?
b. Cửa sổ và cửa ra vào có thể bị cậy mở hay không?
c. Bạn có một hệ thống báo động hay không? Nếu có, bạn có tin tưởng vào giới chức sẽ đáp ứng lời kêu gọi báo động của bạn không?
d. Bạn có sẵn một căn phòng dùng để tiếp khách hoặc để thăm hỏi khách trước khi cho phép họ đi vào văn phòng chính?
e. Bạn có một kho trữ an toàn dành cho những dữ liệu cơ mật, chẳng hạn như tủ hoặc két sắt?
f. Bạn có một cách hủy diệt an toàn (máy xé thành vụn) những dữ kiện mật hay không?
g. Mức độ tin tưởng của bạn như thế nào đối với các thành phần quét dọn văn phòng và khả năng của họ lấy hay đọc được những tài liệu của bạn là như

thế nào?

h. Cách thức bạn dùng để vứt bỏ những tài liệu vô giá trị có loại trừ hẳn xác xuất người ngoài tìm được và thu lượm nó không? Về điểm này, bạn có biết là bạn có bao nhiêu tài liệu mật hay không?
i. Bạn có đóng bảo hiểm và đồng thời có dự trù biện pháp đối phó với những sự cố thiên tai hay bị mất trộm hay không?
j. Người đứng từ cửa sổ bên ngoài văn phòng bạn có dễ dàng nhìn thấy được nhân viên cũng như những gì được hiển thị trên màn hình máy điện toán của bạn không?
k. Bạn có trong tay tất cả là bao nhiêu bản sao chìa khóa cho văn phòng và ngoài bạn ra còn ai có trong tay những chìa khoá này?

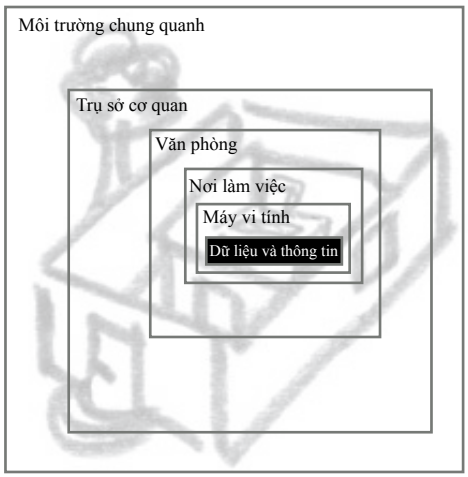
Không gian làm việc cá nhân

a. Ai có thể nhìn thấy được màn hình điện toán của bạn trong lúc bạn đang làm việc trên bàn làm việc của bạn?
b. Ai trong văn phòng biết được mật mã của bạn?
c. Bạn có lưu giữ thông tin mật trong một nơi mà mọi người có thể dễ dàng vào được tại chỗ làm việc hay không?
d. Bạn có khóa máy điện toán của bạn sau khi bạn rời bàn làm việc hay văn phòng hay không?
e. Tại chỗ làm việc, máy điện toán để bàn (desktop computer) hoặc máy xách tay của bạn có được gắn vào ổ một khoá an toàn và không bị tháo gỡ dễ dàng hay không?

Môi trường công cộng (quán café Internet)

a. Người chủ quán có biết tên và những chi tiết cá nhân của bạn không?
b. Người chủ quán có giám sát lưu lượng những trao đổi trên Internet của khách hàng hay không?
c. Bạn có tự tin rằng máy mà bạn đang sử dụng hoàn toàn không chứa virus và những phần mềm gián điệp (spyware) không?
d. Những người trong quán có thể nhìn thấy những gì bạn đang đọc và đánh trên màn hình điện toán không?
e. Khi bạn tải về những tài liệu trên mạng Internet, những tài liệu đó có được lưu lại vào trong máy bạn xử dụng sau khi bạn rời khỏi quán? Làm cách nào để có thể chắc chắn điều này?
f. Hoạt động truy cập trên mạng Internet của bạn có được ghi vào trong máy điện toán không?

Bạn nên biết rằng sự an toàn trong môi trường hoạt động cũng như về những thông tin mà bạn truyền tải đòi hỏi một sự cẩn trọng toàn diện. Có những vấn đề có thể được giải quyết một cách dễ dàng —bằng cách mua về một dây cáp sắt để xích một cách an toàn máy laptop của bạn vào bàn làm việc. Những vấn đề khác đòi hỏi sự hợp tác của toàn thể nhân viên, như việc tiếp khách và chất vấn mục đích của họ khi đến đây, cũng như sự đầu tư về mặt tài chính, chẳng hạn như việc đóng bảo hiểm hoặc mua về một tủ sắt. Đa số những tổ chức nhân quyền hoạt động một cách công khai, không bí mật, mặc dù vậy họ vẫn phải chịu trách nhiệm về sự bảo đảm an toàn cho những đồng nghiệp và những người có liên quan tới những trường hợp mà họ can thiệp (nhân chứng, nạn nhân, người đứng tên tố cáo, vv.)



Khả năng nhìn lại tình hình của chính bạn từ nhiều góc độ khác nhau và ước lượng mức độ thiếu an ninh qua kinh nghiệm của riêng bạn sẽ giúp bạn có khả năng đánh giá và đề ra những việc cần làm nhằm bù đắp lại những điểm không an toàn.

Sự lượng giá mức đe doạ về an ninh của bạn và sự an toàn của máy điện toán cần phải được tiến hành trong môi trường thật ngoài đời. Đây là một lãnh vực mà bạn đã có sẵn kinh nghiệm và trình độ chuyên môn. Việc bạn thành công trong việc loại bỏ các đe doạ nêu ra trong các câu hỏi ở bên trên, sẽ là một bước đầu rất quan trọng nhằm bảo đảm mức an toàn của môi trường điện tử của bạn.

Hãy xem xét đồ hình dưới đây, trình bày các tầng khác nhau về an ninh chung quanh thông tin của máy điện toán mà bạn sử dụng.

An ninh được xây dựng qua tất cả các tầng nhằm bảo đảm khả năng bảo vệ về chiều sâu (layer defense) cho đến việc thiết kế các hàng rào kiểm soát. Bạn cần phải xây dựng nhiều tầng bảo vệ chung quanh những thiết bị và thông tin quan trọng.

1. Tòa nhà hoặc căn hộ nơi bạn đặt những thiết bị và/hoặc tài liệu.
2. Căn phòng nơi bạn lưu trữ thiết bị và/hoặc tài liệu.
3. Nơi làm việc và vị trí đặt máy điện toán.
4. Những tài liệu và dữ liệu của bạn (kể cả tài liệu trên giấy).

Bạn sẽ không bao giờ có được một sự an toàn tuyệt đối. Là con người, chúng ta khó tránh khỏi những sai lầm, chẳng hạn như quên các thông tin quan trọng và thi hành một cách tắc trách những biện pháp bảo toàn do sự lười biếng hoặc thiếu thời giờ. Chúng ta cần có một số nhận thức thông thường khi nghĩ tới an toàn của mình. Mục đích của tài liệu này không phải là để dạy cho người khác những nhận thức thông thường, mà là để liệt kê một danh sách những câu hỏi mà chính tác giả phải trả lời nhằm bảo đảm công việc làm trên và ngoài máy điện toán sẽ được hoàn tất với một cách ít tổn hại nhất. Những chương kế tiếp sẽ giúp bạn thực hành một số những biện pháp dưới đây, và do đó nên bạn không nên quá lo lắng nếu cảm thấy những đề nghị ban đầu của tác giả có vẻ quá cao siêu.

NHỮNG CÂU HỎI CHO CHÍNH MÌNH

Dữ liệu của tôi nằm ở đâu?

Trước hết, lúc nào bạn cũng cần nhớ nơi bạn lưu trữ những tài liệu cực kỳ quan trọng đối với công việc của bạn. Tài liệu có thể nằm trên máy điện toán tại văn phòng hoặc nằm trên máy điện toán cầm tay hay nằm trong thẻ nhớ USB, thậm chí là trên đống CD nằm trong tủ búp phê ở một nơi nào đó. Việc làm một bản sao phòng bị cho những dữ liệu này trong trường hợp bị mất hay bị hư hao do cố ý gây ra sẽ khiến cho bạn mất nhiều năm công việc, là một điều vô cùng thiết yếu. Đồng thời việc đảm bảo an toàn cho bản copy này cũng không kém phần cần thiết. Trong hoàn cảnh mà những chiếc đĩa cứng nằm tứ tung nơi văn phòng hoặc căn nhà của bạn, bạn sẽ không thể nào đảm bảo an toàn cho những dữ liệu được lưu trữ trong đó.

Ai biết được mật mã của tôi?

Không bao giờ đưa mật mã cho bất kỳ một ai, cho dù có những trường hợp mà bạn mong ước mình có thể làm như vậy (như những lúc khẩn cấp, cận kề thời hạn giao nộp—chúng ta ai nấy cũng đều đã từng trải qua những lúc như vậy). Áp lực công việc thường đòi hỏi ta phải hoàn tất trước hết một số việc và do đó phải để qua một bên tất cả những việc làm khác. Trên phương diện an toàn thông tin, đây là một cách hành xử mang tính chất mạo hiểm. Trong trường hợp mật mã của bạn lọt vào tai của một kẻ lạ, được viết xuống và bị đánh mất, hoặc gặp sự cố ngoài ý muốn, bạn sẽ mất vĩnh viễn khả năng truy cập vào trương mục email và tài liệu của mình.

Việc sử dụng mật mã rỗng (mật mã dễ bị đoán ra) tương tự với việc không khóa lại cửa nhà suốt đêm trong một khu xóm nguy hiểm. Có thể sẽ không ai xâm nhập nhà bạn, hoặc nếu có thì kẻ đột nhập sẽ lấy cắp được mọi vật dụng. Trên mạng Internet có những chương trình tự động dò tìm ra những cánh cửa mở sẵn và có khả năng sẽ tìm được khe hỡ để xâm nhập vào nơi làm việc của bạn một cách rất nhanh chóng. Vài năm về trước, một tin tặc người Anh là Garry McKinnon đã thành công đột nhập nhiều lần vào hệ thống điện toán của chính phủ và Bộ Quốc Phòng Hoa Kỳ bằng cách đánh thử các mật mã trống rỗng hoặc thông thường như "admin" hoặc "password". Trong giả thuyết anh ta đã lấy được những thông tin về người ngoài hành tinh và bằng chứng cho thấy sự bưng bít của chính phủ Hoa Kỳ về những thông tin này. Anh có thể bị bắt và bị dẫn độ ra trước tòa án ở Mỹ.[6]

Máy này là máy của ai?

Nhiều lúc chúng ta cần phải làm việc trên máy công cộng trong một quán cà phê Internet hoặc một thư viện nào đó. Đồng thời có những lúc đó chúng ta không thể nào bảo đảm được là chiếc máy đang sử dụng không chứa virus, phần mềm gián điệp, Trojan, hoặc những nhu liệu độc hại khác. Bạn cần phải thận trọng khi chọn lựa những loại dữ kiện thông tin mà bạn muốn mở ra trên những loại máy điện toán này. Nên cố gắng hạn chế tối đa làm việc với những thông tin mật nhất là khi bạn biết được hậu quả nếu những thông tin này bị lấy cắp hay bị hủy hoại. Nên nhớ rằng bất cứ một tài liệu nào đã được mở và đọc trên máy điện toán nơi công cộng sẽ được lưu trữ

6
http://news.bbc.co.uk/2/hi/programmes/click_online/4977134.stm

lại một cách dễ dàng cho sự kiểm tra sau đó; nếu máy điện toán được thiết trí cho khả năng này.

Mỗi chiếc máy điện toán trên mạng Internet đều có một chi tiết nhận diện duy nhất (Xem thêm chi tiết). Nếu người chủ quán café Internet có thể ghi lại tên bạn và giờ giấc bạn truy cập, hoạt động trên mạng của bạn chưa chắc đã được bảo mật. Họ có thể trực tiếp truy ra gốc tích của bạn.

Ai đây?

Mỗi khi bạn nhận được một email lạ hoặc một đường nối vào mạng không rõ gốc tích, luôn luôn tự hỏi mình—ai có thể là người gửi thông tin này? Nếu có những nghi ngờ về nguồn gốc chính đáng của tin nhắn, đừng bao giờ bấm vào để thỏa mãn tính tò mò. Ngược lại, bạn nên xóa tin nhắn ngay lập tức. Đáng tiếc thay, thế giới công nghệ điện toán đã tinh vi đến mức không nhất thiết phải bấm chuột hai lần vào một đường link mới để có thể bị nhiễm virus. Những kỹ thuật công nghệ thông tin tân tiến cho phép những chương trình hủy hoại tối tân nhất đột nhập vào máy của bạn qua một email. Vì thế cẩn thận tối đa là tốt nhất.

Ai có thể vào máy của bạn?

Mỗi khi bạn rời bàn làm việc để về nhà hay đi ra ngoài ăn trưa, hãy tắt máy điện toán. Vô số sự cố có thể xảy ra khi máy của bạn tiếp tục chạy trong lúc không có bạn ở đó. Khi tắt máy, bạn cắt đi nguồn điện lực và bảo vệ máy khỏi những nỗ lực tấn công qua mạng. Mật mã an toàn dành cho BIOS (hệ thống xuất nhập cơ bản) hoặc Windows sẽ không có hiệu lực khi máy điện toán đang chạy. Có những virus không hoạt động cho đến nửa đêm, sau đó kích hoạt modem và quay số viễn liên (long distance). Chỉ cần vài phút là có thể mở lại đa số các máy điện toán cho nên, bạn chỉ cần tốn vài phút là có thể đảm bảo sự an toàn trên nhiều phương diện. An toàn là chính!

Bạn biết như thế nào về môi trường của mình?

Sự hiểu biết về môi trường chung quanh rất quan trọng cho sự an toàn cho bạn. Bạn nên ý thức được những nguy cơ xảy ra trong từng tình huống, cũng như những phương tiện nhằm đối phó với những nguy cơ đó. Làm việc về lãnh vực an toàn điện tử đòi hỏi bạn phải có nhiều kiến thức về luật pháp địa phương liên hệ, sự an toàn tại nơi làm việc, và một mạng lưới giao tế gồm những bạn bè và đồng nghiệp tín cẩn, sau cùng là kiến thức công nghệ thông tin và ý thức về những ưu khuyết điểm của chính bạn và của máy điện toán bạn đang sử dụng. Nhằm đề ra một chính sách an ninh thông tin cho cá nhân bạn và tổ chức của bạn, bạn cần phải xây dựng một mô hình đe dọa (giải trình và lượng giá những khả năng tấn công khác nhau) nhằm tìm cách ứng phó trước.

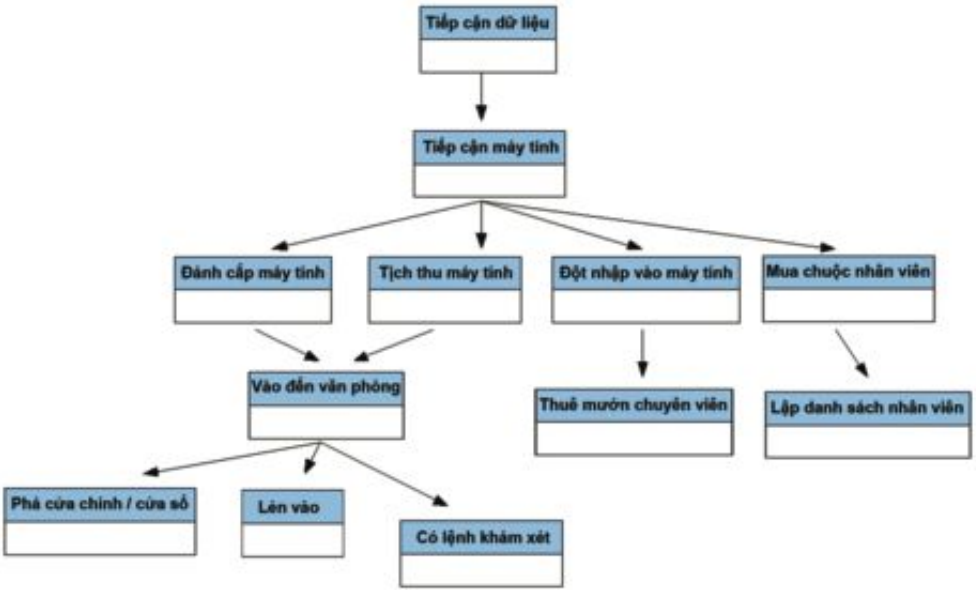
1.3 LƯỢNG GIA VỀ MỐI DE DỌA VÀ CHU TRINH BẢO MẬT

TÓM TẮT

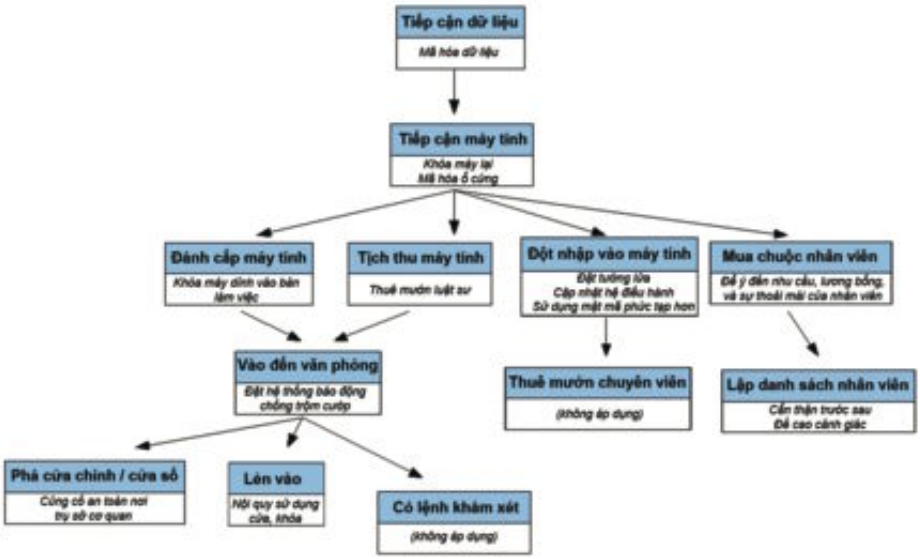
1. Hãy liệt kê những mối đe dọa có thể ảnh hưởng tới an toàn thông tin.
2. Hãy dự phóng trước những mối đe dọa đến an toàn thông tin và dự phòng sẵn những biện pháp cần thiết nhằm ngăn ngừa.
3. Hãy đối phó thật nhạy bén với những sự cố bất ngờ và điều tra cặn kẽ những nguyên do.
4. Khi đối phó với những sự cố liên quan đến an toàn thông tin, hãy nghĩ đến điều tệ nhất có thể xảy ra và lấy ngay những biện pháp thích hợp.
5. Hãy có một cái nhìn toàn diện từ mọi góc độ về an ninh thông tin. Loại bỏ đi những điểm yếu kém nhất trong sách lược của bạn. Đừng vì sự thiếu thận trọng của mình mà gieo tổn hại đến cho những người đồng nghiệp hoặc những người liên lạc với bạn.
6. Hãy trình bày những khám phá của bạn trên một sơ đồ. Điều này sẽ giúp cho bạn và những đồng nghiệp nắm bắt cục diện một cách nhanh chóng hơn.
7. Và hãy tập trung công sức vào những điểm yếu nhất trong sách lược an toàn thông tin mà bạn đã vạch ra.

Để chọn lựa những biện pháp an ninh cần thiết, bạn nên nắm bắt rõ ràng những mối đe đọa bạn phải đương đầu. Việc này bao hàm những mối đe đọa đến sự an toàn của cá nhân bạn và các nhân viên, đến uy tín của bạn và của tổ chức, đến những thông tin do bạn truyền tải, và đến sự ổn định về mặt tài chánh của bạn và tổ chức của bạn. Tất cả những yếu tố trên đều có thể bị tổn hại bằng một hình thức này hay một hình thức khác qua sự thiếu an ninh điện tử. Vì mỗi người đều có một hoàn cảnh khác nhau, tác giả chỉ có thể nêu ra những thí dụ tổng quát nhằm nêu bật lên khái niệm chung về việc thiết kế một mô hình cho những mối đe đọa.

Sơ đồ được vẽ từ trên xuống dưới. Ở tầng cao nhất, chúng ta sẽ định hình những gì chúng ta cần bảo vệ. Mối đe dọa ở đây là khả năng gây hại đến nó. Đi xuống một tầng thấp hơn, bạn có thể liệt kê những tình trạng thiếu an ninh có thể xảy ra, đặc biệt khi nó có khả năng đe đọa đến sự an toàn của tầng ở trên. Thí dụ đầu tiên phác thảo mối đe đọa xảy đến khi một ai đó tiếp cận được tài liệu trong máy của bạn.

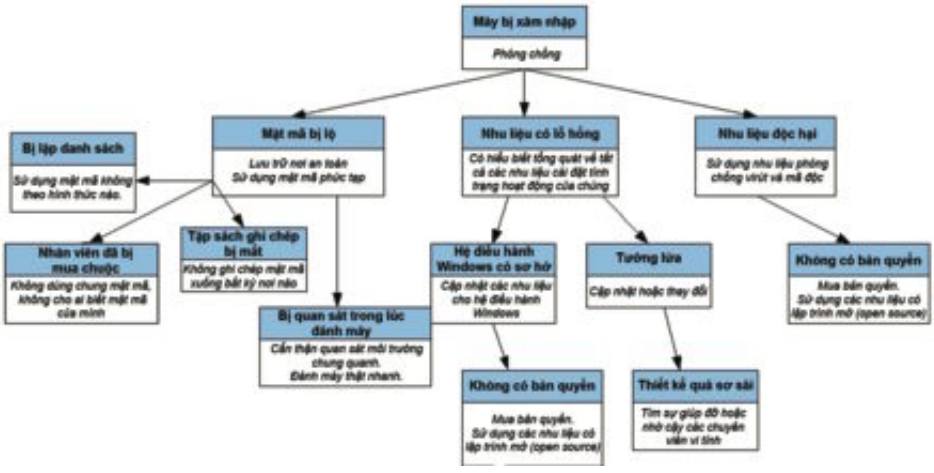


Ở tầng cao nhất, bạn viết vào ô vuông mối đe đọa mà bạn cần phải phòng tránh. Trong trường hợp này, để tiếp cận tài liệu thì trước hết người đó cần phải vào được máy. Việc này có thể xảy ra qua hành vi trộm cắp máy, tịch thu máy, đột nhập vào máy bằng cách tấn công (hack) hoặc mua chuộc đồng nghiệp của bạn, vân vân. Bạn có thể lựa chọn mô hình với số tầng mà bạn muốn, tùy theo đánh giá của bạn và điểm nào là cần thiết, điểm nào là hữu ích.



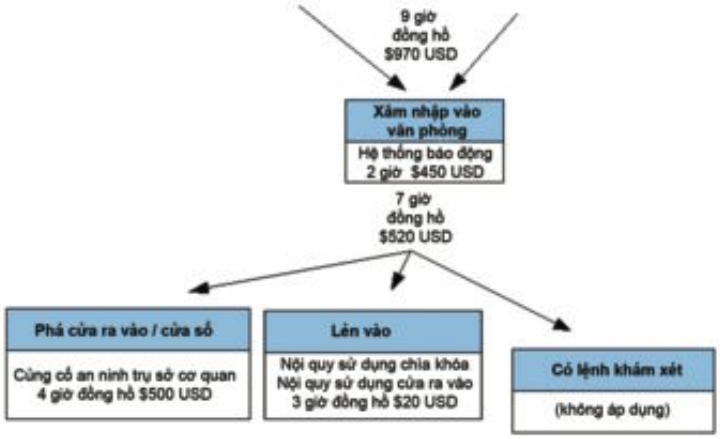
Bây giờ, chúng ta làm việc từ dưới lên trên, điền vào những khung trống những mối đe đọa kèm theo một số biện pháp để loại trừ hay làm giảm thiểu mối đe đọa đó. Có những mối đe đọa không thể loại bỏ được (điển hình là khi cảnh sát có được giấy phép để xét nhà bạn) tuy nhiên bạn có thể tác động trên đa số các yếu tố trên. Làm việc từ dưới lên trên cho đến khi bạn đến được tầng cao nhất.

Tại thời điểm này, bạn đã xác định được những hình thức đe dọa để chuẩn bị và sẵn sàng, cũng như có đủ khả năng ứng phó. Bạn có thể tạo lập và phát triển những phương pháp an toàn nhất định trong nội bộ tổ chức của bạn để hạn chế tối đa mức độ đe doạ. Bạn có thể nghiên cứu thêm những phương thức mà tài liệu này giới thiệu nhằm tìm cách bảo vệ cho chính cá nhân bạn khỏi bị đột nhập thông tin (hack), và đồng thời phòng ngừa, hoặc hạn chế những chi phí mà bạn sẽ phải chi ra để khắc phục những thông tin bị đánh cắp.



Bạn còn có thể đánh giá mức độ các đe dọa như trong biểu đồ trên. Ví dụ, để đánh giá mức độ nguy hiểm khi máy điện toán của bạn đột nhập (tức một kẻ nào đó đã có được khả năng xâm nhập điện tử vào hệ thống máy điện toán của bạn), thì hãy dựa vào biểu đồ dưới đây.

Bạn có thể tự mình tiếp tục mở rộng mô hình trong biểu đồ bằng cách cộng thêm các chi phí hay các hạn chế về thời gian xảy ra trong mỗi ô vuông trong mô hình nhánh này. Mỗi ô ở trên sẽ có giá trị bằng tổng số các ô bên dưới chính nó. Phương pháp này có thể giúp bạn trong việc chuẩn bị một ngân sách giành cho việc phòng chống các đe doạ về an ninh cho máy điện toán của bạn.



Lúc đầu, bạn có thể sẽ gặp nhiều khó khăn để nhận dạng và liệt kê các nguy cơ và đe dọa mà bạn thực sự phải đối phó, đặc biệt trong lãnh vực điện tử. Tuy vậy, kiến thức về lãnh vực này sẽ có được qua việc tự tìm hiểu, cụ thể là trong lãnh vực an ninh điện tử. Mong rằng sau khi tra cứu qua tài liệu này, bạn có thêm kiến thức về một số yếu tố kỹ thuật liên quan đến an ninh mạng. Lời khuyên là bạn cần xem xét lại các công việc của bạn có tính nhậy cảm gì để qua đó đánh giá các mối nguy cơ đe dọa tiềm tàng. Tuy rằng thực hiện việc này có thể được xem như là quyết định một việc gì quan trọng mà thông thường không phải ai cũng dễ dàng làm được, nhưng nếu thực hiện được một cách có bài bản thì sẽ giúp bạn rất nhiều trong việc nhận dạng, liệt kê và xử lý các yếu tố bất an khi vận hành máy điện toán của mình, và đồng thời phòng chống được những sai sót vô tình, nhưng hậu qủa thì có thể nghiêm trọng.

Phòng chống

Không như các mối đe dọa mà chúng ta thường gặp phải trong cuộc sống thật ngoài đời, các mối đe dọa trên thế giới ảo nhiều khi rất khó phân biệt. Vì vậy cũng khó phòng chống. Xu hướng thông thường là chỉ đối phó hay phản ứng một cách thụ động đối với những cuộc tấn công điện tử, chứ ít ai chủ động phòng chống, tuy thế hình thức chủ động phòng chống lại thường hiệu quả hơn nhiều (Vì phòng bệnh hơn chữa bệnh). Chúng ta cần thiết lập hệ thống tường lửa trước khi bị đột nhập, và cần cài đặt bộ chống virus trước khi bị mất tài tiệu thông tin do bị nhiễm virus. Để đối phó một cách đúng đắn với các cuộc tấn công qua mạng, người ta cần phải cẩn trọng tối đa. Các mô hình hay hình thức tấn công cần được xem xét và giả định ngay từ đầu. Cần xem xét và am hiểu cả những trường hợp xấu nhất ngay từ ban đầu và có các nỗ lực phòng chống trước khi các sự xâm nhập của kẻ lạ chưa thực sự xảy ra. Ngày nay tốc độ cao của máy điện toán và mạng Internet cũng có thể đồng nghĩa với việc các hàng rào bảo mật bị xâm nhập hay phá vỡ chỉ trong những khoảng khắc rất nhỏ. Microsoft cho rằng có tới 70% người sử dụng Windows không cài đặt các bộ

chống virus hay chống phần mềm gián điệp[7]. Nguyên nhân không phải là vấn đề chi phí – có khá nhiều các phần mềm chống virus hay chống phần mềm gián điệp và tường lửa miễn phí – mà vấn đề là do sự chủ quan[8] của người xử dụng máy diện toán. Đừng chờ tới ngày mai để cập nhật hệ điều hành hay đừng chờ tới khi có báo bị virus lây nhiễm rồi mới cập nhật phần mềm chống virus. Đừng chờ tới khi máy điện toán của mình bị nhà cầm quyền tịch thu, hay bị phá hoại rồi mới cho chạy các công cụ hữu ích để xóa hay lưu trữ dữ liệu. Hãy chủ động là tốt hơn cả!

7
BBC Online - http://news.bbc.co.uk/1/hi/technology/4694224.stm

8
Xem: '*Malicious software and Spam*', chương về sự khác biệt giữa vi-rút và phần mềm gián điệp.

Ứng Phó

Nếu máy điện toán, mật khẩu hay hệ thống tin học của bạn bị xâm nhập, bạn phải giả định trường hợp xấu nhất và thực hiện mọi biện pháp cần thiết. Nếu phát hiện được một virus trong máy, cần ngưng việc kết nối với Internet ngay. Thực hiện việc truy quét virus cho toàn bộ hệ thống máy điện toán của mình và loại trừ những virus phát hiện được. Chỉ kết nối lại vào mạng Internet khi việc các phần mềm chống virus báo cho biết không còn đưa ra các cảnh báo là máy điện toán của bạn bị virus xâm nhập và việc đầu tiên cần làm làm cập nhật các loại virus mới trong phần mềm chống virus cũng như trong hệ điều hành của Windows, đồng thời tìm hiểu xem những virus mà máy tìm được xem chúng có tác dụng thế nào. Bạn có thể tìm được những thông tin chi tiết về các hậu quả mà những virus này gây ra cho máy cũng như cách loại bỏ chúng một cách triệt để khỏi máy điện toán của mình. Dưới đây là những hướng dẫn trong một số ví dụ cụ thể khi máy điện toán gặp hiện tượng trục trặc và các khuyến cáo nhằm giải quyết.

Hiện tượng	Phản ứng cơ bản	Phương pháp (sử dụng tài liệu này và bộ tài liệu "NGO in a Box Security Edition")	Các việc tiếp theo
Bị virus tấn công	- ngưng kết nối Internet và chạy chương trình quét toàn bộ hệ thống - cập nhật định nghĩa virus mới và cập nhật hệ điều hành - chạy chương trình quét toàn bộ hệ thống một lần nữa	- chạy "boot scan"nếu sử dụng phần mềm diệt virus Avast hoặc quét toàn bộ (full scan) nếu sử dụng AntiVir - cập nhật Avast (hay AntiVir) - chạy "boot scan" với Avast hay quét toàn bộ với AntiVir một lần nữa	- tìm hiểu về những virus này trên mạng Internet - tìm lại thời điểm nghi là bị nhiễm - quét toàn bộ các dữ liệu dự phòng (backup) và các thiết bị phụ trợ (removable devices) - thiết trí lại những cấu hình đã bị thay đổi bởi virus
Bị nhiễm spyware (xem định nghĩa)	- ngưng kết nối Internet và chạy chương trình quét toàn bộ hệ thống - cập nhật định nghĩa chống các phần mềm gián điệp	- quét toàn bộ hệ thống với Spybot - cập nhật Spybot - cập nhật các định nghĩa phần mềm gián điệp mới để nâng cao khả năng miễn nhiễm của hệ thống	- tìm hiểm về những phần mềm gián điệp này trên mạng Internet - thay đổi hết các mật mã hệ thống và mật mã Internet - chuyển sang sử dụng bộ trình duyệt Internet Firefox hay Opera (nếu đang sử dụng Internet Explorer)
Dữ liệu bị hư hại	- Thi hồi các dữ liệu từ dữ liệu dự phòng - tìm trong các hồ sơ tạm thời xem có các dữ liệu nào mới bị thay đổi hay không (xem thêm chương"An ninh hệ điều hành Windows"–"Windows security")	- xem thêm chương (xem thêm chương"An ninh hệ điều hành Windows" để biết những cách tìm duyệt hệ thống máy điệ toán của mình - sử dụng chương trình "Hồi phục"-"Handy Recovery" để phân tích tình trạng máy điện toán	- tìm hiểu nguyên nhân vì sao máy điện toán hay tài liệu bị ngưng hay hư hại - cập nhật các thiết trí hệ thống - cập nhật dữ liệu dự phòng và quy trình dự phòng dữ liệu

Chú ý: Các công cụ và phương pháp dưới đây đều có thể được thực hiện bằng cách sử dụng bộ công cụ Digital Security toolkit, có thể được đặt từ Front Line hay tải từ trang: http://security.ngoinabox.org.

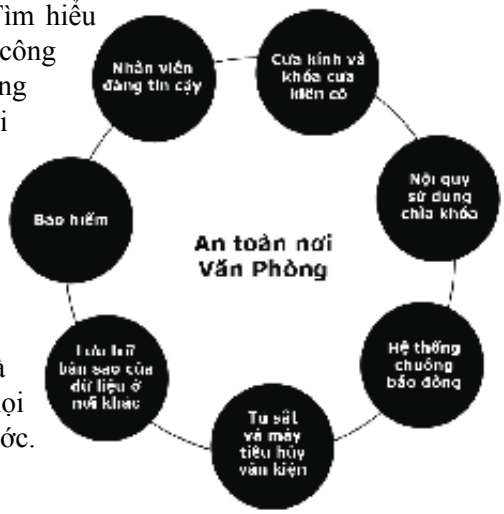
Hiện tượng	Phản ứng cơ bản	Phương pháp (sử dụng tài liệu này và bộ tài liệu "NGO in a Box Security Edition")	Các việc tiếp theo
Máy điện toán vận hành chậm	-kiểm tra xem ổ cứng của máy còn đủ dung lượng hay không - bỏ những chương trình hay công cụ đã được cài đặt mà không cần thiết - nếu sử dụng hệ điều hành Windows (NT,2000, Me, XP) thì kiểm tra danh mục các sự kiện vận hành "event viewer"để xem các triệu chứng nếu có[9] - kiểm tra virus, phần mềm gián điệp	-sử dụng"BCWipe" để xóa các hồ sơ tạm thời (temporary files) trong máy - sử dụng "Registry FirstAid" để quét và dọn sạch Windows (registry)	-ngưng Windows (xem Hướng dẫn Johansson[10]) - mua và cài đặt thêm bộ nhớ RAM - nhờ đến chuyên viên kỹ thuật
Truy cập một trang mạng nào đó bị chặn	- tìm hiểu xem những người khác có vào được trang đó không, hỏi những bạn bè ở các quốc gia khác nhau	- xem Phụ lục B "Giải thích về Internet"- "Internet explained" và chương về"Vượt qua bức tường kiểm duyệt Internet và các bộ lọc"-"Circumvention of Internet censorship and filtering" - cài đặt trình duyệt Mozilla Firefox và bộ đệm Switchproxy - cài đặt Tor hoặc chạy Torpark	- xem Phụ lục B "Giải thích về Internet"- "Internet explained" và chương về"Vượt qua bức tường kiểm duyệt Internet và các bộ lọc"-"Circumvention of Internet censorship and filtering" - cài đặt trình duyệt Mozilla Firefox và bộ đệm Switchproxy - cài đặt Tor hoặc chạy Torpark
Trang mạng của bạn bị chặn	- liên hệ với phía điều hành máy chủ trang mạng để tìm hiểu về việc bị chặn - liên hệ với nhà cung cấp dịch vụ Internet (Internet provider) để tìm hiểu về việc bị chặn - chuyển trang sang một máy chủ hay dùng tên miền (domain name) khác	- xem Phụ lục B "Giải thích về Internet"- "Internet explained" và chương về"Vượt qua bức tường kiểm duyệt Internet và các bộ lọc"-"Circumvention of Internet censorship and filtering" - dùng phần mềm Httrack (OpenCD) hay SmartFTP để chuyển kép (mirror) trang mạng sang một máy chủ khác	- thông báo việc trang bị chặn cho mạng lưới những người truy cập - dựng trang mạng trên các máy chủ khác nhau bằng cách chuyển kép (mirror). Nhờ bạn bè và đồng nghiệp giúp chuyển kép trang mạng của mình. - tìm hiểu những lý do làm sao trang mạng bị chặn và xây dựng chiến lược yêu cầu không chặn, phản đối việc ngăn chặn hoặc nhượng bộ tuân thủ.
Thư điện tử không đến được tới người nhận	- thử gửi thư điện tử từ một trương mục khác tới cùng địa chỉ người nhận (thử cả Webmail) - tìm hiểu đường đi (trace route) tới miền (domain) của người nhận. Xem thêm phụ lục"Giải thích về Internet - kiểm tra lại nếu địa chỉ thư điện tử này là chính xác	- xem Phụ lục B "Giải thích về Internet - xem phần Mã hóa – Encryption trong mục Internet trong chương về mã hóa – "Cryptology" - sử dụng Soft Perfect Network Scanner - sử dụng Hushmail	- quét hết các phần mềm độc hại, gián điệp và cài đặt hay cập nhật tường lửa. - chuyển sang sử dụng trương mục thư điện tử khác (với mức độ bảo mật cao hơn) - liên hệ và trao đổi thông tin bằng các phương thức khác nhau (đàm thoại trực tuyến - online chat, diễn đàn mạng - website forum, điện thoại)
Nhận cảnh báo khám xét	- đánh giá mức độ đe doạ - bảo vệ các thông tin nhậy cảm - xóa các thông tin nhậy cảm - lưu trữ thông tin	- đánh giá lại các chính sách bảo mật - sử dụng Eraser để xóa dữ liệu - sử dụng Truecrypt và Freebyte để lưu trữ dữ liệu vào nơi an toàn - sử dụng DeepBurner để lưu trữ dữ liệu vào đĩa CD hay DVD	- xây dựng chính sách an ninh mạng cho bản thân hay tổ chức - nâng cao mức độ an ninh mạng - đảm bảo nơi lưu trữ dữ liệu an toàn - xây dựng một hệ thống và quy trình hủy dữ liệu trong máy hay hệ thống một cách nhanh chóng
Nhận được thư rác (SPAM)	- cài đặt bộ lọc thư rác (spam filter) hay sử dụng bộ trình duyệt Thunderbird có bộ lọc thích hợp - chặn các địa chỉ gửi thư rác - chạy phần mềm quét virus và phần mềm gián điệp	- sử dụng Mozilla Thunderbird và xem bộ tài liệu "NGO in a Box SE", chương về cách cài đặt bộ lọc thư rác - sử dụng các bộ quét Avast hay AntiVir và Spybot	- thay đổi địa chỉ điện thư - xây dựng một chính sách cẩn thận và chặt chẽ quy định các loại thông tin có thể được đưa lên thông qua các thư điện tử - đăng ký các địa chỉ thư điện tử bổ sung khi đăng ký trương mục để sử dụng các dịch vụ Internet.

Mô hình "vòng tròn an ninh" – an ninh toàn diện

Mức độ an ninh của một hệ thống thông tin nhất định thường là mức độ an ninh ở điểm yếu nhất của toàn bộ hệ thống. Tương tự như khi mua một cánh cửa thép dày cho văn phòng của mình mà không biết cánh cửa này có bao nhiêu chìa khóa và các chìa khóa ở đâu thì sẽ chẳng có ý nghĩa gì. Nếu phải dự một phiên tòa để biện hộ cho thân chủ là nạn nhân của sự vi phạm nhân quyền thì ta có thể sẽ không thành công nếu không nắm giữ đầy đủ các chứng liệu chính xác. Bạn cần luôn luôn đánh giá xem xét tổng quan toàn bộ mức độ an ninh mạng của mình và sẵn sàng xác nhận cũng như đối phó với các điểm yếu trong hệ thống. Việc này cũng áp dụng cho an ninh điện tử. Chi phí để mua và cài đặt một bộ tường lửa đắt đỏ không bảo vệ được hệ thống bị phá hoại vật lý hay lấy cắp tài liệu. Triển khai hệ thống thực hiện việc mã hóa thư điện tử sẽ không có ảnh hưởng tới các chiến lược thông tin trong công việc mà bạn làm nếu các thành viên khác không thực hiện sự ngăn ngừa như bạn đã làm. Do vậy chúng ta cần tiếp cận vấn đề an ninh hệ thống trên phương diện cùng thực hiện ở diện tổng quát, tức là trên một vòng tròn toàn diện. Mỗi cấu thành (component) của hệ thống có tác dụng hỗ tương lẫn nhau và những điểm yếu cần phải được giành nhiều công sức và nguồn lực nhất[11]. Hãy cùng xem xét một quy trình xây dựng một văn phòng có hệ thống điện tử có an ninh.

Bạn có thể tưởng tượng nếu một khâu trong các vòng tròn trên bị mất tác dụng thì toàn bộ hệ thống sẽ sụp đổ như thế nào. Tất nhiên thực tế sẽ phức tạp hơn một chút: Hệ thống báo động và két sắt thường phải có những mã số đặc biệt để mở, kích hoạt hay vô hiệu hóa. Bất cứ ai biết những mã số này đều có thể là nguyên nhân làm lộ và gây ra tình trạng mất an ninh một cách giây chuyền cho toàn bộ hệ thống. Yếu tố "nhân viên đáng tin cậy" đôi khi cũng là nguyên nhân gây mất an ninh cho hệ thống.

An ninh ở mức độ thấp tuy thế vẫn còn hơn là không có an ninh. Đừng quá lo lắng với những trường hợp ví dụ về an ninh phức tạp được đưa ra trong chương này. Tuy vậy cần cẩn trọng đặc biệt để có thể đạt hơn mức mà mình nghĩ là đủ trong khi vận hành hệ thống điện toán. Tìm hiểu học hỏi thêm về những công nghệ mà mình sử dụng cũng như các luật lệ liên quan tại nước mà mình đang cư trú. Nên có mật mã, mã số dài hơn là các mã ngắn, nên sử dụng mã hóa hơn là không. Nhưng cũng không nên dựa quá nhiều vào các hình thức an ninh điện tử mà không nhận thức được hết mọi sự phức tạp và khó khăn trước.



9
Danh mục vận hành (event viewer) được mở bằng cách vào 'Start' > Settings > Control Panel > Administrator functions > Event Viewer. Chức năng này chỉ có trong Windows NT, 2000, XP. Để ý các dấu hiệu hay cảnh báo lỗi đánh dấu bằng dấu chấm than màu đỏ hay dấu hiệu cảnh báo màu vàng.

10
http://www.markusjansson.net

11
Có một cách tiếp cận an ninh hệ thống khác là "phòng thủ chiều sâu" (layer defense). Thông thường mức độ an ninh hệ thống thường được xem là độ an ninh của điểm yếu nhất của hệ thống, nếu được, hệ thống nên được thiết trí với các cấu hình độc lập và bảo vệ kép (mirror) qua đó nếu một khâu bị hư hại hay bị tấn công phá hủy cũng không gây ra tác hại tới các khâu khác, hay lây lan đến toàn bộ hệ thống một cách dây chuyền. Ví dụ: Nếu máy điện toán của bạn bị nhiễm một virus, bạn có thể lấy lại các dữ liệu đã mất từ dữ liệu dự phòng.

2.1 AN NINH CHO WINDOWS

TÓM LƯỢC

1. Thường xuyên cập nhật hệ điều hành.
2. Biết rõ các dữ liệu và tài liệu khác nhau nằm ở đâu trong máy. Sử dụng mật mã BIOS để bảo vệ máy điện toán khi khởi động. Sử dụng khóa màn hình hay màn hình có mật mã để ngăn chặn truy cập trực tiếp vào máy
3. Không sử dụng mật mã trống hay tiết lộ mật mã cho người khác. Cần cẩn thận khi cài đặt phần mềm mới hay mua máy điện toán có cài đặt sẵn các phần mềm. Chỉ sử dụng những phần mềm cần thiết và xóa những gì không cần.

Trong các phần trước chúng ta đã tìm hiểu về vấn đề an ninh trong môi trường làm việc và tầm quan trọng của việc nhận thức được các hoạt động của hệ thống máy điện toán. Chương này sẽ giới thiệu thêm về mặt kỹ thuật. Sự ổn định của hệ điều hành trong máy chính là một phần chính khi vận hành máy. Các cấu thành của phần mềm và phần cứng khác nhau có thể gây ra những ảnh hưởng tiêu cực tới những chức năng và an ninh hệ thống, nếu bạn không giữ được khả năng giám sát và điều khiển hệ thống. Hệ điều hành đem lại cơ hội làm gia tăng (hay suy giảm) mức độ an ninh của máy thông qua việc điều chỉnh một số thiết lập (settings) khác nhau. Tương tự như đầu não của máy điện toán. Trong lúc an ninh máy không chỉ hoàn toàn phụ thuộc vào hệ điều hành (Operating System, viết tắt là OS. Xem định nghĩa) điều quan trọng là phải biết được những yếu tố nhậy cảm và các điểm quản trị trọng yếu trong hệ điều hành máy điện toán của bạn.

Hệ điều hành Windows (OS) được biết tới như là một hệ thống có nhiều lỗ hổng an ninh, nhưng nếu bạn không có ý định chuyển sang sử dụng một hệ điều hành nào khác (ví dụ như Ubuntu dựa trên hệ điều hành Linux), thì bạn nên biết những công nghệ nào là tối ưu nhất để bảo đảm an ninh cho hệ thống của mình. Phần này sẽ được chia ra làm các loại hình khác nhau và phân loại căn cứ vào các phiên bản khác nhau của Windows OS. Cần biết thêm là các phiên bản nhất định của Windows, như XP Professional, có các chức năng an ninh mà không được kích hoạt ở trạng thái mặc định mà bạn cần phải thực hiện việc kích hoạt chúng.

CẬP NHẬT WINDOWS (UPDATE WINDOWS)

Việc cập nhật Windows để bổ sung cho hệ điều hành, vốn sẽ lỗi thời khi phiên bản mới ra đời. Việc này bao gồm cập nhật và vá (patch) những chương trình cũ để giải quyết những lỗ hổng về chức năng, hay bảo mật khi được phát hiện. Những chương trình vá lớn được gọi là những "gói dịch vụ" – (service pack). Microsoft hiện đã ngưng việc thực hiện cập nhật cho các phiên bản Windows 95, 98 và NT. Bạn có thể tìm và tải về các cập nhật trong những năm trước, nhưng hỗ trợ thường xuyên thì không còn nữa. Các cập nhật về an ninh và sửa lỗi cho Windows 2000 và XP sẽ còn được cung cấp ít nhất cho đến năm 2010.[12]

Nếu bạn không có kết nối Internet thì bạn ít bị đe dọa bởi các cuộc tấn công điện tử. Khuyến cáo trong trường hợp này là bạn cần có được các cập nhật cho hệ điều hành từ đĩa mềm hay đĩa CD. Bạn cũng có thể gửi thư điện tử tới Microsoft để yêu cầu gởi đến các gói dịch vụ mới nhất (cần nhớ rằng bạn sẽ phải gửi các chi tiết thông tin về mã số bản quyền trong sản phẩm mà bạn mua).

Nếu bạn có kết nối Internet thì bạn có thể vào trang http://update.microsoft.com và theo hướng dẫn để thực hiện quy trình xác định xem phiên bản Windows nào mình đang có cũng như các cập nhật cần thiết, để rồi tải về và cài đặt những phần cần thiết. Nếu bạn sử dụng Windows XP cho máy của mình, thì trang mạng này trước hết sẽ kiểm tra mã bản quyền của phần mềm Windows mà bạn có. Kể cả khi kết nối Internet của bạn chậm và đắt đỏ, bạn vẫn nên thực hiện cài đặt những cập nhật đó. Nếu kết nối Internet là vấn đề thì hãy cài đặt các cập nhật thật quan trọng (Critical Updates).

Bạn cũng có thể có được các cập nhật cho hệ điều hành Windows của bất cứ phiên bản nào bằng cách vào trang Microsoft Catalogue[13] và tải về các hồ sơ cần thiết. Đây là cách thức ích lợi khi dùng chung các cập nhật Windows giữa các máy điện toán mà không cần kết nối tất cả mọi người vào Internet. Microsoft Catalogue có các chương trình cập nhật cho tất cả mọi phiên bản hệ điều hành và không kiểm tra mã bản quyền của sản phẩm mà bạn có.

Người sử dụng Windows ME, 2000 và XP có khả năng kết nối liên tục vào Internet có thể thiết trí sao cho Windows kiểm tra định kỳ một cách tự động xem có cập nhật mới hay không và cài đặt nếu có. Vào"Control Panel" và chọn (trong 2000 - 'Automatic Updates', trong XP – 'Security Centre'). Định dạng các lựa chọn (Options) cho phép việc tải tự động và cài đặt. Ngoài ra cũng cần xóa các hồ sơ tạm thời này (temporary files) vì chúng chiếm rất nhiều dung lượng trong bộ nhớ trong máy.

12
http://support.microsoft.com/gp/lifesupsps#Windows

13
http://v4.windowsupdate.microsoft.com/catalog/Windows

Người dùng Windows 95, xin xem: http://www.microsoft.com/windows95

Cách Khóa Màn hình của Máy Điện toán

Mọi máy sử dụng hệ điều hành Windows đều cho phép tạo mật mã bảo vệ khả năng truy cập trực tiếp một khi máy khởi động. Đây có thể là việc khóa màn hình, hay ảnh màn hình có mật mã.

Khoá màn hình – **Windows NT, 2000**

Đảm bảo rằng trương mục truy cập máy của bạn được thiết trí với mật mã
Nhấn ba phím CRTL + ALT + DEL cùng lúc
Nhấn: Enter

Khoá màn hình – **Windows XP**

Cách 1) Nhấn phím Windows (nếu có) cùng lúc với phím L 

Cách 2) Bạn phải chuyển chủ đề màn hình thành "Classic" Windows để kích hoạt chức năng khóa màn hình.

Chọn: Start > Settings > Control Panel
Nhấn kép: User Accounts
Nhấn: Change the way users log on or off
Bỏ dấu chọn (un-click): Use the Welcome Screen

Bây giờ bạn có thể dùng ba phím cùng lúc Ctrl + Alt + Del.

Cách 3) Nhấn phải vào một điểm trống trong màn hình Desktop
Chọn: New > Short cut
Chọn: rundll32.exe user32.dll, LockWorkStation
Nhấn: Next
Đánh: tên cho Icon mới (ví dụ: Khóa máy - Lock Computer)
Nhấn: OK

Qua đó sẽ tạo được một Icon mới trong màn hình Desktop. Nhấn kép vào Icon này để khóa màn hình máy. Để mở, bạn sẽ phải đánh mật mã.

Windows 95, 98, ME
Không có chức năng khóa màn hình riêng biệt trong các phiên bản Windows này, do đó bạn sẽ phải tạo một ảnh màn hình có mật mã và tạo một Icon hay thời lượng hạn định để kích hoạt mật mã.

Ảnh màn hình - Screen Saver – (mọi phiên bản Windows)
Trong màn hình Desktop, kích phím chuột phải và chọn"Properties"từ trong Menu hiện ra. Chọn tới nhãn SCREEN SAVER và chọn ảnh màn hình. Chọn (click) ô"Password Protect"và đánh mật mã mình muốn vào đó. Đặt thời lượng hạn định (time limit) là 5 phút. Bây giờ tạo đường dẫn nhanh (Shortcut) để kích hoạt ảnh màn hình khi cần. Do đó bạn sẽ không phải chờ 5 phút để ảnh màn hình được kích hoạt nữa.

Kết quả sẽ cho một danh sách các ảnh màn hình mà máy có. Chọn ảnh bất kỳ mình muốn và nhấn chuột phải vào đó.

Chọn: Send to -> Desktop (Create ShortCut)

Bây giờ bạn đã có thể kích hoạt ảnh màn hình bằng cách nhấn vào Icon vừa tạo trong màn hình Desktop. Nhưng cũng có cách đơn giản hơn:

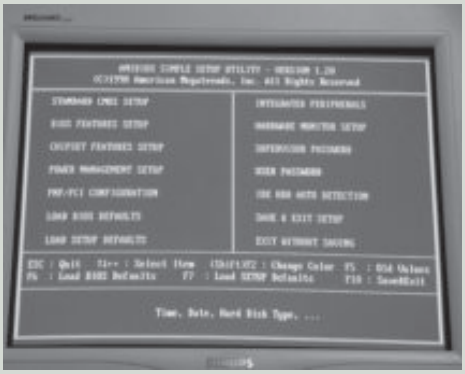
Nhấn chuột phải vào đường kết nối nhanh (Shortcut) này và chọn "Properties"

Nhấn vào ô có chữ "khóa kết nối nhanh" – "short cut key" và nhấn Ctrl + Alt + S

Nhấn: OK.

Bây giờ ảnh màn hình sẽ được kích hoạt mỗi khi bạn nhấn ba phím này cùng lúc.

Đây không phải là một cách thiết trí an ninh cao cấp, nhưng cũng còn hơn là để màn hình chạy mở mà không có mật mã nào.



Ví dụ 2: Màn hình hiển thị menu BIOS của một máy điện toán.

Mọi máy đều có BIOS – Hệ thống Xuất Nhập Cơ Bản - Basic Input/Output System. Mục đích của hệ thống này là đưa ra những lệnh khởi động để bắt đầu quá trình vận hành. BIOS là một bộ các quy trình lệnh, khởi tạo phần mềm cơ bản khi ta bật máy lên. Các lệnh này sẽ kiểm tra các cấu thành của phần cứng, khởi động ổ cứng và hệ điều hành. Các lệnh chạy BIOS được lưu giữ trong ổ nhớ ROM - Ổ nhớ Chỉ đọc - Read Only Memory, và thường người sử dụng không đọc được. Tuy nhiên, phần lớn các máy điện toán có các lựa chọn cho phép người dùng có thể kiểm định và thiết trí các cấu hình BIOS. Việc này bao gồm cả bảo mật bằng mật mã.

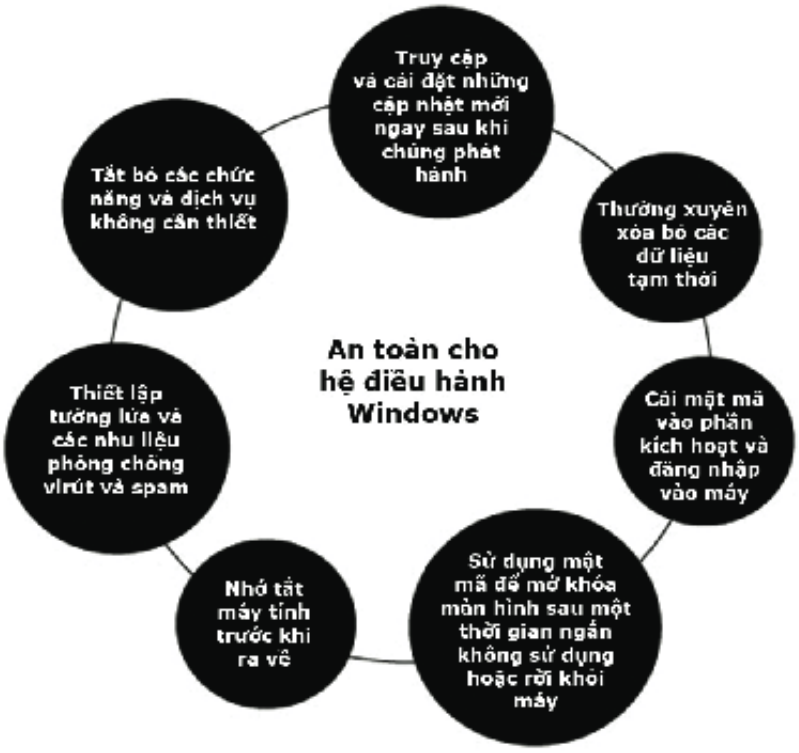
Để truy cập được vào BIOS của máy, thường phải nhấn một phím nhất định trên bàn phím trong khi quá trình khởi tạo bật nguồn đang diễn ra. Thường đây là phím F1 hoặc F2 hay F10, F12, phụ thuộc vào loại hệ thống BIOS mà bạn có. Đôi lúc đây cũng có thể là các phím ESC hoặc DEL key. Một số máy điện toán khởi động qua quá trình này rất nhanh và bạn có thể phải nhấn phím Pause trên bàn phím để đọc các dòng lệnh chạy được dễ dàng. Ở phần này chúng ta sẽ chỉ xem xét về mặt thiết trí mật mã mà thôi. Không được thay đổi các cấu hình BIOS nếu không biết mục đích của các cấu hình đó là gì. Không phải BIOS nào cũng giống nhau, nhưng bạn sẽ thấy hai hoặc tất cả các mật mã trong BIOS của mình.

Mật mã khởi động nguồn - Power On password – Có mục đích bảo vệ **BIOS** không bị khởi động khi chưa có mật mã đúng. Sẽ không có thiết bị phần cứng nào được khởi động và máy sẽ không khởi động.

Mật mã ổ cứng – Có mục đích bảo vệ **BIOS** không bị đưa vào quá trình khởi động và khởi động ổ cứng. Đây là một lựa chọn hữu ích cho các máy xách tay nếu thường để trong trạng thái"chờ"- standby.

Mật mã quản trị - Supervisor password (mật mã **BIOS**) – Đây là mật mã cơ bản có khả năng quản trị hai mật mã ở trên. Bạn không cần phải đặt mật mã này, nhưng nếu bạn quên hay muốn thay đổi mã khởi động nguồn hay mã ổ cứng ở trên thì sẽ phải cần mật mã này.

Việc đặt các mã này sẽ ngăn chặn được xâm nhập trực diện từ máy một khi máy đã bị tắt. Đây là cách nhanh chóng để làm nản lòng những kẻ muốn xâm nhập máy mà không có trình độ quá cao. Mức độ bảo mật này tuy vậy cũng chưa phải là tuyệt đối vì vẫn có những cách đi vòng mà không cần các mật mã **BIOS**. Phần lớn các cách này đều đòi hỏi phải can thiệp trực tiếp tức là mở máy ra. Một khi đã mở máy, bạn có thể Reset hệ **BIOS** hay chỉ đơn giản là tháo ổ cứng ra và lắp vào chạy ở một máy điện toán khác không có mật mã **BIOS**. Do đó, nếu bạn có khóa và túi đựng hay va li đựng máy điện toán xách tay đủ tốt, bạn có thể sẽ làm tăng thêm khả năng chống xâm nhập vào những thông tin trong máy của bạn. Nếu quên mã **BIOS**, bạn sẽ phải dùng các biện pháp nói trên để Reset máy.



CÀI ĐẶT PHẦN MỀM GIÀNH CHO CHUYÊN VIÊN

Phần lớn các máy điện toán đều có một số các phần mềm được cài đặt sẵn. Cần nhớ rằng việc này có thể gây nguy hại cho an ninh máy của bạn. Thực ra bạn chỉ cần đĩa CD cài đặt Windows và bộ công cụ Security-in-a-Box để bắt đầu mà thôi. Bạn có thể tìm các phần mềm mình cần khác trên mạng Internet miễn phí[14]. Các phần mềm được cài đặt sẵn trong máy điện toán thường là các phiên bản thử nghiệm như các bộ quét virus thử (test version), các phần mềm đồ họa. Chúng có thể thậm chí chứa các phần mềm gián điệp (Chính phủ Trung quốc đang xem xét việc đưa ra luật yêu cầu mọi nhà sản xuất máy điện toán và những công ty bán máy điện toán phải cài đặt các phần mềm kiểm duyệt trong các máy mới bán ra). Nếu bạn chỉ sử dụng những phần mềm được khuyến cáo và đáng tin cậy, cài đặt bộ chống virus tốt cũng như thiết trí tường lửa, thì bạn có thể sẽ đảm bảo được an ninh hơn hẳn khi kết nối vào mạng Internet lần đầu tiên.[15]

Khi cài đặt một phần mềm mới, hãy tìm hiểu trước nguồn gốc của phần mềm này để đưa ra đánh giá chính xác về sự đáng tin cậy của nguồn gốc phần mềm. Không nên cài đặt những phần mềm không cần thiết chỉ để trang trí màn hình của bạn hay phần mềm chỉ nhằm giúp điền các mẫu thông tin trên Internet được dễ dàng hơn. Chính những phần mềm đơn giản tưởng như vô hại này lại thường chứa đựng những virus hay nguy cơ gây hại nhất được mô tả trong tài liệu này. Nếu mục đích chính của bạn chỉ là một chiếc máy điện toán để đọc thư điện tử và soạn thảo văn bản thì chỉ cần Open Office (http://openoffice.org) và Mozilla Thunderbird (http://mozillamessaging.com/ thunderbird/) mà thôi. Không cần cài đặt phần mềm nào khác gì khác.

14
Bạn có thể đặt một bản miễn phí từ bộ công cụ NGO-in-a-Box tại: www.tacticaltech.org

15
Xem hướng dẫn từ Markus Johansson đẻ cài Windows 2000/XP

2.2 BẢO VỆ MẬT KHẨU

TÓM TẮT

1. Đừng dựa vào chức năng mật khẩu của Windows để bảo vệ thông tin của bạn. Mật khẩu như vậy rất dễ bị phá.
2. Nên tạo mật khẩu với ít nhất là 10 chữ. Bạn cũng có thể dùng một câu viết ngắn làm mật khẩu.
3. Nên ghi lại mật khẩu và cất giữ nơi an toàn hơn là có một mật khẩu ngắn và dễ đoán[16].
4. Nên dùng số, chữ thường, chữ hoa và ký hiệu trong mật khẩu.
5. Đừng bao giờ dùng lại mật khẩu cũ.
6. Đừng dùng mật khẩu có liên quan đến đời sống hoặc sở thích riêng tư của bạn.
7. Đừng cho bất cứ ai biết những mật khẩu quan trọng.
8. Nên đổi mật khẩu mỗi 3-6 tháng.
9. Nên nhớ rằng có rất nhiều phần mềm miễn phí trên mạng dùng để khám phá ra mật khẩu, mật mã của mạng không dây, hoặc bất cứ mật khẩu điện toán nào của bạn.

Mật khẩu tốt là một phần thiết yếu trong việc sử dụng máy điện toán và việc liên lạc điện toán được an toàn. Mật khẩu được dùng để xác nhận việc được phép gia nhập và sử dụng một chức năng, chẳng hạn như vào một trương mục thư điện tử (email), đăng nhập vào một mạng lưới, hoặc làm việc ngân hàng trực tuyến. Mật khẩu cũng giống như là chìa khóa cửa. Bạn có thể dùng nhiều chìa khóa khác nhau cho nhà, cho văn phòng, cho chiếc xe và cho tủ sắt của bạn. Mỗi ổ khóa đều khác nhau, và bạn có một bộ nhiều chìa khóa khác nhau để mở khóa. Như vậy việc đột nhập sẽ khó hơn. Cho dù tên trộm tìm được đúng một chìa khóa, hắn cũng không thể mở hết tất cả mọi cánh cửa. Ổ khóa càng ngày càng tinh vi và đắt tiền. Ổ khóa được làm bằng nhiều thành phần khác nhau với mục đích duy nhất là ngăn ngừa đột nhập. Nguyên tắc trên cũng được áp dụng cho mật khẩu của bạn. Mật khẩu là ổ khóa cho ngân hàng thông tin của bạn. Với sự ra đời của máy điện toán, mật khẩu dùng để bảo vệ thông tin mà thông thường có giá trị lớn hơn nhiều so với những vật được cất giữ trong ngăn tủ hoặc tủ sắt của bạn. Vì thế, nói theo nghĩa kỹ thuật điện toán, mật khẩu của bạn nên tốt ngang hàng với cái tủ sắt đắt tiền nhất, nhằm mục đích bảo vệ thông tin.

Trong thế giới an ninh điện toán, mật khẩu tốt là yếu tố cần thiết và quan trọng nhất của bất cứ hệ thống nào. Lịch sử đã cho thấy rằng phá mật khẩu là phương pháp thông dụng nhất của bọn tin tặc nhằm tấn công hệ thông tin của bạn.

PHÁ MẬT KHẨU

Làm sao để phá được mật khẩu? Có nhiều cách để thực hiện điều này. Một là lén nhìn khi một người nào đó đang đánh mật khẩu. Một cách khác là cài một phần mềm chuyên theo dõi (spyware) để ghi lại tất cả các chữ được

16
Xin xem bài viết từ blog của Bruce Schneier's tại http://www.schneier.com/blog/archives/2005/06/write_down_your.html.

đánh vào máy điện toán và gửi đến cho tin tặc. Cả hai cách đều có thể ngăn ngừa được nếu bạn cảnh giác. Bạn nhớ phải để ý đến chung quanh bạn và luôn cho chạy phần mềm được cập nhật thường xuyên dùng để chống spyware và chống virus điện toán.

Phác Thảo Mật Khẩu

Phác thảo mật khẩu là phương thức đoán mật khẩu bằng cách sưu tầm dữ kiện và thông tin cá nhân của người chủ mật khẩu. Thông thường, mật khẩu phản ảnh lại một điều gì dễ nhớ, chẳng hạn như năm sinh, tên của một thành viên gia đình hoặc tên một người bạn, nơi sinh, đội bóng thích nhất, v.v. Kẻ phác thảo sẽ lưu ý đến những thông tin này và những dữ kiện tương tự khác. Nếu họ có cách tiếp cận văn phòng làm việc của bạn, họ có thể sẽ để ý đến sách trên kệ của bạn. Cách đặt mật khẩu của bạn có thể tha thứ được (ít nhất là cho tới khi bạn đọc xong chương này!) vì khả năng có thể nhớ được nhiều mật khẩu khác nhau mà vừa khó nhớ và vừa không có liên hệ gì với bạn rất là giới hạn. Tuy nhiên, đoán mật khẩu bằng cách sưu tầm thông tin cá nhân về người chủ mật khẩu vẫn là cách thông dụng nhất để phá hoại một hệ thống, và vẫn tiếp tục là cách thành công nhất cho tin tặc có chủ đích.

Nhiều hệ thống mật khẩu trên mạng cho bạn cơ hội phục hồi mật khẩu mà bạn đã mất, miễn là bạn trả lời một 'câu hỏi bí mật'. Vì một lý do nào đó, những câu hỏi bí mật này (được dựng lên khi bạn thành lập trương mục) thường có dính dáng với tên động vật được ưa thích, tên trường học đầu tiên, hoặc họ mẹ của bạn. Điều này làm cho kẻ phác thảo dễ dàng đoán được mật khẩu. Người này không cần phải suy nghĩ nát óc để đoán mật khẩu, mà chỉ cần trả lời đúng câu hỏi bí mật là sẽ nhận được mật khẩu từ email. Nếu bạn được yêu cầu phải dựng lên một cơ chế phục hồi mật khẩu bằng cách trả lời một câu hỏi đơn giản về đời tư của bạn, thì bạn không nên dùng cơ chế đó. Nếu bắt buộc phải làm để hoàn tất thủ tục đăng ký, bạn cứ ghi đại điều gì đó thật khó hiểu. Đừng dựa vào phương pháp phục hồi có dùng đến câu hỏi bí mật để nhớ lại mật khẩu mà bạn đã quên mất.

►Personal passwords are easily guessed

Khai Thác các Liên Hệ trong Xã Hội (Social engineering)

Nhiều người bị lừa phải tiết lộ mật khẩu qua các câu hỏi và màn đóng kịch khéo léo. Tin tặc có thể giả dạng là nhà cung cấp dịch vụ truy cập mạng (ISP) gọi cho bạn, báo rằng dịch vụ đang nâng cấp máy chủ, và rằng để bảo đảm email của bạn không bị mất trong quá trình nâng cấp, dịch vụ cần biết mật khẩu của bạn. Tin tặc cũng có thể giả dạng là đồng nghiệp từ một chi nhánh khác của tổ chức phi chính phủ của bạn và yêu cầu có được mật khẩu để tiếp cận trương mục email nhiều người dùng chung, với lý do là nhân vật biết được mật khẩu hiện đang bệnh và người đồng nghiệp này cần phải gửi đi một lá email khẩn cấp. Phương pháp này gọi là khai thác các liên hệ trong xã hội. Đã có nhiều trường hợp mà nhân viên một cơ quan tiết lộ thông tin có khả năng phá hoại chỉ vì họ bị lừa. Đây vẫn là một cách hữu hiệu cho tin tặc để tiếp cận một hệ thống thông tin.

Không bao giờ tiết lộ thông tin liên quan đến máy điện toán (đặc biệt là mật khẩu và mật mã để tiếp cận) qua điện thoại cho một người nào đó mà danh tánh không kiểm chứng được[11].

17
Lời khuyên của Steven Murdoch, nhà nghiên cứu tại Nhóm Bảo An của Đại Học Cambridge: trước hết phải kiểm chứng danh tánh và tư cách của người gọi, rồi tìm số người đó trong một sổ điện thoại đáng tin cậy và gọi lại cho họ.

Thử tất các dạng mật khẩu (Brute Force)

Thử tất cả các dạng mật khẩu là cách đoán mật khẩu bằng cách phối hợp tất cả các ký tự. Nó có thể thực hiện bằng cách thử từng từ một trong một cuốn tự điển điện tử. Đối với con người thì công việc này mất rất nhiều thời giờ, nhưng đối với máy điện toán thì chỉ mất vài giây đồng hồ. Nếu mật khẩu của bạn là một từ đánh vần chính xác trong tự điển, thì chỉ trong vòng vài phút mật khẩu có thể bị phá bằng cách tấn công bằng cách thử tất cả các dạng mật khẩu. Phải chăng bạn dùng câu mở đầu của một trong 1000 bài hát hoặc bài thơ nổi tiếng để làm mật khẩu? Thế giới điện toán lúc nào cũng phát triển và bành trướng vì cả thế giới văn chương và tư tưởng cũng được chuyển vào. Hiện tại có những bộ sưu tập văn chương bằng điện toán, có thể được dùng để phá mật khẩu của bạn. Bạn nên suy nghĩ kỹ trước khi dùng một mật khẩu với ngôn ngữ tự nhiên, chẳng hạn như một câu nói dễ hiểu hoặc nổi tiếng, hoặc tập hợp nhiều từ, hoặc một câu viết hoàn chỉnh.

Có nhiều hệ thống mật khẩu được bảo vệ chống lối tấn công bằng cách thử tất cả các dạng mật khẩu. Thí dụ như máy ngân hàng hoặc điện thoại di động. Mặc dù mật khẩu của bạn thường chỉ là một tập hợp có bốn số, hệ thống sẽ ngưng hoạt động (bằng cách tịch thu thẻ ngân hàng hoặc khoá điện thoại) sau ba lần đánh sai mật khẩu.

TẠO MẬT KHẨU

Thuật Ngữ Giúp Trí Nhớ

Có nhiều phương pháp tạo mật khẩu khó phá nhưng lại dễ nhớ. Cách phổ biến là mnemonic (một phương pháp hoặc hệ thống để cải thiện trí nhớ, chẳng hạn như dùng vần thơ hoặc viết tắt[18]). Chúng ta hãy lấy một câu thông dụng:

> To be or not to be? That is the question (Hamlet, Shakespeare)
> Ta có thể chuyển câu này thành 2Bon2B?TitQ

Trong thí dụ này, ta đã thay mỗi từ bằng một con số phát âm gần giống hoặc viết tắt, trong đó danh từ và động từ được viết hoa và còn lại là viết chữ thường. Hoặc lấy thí dụ:

> I had a dream, where all men were born equal (Martin Luther King)
> 1haDwaMwB=

Bề ngoài thì mật khẩu này có vẻ viết lăng nhăng, nhưng đối với bạn thì không khó lắm, vì bạn đã biết cách dàn dựng. Có những cách khác như thay con số cho những chữ cái nhìn giống số, viết tắt những từ nhìn giống số, và dùng emoticons.

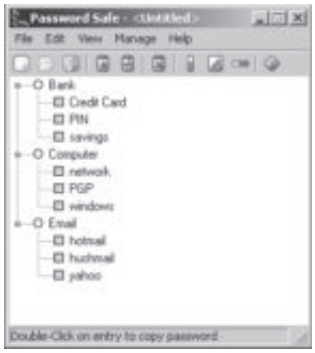
> I, i, l, t = 1 o,O = 0 s, S = 5,2 four, for, fore = 4 two, to, too = 2
> Are you happy today? = rU:-)2d?

Trên đây là những thí dụ căn bản, và bạn luôn có thể tự chế ra phương pháp viết bằng mã số và từ. Bạn nên làm vậy.

Lưu ý: xin đừng dùng những thí dụ trên làm mật khẩu!

18
WordNet – của David Slomin và Randee Tengi

Sử Dụng Phần Mềm



Bước kế tiếp để làm tăng mức độ phức tạp của mật khẩu, là dùng một chương trình tạo ra mật mã[19]. Chương trình này sẽ tạo ra một mật khẩu một cách ngẫu nhiên và lưu lại an toàn. Nhờ vào chương trình tạo ra mật mã, bạn có thể sử dụng mật mã vô cùng phức tạp mà lại không cần phải ghi nhớ! Đây là giải pháp lý tưởng. Chương trình này thường rất nhỏ và có thể chứa trong đĩa mềm hoặc thẻ nhớ USB.

Bạn có thể phân loại mật khẩu của bạn rồi sao mật khẩu lại từ chương trình vào màn hình bằng cách dùng clipboard. Mật khẩu được mã hoá và lưu lại trong chương trình. Do đó, mật khẩu duy nhất mà bạn cần nhớ là mật khẩu để truy cập chương trình.

Phải mất một thời gian bạn mới quen được cách tạo ra và lưu lại tất cả mật khẩu trong một chương trình như vậy, nhưng mà lợi ích an ninh có giá trị rất lớn trong khi bạn chỉ mất chút công tạo ra và lưu lại mật khẩu như vậy.

Mật khẩu là cách bảo đảm an ninh cho thông tin đầu tiên và quan trọng nhất của bạn. Mật khẩu giống như là cửa vào nhà nơi bạn ở. Dùng mật khẩu yếu hoặc không dùng mật khẩu gì cả, thì cũng giống như mở toang cửa nhà suốt đêm. Có thể sẽ không ai đến viếng bạn, nhưng cũng có thể sẽ có người đến ăn trộm hết tài sản của bạn. Xin đặc biệt lưu ý đến cách bạn tạo ra mật khẩu và nơi bạn cất giữ mật khẩu.

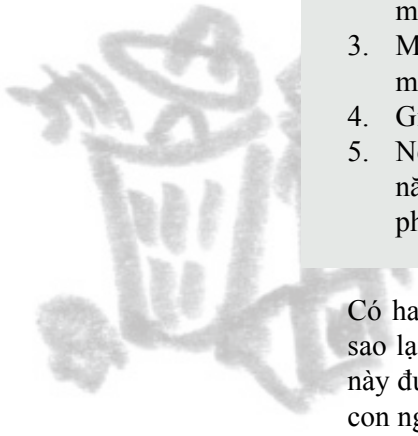
19
Xem chương trình PasswordSafe
http://passwordsafe.scoureforge.net

và Keypass của bộ công cụ NGO-in-a-Box
http://keypass.scourceforge.net

2.3 SAO LƯU, PHÁ HỦY VÀ PHỤC HỒI THÔNG TIN

TÓM TẮT

1. Một kế hoạch sao lưu cần phải bao gồm: tài liệu để lưu trữ, bao lâu phải cập nhật tài liệu lưu trữ, địa điểm và kho lưu trữ.
2. Chỉ xóa dữ liệu khỏi máy điện toán vẫn không đủ vì dữ liệu vẫn có thể phục hồi được. Thông tin nhạy cảm cần phải được lau sạch khỏi máy điện toán.
3. Một thói quen tốt là lau sạch tài liệu tạm thời và dự trữ tạm thời từ mạng, và làm cho máy điện toán có nhiều đĩa trống.
4. Giữ gìn tốt cho nơi chung quanh của máy điện toán.
5. Nếu bạn làm mất đi một tài liệu, thì hãy tìm thật kỹ lưỡng bằng chức năng tìm kiếm của Windows và phân tích đĩa cứng bằng phần mềm phục hồi dữ liệu.



Có hai vấn đề quan trọng nên lưu ý khi làm việc với thông tin là cách sao lại và cách phá hủy thông tin. Máy điện toán làm cho hai quá trình này được thi hành nhanh chóng và hiệu quả, nhưng sơ sót và bất cẩn của con người là nguyên nhân thường gặp nhất làm cho hệ thống bị trục trặc. Chương này sẽ khảo sát lý thuyết đằng sau cách sao lại thông tin điện toán, cách phục hồi dữ kiện bị đánh mất và cách xóa đi mà không cho phục hồi thông tin không cần thiết hoặc nhạy cảm. Chương này cũng sẽ mô tả một thói quen tốt trong lãnh vực này.

Sao Lưu Thông Tin (Backup Information)

Tài liệu quan trọng thường được sao lại. Bản Tuyên Ngôn Độc Lập của nước Mỹ được sản xuất thành 251 bản gốc. Người ta sao chụp hộ chiếu, tờ khai thuế và bằng lái xe của họ. Bản thảo được sao lại trước khi được gửi đến nhà xuất bản. Đây là những biện pháp đề phòng thất lạc tài liệu và thông tin. Máy điện toán làm cho việc sao lại trở thành một thủ tục rất dễ dàng và nhanh chóng. Có nhiều chương trình dùng để tạo một bản sao chính xác của cơ sở thông tin nguyên thủy và lưu bản sao lại tại nơi bạn muốn. Không còn nữa những ngày mà khi bạn làm mất cuốn sổ địa chỉ sẽ làm cho bạn cực nhọc tìm lại những số điện thoại đã quên đi, nhưng bạn sẽ thấy, đó vừa là may mắn vừa là tai họa.

Sao lưu tài liệu điện toán là điều cần thiết, nhưng người ta thường không làm vì tin rằng ‘sẽ chẳng có chuyện gì xảy ra’. Ta dựa vào chính ta và máy điện toán để không bị quên lãng, thất lạc hoặc gây hại thông tin.

Thất lạc thông tin xảy ra ở mức độ cả nhỏ lẫn lớn. Bạn có thể mất một tài liệu vì phần mềm bị trục trặc hoặc bị virus. Bạn cũng có thể mất hết toàn bộ nội dung của máy điện toán vì phần cứng bị trục trặc hoặc bị độc hại. Cho nên bạn phải luôn có một kế hoạch sao lưu cho mọi trường hợp.

Kế Hoạch Sao Lưu
Hãy cân nhắc thể loại, số lượng và nhịp độ sao lưu thông tin của bạn. Bạn nên mang trong người một thẻ nhớ USB có chứa một bản sao của tất cả các tài liệu của bạn. Nếu máy điện toán của bạn có máy chép CD, thì mỗi tuần bạn có thể sao lưu lại rất nhiều tài liệu, hình ảnh và hồ sơ âm thanh và giữ bản sao ở một nơi ngoài máy điện toán. Nếu bạn có một máy chủ tại văn phòng, thì máy này cần phải sao lưu định kỳ không những chỉ tài liệu lưu trong máy mà còn cả cách sắp đặt của phần mềm và của máy.

Hồ Sơ Thường Được Truy Cập
Hồ sơ loại này là tài liệu làm việc mà bạn cần truy cập bất cứ lúc nào. Hồ sơ này được cập nhật thường xuyên, và bạn cần phải có sẵn bản mới nhất.

Dụng cụ thích hợp nhất ở đây là thẻ nhớ USB. Thẻ nhớ USB vừa nhỏ, vừa không có bộ phận không cố định (cho nên ít bị hư hại hơn là đĩa mềm) và thường cung cấp đủ chỗ để chứa đựng nhiều tài liệu. Bạn có thể dễ dàng sao lại nội dung của một folder từ máy điện toán ở nhà hoặc ở văn phòng bạn vào một thẻ nhớ USB[20].

► **Nhịp độ sao lưu: hàng ngày.**

Hồ Sơ Không Thường Được Truy Cập
Đây là toàn bộ hồ sơ lưu trữ, tích lũy theo thời gian. Hồ sơ ít khi được tạo ra và cập nhật. Không cần phải giữ bản mới nhất của mỗi hồ sơ, nhưng sao lưu vẫn cần thiết.

Dụng cụ hữu hiệu nhất dùng để sao lưu trong trường hợp này là CD tẩy chép (CD-RW). Mỗi CD có thể chứa đến 800MB và bạn có thể chép hồ sơ mới chồng lên hồ sơ cũ, và bạn chỉ cần canh giữ một hoặc hai CD mỗi lần[21].

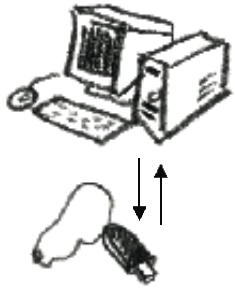
► **Nhịp độ sao lưu: hàng tuần.**

HỒ SƠ HỆ THỐNG

DÀNH CHO CHUYÊN VIÊN

Để tránh quá trình phục hồi mất thời gian trong trường hợp máy điện toán bị trục trặc hoặc hư hại crash, bạn nên theo định kỳ làm một bản sao hình ảnh của toàn bộ máy điện toán bạn. Đây là khả năng cao cấp, có lẽ chỉ giành riêng cho những người quản lý hệ thống hoặc những người canh giữ máy điện toán của bạn. Sao lưu hệ thống là phải sao lại tất cả các chương trình đã được cài đặt (cùng với giấy phép chương trình), phần đăng ký của máy, chương trình điều khiển thiết bị, v.v.

Có một cách sao lưu hệ thống lại là dùng tape drive. Tape drive rất đắt tiền và thường không có kèm theo khi bạn mua máy điện toán. Một cách khác là mua một đĩa cứng di động và sao lưu hệ thống vào đĩa cứng này. Sao lưu toàn bộ hệ thống thường đòi hỏi phải có phần mềm chuyên môn, gọi là chụp ảnh đĩa. Cũng có thể dùng chức năng sao lưu



20
Dùng chương trình như là Allwaysync (http://www.allwaysync.com) để sao lại.

21
Phối hợp dùng chương trình sao lưu Cobian (http://security.ngoinabox.org/cobian_main) và một chương trình chép CD chẳng hạn như DeepBurner Pro (http://www.deepburner.com).

có sẵn trong Windows mà bạn có thể truy cập bằng cách đi đến Start > Programs > Accessories > System Tools > Backup. Để phòng trường hợp máy điện toán bị cháy hoặc bị tai họa gì khác, bạn cần phải có một bản sao của hệ thống được lưu lại ở xa nơi có máy điện toán.

► **Nhịp độ sao lưu: hàng tháng.**

Vì lý do an ninh, đừng làm ra quá nhiều bản sao lưu. Nếu hàng tuần bạn không có khả năng ghi chồng lên CD, thì bạn nhớ phải kỹ càng hủy đi những bản cũ lỗi thời. Làm như vậy thì tin tặc sẽ khó tìm hồ sơ sao lưu hơn, và bạn sẽ không bị nhầm lẫn không biết CD nào chứa đựng bản sao mới nhất của hồ sơ của bạn.

PHÁ HỦY THÔNG TIN

Hầu như không thể nào hoàn toàn xóa hết mọi thông tin lưu trong máy điện toán mà không dùng tới biện pháp cắt đứt, đốt cháy hay đập vỡ máy ra thành nhiều mãnh nhỏ. Mặc dù bạn có thể đinh ninh rằng Windows dọn sạch hết 'Thùng Rác', sự thật không phải là vậy. Ta phải thật đề phòng để đảm bảo là dữ kiện không cần đến nữa sẽ được xóa đi kỹ càng.

Từ năm 2000 đến năm 2002, các nhà nghiên cứu Simson Garfinkel và Abhi Shelat từ MIT mua một số lượng lớn đĩa cứng đã dùng qua từ nhiều tay buôn đĩa qua nhà bán đấu giá trên mạng eBay và kiểm tra các đĩa này xem có còn chứa thông tin thặng dư hay không. Hai nhà nhiên cứu hồi phục được trên 6000 số thẻ tín dụng và các trang mạng được dự trữ tạm thời lại, nơi mà một số thẻ tín dụng này được sử dụng, hồ sơ y khoa, thư tình và tranh ảnh khiêu dâm, cùng nhiều thứ khác. Có một đĩa cứng dường như đã từng nằm trong máy ATM ở Illinois.[22]

Phục hồi (restore) dữ kiện là một công nghệ đang phát triển, và có nhiều hãng cũng như nhiều cơ quan chính quyền đã trở nên tân tiến không ngờ trong việc phục hồi dữ liệu bị mất và hư hại. Còn một yếu tố nữa trong an ninh thông tin là các tổ chức nhân quyền không những chỉ cần phải giữ cho thông tin nhạy cảm được an toàn, mà còn cần phải xoá bỏ thông tin cho kỹ lưỡng. Trong phần này, ta sẽ khảo sát quá trình xoá bỏ vĩnh viễn thông tin không cần đến nữa từ máy điện toán của bạn.

Các Vấn Đề Khi Xoá Thông Tin

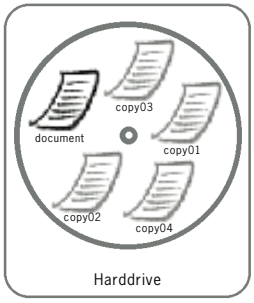
Không có chức năng điện toán nào có thể xoá thông tin cả. Nói cho chính xác, máy điện toán chỉ có khả năng ghi lại thông tin mới vào đĩa cứng. Khi bạn xoá một hồ sơ trong Windows, chẳng qua là bạn bảo máy điện toán rằng khoảng đĩa này có thể ghi chồng thông tin mới lên (mặc dù bề ngoài khoảng đĩa này giống như là 'trống không'). Windows chỉ xoá đi cái icon của hồ sơ và cái reference tên từ màn hình, làm ra vẻ là hồ sơ không còn đó nữa. Nhưng Windows không thực sự xoá dữ kiện đi từ đĩa cứng. Bạn có thể so sánh việc xoá hồ sơ đây giống như là việc lấy đi cái nhãn hiệu của một tủ đựng hồ sơ, nhưng vẫn để hồ sơ y nguyên trong ngăn tủ. Miễn là bạn chưa ghi thông tin mới chồng lên đúng chính xác vào khoảng đĩa đó trong đĩa cứng, thông tin cũ vẫn còn đó và vẫn có thể nhìn thấy được dễ dàng nhờ vào phần mềm chuyên môn.

22
Remembrance of Data Passed: A Study of Disk Sanitization Practices, Xuất bản IEEE

An ninh & Đời tư, Quyển 1, số 1, 2003 By Simson L. Garfinkel and Abhi Shelat, Massachusetts Institute of Technology.

Lau Sạch

Ngoài việc giải từ, đốt cháy, hâm bằng máy vi ba, hay nuốt vô bụng dụng cụ lưu hồ sơ điện toán, chỉ còn một cách chắc ăn để xoá đi thông tin không cần thiết mà không phá hư dụng cụ. Đó là dùng dữ kiện vô nghĩa để ghi chồng lên dữ kiện hiện có. Phương pháp này được gọi là lau sạch. Bạn có thể lau sạch một hồ sơ, hoặc lau sạch khoảng đĩa 'trống không' trong đĩa cứng. Lau sạch khoảng 'trống không' bằng cách truy tìm tất cả các khoảng trống hiện chưa sử dụng phân bố (hoặc khoảng trống không được hồ sơ nào sử dụng) và ghi chồng lên bằng thông tin vô nghĩa. Các chuyên gia đồng ý rằng ít nhất là cần lau sạch qua một lần để tránh phục hồi thông tin của bạn.[23]



►Multiple copies of your document are c reated every time you edit it

Phần mềm lau sạch như là Eraser có thể hợp nhất với Windows để lau sạch hồ sơ hoặc nội dung của 'Thùng Rác' mà chỉ bằng hai cái nhấp chuột. Eraser cũng có thể lau sạch hết mọi tàn dư của hồ sơ cũ còn lưu lại trong 'khoảng trống' của đĩa cứng hoặc dụng cụ truyền thông của bạn. Chức năng này còn gọi là lau sạch khoảng trống.

Bạn phải biết rằng không những là tài liệu của bạn, mà các hồ sơ khác do Windows sử dụng và thu thập trong lúc bạn dùng máy điện toán và lướt mạng cũng nên được lau sạch.

DÀNH CHO CHUYÊN VIÊN

SWAP FILE

Có một chức năng khác của Windows mà ít người biết đến, là lưu lại tài liệu cá nhân của bạn trong swap file (còn gọi là paging file). Windows sử dụng swap file để hoạt động được dễ dàng hơn. Nói một cách đơn giản, swap file là một phần của đĩa cứng mà Windows tự ấn định ra để quản lý mọi hoạt động của bạn. Khi bạn tắt máy đi, swap file vẫn còn giữ lại tất cả mọi thông tin trong đó. Cho dù bạn dùng phần mềm để mã hóa, lúc lưu lại trong swap file hồ sơ của bạn cũng không được mã hóa. Tốt hơn hết là nên tắt cái chức năng dùng swap file (bạn nên có ít nhất 256MB RAM trong máy để thay thế chức năng dùng swap file), hoặc dùng một dụng cụ lau sạch để an toàn xóa bỏ thông tin từ swap file trước khi tắt máy.[24] Để tắt chức năng dùng swap file trên Windows 2000 và XP:

Chọn: Start > Settings > **Control Panel** > System
Nhấn: Advanced tab
Nhấn: Performance
Nhấn: Virtual memory (advanced > virtual memory for XP)
Chọn không dùng swap file option, hoặc sửa nó thành '0'.

Nếu máy của bạn là laptop, thì bạn hãy tắt chức năng hibernation. Không có chức năng này, thì bạn sẽ mấy thêm 30 giây, nhưng sẽ làm giảm đi rất nhiều nguy cơ có người cập nhật thông tin trên laptop của bạn.

Chọn: Start > Settings > **Control Panel** > Power Options
Nhấn: Hibernation tab
Chọn không dùng: Enable Hibernate

23
Công trình Security-in-a-Box có cung cấp dụng cụ Eraser để lau sạch đi thông tin không cần thiết từ máy điện toán http://security.ngoinabox.org/eraser_main

24
Xin xem thêm các dụng cụ lau sạch như Eraser (http://www.heidi.ie/eraser) hoặc BCWipe (http://www.jetico.com/bcwipe.htm), cũng nằm trong CD Digital Security Toolkit.

Hồ Sơ Tạm
Đây là các hồ sơ mà máy điện toán thu thập được trong khi bạn đang sử dụng máy. Hồ sơ này gồm có tài liệu còn đang viết dang dở hoặc chưa được lưu lại, đồ thị và hình ảnh từ mạng (còn gọi là cache), cùng vô số hồ sơ khác, mà có thể tiết lộ được hoạt động của bạn trên máy điện toán.

Hãy hình dung bạn đang viết một bản báo cáo lớn. Bạn mất đi một tuần để viết báo cáo, trong đó mỗi ngày mất đi vài tiếng. Mỗi lần bạn nhấn 'save' trước khi tắt máy và rời sở làm, Windows sẽ tạo ra một bản sao khác của tài liệu này và lưu lại trong đĩa cứng. Sau một tuần sửa chữa bài viết, bạn sẽ có nhiều bản được tạo ra tại mỗi giai đoạn viết bài, được lưu lại trong đĩa cứng. Lý do là vì mỗi lần bạn lưu hồ sơ lại, Windows sẽ không tìm ra đúng chính xác địa điểm trong đĩa của bản đầu tiên và viết chồng lên. Thực sự Windows chỉ ghi lại bản mới nhất vào một khoảng chưa phân bố trong đĩa cứng. Cho nên đây có thể gây ra rắc rối khi bạn cần phải xóa hết mọi dấu vết của hồ sơ này từ máy điện toán của bạn

Bạn nên thường xuyên xóa đi nội dung của những folder này. Để xóa đi các hồ sơ tạm này một cách an toàn (không phục hồi được), bạn hãy sử dụng dụng cụ CCleaner (xin xem thêm từ công trình Security-in-a-Box[25]).

Một điều rất quan trọng là bạn phải xóa hết mọi hồ sơ tạm mà máy thu thập được trong lúc bạn đang sử dụng máy, đặc biệt là khi bạn sử dụng máy công cộng, chẳng hạn như máy từ dịch vụ Internet hoặc từ thư viện. Bạn có thể mang theo một bản lưu động của phầm mềm CCleaner trong thẻ nhớ USB và dùng nó để lau sạch hết mọi hồ sơ tạm từ máy điện toán.[26]

Nguyên tắc lau sạch
Nếu bạn quyết định xóa hết mọi dấu vết của hồ sơ cũ và hồ sơ tạm từ máy bạn, thì bạn có thể làm theo những bước sau, bằng cách sử dụng một dụng cụ lau sạch từ công trình Security-in-a-Box, hoặc bằng cách tự viết ra phần mềm lau sạch.

- Nhớ làm một bản sao lưu của mọi tài liệu, giấy phép phần mềm và registry của Windows.
- Lau sạch mọi folders tạm từ máy.
- Lau sạch mọi 'khoảng trống' từ máy.
- Tập thành thói quen lau sạch mọi hồ sơ tạm trước khi tắt máy và sau khi sử dụng máy công cộng.
- Lau sạch khoảng trống trên thẻ nhớ USB, thẻ nhớ của máy ảnh kỹ thuật số và các CD tẩy chép.

HỒI PHỤC THÔNG TIN
Hồ sơ chưa được lau sạch vẫn có thể phục hồi được. Có những phần mềm dùng để truy tìm hồ sơ bị mất hoặc hư hao từ trong đĩa cứng hoặc dụng cụ truyền thông khác. Dùng từ khóa 'data recovery tools' để tìm trên mạng, hoặc cài đặt chương trình UndeletePlus từ trong công trình Security-in-a-Box[27].

25
http://security.ngoinabox.org/ccleaner_main

26
Muốn biết thêm chi tiết xin hãy xem công trình Security-in-a-Box http://security.ngoinabox.org/chapter_6_2

27
http://security.ngoinabox.org/undelete_main

Bạn cũng có thể lợi dụng việc dụng cụ điện tử thiếu khả năng xóa thông tin một cách hợp lý. Chẳng hạn bạn có thể chụp một tấm ảnh trên máy chụp kỹ thuật số, rồi xóa ảnh đi. Dùng cách này, bạn có thể làm rối đi hình ảnh đầu tiên. Sau đó, khi cần thiết bạn có thể sử dụng chương trình phục hồi thông tin để phục hồi lại phần thông tin bị xóa đi. Tuy nhiên bạn nên cẩn thận đừng để ghi chồng lên tấm ảnh cần thiết (bằng cách chụp một hình khác chồng lên). Cần phải tính toán trước và nghiên cứu kỹ để có thể sử dụng phương pháp này được an toàn.

Phòng Ngừa

Để tránh máy không bị hư hại và mất tài liệu, bạn cần phải cẩn thận quan tâm đến sự ổn định và môi trường chung quanh máy. Đừng ăn uống, hay làm gì khác mà có khả năng gây ảnh hưởng đến máy trong khi bạn đang ở gần máy. Vì bản chất phức tạp của mạch điện, máy điện toán không thích hợp được với nước hoặc từ trường. Giữ máy bạn cách mặt đất, nếu không khi có bước chân mạnh hoặc có người nhảy nhót, máy sẽ lắc lư. Bảo vệ máy đừng để cường độ (tension) điện đột nhiên tăng cao bằng cách tạo sự quân bình hoặc bằng fused sockets. Bạn nên cân nhắc để mua nguồn điện phụ trợ. Tốt hơn hết là bạn hỏi một chuyên gia tại một cửa hàng bán máy điện toán để được giải thích cặn kẽ hơn về những điều trên và làm thế nào để đề phòng máy bạn bị hư hại.

2.4 MẬT MÃ HỌC

TÓM TẮT

1. Mã hóa là quá trình biến thông tin trở thành không truy cập được với mọi người, trừ những người liên quan. Bạn có thể mã hóa một bức thư, một bức email hoặc cả một máy điện toán.
2. Để liên lạc bằng mã hóa, ta dùng hệ thống dùng khóa chung. Phương pháp mã hóa của ta gồm có một khóa chung và một khóa riêng. Ta dùng chung khóa chung với những ai muốn liên lạc với ta, và họ phải mã hóa mỗi bức thư gửi đến ta bằng khóa chung này.
3. Mức an ninh của một hệ thống mã hóa dùng khóa chung lệ thuộc vào hiệu lực của cái khóa chung, vào một máy điện toán không có virus và spyware, và vào một mật khẩu tốt để bảo vệ khóa riêng của bạn.
4. Ta có thể đề phòng email bị lục soát trong khi thư đang được chuyển đến nơi gửi bằng cách dùng chữ ký kỹ thuật số.
5. Mức độ an ninh mà mã hóa cung cấp đã làm cho sự thực hành và lý thuyết của mã hóa bị cấm trong vài đất nước.

LỊCH SỬ

Mật mã học là môn học có liên quan đến kỹ thuật ngôn ngữ học và toán học để bảo vệ thông tin. Bức thư được mã hóa để không ai đọc được, trừ những người có liên quan. Lịch sử lâu dài và đầy màu sắc của mật mã học được bắt nguồn tư thế kỷ thứ 5 trước công nguyên, khi người Spartan phát minh ra phương pháp mã hóa đầu tiên của nhân loại bằng cách dùng hai gậy gỗ giống hệt nhau và một tờ giấy da. Giấy da được cuộn chung quanh gậy, và bức thư được viết theo chiều dọc. Khi mở giấy da ra, chữ có vẻ như được viết không theo thứ tự gì cả. Giấy da được gửi đến người nhận, và người nhận có một cây gậy giống hệt để đọc bức thư. Có những phương pháp khác để bảo vệ an ninh thông tin gồm có mật mã học ngôn ngữ (chẳng hạn như viết tượng hình) và steganography, nghĩa là quá trình che dấu sự tồn tại của chính bức thư.

Scytale
Source: Wikipedia.org
http://en.wikipedia.org/wiki/Cryptology

Bức thư được viết trên giấy da dọc theo chiều dài cây gậy (scytale). Scytale sử dụng cái mà ngày nay gọi là mật mã hoán vị, tức là cách sắp xếp lại thứ tự của các chữ cái trong một bức thư12.

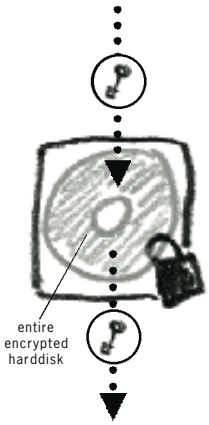
Không nên quá đề cao sự an toàn, nếu chỉ do ngành mật mã học cung cấp. Yếu điểm của nó thường là kết quả của lỗi con người phạm phải hoặc lỗi kỹ thuật trong toàn bộ thủ tục an ninh. Một số quốc gia cũng đã ban ra luật cấm không cho dùng mật mã học. Các nhà toán học, khoa học gia và hoạt động dân quyền ở Mỹ đã phải chiến đấu suốt 20 năm dài để ngăn cản chính phủ Mỹ không được ngăn cấm công chúng được truy cập và sử dụng mật mã học, cái mà ngày nay gọi là Cuộc Chiến Mật Mã.

MÃ HÓA

Mã hóa (và ngược lại là giải mã) là một ngành học phổ biến trong ngành mật mã học. Mã hóa hoạt động bằng cách áp dụng một mô hình toán học lớn vào một tập hợp thông tin rồi chuyển thông tin sang mật mã, làm cho thông tin trở thành không đọc được đối vơi những ai không có cách giải mã, mà còn gọi là mã khóa.

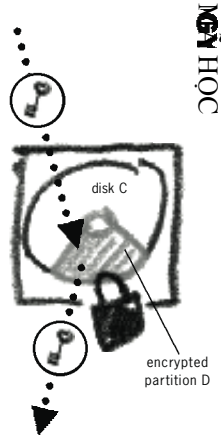
Mã Hóa Đĩa

Bạn có thể dùng mã hóa để bảo vệ toàn bộ đĩa cứng. Thực chất là bạn mã hóa từng bit thông tin trên đĩa, để chỉ có bạn là người có mật khẩu có thể truy cập được thông tin. Mỗi khi thông tin được rút ra từ máy bạn (chẳng hạn như từ đính kèm email) thông tin được tự động giải mã. Nếu máy bạn bị mất cắp, người khác sẽ không truy cập được thông tin nằm trong máy[28].



Trên máy bạn cũng có thể tạo ra một đĩa ảo được mã hóa. Cách này có thể thích hợp với những ai không muốn mã hóa toàn bộ máy điện toán, mà chỉ muốn phân bố khoảng trống để lưu lại thông tin được an toàn. Nếu máy bạn còn dư 5GB trên đĩa, bạn có thể phân bố ra một khoảng trống chiếm 1GB. Khoảng phân bố này trông giống như là một đĩa mới gắn vào máy (thực sự ra đĩa này không phải là mới, cho nên mới gọi là đĩa ảo). Khoảng phân bố này được mã hóa, và bạn có thể lưu tài liệu vào đây.[29]

Bạn có thể sắp đặt cho chương trình email (thí dụ Thunderbird) để lưu lại tất cả email vào trong khoảng phân bố đã được mã hóa. Chỉ có bạn là người có mật khẩu mới có thể truy cập được email trên khoảng phân bố này.



Bạn cũng có thể mã hóa toàn bộ thẻ nhớ USB hoặc các dụng cụ di động khác. Việc này rất là có ích khi ta đi du lịch với mọi tài liệu nằm trong thẻ nhớ USB. Bạn có thể chạy chương trình như TrueCrypt trực tiếp từ thẻ nhớ USB, để bạn không cần phải cài đặt chương trình này vào mỗi máy điện toán có chứa những tài liệu được mã hóa mà bạn muốn truy cập.

Mã Hóa Dùng Khóa Chung

Các phương pháp truyền thống để mã hóa thông tin mà bạn muốn chia sẽ với người khác đòi hỏi bạn phải đưa người kia mật khẩu để giải mã. Đây không phải là cách an toàn lắm, vì mật khẩu của bạn có thể bị tiết lộ trong quá trình giải mã. Để tránh tình trạng này, các nhà toán học đã sáng tạo ra cách mã hóa dùng khóa chung (PKE). Đây là phương pháp thông dụng nhất cho việc mã hóa liên lạc (thí dụ là email) ngày nay.

Khi sử dụng PKE, khóa của bạn gồm hai phần: một khóa chung (public key) và một khóa riêng (private key). Hai khóa này gom lại thành một đôi khóa. Hai khóa phối hợp chặt chẽ; khi bạn mã hóa bằng khóa này thì bạn giải mã bằng khóa kia. Đây là một phần thiết

28
Vì dụ của một phần mềm có thể mã hóa toàn bộ đĩa cứng là CompuSec (http://www.ce-infosys.com) Bạn cũng có lấy thêm chi tiết ở NGO in a Box.

29
Một chương trình điển hình để mã hóa toàn bộ đĩa cứng, tạo ra một khoảng phân bố được mã hóa hoặc đĩa ảo, là TrueCrypt, có sẵn trong công trình Security-in-a-Box (http://security.ngoinabox.org/truecrypt_main)

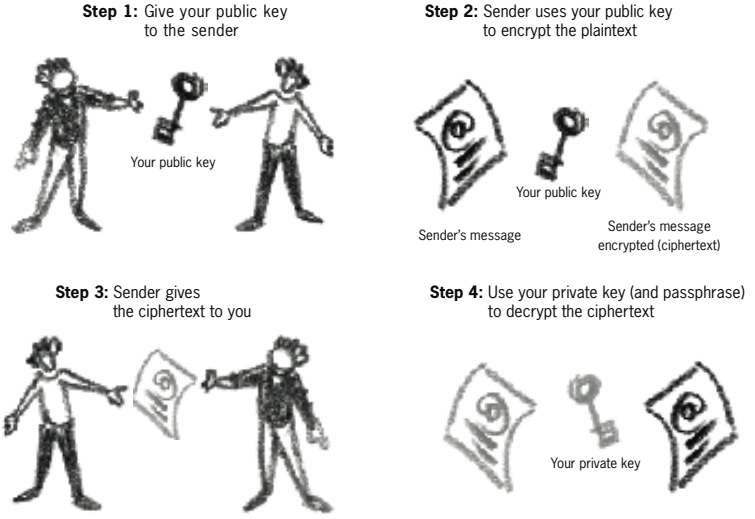
yếu của PKE và là nền tảng cho sự an toàn và cũng là yếu điểm của PKE.

Bạn chia sẽ khóa chung với những ai bạn muốn liên lạc. Bạn cũng có thể tải khóa chung lên một máy chủ để chứa khóa trên mạng. Khóa riêng thì được giữ bí mật trên máy hoặc đĩa mềm của bạn và hơn nữa còn được bảo vệ bằng một mật khẩu mà chỉ riêng bạn mới biết. Đừng cho bất cứ ai biết khóa riêng này. Nếu bạn nghĩ rằng mật khẩu đã bị tiết lộ (hoặc mất cắp) thì bạn phải hủy bỏ đôi khóa đi và tạo lại đôi khóa từ đầu.

Mã Hóa và Giải Mã Một Bức Thư[30]

Trong hệ thống PKE, bức thư được mã hóa bằng khóa chung trước khi gửi đến cho ta, và ta giải mã bằng khóa riêng. Khi có người muốn gửi cho bạn một bức thư được mã hóa, để lấy khóa chung họ sẽ hỏi bạn hoặc tự tìm ra trên một máy chủ chứa khóa trên mạng.

Thí Dụ: Bạn có một bức thư mà bạn muốn mã hóa trước khi gửi đến cho tôi. Trước tiên tôi phải đưa bạn cái khóa chung. Bạn dùng khóa chung này để mã hóa bức thư và gửi cho tôi bằng email hoặc bằng cách khác. Chỉ có tôi là người duy nhất có thể



giải mã được bức thư này, bởi vì chỉ có tôi mới có được mắt xích thất lạc, tức là cái khóa riêng của tôi.

Lưu Ý: chữ "plaintext" có nghĩa là bức thư còn nguyên thủy, trong khi "cipher text" có nghĩa là bức thư đã được mã hóa.

Phương pháp này làm thuận tiện cho việc trao đổi bức thư được mã hóa mà không phải chia sẻ mật khẩu, và đột ngột làm tăng lên sự an ninh và tính thiết thực trong liên lạc. PKE đã được ứng dụng trong email, chat mạng, lướt mạng và nhiều chức năng mạng khác. Mức độ an ninh của phương pháp này gây ra nhiều khó khăn đối với nhiều chính quyền. Ứng dụng thành công của

30
Đề nghị bạn dùng chương trình có thể thi hành PKE là GPG4Win (http://www.gpg4win.org) hoặc bạn có thể cài đặt chương trình email Thunderbird có gồm Engimail extension, có ghi rõ trong công trình Security-in-a-Box (http://security.ngoinabox.org/thunderbird_usingenigmail)

phương pháp này tạo ra mức độ kín đáo cao làm cho nhiều cơ quan theo dõi và tình báo rất lo ngại.

An Ninh Của Khóa

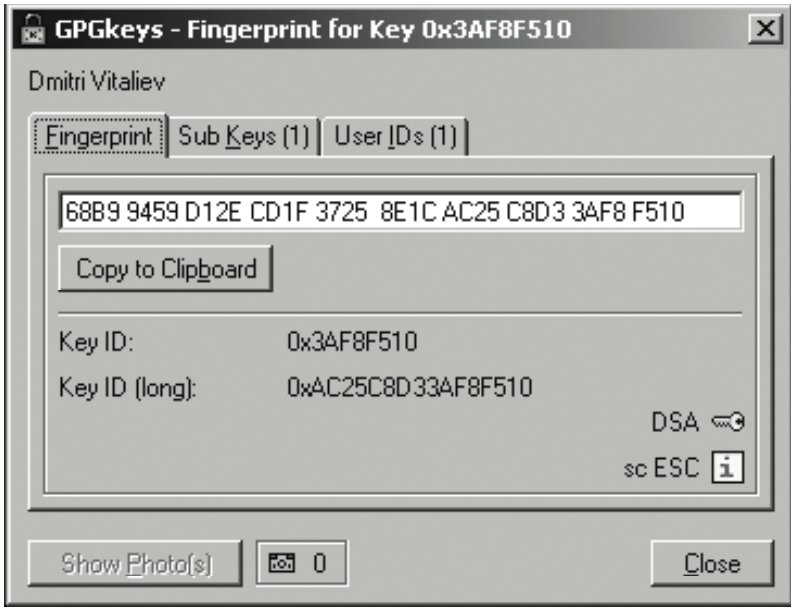
Mức độ an toàn của mã hóa lệ thuộc vào:

- Kích thước của đôi khóa (thường dài 2048 bit)
- Khả năng làm cho khóa chung của người nhận được có hiệu lực
- Sự bảo vệ mật khẩu dùng để mở khoá riêng

Hệ thống PKE dựa vào cách nhận diện chính xác của khóa chung và khóa riêng. Khi bạn mã hóa một bức thư dành cho tôi bằng khóa chung của tôi, bạn muốn bảo đảm rằng cái khóa này thuộc về tôi. Hãy nghiên cứu đặc tính của một đôi khóa.

Một đôi khóa được nhận diện bởi 5 đặc điểm rõ ràng:

- Nhận diện người dùng: thường là địa chỉ email của người giữ khóa. Nhớ là phải đánh vần địa chỉ cho đúng.
- Nhận diện khóa: một cách nhận diện đặc biệt do chương trình mã hóa tự động sinh ra.
- Dấu tay (fingerprint): (cũng được gọi là MD5 và SHA1. Xin đọc phần 'Mã Hóa Trên Mạng' để biết thêm chi tiết) đây là một cách nhận diện đặc biệt do khóa chung sinh ra.
- Ngày làm ra: ngày đôi khóa được tạo ra.
- Ngày mãn hạn: ngày đôi khóa mãn hạn.



►Fingerprint as seen in the GPGshell program

Bạn hãy thử kiểm tra lại các chi tiết nói trên trước khi dùng khóa chung để liên lạc với một người khác. Bởi vì mã hóa dùng khóa chung không đòi hỏi bạn phải dùng chung mật khẩu với người nhận bức thư, điều quan trọng là bạn phải nhận diện chính xác cái khóa chung. Khóa chung dễ chế tạo nhưng những đặc điểm

nhận dạng cũng có thể bị giả mạo. Vì vậy bạn nên xác minh khóa chung của người đó trước khi sử dụng khóa (xem thêm ở phần 'Chữ Ký Điện Tử' ở dưới đây). Sau khi bạn đã xác định được rằng khóa chung này do người đó làm ra, bạn có thể 'ký' vào khóa. Làm như vậy tức là bạn bảo cho chương trình biết là bạn tin tưởng giá trị của khóa và muốn dùng khóa[31].

Kích thước của khóa thường là 2048 bit. Người ta cho rằng mức độ mã khóa này phức tạp đến nỗi không máy điện toán hiện đại nào có thể phá nỗi[32].

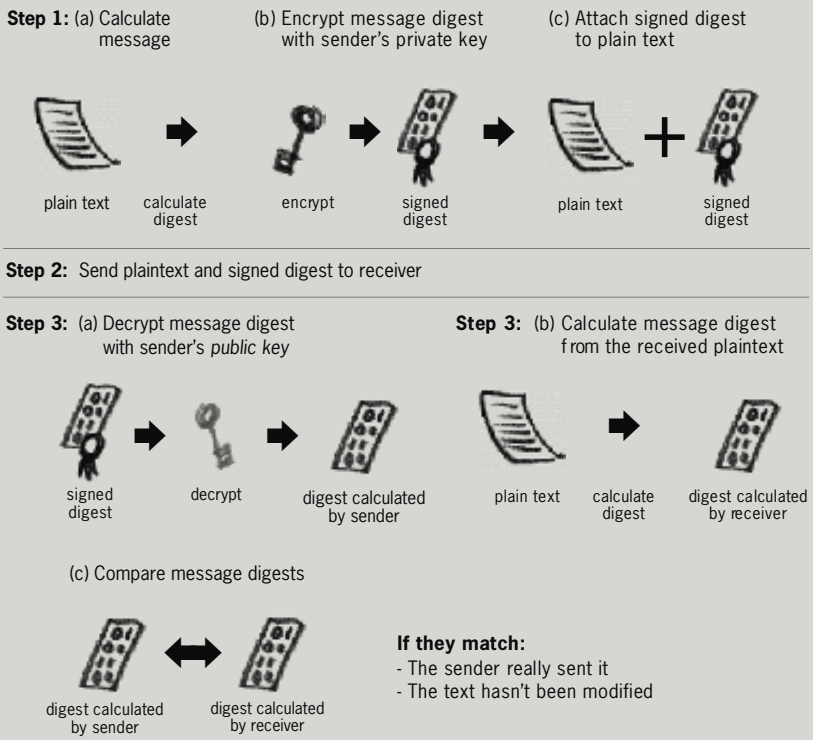
31
Khi làm vậy, bạn cũng bỏ chữ ký vào trong khóa này; nếu bạn gửi khóa đó cho ai đó, người ta sẽ thấy chữ ký của bạn và biết được rằng bạn tin tưởng giá trị của khóa này.

32
Xin xem bài viết tại http://www.keylength.com/en/3/ để biết thêm chi tiết về kích thước cần thiết của khóa trong hiện tại và tương lai.

DÀNH CHO CHUYÊN VIÊN

Chữ Ký Điện Tử (Digital Signature)

Chúng ta cần khả năng kiểm tra xem bức thư có bị giả mạo không. Có thể kiểm tra bằng chữ ký điện tử, vốn cũng dùng PKE để hoạt động. Khi bạn ký điện tử vào một bức thư, bạn bỏ vào bức thư một công thức toán đặc biệt, rút ra từ kích thước, ngày và nội dung riêng của bức thư. Công thức này lại được mã hóa bằng khóa riêng của bạn, để người nhận có thể kiểm chứng được. Sau khi giải mã, công thức trong chữ ký được so sánh với bức thư nhận được và xác nhận là bức thư đã được thay đổi chưa từ khi được ký điện tử vào. Hầu như không thể nào thay đổi nội dung bức thư mà không làm mất hiệu lực chữ ký được.



▶ Digital signatures schematic

Một số chương trình (chẳng hạn là GnuPG) có chức năng PKE có thể hợp nhất với chương trình email (chẳng hạn GnuPG với Thunderbird sử dụng Enigmail extension[33], hoặc với MS Outlook sử dụng G Data GnuPG plug-in[34]), làm cho cả hệ thống được hoạt động đơn giản và nhanh hơn.

Bạn nên mã hóa mọi thư từ trao đổi sau khi bạn và những người bạn liên lạc đã cài đặt và bắt đầu sử dụng PKE. Điều này loại trừ đi khả năng làm người khác nghi ngờ khi bạn gửi đi một lá thư đơn độc được mã hóa mà có chứa đựng thông tin nhạy cảm.

Tóm lại, sử dụng mã hóa thực sự không khó lắm khi ta có sẵn phần mềm hiện đại.

Những điểm chính cần nhớ gồm:

- Bạn phải tạo ra một đôi khóa và giữ khóa riêng được an toàn.
- Bạn mã hóa bức thư bằng khóa chung của người nhận.
- Bạn nên luôn kiểm tra khóa của người nhận bằng cách kiểm lại dấu tay.

Sự Bất An Của Mã Hóa

Vấn đề lớn nhất khi mã hóa là đôi khi mã hóa làm cho ta một cảm giác an toàn giả tạo. Chỉ vì bạn đã sử dụng mã hóa, không có nghĩa là bức thư của bạn sẽ được an toàn 100%. Đương nhiên mã hóa vẫn là một phương pháp xuất sắc để nâng cao mức độ an toàn, nhưng mã hóa không phải là hoàn hảo. Vấn đề chính đối với an ninh của PKE là yếu tố con người: những lỗi lầm phạm phải khi ta bất cẩn hoặc thiếu ý thức. Sau đâu tôi sẽ trình bày ba cách để phá mã hóa của bạn.

- Khóa riêng bị lộ. Nếu tin tặc lấy được khóa riêng của bạn bằng cách truy cập máy bạn hay bằng cách nào khác, hắn chỉ cần phá mật khẩu bảo vệ khóa riêng là xong. Phá mật mã bằng cách thử tất cả các dạng mật khẩu (dùng một chương trình phá mật khẩu để thử hết mọi phối hợp thông thường và ngẫu nhiên) hoặc bằng cách lén nhìn bạn trong khi bạn đang đánh mật khẩu trên bàn phím. Có một cách khác để ăn cắp mật khẩu là cài đặt chương trình thâu chữ (keylogger), bằng cách truy cập vào máy bạn nhờ vào đính kèm trong email. Keylogger sẽ thâu lại mọi chữ bạn đánh vào bàn phím, rồi gửi thông tin này cho một địa chỉ trên mạng hoặc email. Bằng cách này, tin tặc có thể lấy được mật mã mà bạn dùng để truy cập khóa riêng mà không cần có mặt cạnh bên máy để truy cập máy của bạn.

Giải pháp ở đây là dùng chương trình được cập nhật để chống virus và chống spyware, và tường lửa. Hy vọng giải pháp này hoặc sẽ khám phá ra sự hiện diện của một chương trình thâu chữ, hoặc sẽ ngăn chương trình này không được gửi mật khẩu của bạn ra ngoài. Nên cẩn thận khi bạn đánh mật khẩu, và nên lưu ý đừng để ai khác thấy được bàn phím hoặc màn hình của máy bạn. Hầu hết các chương trình mã hóa đều không cho hiện mật khẩu ra trên màn hình. Bạn phải đánh mật khẩu theo kiểu 'mù'.

33
Hãy xem NGO in a Box – Security Edition

34
http://www3.gdata.de/gpg/download.html

- Hệ phục hồi khóa (key recovery). Bởi vì mã hóa hiện đã được hợp nhất vào nhiều dụng cụ điện tử hơn và được sử dụng hàng ngày, cơ cấu an toàn cao độ của mã hóa đã trở thành một vấn đề đối với nhiều cơ quan chính phủ và cơ quan hành pháp. Qua nhiều năm, các cơ quan này đã và đang cố gắng hoàn thành hệ phục hồi khóa (giao kèo khóa) nhằm mục đích giúp các cơ quan truy cập được khóa riêng của bạn. Ngoài ra, nhiều chính phủ đã bắt đầu ban ra luật lệ bắt buộc bạn phải nộp khóa riêng của bạn để chính phủ lưu lại. Một số chương trình mã hóa có nguồn kín, mà phương pháp mã hóa chưa được thử nghiệm công khai, thực ra cung cấp một cửa hậu cho các cơ quan an ninh. Mặc dù hành động này đã bị nhiều quốc gia cho là bất hợp pháp, nó vẫn còn nằm trong nhiều bản phần mềm và phần cứng. Giải pháp cho nó là bạn hãy sử dụng các sản phẩm có nguồn mở (như GnuPG), đã được cộng đồng mạng phân tích và thử nghiệm kỹ lưỡng.

- Giá trị và nguy hiểm của khóa chung. Như đã trình bày trong chương này, giá trị của cái khóa chung mà bạn dùng để mã hóa là trọng tâm của mọi vấn đề an ninh trong ngành mật mã học sử dụng khóa chung. Vấn đề là ở chỗ khóa chung có thể bị giả mạo dễ dàng. Khi một người dùng mã hóa bất cẩn, có thể làm cho ta sử dụng khóa của đối phương mà cứ tưởng là khóa của người khác. Hãy lưu ý kỹ càng khi nhận và nhập khóa chung. Những bước để kiểm chứng giá trị của khóa chung đã được trình bày ở phần trên. Mặc dù việc này có thể làm chậm đi chút đỉnh quá trình liên lạc, bạn không nên bỏ qua những bước này.

Đương nhiên là cũng có những phương pháp truyền thống là ra mặt hăm dọa và ép buộc để bạn tiết lộ mật khẩu.

Nên chọn chương trình mã hóa đã được công khai kiểm tra là không có cửa hậu (chẳng hạn như PGP, GnuPG, TrueCypt). Hãy lưu ý xem luật lệ nơi bạn ở có cho phép dùng mã hóa không, và nếu có thì ở mức độ phức tạp nào (kích thước của khóa)[35]. Bạn cũng nên biết rằng luật lệ hiện tại ở xứ bạn có thể bắt buộc bạn phải tiết lộ mật khẩu cho chính quyền. Hãy gắng tìm hiểu xem có luật bảo vệ sự riêng tư hay không, để bạn dùng để tránh tình trạng phải tiết lộ mật khẩu.

25
Xin xem thêm bản thăm dó Luật Mã Hóa do tiến sĩ Dr. Bert-Jaap Koops duy trì tại http://rechten.uvt.nl/koops/cryptolaw/

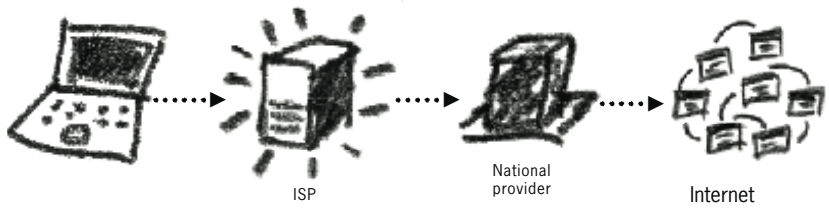
2.5 THEO DÕI TRÊN MẠNG

TÓM TẮT

1. Theo dõi hoạt động trên mạng và email của bạn là một công việc đơn giản mà nhiều cơ sở thương mại và chính quyền trên toàn thế giới đang thi hành.
2. Cookie thâu lại hoạt động trên mạng rồi lưu lại trên máy bạn và trên những trang mạng mà bạn đã viếng.
3. Email có thể sàng lọc lại bằng cách truy tìm những từ và cụm từ đặc biệt từ thư tín của bạn.
4. Những cuộc truy tìm trên mạng và những trang mạng mà bạn đòi hỏi có thể được lọc lại bằng cách loại trừ ra một số từ khóa đặc biết.
5. Truy cập đến một số trang mạng có thể bị chặn với tất cả mọi người từ một đất nước nào đó.
6. Truy cập đến trang mạng thường được chặn lại bởi địa chỉ IP của trang mạng hoặc tên miền trên mạng.

Theo dõi và thu thập tin tình báo đã phát triển, từ việc nghe lén điện đàm và đọc lén thư từ, đến trên mạng. Vì cơ sở hạ tầng của mạng được mở rộng cho việc truy tìm và gửi gắm thông tin, theo dõi của ngày nay có thể được thực hiện bởi các chính quyền, cơ sở thương mại, tin tặc và tội phạm. Việc thiết lập kỹ thuật thâu lại và theo dõi mọi hoạt động mạng của bạn là tương đối dễ dàng. Mọi trang mạng đều có ghi lại thông tin về người đến viếng (địa chỉ IP và thời gian viếng), và phần lớn các dịch vụ email cũng làm vậy. Các ISP cũng có ghi lại mọi hoạt động diễn ra tại các máy chủ của họ. Tại một số quốc gia, việc 'giữ hồ sơ' như vậy đã trở thành bắt buộc. Vào năm 2006, Liên Minh Châu Âu ban hành luật bắt buộc các ISP phải lưu lại thông tin trên mạng của mọi người mua dịch vụ trong thời gian 2 năm[36] mặc dù các nước trong Liên Minh có quyền lưu thông tin lại lâu hơn. Ta hãy thử nhìn xem cách theo dõi hoạt động mạng của bạn như thế nào.

THEO DÕI LƯỚT MẠNG



► The ISP can monitor your Internet connection

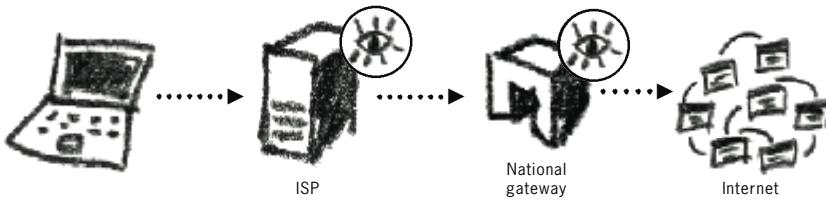
Thực chất mạng Internet chỉ là mạng trong văn phòng được làm lớn hơn. Mạng Internet gồm có nhiều máy điện toán, được liên kết bởi dây cáp và được phụ trợ bởi các máy chủ, cầu dẫn (router) và modem. Mặc dù bức thư trên mạng của bạn có thể băng qua đại dương nhờ vào dây cáp ngầm, nhảy qua hai vệ tinh nhân tạo và gửi tới điện thoại di động của ai đó đang đi xe điện, cả hệ thống chỉ giống như là một bản cập nhật của cuộc điện

36
Chỉ thị số 2006/24/EC của Nghị Viện Châu Âu và của Hội Đồng Ngày 15 Tháng 3 Năm 2006.

đàm. Và khi bạn là một người coi tổng đài, một kẻ bắt dây nghe trộm, hay là một bạn trai ghen tuông, bạn chỉ cần bắt thêm một máy thâu trên đường dây liên lạc là bạn có thể nghe trọn cuộc đối thoại. Trên mạng cũng vậy. Bất cứ ai có đúng dụng cụ truy cập vào mạng đều có thể đánh cắp và đọc bức thư của bạn trong khi bức thư đang chu du thế giới.

Trong khi việc nghe lén đường dây điện thoại hoặc dây mạng đòi hỏi kỹ năng đặc biệt và hàng động lén lút, việc gây áp lực cho các ISP thì dễ hơn nhiều. Có nhiều quốc gia chỉ có một ISP, và thường thì hãng phục vụ chấp nhận sự khống chế của chính quyền. Có những nước như Nga đã ban hành luật bắt buộc mọi ISP phải gắn một máy điện toán với mục đích theo dõi hoạt động mạng của khách hàng. Thông tin này được chuyển trực tiếp tới cơ sở dữ liệu của Cơ Quan An Ninh Liên Bang (Federal Security Service hay FSB)[37].

Các nước trên thế giới cho công dân được nối lên mạng bằng cổng điện toán quốc gia. Cho nên mọi giao thông mạng đều phải đi qua cổng điện toán, và có khả năng bị theo dõi[38]. Trung Quốc đã cài đặt một hệ thống theo dõi và giới hạn giao thông mạng trên các cổng điện toán. Công trình 'Khiên Vàng' sàng lọc và điều chỉnh sự truy cập mạng của toàn dân Trung Hoa[39].



► Internet monitoring at the ISP and the national gateway

Vào cuối thập niên 1980, các nước Mỹ, Anh, Canada, Úc và Tân Tây Lan bắt đầu phát triển một hệ thống theo dõi toàn cầu để tóm lược lại mọi điểm giao thông lớn trên mạng. Biến cố 11 tây tháng 9 ở Mỹ dẫn đến những đầu tư khổng lồ để cải thiện hệ thống gọi là ECHELON (BẠC THANG) được hoạt đồng dưới quyền kiểm soát của Cục An Ninh Quốc Gia (National Security Agency, hay NSA). Không ai biết được ECHELON tồn giữ thông tin lại bao lâu. Mặc dù có vẻ khó mà phân tích và phân loại trong tích tắc và có hiệu quả mọi thông tin mạng và điện thoại trên toàn cầu, nhưng NSA tuyên bố là họ đã thành công 90%[40].

Theo Dõi Hoạt Động Tại Các Trang Mạng

Ngoài ra, hồ sơ hoạt động mạng còn được lưu lại tại các trang mạng bạn đến viếng và trên máy điện toán của bạn. Nhiều trang mạng đòi hỏi máy của bạn phải cài đặt cookie. Cookie là một số lương thông tin nhỏ có chứa thông tin đặc biệt của người dùng. Thí dụ, cookie có thể ghi lại đất nước nơi bạn ở, để sau đó khi bạn đến viếng một trang mạng nào đó, thông tin có liên quan đến nước bạn được trình bày ra. Các trang mạng của hãng hàng không thường hay làm điều này. Có những thông tin khác, chẳng hạn như những trang chuyển tiếp mà bạn đã đi qua để

37
Sự Riêng Tư Quốc Tế -- Báo Cáo về Sự Riêng Tư và Nhân Quyền năm 2005 – Mối Đe Dọa cho Sự Riêng Tư.

38
Tại vài nước, liên kết qua vệ tinh nhân tạo được dùng để thay cho các dịch vụ truy cập mạng. Việc này làm cho việc theo dõi khó thi hành hơn nhiều.

39
http://www.guardian.co.uk/commentisfree/2008/aug/13/china.censorship

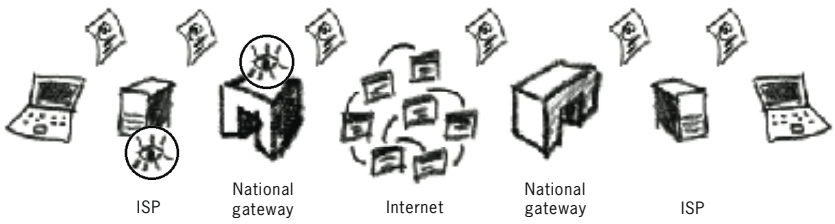
40
Canh Chừng Echelon tại http://www.nsawatch.org

đến được trang mạng này, hoặc như ngay cả thông tin cá nhân từ trong máy của bạn. Sau khi lướt mạng khoảng chừng một tháng, có thể bạn đã có vài trăm cookie trong máy. Đọc các cookie này có thể biết được thông tin về sở thích và hội đoàn của bạn. Cookie nằm trên máy của bạn có thể dùng làm bằng chứng rằng bạn đã từng viếng trang mạng nào đó. Nhà phục vụ quảng cáo trên mạng lớn nhất, DoubleClick, có giao kèo với hàng ngàn trang mạng và duy trì cookie của hơn 100 triệu người dùng mạng, mỗi cookie có chứa hàng trăm chi tiết về thói quen lướt mạng của người dùng[41].

Có thể xóa cookie từ máy của bạn. Xóa từ chương trình lướt mạng hoặc xóa bằng cách vào thẳng trong máy truy tìm và xóa. Hoặc cũng có thể bạn sắp xếp để chương trình lướt không được nhận bất cứ cookie nào hết. Làm như vậy có thể sẽ làm cho nhiều trang mạng từ chối không cho bạn truy cập, nhưng bạn sẽ được bảo vệ tối đa không cho cookie xâm nhập. Dùng chương trình Ccleaner trong công trình Security-in-a-Box để xóa cookie từ máy[42].

Theo Dõi Email

Việc liên lạc qua email hoạt động trên nguyên tắc cũng giống như việc lướt mạng, chỉ có khác là mỗi bức thư có nơi đến là một người hay một nhóm người, và những người nhận cũng kết nối mạng qua ISP của mình.



►Monitoring email at the ISP and national gateway

Vì vậy cho nên mỗi một lá thư email sẽ phải đi ngang qua ISP của bạn, cổng điện toán quốc gia của bạn, đi một vòng trên mạng, rồi đến cổng điện toán quốc gia của người nhận, đến ISP của họ, rồi cuối cùng được họ đọc. Theo hình thức này, một lá thư email của bạn có thể bị đánh cắp ở mọi điểm lưu thông chính trên đường. Nếu bạn sống tại một nước có luật pháp bảo vệ quyền riêng tư một cách chặt chẽ, thì luật pháp này không có quyền hạn khi thư của bạn đến ISP của người nhận trong một nước có luật riêng tư và theo dõi hoàn toàn khác. Nên lưu ý rằng trong khi lá thư của bạn đang trên đường đi từ nước A đến nước B, nó có thể đi ngang cầu dẫn của nhiều nước và hãng tư nhân khác dọc đường.

Có nhiều ISP và dịch vụ email giữ một bản sao của tất cả thư email trên máy chủ của họ. Đôi khi đây là lợi điểm cho ta, vì ta có thể muốn moi lại một lá thư đã gửi cho ta cách đây 3 năm. Tuy nhiên có thể có kẻ thứ ba đòi hỏi được truy cập trương mục email của ta. Hãng Yahoo! đã từng giao lại cho nhà cầm quyền Trung Quốc thông tin trương mục của bốn nhà hoạt động dân chủ và nhà học giả Trung Hoa, làm cho họ bị bắt và bị tù tội[43].

41
Sự Riêng Tư Quốc Tế -- Báo Cáo về Sự Riêng Tư và Nhân Quyền năm 2004 – Mối Đe Dọa cho Sự Riêng Tư.

42
http://security.ngoinabox.org/ccleaner_main

43
Tổ Chức Giám Sát Nhân Quyền – "Cuộc Chạy Đua tới Đáy" Vụ Đồng Lõa của Công Ty Tư Nhân trong Vụ Kiểm Duyệt Mạng ở Trung Quốc, tháng Tám 2006.

► Your message or identity can be spoofed by an adversary on the Internet

SÀN LỌC VÀ KIỂM DUYỆT TRANG MẠNG

Ngoài việc theo dõi giao lưu trên mạng, các chính phủ và hãng viễn thông có khả năng ngăn chặn không cho truy cập một số trang mạng hoặc khống chế được kết quả của một cuộc truy tìm trên mạng. Sàng lọc truy cập thông tin trên mạng thực chất là một hình thức kiểm duyệt và vi phạm các Điều Lệ 18, 19 và 20 của Bản Tuyên Ngôn Nhân Quyền[44] trong đó tuyên bố rằng mỗi con người có quyền tự do tư tưởng, tôn giáo, phát biểu và hội họp, cũng như tự do "...tìm, nhận và phổ biến thông tin và tư tưởng qua bất cứ phương tiện gì và trên bất kể mặt trận nào."

Kiểm Duyệt Mạng

Có nhiều quốc gia cấm công dân của mình không được truy cập một số trang mạng. Thông thường những trang này có chứa thông tin về quan điểm và tuyên truyền tôn giáo cực đoan, cổ động và giúp truyền bá tâm lý khủng bố, hoặc chỉ để trưng bày và phân phối tranh ảnh khiêu dâm của trẻ em. Có nhiều nước ngăn không cho truy cập những trang chỉ trích hoặc tiết lộ chính sách của chính quyền, thảo luận những vấn đề nhân quyền hoặc cung cấp dụng cụ để người dùng có thể vượt qua được kỹ thuật kiểm duyệt của các nước này. Vụ đề xướng OpenNet chuyên nghiên cứu các khuynh hướng và kỹ thuật kiểm duyệt và sàng lọc nội dung mạng ở khắp thế giới[45].

44
Văn Phòng Cao Ủy Nhân Quyền của Liên Hiệp Quốc http://www.unhchr.ch/udhr/lang/eng.htm

45
http://opennet.net/research

Có thể ngăn không cho truy cập trang mạng bằng ba cách thông dụng: chặn địa chỉ IP, làm giả các bản sao hệ thống tên miền (domain name system, hay DNS), và chặn các URL. Nói đơn giản, đây có nghĩa là một trang mạng có thể bị chặn theo địa chỉ mạng của trang, tên của trang, hoặc hệ thống chuyển đổi tên thành địa chỉ mạng.

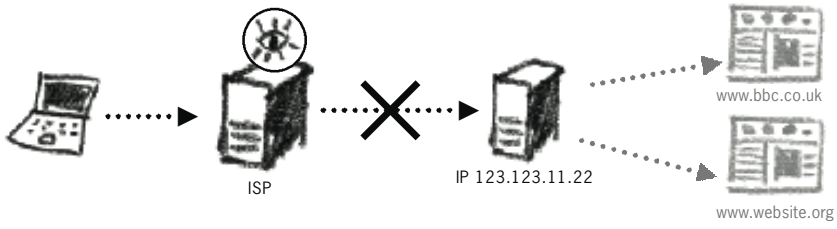
Tại một số nước, kiểm duyệt mạng chỉ chủ yếu là do ở thái độ của người dùng máy điện toán, thí dụ là cha mẹ ngăn không cho con cái truy cập một số loại trang mạng, hoặc là do người quản lý mạng cài đặt chương trình sàng lọc nội dung vào một máy của ai đó hoặc vào cổng điện toán mạng.

Phần lớn các quốc gia có kiểm duyệt mạng theo nội dung đều ấn định các ISP có trách nhiệm cài đặt và chạy chương trình kiểm duyệt. Các nước khác thì lại kiểm duyệt tại cổng điện toán quốc gia. Mọi giao lưu phải thông qua các trạm kiểm duyệt quốc gia này trước khi đến được mục tiêu. Trung Quốc và Pakistan là những quốc gia tiêu biểu đã cho thi hành chương trình sàng lọc, với nhiều mục đích và hậu quả, tại cả ISP và cổng điện toán[46], trong khi Úc và Iran lại ban hành luật pháp bắt buộc các ISP phải kiểm duyệt mạng.

Sổ Đen và Giả Mạo DNS

Lưu Ý: cần phải có kiến thức căn bản mạng hoạt động như thế nào trước khi đọc những phần sau. Xin xem ở 'Phụ Lục B – Giải Thích về Mạng'.

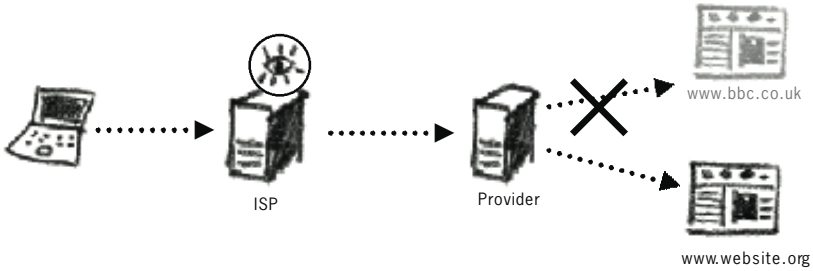
Mặc dù các hệ kiểm duyệt mạng khác nhau về giá cả và nơi cài đặt, tất cả đều hoạt động theo cùng nguyên tắc. Khi có người dùng yêu cầu truy cập trang mạng nào đó, thì trang mạng được kiểm tra theo danh sách các trang bị cấm. Nếu trang mạng nằm trong danh sách, thì yêu cầu bị từ chối. Tương tự, sổ đen có thể chứa địa chỉ IP của một số máy chủ, và từ chối yêu cầu được đưa đến địa chỉ đó.



Phương pháp này sẽ ngăn không cho truy cập địa chỉ IP của một trang mạng. Nhưng ngăn bằng địa chỉ IP có thể có vấn đề. Có khi trang mạng muốn chặn lại nằm trong một máy chủ có chứa vài ngàn trang mạng, và máy chủ này chỉ có một địa chỉ IP. Chặn địa chỉ IP của trang đó trở thành chặn mọi trang nằm chung trong máy chủ đó[47].

46
Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Từ Chối Truy Cập: Thực Hành và Chính Sách Kiểm Duyệt Mạng Toàn Cầu, (Cambridge: MIT Press) 2008.

47
"..hơn 87% tên miền đang hoạt động đều dùng chung địa chỉ IP với ít nhất là một miền khác, và hơn hai phần ba tên miền dùng chung địa chỉ IP với ít nhất 50 miền.." / Ben Edelman, Các Trang Mạng Dùng Chung Địa Chỉ IP: Sự Thịnh Hành và Ý Nghĩa, tháng 2 năm 2003.

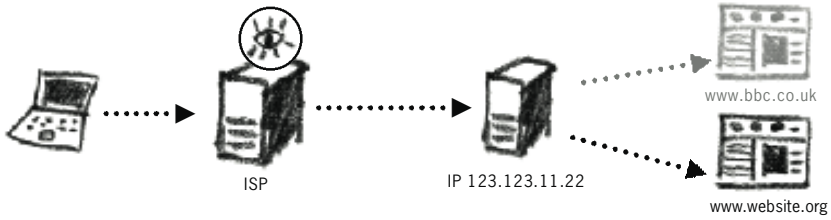


Trong minh họa trên, hệ kiêm duyệt ngăn lại mọi yêu câu được cập nhật www.bbc.co.uk.

Khi trang mạng được đăng ký lại hoặc sao lại dưới một tên miền khác, thì trang mạng có thể truy cập lại được

Những quy luật trên có thể áp dụng riêng rẽ hoặc chung lại với nhau để tạo khả năng sàng lọc và ngăn chặn. Có một số nước dựa vào các phân loại định sẵn trong chương trình sàng lọc rồi cho thêm những trang mới vào cách sắp đặt, và một số nước khác sử dụng nhiều đội ngũ nhân lực khổng lồ để thăm dò trên mạng và xác định ra trang nào phải được lọc bỏ đi.

Cướp DNS (DNS Hijacking)
Đây là phương pháp để đưa một yêu cầu của người dùng mạng vào một trang khác. Khi bạn đánh vào địa chỉ của một trang mạng mà bạn muốn viếng, bạn được tự động đưa đến một trang khác. Có nhiều người dùng mạng không hề biết sự khác biệt.



Người dùng mạng có thể vượt qua kỹ thuật kiểm duyệt này bằng cách đánh vào rõ ràng địa chỉ máy chủ gốc là điểm tựa miền, chứ không phải đánh dựa vào một bản sao có lưu sẵn tại ISP[48].

Vào ngày 8 tháng 9 năm 2002, người dùng mạng tại Trung Quốc bị ngăn không vào được trang chủ của Google. Thay vì vậy, họ được đưa đến một số trang khác xuất phát tại Trung Quốc. Địa chỉ trong URL vẫn ghi là www.google.com[49].

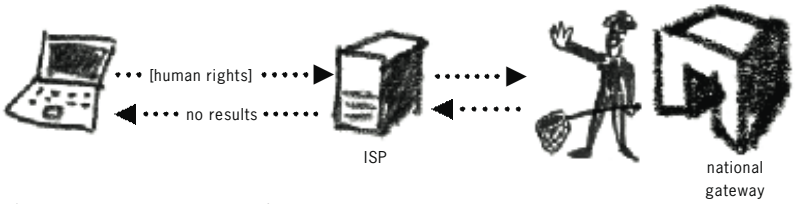
Sàng Lọc Theo Từ Khóa
Một phương pháp kiểm duyệt tương đối mới, nhưng đang phát triển và được phổ biến là sàng lọc theo từ khóa. Phương pháp này được thực hiện bằng cách nhận diện một số từ hoặc cụm từ trong trang web (hoặc URL) mà bạn muốn vào, rồi chặn luôn các trang web đó. Phương pháp này có khả năng kiểm duyệt các trang mạng và những sự liên lạc qua mạng. Tuy nhiên, cách sàng lọc theo từ khóa hơi đơn giản; nó không

38
http://www.root-servers.org/

49
49. Phân Tích theo Kinh Nghiệm Việc Kiểm Duyệt Mạng tại Trung Quốc, Trung Tâm Berkman cho Mạng và Xã Hội, Jonathan Zittrain và Benjamin Edelman, 2002.

những ngăn chặn các trang web độc hại mà còn cả luôn những trang web vô hại.

Sàng lọc theo từ khóa có thể được bố trí để ngăn cấm không cho người lướt mạng yêu cầu được truy cập một trang web có chứa cụm từ 'human rights' (nhân quyền) hoặc 'freedom of expression' (tự do ngôn luận). Trên thực tế, người ta có thể bố trí hàng ngàn từ và cụm từ khóa cho mục tiêu này. Mỗi khi một thông điệp email hoặc tin nhắn có chứa từ khóa đã được bố trí, thì thông điệp đó sẽ bị cản lại và không được chuyển đến người nhận, hoặc bị lưu lại để điều tra thêm nhằm truy ra người gửi lẫn người nhận. Sàng lọc có thể được thực hiện tại bất cứ điểm nào mà thông tin đi qua trên mạng.



► Certain words in your email could trigger the filtering mechanisms

Cùng một phương pháp đó được áp dụng vào các máy truy tìm và các ứng dụng nhắn tin nhanh (instant messenger) như là Yahoo chat, hoặc Skype. Khi bạn đánh một cụm từ vào Google, cụm từ đó được vận chuyển ngang qua ISP (hãng cung cấp dịch vụ Internet) và cổng điện tử quốc gia, trước khi bạn nhận được kết quả. Một hệ thống sàng lọc có thể chặn bắt từ khoá 'nhân quyền' mà bạn đánh đi từ máy điện toán của bạn. Vì yêu cầu của bạn chứa từ khoá 'nhân quyền' bị chặn, kết quả yêu cầu vào trang web của bạn sẽ là "sai"hoặc "không tìm thấy" (no results), xin xem hình trên.

Dưới đây là hình minh họa kết quả tìm chữ 'falundafa' (Pháp Luân Đại Pháp, là một phong trào tôn giáo bị cấm tại Trung Quốc) vào năm 2004 tại Trung Quốc trên Google.com.

Bề ngoài xem như có vẻ như Google không tìm được bất cứ một thông tin nào cả về đề tài này, nhưng thực ra cái thông báo về việc không truy cập được, đã được gởi ra từ chính phần mềm sàng lọc chứ không phải từ Google[50].

Hệ thống sàng lọc trên mạng cũng có thể đọc sơ qua nội dung của trang mạng mà bạn muốn đến, và nếu trang mạng có chứa bất cứ từ cấm nào thì nó sẽ ngăn không cho bạn truy cập đến trang mạng đó.

►A screenshot of the Chinese Internet hijacking the www.google.com DNS

50
Gần đây, cách kiểm duyệt này đã thay đổi. Ngày nay, Google sẽ hiện lên một thông điệp ghi rằng chính quyền địa phương không cho phép cụm từ truy tìm của bạn.

2.6 VƯỢT QUA KIỂM DUYỆT VÀ SÀNG LỌC MẠNG

TÓM TẮT

1. Có thể vượt qua kiểm duyệt mạng bằng một số phần mềm và phương pháp. Các cách phá khác nhau ở sự phức tạp, mức xác suất bảo đảm sự thành công trong việc đối phó với hệ thống kiểm duyệt của một quốc gia nào đó.
2. Có thể khắc phục kỹ thuật sàng lọc theo từ khóa bằng cách mã hóa.
3. Có thể dùng trạm proxy để lướt mạng mà không bị giới hạn hoặc để lại dấu vết.
4. Ngày nay có nhiều cách để vượt qua kiểm duyệt mạng. Bạn cần phải biết cách ước lượng khả năng ứng dụng và phương thức hoạt động của mỗi cách để thích ứng với nhu cầu và hòan cảnh.

Chương này sẽ mô tả nhiều phương pháp để vượt sự kiểm duyệt mạng và đề phòng bị sàng lọc từ khóa. Nói một cách khác, chương này sẽ giải thích cách truy cập những website bị chặn, cách giữ kín điều bạn đọc hoặc gửi đi trên mạng để không bị theo dõi, và cách hoạt động an toàn trên mạng. Nếu bạn không chuyên về kỹ thuật, thì trước hết bạn nên xem lại chương trước về 'Theo Dõi Trên Mạng' và phụ lục 'Giải Thích về Mạng' để hiểu rõ được phần này.

Có nhiều dụng cụ dưới dạng nhu liệu và phương thức để giúp bạn vượt qua những hệ thống kiểm duyệt mạng đang được thiết trí[51]. Chương này sẽ giới thiệu đến bạn một số ít dụng cụ và phương thức. Theo thời gian, chính những dụng cụ và trang web hướng dẫn cách vượt hệ thống kiểm duyệt này cũng có thể sẽ bị địa phương bạn kiểm duyệt. Để duy trì quyền tự do ngôn luận và tự do lập hội trên mạng, bạn sẽ phải tự đi tìm những dụng cụ và trang web mới mà có chức năng tương tự. Có thể tìm bằng cách truy tìm thật nhiều nơi trên mạng và bằng cách trao đổi với những người trong hoàn cảnh tương tự. Mục đích của chương này là để cho bạn nhận thức được là có những dụng cụ và cách thức để sử dụng trong tương lai.

Trở Lại Vấn Đề Kiểm Duyệt

Kiểm duyệt mạng có thể thực hiện được là nhờ vào chính những cơ sở hạ tầng của mạng và mạng lưới toàn cầu. Có nhiều quốc gia cấm không cho dân chúng truy cập một số trang web bằng cách cài đặt 'danh sách đen' (black list) tại điểm xuất nhập của mạng, tức là cổng (gateway) điện toán quốc gia. Các danh sách này gồm có tên các trang web (URL của trang) và thường là địa chỉ IP của máy thầu mạng đang làm chủ nhà cho các trang đó. Khi bạn yêu cầu được truy cập trang bị liệt vào danh sách đen, yêu cầu của bạn sẽ được cổng điện toán duyệt qua và từ chối. Yêu cầu cũa bạn được ghi nhận lại và có thể sau này được sử dụng như bằng chứng nhằm dẫn đến một sự trừng phạt.

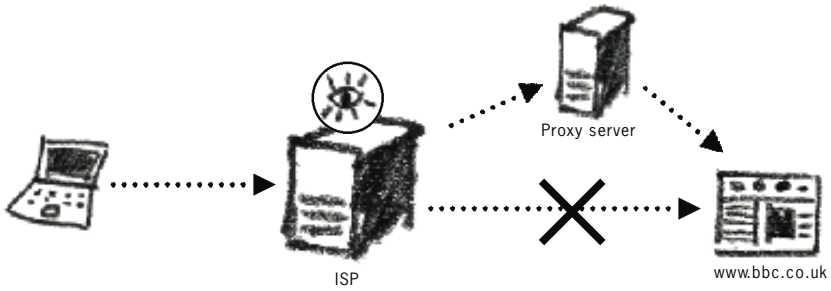
Dùng Trạm Proxy Để Liên Kết

51
Xin xem thêm bài hướng dẫn và dụng cụ phá kiểm duyệt của công trình The Sesawe tại https://www.sesawe.net; 'Cách Vượt Qua Kiểm Duyệt Mạng' của FLOSS Manuals Community Members tại http://en.flossmanuals.net/CircumventionTools/Introduction và 'Dụng Cụ An Ninh Điện Tử' tại http://security.ngoinabox.org/chapter-8

Danh sách đen chỉ có hiệu lực khi bạn yêu cầu được truy cập trực tiếp môt trang mạng. Nếu dùng một nhân vật thứ ba thu thập giùm nội dung của trang, thì danh sách đen trở nên vô hiệu lực. Hơn một thập kỷ qua, công dân mạng sống tại những địa phương bị kiểm duyệt mạng đã và đang dùng dịch vụ thông dịch và dự trữ thông tin để gián tiếp truy cập mạng. Còn những người khác thì dựa vào trạm proxy nặc danh (trạm này có mục đích ban đầu là để che đậy không cho bạn bị trang mạng nhận dạng), ngày nay dùng để che giấu nơi bạn muốn thật sự cập nhật mà không bị hệ thống kiểm duyệt sàng lọc đi.

Nếu bạn không được phép truy cập www.bbc.co.uk từ đất nước mình, thì bạn có thể dùng một máy khác (trạm proxy) để thu thập nội dung của trang mạng giùm bạn. Trạm proxy này sẽ nằm tại một quốc gia khác mà không bị giới hạn bởi những luật kiểm duyệt của địa phương bạn. Đối với hệ kiểm duyệt, hành động của bạn chỉ là truy cập một máy (hoặc trang mạng) không nằm trong danh sách sàng lọc của hệ thống kiểm duyệt mà thôi.

Có hàng ngàn trạm proxy như vậy, được bố trí bằng nhiều cách, và sứ mạng của các trạm là làm trung gian giữa máy của người sử dụng mạng và trang mạng.

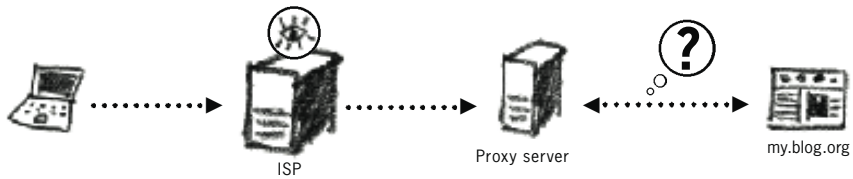


Minh Họa 15: Đổi từ một kết nối bị kiểm duyệt để đi qua trạm proxy.

Dịch vụ trạm proxy có nhiều hình thức khác nhau. Điều quan trọng là bạn phải phân biệt được chức năng và an ninh của trạm proxy. Nên nhớ rằng vào bất cứ lúc nào, bạn cũng không thể kiểm soát được phương pháp liên lạc hoặc sự kín đáo trong mối liên kết giữa trạm proxy đã chọn và trang mạng muốn truy cập. Chương này có liên quan đến những phương pháp vươn tới một trạm proxy hoạt động tốt và thoát khỏi kỹ thuật kiểm duyệt của quốc gia.

Trạm Proxy Nặc Danh (Anonymiser)

Dạng trạm proxy đơn giản nhất cũng được gọi là trạm proxy nặc danh. Phần mềm cho hoạt động trạm proxy được cài vào trong trang mạng, để qua trang đó bạn có thể trực tiếp duyệt mạng. Mặc dù ban đầu trạm proxy nặc danh được tạo ra để che không cho các trang trên mạng biết nơi bạn xuất phát, nhưng trạm proxy nặc danh cũng được dùng để che giấu nơi bạn truy cập trên mạng.



Minh Họa 16: Khi dùng trạm proxy nặc danh, trang mạng được bạn viếng không biết được xuất xứ (địa chỉ IP thật) của máy bạn. ISP không biết được mục tiêu thực sự của bạn.

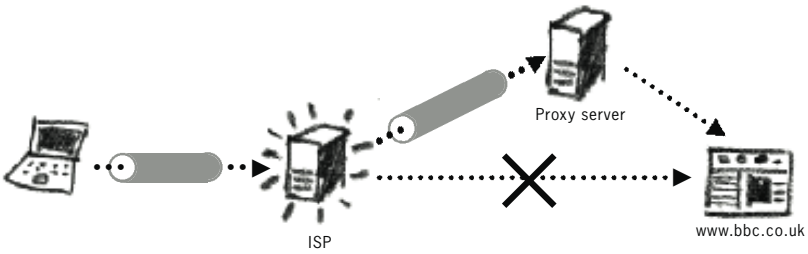
Có vài trạm proxy nặc danh khá nổi tiếng như sau:

- http://www.anonymizer.com
- http://www.anonymouse.org
- http://www.the-cloak.com
- http://www.peacefire.org[52]
- http://www.stupidcensorship.com

Tuy nhiên, vì các trạm proxy này rất nổi tiếng, nên nhiều quốc gia có thi hành kiểm duyệt mạng cũng ngăn chặn không cho truy cập các trạm này. Nên nhớ rằng nếu liên kết đến một trạm proxy phải đi qua một đường dây truy cập mở (HTTP chứ không phải HTTPS – xin xem chương sau để biết thêm chi tiết), thì thông tin gửi và nhận qua dịch vụ trạm proxy vẫn không thoát khỏi sự theo dõi.

Sử Dụng Dịch Vụ Trạm Proxy Đã Mã Hóa

Một đường hầm mã hóa được tạo ra giữa máy bạn và trạm proxy bạn chọn sử dụng. Kỹ thuật theo dõi mạng không thể nhìn thấy được thông tin được gửi và nhận qua dịch vụ này, mà chỉ thấy được là bạn đang sử dụng dịch vụ. Dùng trạm proxy đã mã hóa làm tăng thêm sự kín đáo cho kỹ thuật phá kiểm duyệt và nên được dùng trong mọi trường hợp. Tuy nhiên, nên lưu ý những vụ tấn công Kẻ-Trung-Gian (Man In The Middle) (xin xem chương sau) và nên biết rằng thông tin bạn gửi và nhận thì không giấu được chính trạm proxy.



Minh Họa 17:Mã hóa sự liên kết đến trạm proxy qua SSL.

Dịch Vụ Vượt Kiểm Duyệt Của Tư Nhân

Đây là những trạm proxy, do bạn bè hoặc đồng nghiệp sắp đặt từ trong những quốc gia không có kiểm duyệt các trang mạng mà bạn muốn truy cập. Dùng các trạm này cũng tương tự như bạn có cổng riêng để truy cập mạng mà không bị giới hạn. Lợi điểm chính của các trạm vượt kiểm duyệt tư nhân này là họ dùng mạng lưới tín nhiệm, tức là một nhóm bạn

52
Các nhà hoạt động tại peacefire.org thường xuyên thay đổi địa chỉ của trạm proxy, vì lẽ trạm bị một số nước chặn lại. Bạn có thể ghi danh vào trong danh sách email của trang này để được nhận địa chỉ của những trạm proxy mới tại http://www.peacefire.org/circumventor/

bè hoặc đồng nghiệp chia sẽ tài nguyên máy điện toán để giúp đỡ nhau. Mạng lưới trên làm tăng sự kín đáo vì lý do không ai khác ngoài mạng Internet biết đến và sẽ làm cho kỹ thuật kiểm duyệt khó có thể khám phá và cho tên họ vào danh sách bị chặn.

Một thí dụ về trạm vượt kiểm duyệt tư nhân là Psiphon[53] – cho phép cài đặt chương trình trạm proxy trên bất cứ máy nào chạy Windows. Psiphon dựa vào các mối quan hệ tín nhiệm giữa những người muốn giúp đỡ bạn bè còn đang sống trong đất nước bị kiểm duyệt mạng. Trạm proxy sẽ tạo ra chi tiết đăng nhập cho người dùng, gồm có địa chỉ IP của máy điện toán, tên người dùng và mật khẩu hợp lý. Những chi tiết này sẽ được gửi đến bạn bè hoặc đồng nghiệp của bạn, và những người này sẽ dùng các chi tiết đó để kết nối với trạm proxy Psiphon và duyệt mạng qua trạm. Mặc dù rất dễ cài đặt, Psiphon bắt buộc bạn phải truy cập được modem và có thể bố trí modem để cho phép bạn của bạn có thể kết nối đến từ Internet. Trạm Psiphon còn cung cấp 'Hệ Thống Chuyển Giao Có Trật Tự', một dịch vụ cung cấp nội dung các trang mạng bị chặn cho dù bạn không có bạn bè hay đồng nghiệp cung cấp cho bạn trạm proxy[54].

Minh Họa 20:Psiphon bỏ thêm một thanh truy tìm vào trình duyệt mạng. Bạn nên đánh ngay tất cả các địa chỉ mạng vào đó để Psiphon đi thu thập các trang mạng bị chặn tại đất nước của bạn.

53
http://www.psiphon.ca/node/16

54
http://www.psiphon.ca/node/17

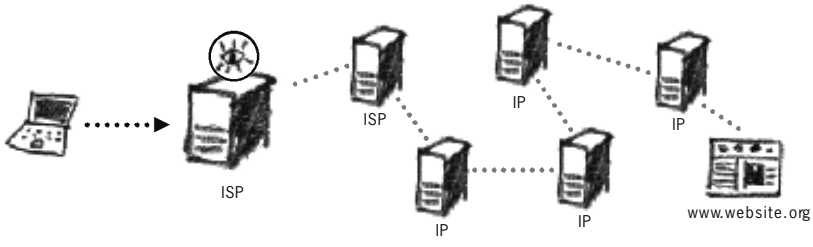
Phần Kỹ Thuật
Peacefire Circumventor[55] – cho phép bạn tự tạo ra trạm proxy riêng giành cho người khác dùng. Bạn sẽ cần một máy chuyên làm trạm proxy, và một liên kết mạng để cài đặt và chạy trạm này. Bạn nên cài đặt trạm tại một quốc gia không có áp dụng sự kiểm duyệt mạng. Các chi tiết để kết nối đến trạm proxy này sẽ được gửi đến cho những người đang sống trong các quốc gia có kiểm duyệt mạng.

Mạng Ảo Riêng (Virtual Private Network)
Một cách khác để vượt qua kiểm duyệt mạng là dùng mạng ảo riêng (VPN). Đây chẳng qua là một mạng văn phòng được mở ra băng ngang qua Internet. Có nhiều tổ chức dùng VPN khi họ muốn nhân viên được truy cập vào network drive và tài nguyên nội bộ, trong khi nhân viên không có mặt tại văn phòng. VPN tạo ra mối liên kết được mã hóa đến máy chủ trung tâm và chuyển giao thông tin gửi và nhận từ máy tính qua liên kết này. Cho nên nếu máy chủ VPN nằm trong quốc gia không có kiểm duyệt mạng, thì bạn có thể dùng dịch vụ này để chuyển giao thông tin mạng qua máy.

Freedom[56] và HotSpot Shield[57] là những ví dụ cụ thể cho phép bạn truy cập VPN của họ để vượt qua kiểm duyệt. Bạn sẽ được cung cấp chi tiết đăng nhập và chương trình để kết nối với máy của họ. Xin lưu ý rằng phương pháp này chỉ có công dụng để mục tiêu bạn muốn đến trên mạng được che giấu không bị kiểm duyệt từ chính nước bạn, chứ không che giấu được chính những kẻ cung cấp các dịch vụ này.

Dùng Những Trang Mạng Ẩn Danh (Anonymity Networks)
Còn một cách nữa là vào các mạng lưới ẩn danh có trên Internet trước rồi mới truy cập vào trang web bạn muốn. Lướt Internet bằng các trang web ẩn danh như thế này sẽ giúp bạn ngụy trang danh tính thật của bạn và có thể vô hiệu hoá hệ thống sàng lọc và lưu trữ thông tin điện tử tại quốc gia bạn ở.

Một mạng lưới ẩn danh mà bạn có thể xử dụng là trang Tor (http://torpro-



► Anonymising your Internet presence on the TOR network

55
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

56
http://www.your-freedom.net/

57
http://hotspotshield.com/

ject.org). Tor là từ viết tắt cho The Onion Router. Trang này có một đội ngũ hỗ trợ viên và cộng tác viên trên khắp thế giới, cho nên có thể giao dịch bằng rất nhiều ngôn ngữ khác nhau. Khởi đầu nó được triển khai bởi Phòng Nghiên Cứu của Hải Quân Hoa Kỳ (US Naval Research Laboratory) để trợ giúp các dịch vụ quốc phòng và tình báo bằng cách cho phép liên lạc ẩn danh qua Internet. Hiện nay, trang Tor được bảo trì bởi một nhóm các chuyên gia ẩn danh và an ninh trên toàn thế giới.

Mạng lưới Tor vận hành được nhờ một hệ thống server (ổ điện đài) lớn, cung cấp bởi các tình nguyện viên trên toàn thế giới. Hiện nay, có gần một nghìn điện đài như thế. Khi bạn vào mạng lưới Tor, bạn sẽ được cung cấp một mạch điện ngẫu nhiên (random circuit) qua ba hoặc nhiều hơn ba ổ điện đài của Tor, để qua đó bạn được trao những bộ chìa khóa mã hoá cá biệt tại mỗi ổ điện đài. Cách này bảo đảm rằng không một ổ điện đài nào, kể cả những ổ điện đài mà bạn xử dụng, có thể lần mò và tìm ra nơi xuất phát, và nơi đến của bạn. Hãy hình dung việc bạn gửi một bức thư đến một người bạn. Nhưng, bạn không gửi trực tiếp, mà gửi bức thư ấy qua một chuỗi phong bì thư khác nhau với nhiều đia chỉ khác nhau trên mỗi phong bì thư. Khi bức thư được gửi từ nơi này sang nơi khác, người nhận sẽ không thể nào biết được nguồn gốc và nơi đến thật sự của lá thư. Nếu một trong những người nhận muốn đọc thư thì cũng sẽ không thể đọc được nội dung, bởi vì nó được mã hoá và cần ở mỗi lượt hai địa chỉ người nhận (ổ điện đài) để tạo nên chìa khoá giải mã nhằm giải mã bức thư. Khi bạn xử dụng Tor, ISP hoặc những cơ quan giám sát quốc gia không thể biết bạn truy cập vào trang web nào vì vậy không thể ngăn cản bạn. Còn trang web mà bạn viếng cũng sẽ không biết bạn đến viếng từ đâu. Hiện này, có hơn một trăm nghìn khách hàng xử dụng mạng lưới Tor để gia tăng sự riêng tư và duy trì tính ẩn danh khi lướt mạng. Bạn cũng có thể xử dụng bản di động của Tor với tên gọi là Tor Browser. Bản này không cần phải cài đặt vào máy điện toán, và có thể di chuyển bằng thẻ nhớ USB (USB memory stick), rất hữu dụng khi phải dùng máy điện toán ở quán cà phê hoặc máy của người khác.

Mạng lưới Tor cũng rất hữu dụng ở lãnh vực vượt thoát khỏi kiểm duyệt, nhưng tính ẩn danh rất mạnh của nó sẽ trở thành một khuyết điểm khi bạn dùng nó để lưu hành những bài viết, ví dụ như trên Wikipedia, một trang rất đa dạng và mở. Bạn phải kiểm tra nếu trang web bạn muốn vào có thể vận hành song song với Tor. Và điều quan trọng là, không nên dùng Tor để truy cập vào các trương mục Internet không an ninh. Bởi vì Tor chỉ bảo vệ trạng thái ẩn danh của bạn khi lướt net, chứ không bảo đảm an ninh cho bạn.

Xuất Bản bài viết Ẩn Danh trên Internet

Các bạn nào sở hữu trang dân báo (blog) hoặc đóng góp bài vở cho một blog, hay một diễn đàn trên Internet cần lưu ý rằng sự ẩn danh của bạn sẽ không được bảo đảm nếu bạn chỉ đơn thuần dùng bí danh khi đăng nhập. Mỗi bài viết trên blog đều có địa chỉ của máy điện toán gửi bài đến, và những ISP thường lưu lại tất cả địa chỉ này. Vì vậy, nếu bạn muốn phổ biến những thông tin nhạy cảm trên Internet, bạn phải thật cẩn thận để không bị phát hiện. Bằng cách xử dụng những mạng lưới proxy nặc danh và các mạng lưới ẩn danh, bạn có thể ngụy trang địa chỉ IP từ máy ví tính của bạn. Ví dụ, bằng cách xử dụng proxy SSL, bạn có thể lén tải bài viết của bạn lên Internet mà không sợ bị lộ danh tính thật. ***Để có thêm thông tin tường tận trong lãnh vực này, xem phần "Hướng Dẫn cho các bloggers và Các Nhà Bất Đồng trên Mạng."***

2.7 MÃ HOÁ TRÊN INTERNET

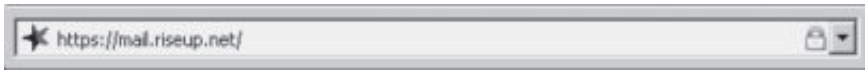
TÓM TẮT

1. Các thông tin mà bạn gửi hoặc nhận trên Internet truyền tải dưới hình thức mở
2. Một vài trang web có thể giúp bạn bảo mật thông tin bằng cách xây dựng một hành lang để mã hoá thông tin khi truyền tải giữa chúng và máy điện toán của bạn.
3. Hành lang này được thành lập một cách tự động, được bạn xác nhận chính danh và có những chức năng đặc biệt nhằm giúp bạn biết được sự hiện diện của nó.
4. Hệ thống an ninh này vẫn có thể bị xâm nhập qua cuộc tấn công mang tên Người Trung Gian (Man-In-The-Middle)
5. Bạn phải thật thận trọng xác minh lại những chứng chỉ an ninh từ các trang web cung cấp những đường kết nối đã được mã hoá sẵn.

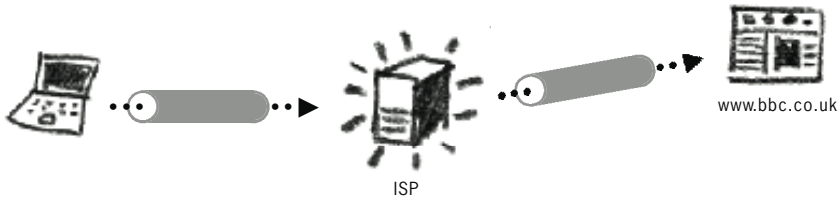
Mã hoá đã và đang trở thành một trong những biện pháp cuối cùng để bảo đảm quyền riêng tư trên Internet. Nó cho phép chúng ta bảo đảm được rằng không một ai có thể đọc được những tin nhắn và những thông tin trao đổi trên Internet, ngoại trừ người được chỉ định. Một lớp bọc an ninh để phục vụ cho công tác mã hoá thậm chí còn được lắp đặt vào cơ sở hạ tầng Internet (Internet infrastructure) để bảo mật những trao đổi về tài chánh. Lớp bọc an ninh này có tên là Secured Sockets Layer, đại ý nghĩa là Vỏ Bọc An Ninh, được viết tắt thành SSL. Lúc vừa chào đời, SSL bị chống đối dữ dội bởi chính phủ Hoa Kỳ. Khi ấy, cả ba ngành trong chính quyền liên bang Hoa Kỳ (Lập Pháp, Tư Pháp, Hành Pháp) đều ngăn cấm tất cả những dịch vụ mã hoá bằng SSL, nếu sự mã hoá đó tạo khó khăn cho khả năng giải mã. Dần dần chính sách này được nới lỏng, nhờ vào sự nỗ lực liên kết đấu tranh của những nhà toán học và những nhà vận động trong thời kỳ với tên gọi là "Crypto Wars,"tức những cuộc chiến về mã hoá.

Ngày nay, SSL được xử dụng rộng rãi khắp mọi nơi trên Internet. Cái lợi của SSL trong các dịch vụ điện thư mạng (webmail) là ở chỗ kỹ thuật này đã được cài đặt sẵn trên Internet, cho nên những luật pháp quốc gia nhằm hạn chế việc mã hoá thông tin không thể áp dụng được. Nói cách khác, nếu một quốc gia cho phép Internet hiện diện trong trong phạm vi lãnh thổ của mình thì quốc gia ấy chấp nhận sự hiện diện của SSL, bởi vì SSL được xử dụng rộng rãi trong tất cả các hoạt động trên Internet. Những tổ chức cũng có thể (và họ thường làm vậy) cung cấp các dịch vụ điện thư nội bộ, cũng được bảo vệ bởi SSL. Đây là cách tối thiểu ngày nay để có được một mức độ riêng tư thích hợp khi trao đổi thông tin trên Internet.

Sự hiện diện và vận hành của SSL khi kết nối vào một trang web có thể được xác định một cách cụ thể bởi các yếu tố nổi bật sao đây:



- Địa chỉ của trang web bắt đầu với https:// (mẫu tự 's' đại diện cho secure, tức bảo mật).
- Ký hiệu của một ổ khoá nhỏ sẽ xuất hiện ở address bar hoặc bên dưới của tool bar, tùy thuộc vào Internet browser của bạn.



Điều này có nghĩa là trang web mà bạn đang xem và Internet browser đã thoả thuận để thành lập một hành lang chung được mã hoá để trao đổi thông tin. Để tìm hiểu thêm tính bảo mật của cách này, chúng ta hãy tìm hiểu cách vận hành của SSL.

Chứng Nhận SSL (SSL Certificate)
Hệ thống SSL vận hành theo quan niệm Public Key Infrastructure (PKI), nghĩa là hệ thống chìa khoá công cộng. Tất cả các trang web muốn sử dụng mã hoá bằng phương pháp SSL phải có được Chứng Chỉ SSL (SSL Certificate). Internet browser của bạn liên lạc với tổng đài mạng (web server) và mã hoá tất cả dữ liệu trao đổi giữ hai phía. Sự vững chắc của mã hoá đó tùy thuộc vào chứng chỉ SSL bên phía web server. Tiêu chuẩn an toàn trên Internet hiện nay là 128/256 bits, đủ mạnh để đối phó với hầu hết các tình huống xấu.

Internet Browser của bạn (nếu là Internet Explorer hay Mozilla Firefox) có sẵn một danh sách các Ủy Quyền (Certification Authority) để trao Chứng Chỉ SSL. Nếu bạn lướt vào trang mạng nào có cài SSL, thì browser của bạn sẽ tự động kiểm tra lại xem Chứng Chỉ SSL đó đáng tin cậy hay không, do Ủy Quyền nào trong danh sách cung cấp. Mỗi chứng chỉ SSL chứa đựng ít nhất các dữ kiện sau đây:

- Chìa khoá giải mã của chủ nhân (máy điện toán)
- Tên thật hoặc bí danh của chủ nhân
- Ngày hết hạn của chứng chỉ
- Mã số của chứng chỉ
- Tên của tổ chức cung cấp chứng chỉ
- Chữ ký điện tử của tổ chức cung cấp chứng chỉ

Nếu Ủy Quyền cấp chứng chỉ SSL không có trong danh sách, hoặc nếu những chi tiết trong chứng chỉ SSL không ăn khớp với những chứng chỉ trong danh sách, thì điều này có thể gây ra một mối âu lo về an ninh. Vì vậy, browser của bạn sẽ phát ra một bản cảnh báo và cho phép bạn giám định lại chứng chỉ. Xem các hình bên dưới:

Lưu Ý: Các hình này sẽ không tự động hiện lên nếu bạn dùng Internet Explorer 6 hoặc thập hơn. Trong trường hợp đó, bạn cần thiết lập chọn lựa sau đây:

Chọn: Tools > Internet Options
Nhấc chuộc: Advanced

Kéo xuống danh sách (scroll down) đến phần "Securiy" đến khi bạn thấy một ô trống và dòng chữ "Warn about invalid certificate"kề bên. Hãy nhấn chuột (click) vào ô vuông đó.

Nếu bạn dùng Mozilla Firefox cũng có thể gặp phải trường hợp trên, mặc dầu màn hình sẽ khác, nhưng vấn đề vẫn giống nhau. Ở cả hai trường hợp trên, bạn cũng thể

kiểm tra lại chứng chỉ (examining the certificate) và sau đó quyết định chấp nhận nó hay không. Nếu bạn không chấp nhận, bạn sẽ không được truy cập vào trang web bạn muốn. Nếu bạn chấp nhận nó ("Accept this

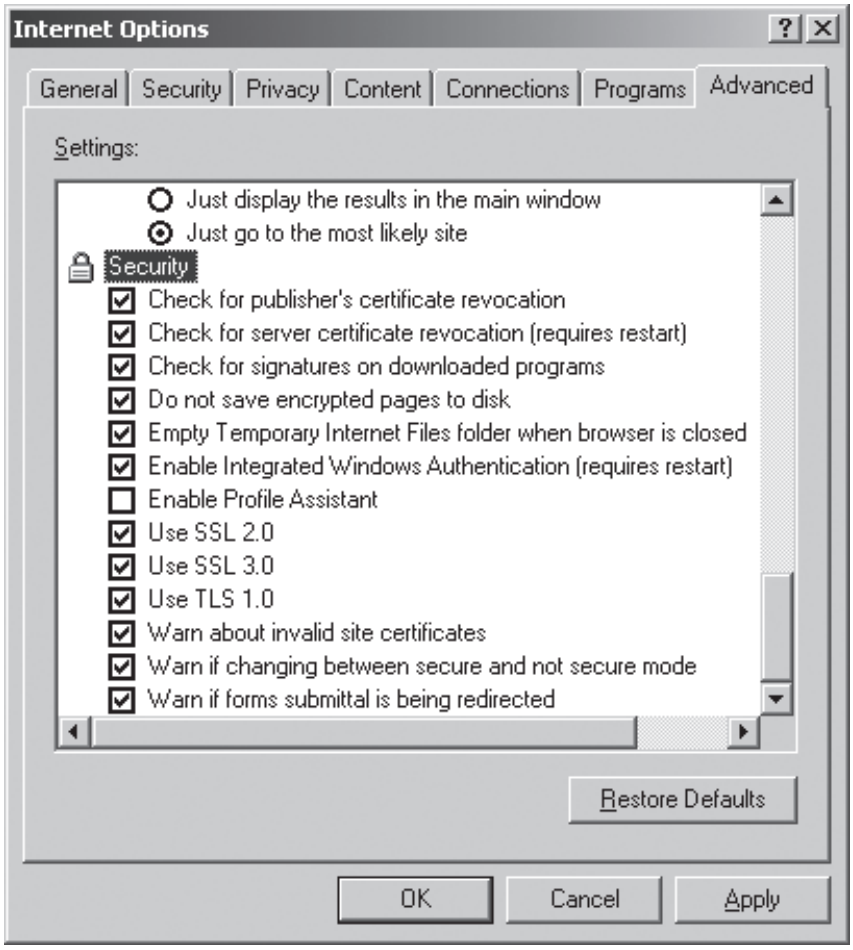


Illustration 25: Advanced Internet settings of Internet Explorer

Hình 23: Một cảnh báo từ chứng nhận SSL của Internet Explorer

Hình 24: Cảnh báo của Mozilla Firefox

certificate permanently" ở Mozilla Firefox), thì chứng chỉ và Ủy Quyền của nó sẽ được lưu vào danh sách tin cậy trong máy điện toán của bạn, và bạn sẽ không được thông báo để chấp nhận một chứng chỉ như thế trong tương lai.

Lưu Ý: Các thế hệ browser khác nhau có thể đưa ra lời cảnh báo khác nhau. Tuy nhiên những căn bản kỹ thuật và phương cách ứng phó đều giống nhau.

Nếu bạn cần xác minh chứng chỉ SSL lại, thì bạn nên thấu hiểu những yếu tố nào cần lưu ý. Yếu tố chính để nhận diện một chứng chỉ SSL (thật) là dấu tay (fingerprint), cũng thường gọi là thumbprint (dấy tay cái). Dấu tay ở đây thật ra là một mã số điện tử đặc biệt mà mỗi chứng chỉ SSL đều có. Chỉ khi xác minh được dấu tay thật thì ta mới có thể an tâm rằng chứng chỉ SSL là chứng chỉ thật, và thật sự đã được cung cấp bởi các chủ nhân của trang web mà bạn đang xem. Để xác nhận chính danh của nó, bạn cần phải liên lạc với chủ nhân của trang web để đối chiếu dấu tay trực tiếp, hoặc gián tiếp qua điện thoại, fax và Internet chat.

Mặc dầu nghe có vẻ rất phiền phức, nhưng rất cần thiết để có một mức an ninh tốt. Phần kế đến trong tiêu đề này sẽ giải thích nguy cơ bị lộ của bạn nếu bạn không làm thêm quy trình này.

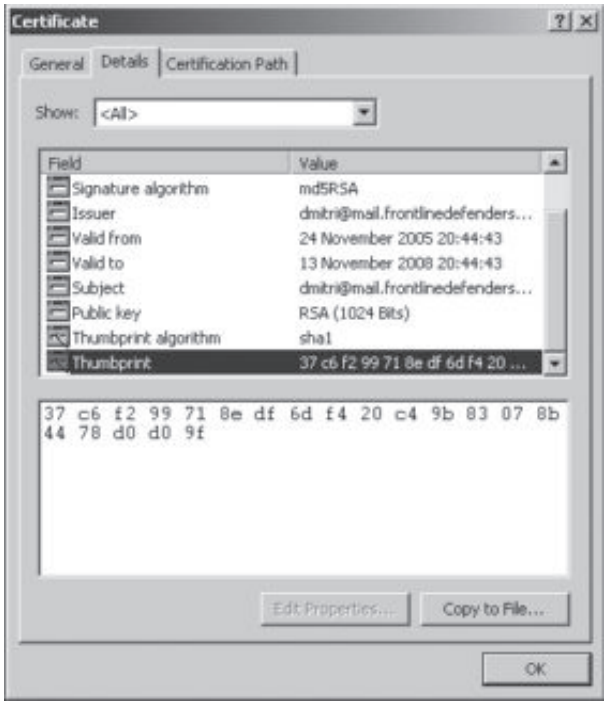
Nếu dấu tay không ăn khớp, xin đừng chấp nhận nối kết. Bạn sẽ không truy cập được và trang web như ý muốn, nhưng điều này sẽ bảo vệ bạn không trở thành nạn nhân của cuộc tấn công Người Trung Gian (xem bên dưới).

Điện Thư Được Bảo Mật (Secure Email)

Tuy ứng dụng SSL đã được gài đặt ở cơ sở hạ tầng của Internet, nhưng nó không bảo đảm an toàn cho các đường kết nối vào trương mục điện thư cá nhân trên Internet. Việc này cũng áp dụng cho webmail (điện thư trên Internet toàn cầu, như của Google hoặc Yahoo) và hosted email (điện thư nội bộ dành riên cho thành viên của một tổ chức). Một vài dịch vụ webmail có các biện pháp bảo đảm an toàn miễn phí là:

- https://mail.riseup.net
- https://bluebottle.com
- https://fastmail.fm
- https://mail.google.com (an option in 'Settings' can force an SSL connection)

Những dịch vụ webmail này cho phép bạn truy cập vào trương mục điện thư của bạn với đường kết nối đã được mã hoá để bạn trao đổi thông tin một cách an toàn hơn. Mặc dầu các dữ liệu trao đổi vẫn có thể bị sàng lọc hoặc giám sát, nhưng hầu như



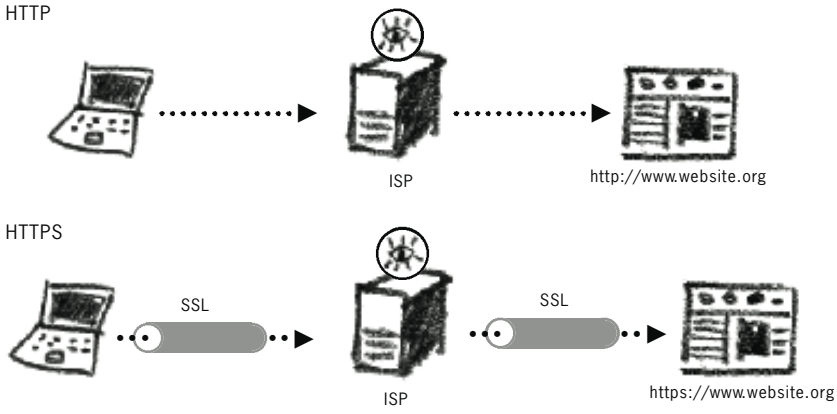
Hình 26: Thông tin trên chứng nhận SSL của Internet Explorer

Hình 27: Thông tin chứng nhận SSL của Mozilla Firefox

không cách nào để kẻ gian có thể đoán ra nội dung hoặc giải mã được thông tin mà bạn trao đổi.

Quan trọng hơn, nhờ cách này mà việc đọc và viết điện thư được bảo đảm an toàn cao hơn. Khi dùng với một mật khẩu tốt (xem chương về Mật Khẩu), nó gần như tuyệt đối bảo đảm an toàn khi trao đổi thông tin qua Internet. Việc ghi danh để có trương mục với những dịch vụ này không khác gì so với cách ghi danh để mở trương mục điện thư trên Yahoo hay Hotmail. Xin lưu ý rằng hầu hết các nhà cung cấp điện thư (webmail provider) không cung cấp đường kết nối SSL với thân chủ của họ. Cho nên, phải lưu ý sử dụng các dịch vụ bảo an điện thư như nêu trên để bảo đảm sự an toàn khi trao đổi thư tín trên Internet.

Chu kỳ an toàn điện thư

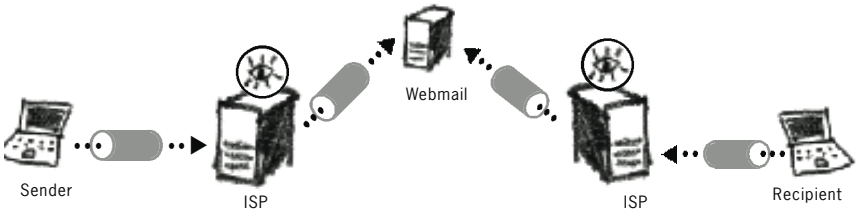


Bạn hãy nghĩ rằng người nhận điện thư của bạn có thể không dùng các biện pháp an toàn tương tự như bạn khi truy cập vào trương mục thư tín điện tử của họ. Vì vậy, ngay khi bức điện thư của bạn được gửi đến mạng thư tín của người nhận, nó sẽ có xu hướng theo tiêu chuẩn an ninh mạng của người nhận, do người nhận đã cài đặt trên máy của họ. Nếu người nhận kết nối vào mạng để vào trương mục điện thư của họ một cách cởi mở, thiếu thận trọng (không mã hoá), kẻ gian tại nơi cung cấp dịch vụ mạng, hoặc tại cổng điện tử quốc gia có thể trộm lướt nhìn hoặc đọc toàn bộ bức điện thư do bạn gửi.

Để bảo đảm và duy trì an ninh và sự riêng tư với mức độ cao khi liên lạc bằng thư điện thư, cả hai phía phải được kết nối an toàn đến tổng đài điện thư (mail server), bằng cách này hoặc cách khác có thể. Nếu sự mong muốn của bạn là "thoát khỏi" sự kiểm soát tại quốc gia, nơi mà bạn gởi điện thư đi, hoặc nếu đường truyền điện thư giữa bạn và người nhận tuyệt đối an toàn và không cần chú tâm thì bạn có thể không chú ý đến ví dụ dưới đây. Nhưng, hãy nhớ để duy trì chu kỳ an toàn riêng tư và an ninh gữa các mối liên lạc, bạn phải luôn luôn hình thành một mô hình và rèn luyện kỹ năng an toàn mạng thật tốt.

Tính chất an toàn của phương pháp này có thể được cải thiện thêm nếu cả hai phía xử dụng dịch vụ điện thư SSL (SSL webmail server) giống nhau (như RiseUp, Bluebottle).

Điện thư thường di chuyển trên mạng giữa các server, thường không được mã hoá và có thể dễ bị đọc lén. Và hãy quan tâm đến vấn đề an ninh hơn nếu cả hai (người gửi và người nhận điện thư) cùng xử dụng dịch vụ SSL webmail giống nhau. Bởi vì tuy rằng đường nối kết vào trương mục điện thư của bạn được mã hoá, nhưng vì webmail server lưu trữ và điều phối những bức điện thư của bạn, cho nên những trao đổi bằng điện thư của bạn vẫn có thể bị lộ nếu nhân viên quản lý webmail server cố tình đột nhập, hoặc webmail server bị tin tặc (hacker) tấn công. Bạn có thể tìm hiểu về mức độ an ninh và sự khả tín của nhà cung cấp webmail mà bạn đang xử dụng, cũng như vị trí của những server phục vụ



►All-round **SSL** encryption in email communications

cho dịch vụ webmail đó. Những yếu tố này có thể trở thành một vấn đề lớn nếu chính phủ sở tại, ví dụ như chính phủ Hoa Kỳ, ban hành pháp lệnh tịch thu các server và những thông tin và điện thư bên trong. Những webmail server nêu trên được đặt tại các quốc gia sau đâu:

- https://mail.riseup.net – Hoa Kỳ
- https://bluebottle.com – Anh quôc
- https://fastmail.fm – Hoa Kỳ
- https://mail.google.com – nhiều mạng cục bộ bao gồm Hoa Kỳ, Úc, Nam Hàn và Trung Quốc

Phương thức bảo vệ dữ liệu (trong trương mục điện thư) của bạn đã và đang được ban phát bởi môt số dịch vụ webmail. Gần đây, bạn không những có thể sử dụng một kênh an toàn để trao đổi điện thư, mà còn có thể mã hoá thông tin của bạn trên các server nữa. Tóm lại, trương mục điện thư của bạn chỉ có mình bạn mới có thể truy cập và mở thư.

Còn điện thư gửi đến người nhận nào có trương mục điện thư trùng với nhà cung cấp của bạn, thì bức điện thư ấy có thể được mã hoá để bảo đảm được an toàn. Nhưng việc này đòi hỏi bạn cần một đường kết nối vào Internet tương đối nhanh, bởi vì mỗi lần bạn truy cập vào trương mục điện thư của bạn là mỗi lần một chương trình mã hoá dữ liệu sẽ tự động tạm thời tải vào máy điện toán của bạn. Bạn có thể tạo trương mục điện thư, miễn phí, loại này tại các trang sau đây:

- https://www.hushmail.com
- https://www.vaultletsoft.com
- https://www.s-mail.com

MAN IN THE MIDDLE

GIÀNH CHO CHUYÊN VIÊN

Sự đe dọa được xem là lớn nhất đối với mô hình chứng chỉ SSL là sự tấn công của Man in the Middle (viết tắt là MITM, nghĩa là tấn công qua trung gian). Căn bản nhất, nó là một sự chặn bắt nguồn thông tin trên mạng của bạn- sự liên lạc của bạn với web server. Cụ thể, nó có thể được dùng để phá vỡ mô hình SSL, đã được giải thích ở phần trước. Bước đầu tiên, kẻ gian phải đột nhập vào đường liên kết Internet của bạn. Việc này có thể thi hành tại nhà cung cấp dịch vụ Internet (ISP), cổng điện tử quốc gia, hay thậm chí tại một server đia phương. Kẻ gian sau đó đánh lừa bạn bằng cách tráo đổi chứng chỉ SSL thật với chứng chỉ SSL giả, trong lúc bạn chủ ý truy cập vào trương mục điện thư (đã được bảo an) của bạn. Chứng chỉ này không phải của nhà cung cấp điện thư mà là của kẻ gian. Cho nên, một khi bạn chấp nhận chứng chỉ SSL giả mạo, bạn sẽ bị dẫn sang một đường kết nối khác để đến server của kẻ gian. Và khi bạn vô tình cung cấp các thông tin của bạn như mật khẩu đăng nhập vào trương mục điện thư, các chi tiết về tài chính, vân vân thì kẻ gian đều nhận được hết mà không cần tốn sức gì cả. Vấn đề chính ở đây là kẻ gian rất dễ tráo đổi một chứng nhận SSL giả với một chứng nhận SSL thật. Bởi vì tâm lý chung là chúng ta có khuynh hướng nhấp chuột vào "OK" mà không cần đọc biết đến nội dung của một thông điệp. Kẻ gian có thể bị kích thích để tấn công bạn bằng phương pháp MITM khi không thể đọc thư điện thư của bạn, hay biết được nội dung của những lần bạn giao dịch trên mạng,

Vấn đề chính ở đây là kẻ gian rất dễ tráo đổi một chứng chỉ SSL giả với một chứng chỉ SSL thật. Bởi vì tâm lý chung là chúng ta có khuynh hướng nhấn chuột vào "OK" mà không cần biết đến nội dung của một thông điệp. Kẻ gian có thể bị kích thích để tấn công bạn bằng phương pháp MITM khi không thể đọc được điện thư của bạn, hay biết được nội dung của những lần bạn giao dịch trên mạng, vì bạn liên lạc qua đường kết nối bảo an 'HTTPs'. Cho nên nếu không tấn công được thì họ chỉ quan sát được rằng bạn truy cập vào một webmail server, chứ không cách nào biết được bạn trao đổi những gì qua điện thư.

Khi đường nối kết vào mạng của bạn bị chận bắt và bạn chấp nhận chứng chỉ SSL giả của kẻ gian, thì tất cả dữ liệu của bạn lúc đó (và có thể sau này nữa) sẽ bị truyền tải vào server của kẻ gian. Đây có nghĩa là tất cả các chi tiết đăng nhập, thư điên tử riêng tư của bạn, vân vân sẽ bị đánh cắp. Một vấn đề khác nữa là một khi bạn đã bị tấn công rồi, thì rất khó khăn phát hiện đường nối kết vào Internet của bạn đã bị chuyển sang server của kẻ gian.

Bất cứ khi nào trang web mà bạn vào yêu cầu bạn xác nhận chứng chỉ SSL thì hãy tự hỏi mình hai câu hỏi:

1. Đây có phải là lần đầu tiên ta đi vào trang web này bằng máy điện toán này hay không?
2. Ta có từng kiểm tra lại các chi tiết của chứng chỉ SSL đúng mức chưa?

Nếu câu trả lời cho câu hỏi số 1 là "Không", thì nghĩa là bạn chưa lưu chứng chỉ SSL một cách cố định, hoặc là bạn đang đối diện với một cuộc tấn công Man in the Middle (MITM). Như đã nêu trước đây, trang web sẽ không yêu cầu bạn chấp nhận lại một chứng chỉ SSL khác nếu bạn đã lưu nó (trong những lần truy cập trước). Nếu bạn được yêu cầu chấp nhận một chứng chỉ SSL lần thứ hai, mà đáng lẽ nó đã trong danh sách SSL khả tin trong máy điện toán của bạn rồi, thì có thể đây là một trang web khác.

Chú ý: Nếu bạn xử dụng máy điện toán tại quán Café Internet, thì bạn khó mà xác nhận được chứng chỉ SSL là thật (vì không thể xử dụng một máy điện toán cố định). Cho nên, bạn cần nên ghi lại các fingerprint (ký hiệu điện tử của một trang web) của trang web mà bạn truy cập lần đầu tiên ở nơi an toàn, để tiện cho việc đối chiếu sau này.

Trả lời câu hỏi số 2 bằng cách kiểm tra lại các fingerprint của chứng chỉ SSL và tham khảo với chủ nhân của trang web (cách làm tốt nhất là bằng điên thoại hay diện thư được an toàn) để xác nhận nó. Việc này có thể tốn thời gian và phiền phức. Nhưng tiếc thay, đây là cách duy nhất.

Thật ra, không có bao nhiêu trang web xử dụng kỷ thuật bảo an SSL. Những trang web sử dụng kỹ thuật này chỉ bao gồm các nhà cung cấp dịch điện thư webmail, các trang mua và bán hàng hoá trên mạng và những công ty phục vụ tài chính trên mạng. Bạn có thể đã vào 2 hoặc 3 trang web như thế. Khi liên lạc với tổng đài của các trang web này, hãy ghi lại fingerprint của chứng chỉ SSL của trang web mà bạn muốn vào. Như thế, bạn sẽ an tâm hơn về tính xác thực và sự phục vụ của trang web đó.

Tóm lại, một khi kẻ gian đánh lừa được bạn, họ sẽ biết hết các thông tin quan trọng mà bạn trao đổi qua mạng. Do đó, đây là một việc rất quan trọng khi bạn biết được chứng chỉ SSL có thật hay không và xử dụng nó nhằm tự bảo vệ mình.

2.8 THUẬT ẨN NGỮ (STEGANOGRAPHY)

Phương thức, hay kỹ thuật ngụy trang một thông điệp gọi là steganography (tạm dịch là thuật ẩn ngữ). Trong khi sự mã hoá một thông điệp là nhằm để người ngoài không thể đọc được, mục đích của steganography là che che giấu bức thông điệp khi nó được truyền tải. Bạn có thể đã nghe đến mực vô hình hay, là viết một lá thư bằng nước chanh. Đây là những cách áp dụng trong lãnh vực stenography. Một ví dụ cổ điển trong lãnh vực này, là thông điệp bí mật được gửi bởi Herodotus circa năm 440 trước công nguyên khi ông đang bị giam giữ rất cẩn mật. Ông cạo đầu một nô lệ tín cẩn của ông, xăm chữ trên da đầu và chờ cho tóc của nô lệ đó mọc lên, nhờ vậy mà qua mặt được những người lính gác. Một phương pháp tương tự như vậy cũng được xử dụng bởi quân đội Đức ở đầu thế kỷ 20.

Khi những luật pháp quốc tế ngày càng kiểm soát những phương cách mã hoá thông tin phức tạp, chúng ta phải đối diện với vấn đề này: ta phải gìn giữ thông tin cá nhân trong khuôn khổ luật pháp. Steganography thách thức người ngoài tìm ra một mật mã phức tạp, mà đơn giản chỉ ngụy trang nhằm qua mặt sự chú ý, nghi ngờ của kẻ ngoài. Bởi vì không thể có được những điều luật cụ thể để xác định thế nào là một thông điệp steganography (vì quá đa dạng), nên luật pháp không cấm nổi steganography (ví dụ, những lời nhắn với nội dung ngụ ý điều gì là một dạng của steganography). Một vài tiến triển lý thú trong lĩnh vực steganography sẽ được bàn đến ở chương này.

Có hai phương pháp steganography hiện nay. Một là steganography số liệu. Cách này là giấu một thông điệp giữa các giải số nhị phân của một hồ sơ điện tử. Phương pháp kia là steganography ngôn-ngữ; tức dùng ngôn ngữ thông thường để gửi đi những lời nhắn mang ý nghĩa bí mật.

CÁCH STEGANOGRAPHY NGÔN-NGỮ (LINGUISTIC STEGANOGRAPHY)

Cách steganography ngôn-ngữ được sự chú ý gần đây. Bởi vì cấu tạo của cách này là ngụy trang thông tin, với sự trợ giúp của máy điện toán, và cách này phụ thuộc vào một kỹ năng duy nhất mà con người giỏi hơn máy: sử dụng và thông thạo ngôn ngữ. Sự thấu hiểu các từ ngữ, và sử dụng chúng để truyền đạt một thông tin hữu ích, một câu chuyện cười, hay một hàm ý nào đấy vẫn luôn là một độc quyền trong tâm trí loài người, mà thế giới điện toán không cách nào sánh vai kịp. Phần này sẽ giới thiệu đến bạn những ứng dụng trong lĩnh vực Steganography Ngôn Ngữ mà bạn có thể sử dụng để vượt thoát khỏi các hệ thống giám sát thông tin tối tân. Xin lưu ý rằng Steganography không nhất thiết là một ngành khoa học và sơ xuất vẫn có thể xảy ra; cho nên bạn hãy sử dụng các ứng dụng một cách thận trọng, và thử nghiệm thật nhiều trước khi áp dụng cho trường hợp cấp bách.

Ngôn Ngữ là gì?

Ngôn ngữ là một loại mật mã; sẽ không ai hiểu chúng ta nói gì nếu người đó chưa học được ngôn ngữ của ta. Những máy điện toán thì không thể học được ngôn ngữ. Các phần mềm kích hoạt bởi âm thanh (voice recognition software) hoạt động được đơn giản vì nhận diện các tầng số (sống âm thanh) trong giọng nói của chúng ta rồi đối chiếu lại với những ký hiệu tương xứng trong một phần mềm khác đã được cài trong máy. Dù chúng ta có cố gắng đến cở nào để dạy một ngôn ngữ cho một máy điện toán, thì sự thật phủ phàng vẫn là trí thông minh giả tạo (artificial intelligence) của máy vẫn không thể tiếp thu được như theo ý ta muốn. Vì vậy, cách Steganography ngôn-ngữ khai thác sự yếu kém này để vận hành.[58]

Thuật Text Semagrams

Text semagrams là những thông điện được ẩn ý trong một đoạn. Những chữ viết hoa, viết thường, nhấn âm, dạng chữ đặc biệt, ô trống giữa các từ, vân vân có thể là những ký hiệu cho một thông điệp ẩn ý, nếu được quy định trước. Các thông điệp mà cần đến linh tính để hiểu được nằm trong dạng này. Chúng rất hữu dụng khi bạn cần trao đổi một thông tin nhỏ. Ví dụ, bạn thoả thuận trao đổi tin thời tiết ẩn ý với các đồng sự qua điện thư hàng ngày. Bản tin "trời hôm nay u ám" có thể đồng nghĩa với bạn đang bị nạn, và các đồng sự của bạn nên liền cấp tốc vận động quốc tế để can thiệp và giải vây cho bạn.

Thuật Viết Sai Chính Tả

Bởi vì những hệ thống giám sát thông tin điện tử được thiết kế để nhận diện những từ cụ thể, ta có thể trọng dụng điểm yếu này để qua mặt các hệ thông trên; bằng cách là viết một từ cực kỳ sai chính tả, nhưng vẫn giữ được nghĩa của từ đó. Vì dụ, cụm từ "human rights," nghĩa là nhân quyền có thể được cố tình viết sai chính tả như sau:

hoomaine roites ***umane reites*** ***huumon writes***

và nhiều hơn thế nữa. Trong khi cách này không hữu dụng cho những thông điệp dài, nhưng bạn có thể xử dụng nó để viết những từ mà bạn nghi nằm trong hệ thống sàng lọc.[59]

58
Nguồn: Phân chia cách thức thuật ẩn ngữ (Adapted from Bauer 2002).

59
Xem Báo cáo của OpenNet Initiative tại http://www.opennetinitiative.net/studies/

Thuật Phiên Âm

Đa số các hệ thống giám sát và sàng lọc ở một quốc gia chú trọng nhận diện những ngôn từ địa phương. Thỉnh thoảng, chúng được thiết kế để nhận dạng thêm các từ thông thường được xử dụng ngoài đời hay trên các trang web, bằng một ngôn ngữ khác (Anh, hay Pháp). Một lần nữa, ta không thể nào biết chắc hệ thống sàng lọc được thiết kế ra sao, nhưng để dễ hiểu và tạo sự đa dạng khi qua mặt hệ thống này, bạn có thể xử dụng phiên âm của các từ để tạo nên một thông điệp cụ thể. Ví dụ, cụm từ "human rights" có thể phiên âm ra thành "hưu mờn rài" (nhân quyền), hoặc "democracy" phiền âm ra thành "đề móc ra xi" (dân chủ).

Thuật Biệt Ngữ

Một biệt ngữ trong lời nhắn của bạn có thể là vô nghĩa đối với người bên ngoài. Nhưng, nếu bạn đã có sắp đặt trước thì những thông điệp vô nghĩa kia lại trở thành rất ý nghĩa. Ví dụ, câu "ấu đí anh tri ân di ủ chỉ" có nghĩa là "đấu tranh dân chủ" nếu bạn ghép vần như sau: lấy vần đ trong từ "đí' và ghép với từ "ấu" sẽ thành từ "đấu", vần tr của từ "tri" với từ "anh" để thành từ "tranh", vân vân. Tóm lại, giới hạn của thuật biệt ngữ là sức sáng tạo và những từ bạn có thể xử dụng.

Thuật Ẩn Ngữ (Covered Ciphers)

Ẩn Ngữ là phương pháp hoặc là cách bí mật để cải trang một thông điệp bằng một thông điệp có nội dung mở, bình thường khác. Thông điệp với nội dung mở, bình thường này gọi là carrier message, nghĩa là thông điệp đưa đò, bởi vì nó có vai trò đưa đò một thông điệp thật. Đôi khi, thuật ẩn ngữ bao gồm luôn những cách đơn giản như nhồi nhét một thông điệp vào những từ của thông điệp đưa đò kia. Cái lợi của việc xử dụng cách này là ở chỗ thông điệp đưa đò bề ngoài chỉ trông như một thông điệp bình thường trong giao tiếp bình thường, cho nên sẽ không khêu gợi sự hoài nghi về bất kỳ nội dung có ý nghĩa gì ở bên trong nó.

Hãy quan sát cách trang web sau đây ngụy trang thông điệp của bạn thành thông điệp rác (spam). Nếu bạn có được nối kết với Internet, hãy vào trang web www.spammimic.com/encode.shtml và đánh vào đấy thông điệp "Cứu tôi với".

Thông điệp của bạn sẽ được cải trang thành y như thư rác như sau:

Bạn thân: Bạn đã có quyết định đúng đắn khi ghi danh vào danh sách điện thư này. Đây là bức thư nghìn năm một thủa, bạn không cần yêu cầu để được xoá khỏi danh sách này nếu bạn không muốn nhận thư nhừ vậy nữa. Thư này được gửi hợp pháp theo dự luật 216, Tựa I, Đoạn 302 của Thượng Viện Quốc Hội. Đây không phải là một âm mưu đề làm giàu! Tại sao phải làm việc cho người khác khi bạn có thể làm giàu trong vòng 52 tuần. Bạn có khi nào nhận thấy rằng không một ai sẽ càng ngày càng trẻ, nhưng càng ngày càng nhiều người lướt mạng….

Lưu ý: Để giải mã thông điệp trên, hãy cho vào (bằng cách copy và paste nguyên văn) vào trang web: www.spammimic.com/decode.shtml.

Ở đây, thông điệp rác (spam message) được cải trang để chuyển giao một thông điệp tiềm ẩn bên trong nội dung của nó. Lời văn trong thư rác được cấu tạo bởi một công thức do những ngôn từ hình thành, và nó có thể hoán đổi cho nhau tùy thuộc theo thông điệp của bạn. Nó bảo đảm thông điệp thật trong thư rác vẫn còn nguyên vẹn và đọc được sau khi đã được ẩn mình trong thư rác.

Bạn có thể tạo các thông điệp cho riêng bạn bằng cách xử dụng một công thức tiêu chuẩn nào đấy để giấu những thông điệp cụ thể vào những thư một bức thư rác, hoặc bằng một phương pháp nào khác mà nó cho phép bạn cất giấu một thông điệp cụ thể vào trong lời văn của thư rác.

Trong Tương Lai

Tương lai của Ẩn Ngữ Học sẽ là phát triển phần mềm để cấu tạo những lời văn tuy rất dễ đọc, nhưng chứa đựng những thông điệp thật bên trong, bằng cách phối hợp và xử dụng những ngữ vựng lạ, quen và những ngôn từ mơ hồ. Tuy nhiên, các chuyên gia chưa thể biết chắc máy điện toán có khả năng tạo nên những lời văn ý nghĩa và ẩn những thông điệp thật của chúng ta vào những thông điệp đấy, bằng cách xử dụng những ngữ thuật và ảnh thuật.

Thuất Ẩn Ngữ đối với Nhu Liệu (Data Steganography)
Sự xuất hiện của máy điện toán đã cho phép ta ẩn (cất giấu) thông điệp vào hình ảnh hoặc các hồ sơ âm thanh (sound files). Với đôi mắt thường, một bức ảnh chỉ là một bức ảnh, nhưng bên trong nó có thể là những nhu liệu mà cả một quyển sách cũng chứa không hết.

Máy điện toán, chắc bạn đã biết, vận hành bằng ký hiệu nhị phân (binary). Điều đấy có nghĩa là mỗi một mẫu tự và chỉ thị đều được phân thành ký hiệu 1 và 0. Ví dụ ký hiệu nhị phân của mẫu tự A là:

11101101

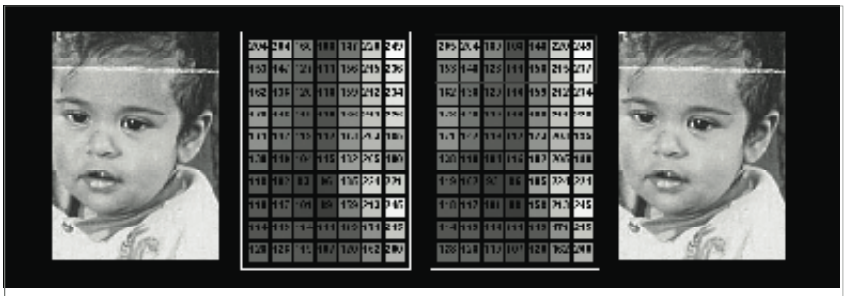
Thuở đầu, các kỹ sư điện toán thiết kế hệ thống nhị phân này để làm sao mỗi ký hiệu 1 hoặc 0 sau cùng tuyệt đối không ảnh hưởng đến giá định của mẫu tự đã được ấn định. Cho nên, nếu ký hiệu cuối cùng của thông điệp trên là 0 thay vì 1, thì máy ví tính vẫn hiểu thông điệp này là mẫu tự A, như sau:

11101100

Ký hiệu cuối cùng, tức ký hiệu mà không ý nghĩa và không cần thiết, của tất cả những thông điệp nhị phân, có tên gọi Least Significant Bit (LSB), nghĩa là ký tự không đáng kể. Một phương pháp ẩn ngữ, dùng bởi các phần mềm ẩn ngữ nhu liệu, là phân chia một thông điệp ẩn giữa các ký tự LSB theo khuôn mẫu đã được định trước. Cách này sẽ không làm thay đổi ý nghĩa của thông điệp ẩn. Tuy nhiên, mức hạn chế của cách này là thông điệp ẩn phải thật, thật nhỏ so với thông điệp đưa đò (carrier message).

Thuật Ẩn Ngữ Trong Ảnh
Các ảnh điện tử (những ảnh hiện lên trên màn hình điện toán) đều được phân chia ra thành pixel-những chấm cực nhỏ, mỗi chấm với một màu cụ thể và khi chúng kết hợp lại sẽ tạo thành tấm ảnh mà đôi mắt của bạn nhìn thấy. Đối với các hình ảnh điện tử, những nhà ẩn ngữ học ẩn thông điệp cần thiết vào các LSB của từng pixel. Điều này có nghĩa là đối với mắt người thì tấm ảnh, được kết thành bởi nhiều chấm với các sắc màu khác nhau, không thay đổi. Nhưng, thông điệp ẩn bên trong có thể được truyền đạt và ghi nhận nếu bạn biết: a) bên trong tấm ảnh có thông điệp ẩn và b) bạn xử dụng một chương trình ẩn ngữ để giải mã giống như chương trình ẩn ngữ đã được xử dụng để mã hoá thông điệp ẩn kia.

Lưu Ý: Những bức ảnh ẩn ngữ vẫn có thể bị phát giác. Mặc dầu đối với đôi mắt của con người, chúng không hề khác biệt so với ảnh thường, nhưng máy điện toán, nếu được cài đặt chương trình rà soát, vẫn có thể phát hiện những biến dạng tại các ký tự LSB. Vì lý do này, nhiều nhà an ninh chuyên môn nghi ngờ tính công dụng của thuật ẩn ngữ bằng phương pháp điện tử này. Những phương pháp khác, như mã hoá, cũng có thể được xử dụng để gia tăng an ninh cho thông tin. Có nhiều chương trình điện toán chẳng những cải trang thông điệp của bạn thành một tấm hình, mà còn sẽ mã hoá nó luôn. Như vậy, các nhà chuyên môn giải mã (những thông điệp ẩn) sẽ phải giải mã thêm một thông điệp đưa đò trong bức ảnh, trước khi tìm ra được thông điệp ẩn.



The carrier image | A fragment from the photo, representing different values of individual pixels | The top two rows of the palette have the word 'OK' embedded into the LSBs | The resulting steganographic image

Source: The Code Book, Simon Singh

Nguồn: The Code Book (Cuốn Mật Mã Sách), của tác giả Simon Singh.

Thuật Ẩn Ngữ Trong Âm Thanh

Phương pháp ẩn ngữ cũng có thể áp dụng vào các hồ sơ âm thanh (audio file). Hãy lấy ví dụ là dạng MP3. Đây là cách ép (zip) một hồ sơ âm thanh bình thường thành kích thước nhỏ hơn. Cách này được thực hiện bằng cách loại bỏ những sóng âm thành mà con người không thể nghe được : Màn nhĩ con người chỉ có thể ghi nhận được âm thanh ở một phạm vi tầng số âm thanh nhất định. Thường, âm thanh thiên nhiên được lưu ở tầng số rất cao, bởi vì do những tầng số nhiễu âm, nhưng vì con người không nghe được nên không biết, cho nên việc xoá bỏ những nhóm tầng số nhiễu âm không cần thiết này sẽ không làm thay đổi chất lượng âm thanh một cách đáng kể. Âm thanh dạng MP3 được thực hiện bằng cách này. Cho nên, phương pháp ẩn ngữ bằng âm thanh (audio steganography) được tiến hành bằng cách nạp thông điệp ẩn vào tầng số âm thanh mà con người không thể nghe (tức tầng số mà dạng âm thanh MP3 loại bỏ). Vì vậy màn nhĩ của con người không thể phân biệt giữa âm thanh có chứa thông điệp ẩn và âm thanh bình thường.

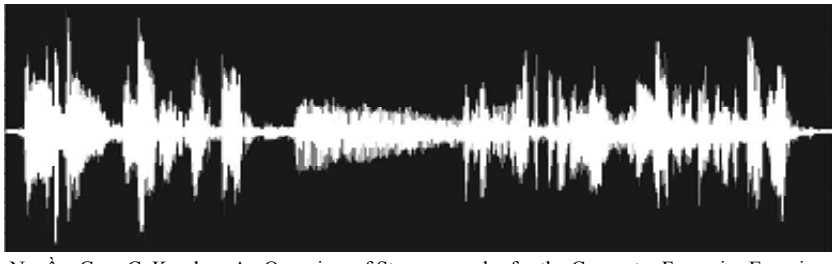
Tuy bạn có thể phát hiện sự khác biệt giữa hai tầng số âm thành khi nhìn vào sơ đồ, nhưng sẽ rất khó phân biệt sự khác biệt giữa hai âm thanh khi bạn nghe chúng.

Thuất Ẩn Ngữ Trong Lời Văn

Những phương pháp ẩn ngữ cũng có thể áp dụng vào các lời văn thường. Đôi khi, điều này được thực hiện bởi ẩn một thông điệp vào những

► Đây là sơ đồ của tầng số âm thanh bình thường:

► Còn đây là sơ đồ của tầng âm thanh trên, nhưng với một ẩn điệp bên trong:



Nguồn: Gary C. Kessler - An Overview of Steganography for the Computer Forensics Examiner

khoảng trống giữa các từ. Thông điệp ẩn được phân chia giữa những LSB của các ký tự nhị phân tại những khoảng trống trong cả bài văn. Một lần nữa, cách này bắt buộc thông điệp ẩn mà bạn muốn gửi đi phải ngắn hơn thông điệp đưa đò. Bạn cũng có thể ẩn các thông điệp ở dạng PDF hoặc ở các dạng khác, tùy theo bạn muốn dùng chương trình ẩn ngữ nào.

Phần Mền hổ trợ Ẩn Ngữ (Steganography software)

Hiện nay có đến hàng trăm chương trình ẩn ngữ khác nhau để phục vụ công việc ẩn ngữ trong nhu liệu, âm thanh, và lời văn. Mỗi phần mềm có phương pháp riêng biệt để sắp xếp thông điệp ẩn của bạn vào trong thông điệp đưa đò. Một vài phần mềm quen thuộc được biết đến là jphide và jpseek. Hãy vào các link này:

- http://linux01.gwdg.de/~alatham/stego.html
- mp3stego: http://www.petitcolas.net/fabien/steganography/mp-3stego/
- hoặc sản phẩn phục vụ thương mại Steganos Security suite: http://www.steganos.com

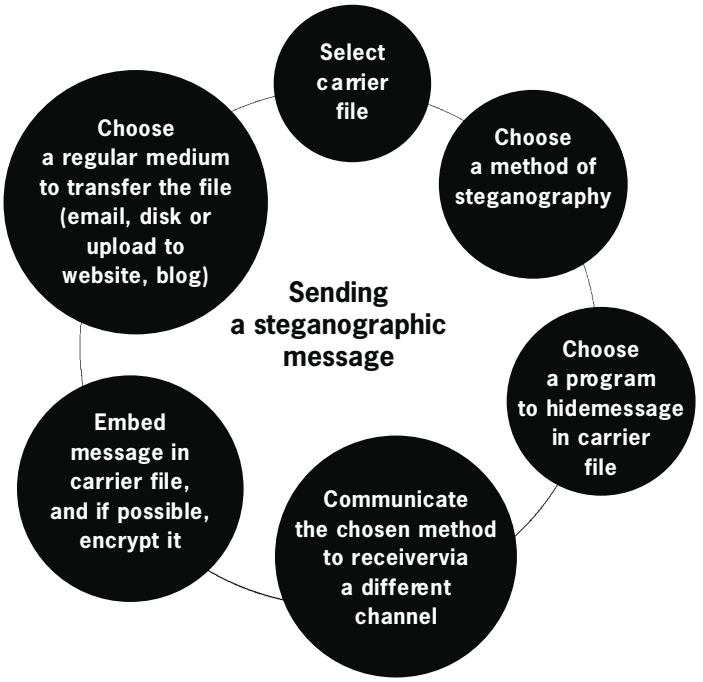
Bạn cũng có thể tìm thêm nhiều sản phẩm nữa tại http://www.stegoarchive.com/.

Cách Phát Hiện Tin Nhắn Ẩn

Steganalysis là kỹ thuật phát hiện ra tin nhắn ẩn trong thông tin (steganography). Mặc dù máy điện toán có thể dễ dàng phát hiện ra nội dung có ẩn tin nhắn, nhưng trước hết máy phải có được lập trình sẵn để dò tìm. Lợi điểm của việc ẩn tin nhắn bắt nguồn từ nguyên tắc 'mò kim đáy biển'. Hằng ngày có hàng triệu hình ảnh, tài liệu MP3 và văn kiện không mã hóa được phát tán khắp nơi trên mạng. Các hình ảnh, tài liệu và văn kiện này không làm cho các cơ quan theo dõi nghi ngờ, và khác với thông điệp đã được mã hóa, không được lưu lại để phân tích. Khi gửi nhiều ảnh qua mạng, bạn có thể ẩn tin nhắn vào một tấm ảnh. Khi

chia sẻ một bộ sưu tầm nhạc với bạn bè qua mạng, bạn có thể ẩn tin nhắn ngắn vào một bản nhạc. Bạn có thể hình dung rằng việc dò tìm tin nhắn bị ẩn từ số lượng thông tin khổng lồ được tán phát trên Internet là một việc bất khả thi.

Nguyên tắc 'mò kim đáy biển' chỉ có hiệu quả nếu có 'đáy biển'. Nếu bạn thường xuyên chia sẻ ảnh và nhạc yêu thích cho người quen qua mạng, thì khi bạn chỉ gửi thêm một hình ảnh hoặc bài nhạc, tin nhắn ẩn càng không bị để ý. Đừng dùng hình ảnh phổ biến hoặc 'lạc quẻ'. Đừng tải ảnh từ mạng về và ẩn tin nhắn vào trong ảnh (tin tặc có thể tải về đúng ảnh đó và so sánh hai ảnh bằng điện tóan). Tóm lại, đừng để lộ việc bạn ẩn tin nhắn qua hành động bất thường. Hãy thiết lập một hình thức liên lạc và lâu lâu mới ẩn tin nhắn. Không nên bị phụ thuộc vào kỹ thuật ẩn tin nhắn để bảo đảm an toàn liên lạc. Cho dù bị tin tặc phát hiện ra tin nhắn ẩn, họ cũng không đọc được nội dung. Hãy gia tăng an toàn của tin nhắn bằng cách mã hóa nó trước khi ẩn vào dữ liệu truyền thông.



2.9 PHẦN MỀM ÁC TÍNH (MALWARE) VÀ EMAIL RÁC (SPAM)

TÓM TẮT

1. Có nhiều loại phần mềm ác tính, được chuyển từ máy này sang máy khác qua nhiều hình thức khác nhau, gây ra nguy hại không kể xiết cho thông tin.
2. Cài đặt và thường xuyên cập nhật chương trình diệt virus (anti-virus), chương trình chống phần mềm gián điệp (anti-spyware). Cho tường lửa chạy và hết sức thận trọng khi mở email hoặc gài thông tin lạ vào máy.
3. Spam là email rác không mời mà đến; ngày nay spam trở thành một phần khổng lồ của mọi lưu thông trên mạng và trở thành một vấn đề lớn cho người xử dụng và cho các mạng lưới.
4. Hãy cẩn thận khi cho người khác biết địa chỉ email và đừng bao giờ trả lời và mở spam ra đọc.

Malware là từ dùng để diễn tả phần mềm phá hoại máy điện toán và phá hoại an toàn cá nhân và bí mật của thông tin. Malware gồm nhiều loại, trong đó có virus và spyware. Hàng triệu máy trên thế giới đã bị nhiễm virus hay spyware, gây ra nhiều vấn đề lớn cho kỹ nghệ điện toán. Mạng Internet đã trở thành môi trường phổ quát nhất để truyền bá malware, và lúc nào chúng ta cũng phải vật lộn để tự phòng vệ chống lại vô số cách nhiễm độc cả mới lẫn cũ.

Trên mạng ngày nay, khi một máy đã bị malware nhiễm, thì có thể xử dụng máy đó để tấn công vào máy khác. Khi hệ phòng vệ của máy có lỗ hổng (security hole), tin tặc có thể khai thác bằng cách nhiễm virus vào máy. Virus cho tin tặc khả năng điều khiển máy từ xa, tạo nên một tập hợp robot phần mềm (Botnet). Botnet có thể dùng để tấn công một trang mạng nào đó hoặc máy chủ của một tổ chức hoặc một chính quyền. Tấn công bằng cách đó được gọi là tấn công từ chối dịch vụ phân tán (tấn công Distributed Denial of Services hoặc tấn công DDoS), vì nó áp đảo máy chủ bằng cách cùng lúc gửi hàng triệu yêu cầu dịch vụ.

Trong thập niên vừa qua các cuộc tấn công DDoS ngày càng phổ biến hơn, và thường được thi hành bằng cách sử dụng đồng loạt những máy đã bị nhiễm. Các trang mạng của các tổ chức nhân quyền thường bị tấn công DDoS làm cho ngưng hoạt động. Rất khó chống lại tấn công DDoS, cho nên phòng bị không cho máy bị nhiễm là việc quan trọng nhất. Cần phải dứt khoát dùng phần mềm chống virus ngay từ đầu, nếu không thì chính máy của bạn có thể đã bị nhiễm và đang tham gia vào một cuộc tấn công DDoS vào một trang mạng mà bạn không biết.

VIRUS

Cũng giống như virus của người, virus của máy nhiễm máy và dụng cụ kỹ

thuật với mục đích thay đổi sự ổn định, khả năng hoạt động hoặc sự nguyên vẹn của máy. Virus thường là chương trình nhỏ được chạy trên máy sau khi bạn làm một việc gì đó. Virus có khuynh hướng tự sinh sôi nẩy nở. Bạn có thể nhận virus từ email, trên thẻ nhớ USB, hoặc qua việc bạn đến viếng một trang mạng nào đó. Có khi cũng có thể bị nhiễm virus qua cách liên kết đến mạng.

Lịch Sử

Trường hợp đầu tiên được biết đến của virus máy có thể lây lan được là Elk Cloner. Virus được anh học sinh trung học 15 tuổi tên Rick Skrenta viết ra vào khoảng năm 1982 và được nhắm vào hệ Apple II. Elk Cloner lây lan bằng cách nhiễm hệ điều hành của Apple II và chuyền đi qua đĩa mềm. Khi mở máy lên từ đĩa mềm đã bị nhiễm, virus sẽ tự động chạy. Khi nào có đĩa mềm được cài vào máy đã bị nhiễm, virus tự sao chép một bản vào đĩa mềm, rồi từ đó mà lan đi. Virus không gây nguy hại gì cho máy, mà chỉ làm quấy rầy chút đỉnh. Khi máy được mở lên lần thứ 50, virus sẽ cho hiện lên một 'bài thơ' ngắn:

Elk Cloner: chương trình có cá tính

Sẽ vào mọi đĩa
Sẽ xâm nhập mọi vi mạch
Nó chính là Cloner!

Sẽ bám vào như keo
Sẽ thay đổi bộ nhớ luôn
Hãy cho Cloner vào![60]

Sâu (Worm) Morris, do Robert Tappan Morris viết vào năm 1998, trở thành malware nổi tiếng đầu tiên được tán phát trên mạng. Có ước lượng rằng malware này nhiễm khoảng 6000 máy trên thế giới và dẫn đến việc hình thành một kỹ nghệ mới để chống lại những tấn công tương tự, cầm đầu do CERT (Computer Emergency Response Team), một học viện nghiên cứu và trung tâm phát triển do chính phủ liên bang Mỹ tài trợ (http://www.cert.org).

Virus MyDoom của năm 2004 nhiễm 1 phần 12 tổng số email gửi đi trên mạng và phối hợp được vụ tấn công DDoS lớn nhất, liên quan đến hơn 1 triệu máy trên khắp thế giới.

Các Dạng Malware; virus, worm, trojan, keylogger

Có nhiều loại malware, mỗi loại có một phương cách hoạt động và phân phối riêng.

Virus là chương trình máy điện toán làm hại phần mềm (và gần đây hại cho cả phần cứng) của máy, với kết quả là làm mất dữ liệu hoặc làm hư máy. Virus phải do người cho hoạt động (bằng cách cho chạy hoặc mở ra) và có thể tự sinh sôi nẩy nở để nhiễm qua máy khác.

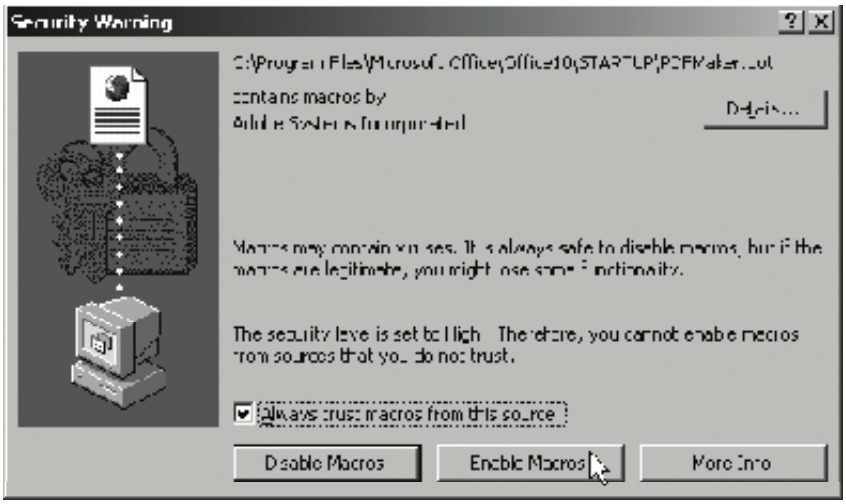
Cách nhiễm máy: virus đến bằng tài liệu đính kèm trong email, tài liệu tải từ đĩa mềm (USB key) hoặc các loại đĩa lưu động khác (removable hard disk). Tài liệu có thể có chứa virus thông thường

60
Wikipedia - http://en.wikipedia.org/wiki/Elk_Cloner

(nhưng không phải luôn luôn) có những đuôi như sau: .exe, .com .bat .vbs .php .class .jbs .scr .pif.

Sâu (Worm) cũng tương tự như virus, nhưng virus không tìm cách xóa hoặc làm hư thông tin trên máy. Sâu thường nằm ẩn trong thư email. Sâu khai thác những lỗ hổng an ninh trong hệ điều hành và tự lây qua máy khác qua đường mạng.

Cách nhiễm máy: sâu sẽ nhiễm máy ngay khi bạn mở thư email có sâu ẩn nấp. Máy đã bị nhiễm cũng có thể gửi và nhận sâu bằng cách kết nối lên mạng



► A warning of a macro inside an Adobe PDF document

Ngựa Troia (Trojan) là chương trình giả làm phần mềm hợp pháp nhưng thực ra có chứa mã ác tính. Trojan không tự sản sinh được, nhưng có thể buộc máy phải tải virus về hoặc phải thực hiện một chức năng định sẵn (chẳng hạn như tấn công một trang mạng khác). Trojan mở ra một cửa sau (back door) trên máy và cho phép người ngoài được toàn quyền truy cập máy. Nó cũng có thể làm cho tin tặc truy cập được mọi chương trình và tài liệu trên máy.

Cách nhiễm máy: Trojan giả làm phần mềm hợp pháp và chỉ hoạt động khi bạn cho chạy phần mềm. Đôi khi virus cũng cài đặt trojan vào máy.

Nhu liệu theo dõi thao tác bàn phím (keylogger) là chương trình ác tính chuyên theo dõi thao tác của bạn trên máy và trên mạng rồi gửi thông tin này cho một người ngoài. Mục tiêu chính của keylogger là phá hoại sự an ninh của máy và tiết lộ thông tin liên quan đến người sử dụng máy để có thể kiếm tiền.

Cách nhiễm máy: Keylogger có thể đến từ email hoặc ẩn kín trong phần mềm bạn cài vào máy. Bạn có thể bị nhiễm bằng cách viếng trang mạng lạ (chuyện này rất dễ xảy ra đối với Internet Explorer) hoặc sử dụng chương trình chuyên dùng chung tài liệu. Keylogger có thể đến từ tài liệu đính kèm email hoặc do virus cài vào máy.

Trên thế giới đầy rẫy virus của ngày nay, cả điện thoại di động cũng bị nhiễm, vì BlueTooth và Media Messaging bị virus lợi dụng để phát tán. Blackberry cũng không được xem là ngoại lệ, vì có lỗ hổng làm cho malware có thể trở thành phần mềm ứng dụng được tín nhiệm (trust). Skype và MSN, máy quay phim gắn liền với iMac và ngay cả máy trợ tim không dây mới phát hành cũng đều có thể bị người lập trình virus 'làm chủ'. Mã ác tính đã được phát hiện trong hình ảnh nằm trên các trang mạng chia sẻ ảnh và có hàng triệu trang mạng vô tình (và được giàn dựng thô thiển hoặc không cập nhật) đã bị mã ác tính cài vào. Hoặc do ta ngu dốt, hoặc do óc sáng tạo của kẻ làm virus, mà đã sản sinh ra một thế giới điện toán thù địch không cho phép chúng ta phạm vào bất cứ một lỗi nào dù nhỏ. Hy vọng duy nhất là bạn tự trang bị bằng phần mềm có chất lượng tốt và nhiều kiến thức phổ thông, để xây dựng lâu đài bảo vệ căn nhà điện toán của bạn.

Cần phải có một chính sách có tổ chức để tích cực ngăn không cho tải về và chạy virus. Một phần nào có thể được thực hiện ở mức độ phần mềm, bằng cách lập trình để phần mềm được vững vàng đối phó với virus và bằng cách chạy chương trình diệt virus, chống spyware và chương trình tường lửa. Cần phải tích cực truy tìm và cập nhật mọi phần mềm, bao gồm cả phần sửa chữa cho Windows (Windows Update). Làm như vậy sẽ làm gia tăng khả năng phòng vệ chống malware mới vừa được viết ra. Biện pháp chính là ngăn ngờ malware từ mức độ chính sách.

Bạn cần phải:

- Lưu lại một bản sao các tài liệu quan trọng vào một đĩa lưu động
- Ngăn hết mọi tài liệu đính kèm ác tính trong email từ máy chủ email hoặc từ phần mềm đọc email.
- Đừng bao giờ mở tài liệu đính kèm của email mà bạn không chờ nhận và của email có xuất xứ từ nơi lạ, và cố gắng đừng click vào link nằm trong thư email, nhất là từ người gửi mà bạn chưa biết là ai.
- Chạy kiểm sóat virus và spyware trên toàn máy, ít nhất là mỗi tuần một lần
- Đừng tải phần mềm không cần thiết về máy. MSN và Yahoo Chat là những đối tượng phổ biến để truyền lan virus. Cố gắng đừng sử dụng 2 chương trình này và phần mềm chia sẻ tài liệu trên máy làm việc.
- Luôn có tin tức về malware mới nhất

Nếu máy bạn đã lỡ bị nhiễm virus:

- Cắt liên kết vào mạng Internet và mọi mạng lưới ngay lập tức
- Đóng hết mọi phần mềm và cho chạy chương trình diệt virus trên toàn bộ máy. Cài đặt chương trình có khả năng kiểm soát toàn bộ máy ngay tại lúc máy mới vừa khởi động. Làm như vậy có lợi vì có loại virus ẩn vào trong tài liệu mà Windows không kiểm soát được khi Windows đang chạy. Xóa hết mọi virus tìm thấy và ghi lại tên virus. Rồi cho chạy chương trình một lần nữa, cho đến khi máy không còn cảnh báo có virus nữa.
- Liên kết lên mạng và thu thập thông tin mới nhất về virus mà bạn

ghi lại. Bạn có thể đến www.symantec.com hoặc www.sophos.com hoặc www.f-secure.com để lấy thông tin mới nhất về các loại virus, về khả năng gây nguy hại và về phương pháp phát hiện, phòng ngừa và diệt xóa virus. Cập nhật hệ điều hành Windows với các phần chỉnh sửa cần thiết.

- Nếu virus nhiễm máy nằm trên một mạng lưới, thì ngắt liên kết mọi máy từ Internet, rồi từ mạng lưới đó. Mọi người phải ngưng sử dụng máy, và phải thực hành mọi bước đã mô tả ở phần trên cho mỗi máy. Mặc dù đây là một quá trình đầy mệt mỏi, nhưng là hoàn toàn cần thiết.

Vào năm 1999, BubbleBoy trở thành sâu đầu tiên không cần người mở tài liệu đính kèm email để nhiễm máy. Ngay khi thư email đã bị nhiễm được mở ra đọc, thì sâu bắt đầu làm việc. Khuynh hướng này được nhiều người lập trình virus bắt chước và tiếp tục làm cho những hệ bảo an đắt tiền nhất bị bất lực, vì nó khai thác sự tò mò bất tận của bạn muốn được nhìn thấy nội dung của một email có vẻ nghi ngờ.

Hãy tắt đi chức năng duyệt trước email trong phần mềm email. Hơn nữa, hãy mở duy nhất email nào có chứa toàn chữ đọc được. Làm vậy sẽ ngăn mã ác tính đang ẩn trong nội dung email không hoạt động được.

Trên mạng bạn sẽ không có khả năng tự vệ nếu bạn không cài chương trình diệt virus, chống spyware và tường lửa vào máy. Các chương trình này cần phải được cập nhật liên tục và cài đặt nghiêm ngặt. Bạn không cần phải tốn tiền chi cả. Có những công ty như Avast, Comodo và Safer Networking cho không chương trình chống malware và tường lửa để dùng ở nhà[61].

61
Mọi phần mềm và sách hướng dẫn cài đặt và sử dụng đều có thể tải về từ Digital Security Toolkit tại http://security.ngoinabox.org.

Nguyên tắc quan trọng nhất là phải ý thức và cảnh giác. Phải phòng ngừa đầy đủ, nhưng đừng để chương trình diệt virus hoặc chống spyware làm cho bạn cảm thấy an toàn giả tạo. Có thể bạn đã đoán ra rằng đây là một cuộc chiến bất tận. Virus truyền lan được không chỉ nhờ vào cách lập trình khéo léo mà còn do người dùng bất cẩn và vô tình.

SPAM

Spam là quá trình gửi email không mời mà đến và có số lượng lớn. Thông thường spam có dạng quảng cáo hoặc tin nhắn vô nghĩa, làm đầy ắp hộp thư email. Spam là một hoạt động nhằm gia tăng lợi nhuận cho nhiều công ty, và càng ngày là gia tăng lợi nhuận cho nhiều nhóm làm spam. Đây là một phương pháp nhiều lợi tức, vì việc phân phối khối lượng lớn rất là ít tốn kém, ít hơn nhiều so với thư rác bằng bưu điện và các thể loại quảng cáo khối lượng lớn khác. Hiện nay spam chiếm khoảng 50% tổng số hoạt động trên mạng và là một vấn đề nan giải cho nhiều cá nhân và hãng thương mại. Phần này sẽ hướng dẫn cho bạn cách làm giảm thiểu số lượng spam trong hộp thư email của bạn.

Có nhiều công ty trên mạng cung cấp danh sách địa chỉ email của khách hàng của mình cho các tổ chức chuyên môn gửi email thương mại không mời (spam). Có những công ty khác lục tìm địa chỉ email từ những thư gửi trong những danh sách địa chỉ, nhóm thảo luận, hoặc dữ kiện đăng ký tên miền. Trong một cuộc thí nghiệm do Federal Trade Commission của Mỹ thực hiện, một địa chỉ email được đăng trong phòng chat, bắt đầu nhận spam chỉ trong vòng tám phút sau khi đăng[62].

Lịch Sử

Khái niệm gửi spam như là một kỹ thuật quảng cáo do hai luật sư di trú tại New York mở đầu vào năm 1994, khi họ muốn quảng cáo nghề nghiệp của mình qua việc gửi email với khối lượng lớn. Họ cho rằng spam là phương pháp tiếp thị mới rất chính đáng và có khả năng thành tựu, và gán cho những ai chỉ trích họ là "bọn quá khích chống thương mại". Từ đó, spam nhanh chóng trở nên phổ biến.

Ngăn Ngừa Spam

Có vài phương pháp làm giảm bớt khối lượng spam mà bạn nhận, nhưng bạn sẽ không bao giờ hoàn toàn loại trừ nó được. Nếu bạn sử dụng trương mục webmail (như Hotmail, Gmail hoặc Yahoo), thì các trương mục đó đã cài sẵn phần mềm lọc bỏ spam một cách tự động.

Cách ngừa spam chính là đừng trả lời hoặc click vào bất cứ cái link nào bên trong thư spam. Cho dù số lượng spam làm cho bạn bực tức và bạn muốn trả lời lại thư spam để phàn nàn hoặc để yêu cầu họ ngưng gửi spam, làm như vậy chỉ là xác nhận địa chỉ email của bạn là có thật và tự liệt mình vào loại người đọc spam và phản ứng lại spam. Đừng bao giờ mua bất cứ thứ gì quảng cáo trong thư spam. Cho dù hàng hóa đó có chính đáng đi nữa, làm như vậy bạn cũng chỉ là tài trợ cho thị trường làm spam mà thôi.

62
Sự Riêng Tư Quốc Tế -- Báo Cáo về Sự Riêng Tư và Nhân Quyền năm 2004 – Mối Đe Dọa cho Sự Riêng Tư.

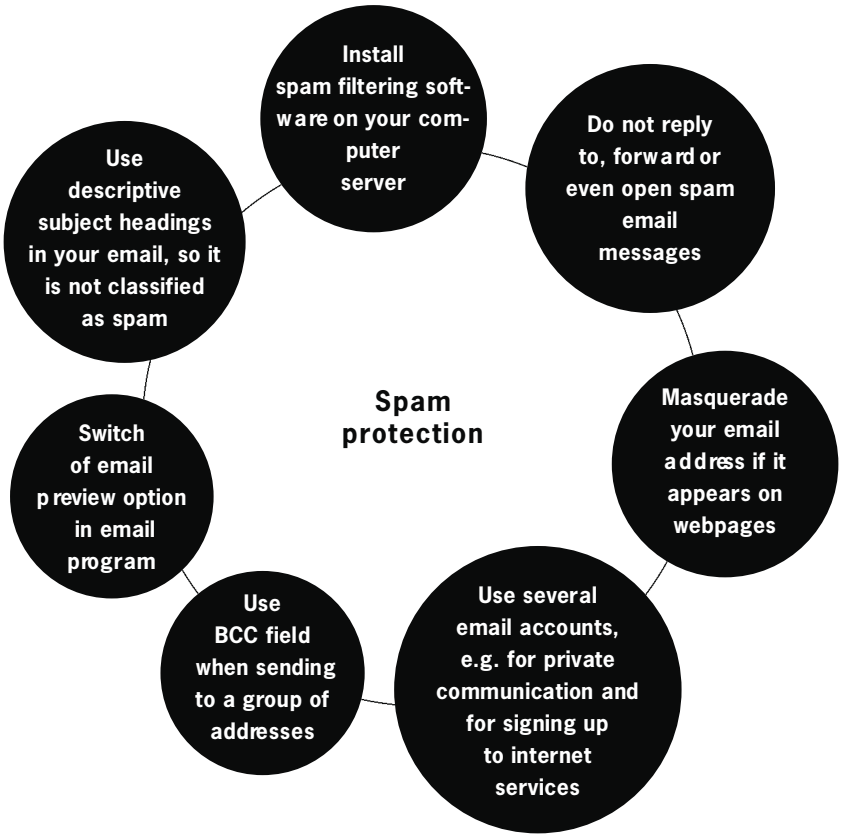
Đừng bỏ địa chỉ email của bạn vào bất cứ trang mạng hay list server nào. Nếu không tránh được việc này, thì hãy cải trang địa chỉ bằng cách thay dấu @ bằng dấu # hoặc chữ 'at'. Làm cách này sẽ ngăn không cho nhện mạng lấy được địa chỉ email. Thí dụ:

user#frontlinedefenders#org
user AT frontlinedenfeders DOT org

Nếu bạn gửi email đến một nhóm nhiều người nhận, thì hãy bỏ các địa chỉ email người nhận vào trong ô 'Bcc'. Làm như vậy sẽ không cho người khác biết rằng bạn đang gửi email số lượng lớn và ngăn không cho kẻ làm spam lấy và sử dụng danh sách địa chỉ email cho mục đích riêng của họ.

Thử dùng nhiều địa chỉ email. Giành một cái là địa chỉ riêng mà bạn chỉ cho những người bạn tin tưởng biết đến. Bạn có thể dùng các địa chỉ khác để đăng ký và xác nhận các trương mục trên mạng. Như vậy bạn sẽ phân biệt ra trương mục email riêng tư và trương mục có thể bị spam.

Nếu trương mục email của bạn đã bị nhận quá nhiều spam và phần mềm sàng lọc không còn hiệu lực nữa, thì chỉ còn có nước mở một trương mục email khác và lần này nên thận trọng hơn.



2.10 PHÁC THẢO & NHẬN DẠNG

TÓM TẮT

1. Danh tính điện tử của bạn là tập hợp các hồ sơ máy điện toán, điện thoại và mạng hoặc có liên quan đến bạn hoặc có thể dùng để nhận dạng bạn. Danh tính cũng tiết lộ thông tin mà bạn (cũng như bạn bè và đồng nghiệp của bạn) chia sẻ trên các trang mạng xã hội và các trang blog.
2. Kỹ thuật phác thảo thừa nhận một số thói quen, tính cách, đoàn thể chính trị và xã hội của bạn, cũng như của bạn bè và đồng nghiệp của bạn. Internet là một tài nguyên xuất sắc để phác thảo nhận dạng bạn.
3. Kỹ thuật ẩn danh là một công cụ quan trọng cho các nhà hoạt động trên mạng khi sử dụng các công cụ liên lạc, nhưng đây là công tác khó khăn trong kỹ thuật hiện đại ngày nay.

Chương này sẽ giải thích về danh tính điện tử của bạn và mô tả cách dùng kỹ thuật hiện đại để phác thảo ra tính cách, các lãnh vực hoạt động và mối giao thiệp của bạn. Chương này sẽ nhắc đến một số đề tài đã được giải thích trong tài liệu hướng dẫn này gồm có kỹ thuật theo dõi và ẩn danh, và sẽ cố gắng trình bày các cạm bẫy cố hữu và sự bất an của kỹ thuật mạng và điện thoại di động. Mục đích của chương là để giáo dục người đọc về những lỗ hổng tiềm tàng về an ninh và tự do hội họp hiện hữu trong hệ thống mạng và viễn thông ngày nay, và để hướng dẫn cách đối phó với và cách giảm thiểu hậu quả của các lỗ hổng.

Mặc dù có nhiều người quen thuộc với những thuật ngữ như Web 2.0, mạng xã hội, tin nhanh twitter, truyền bá phim đoạn, v.v., nhưng rất ít người để ý đến khả năng xâm nhập của hệ thống mạng toàn cầu dùng để cung cấp các dịch vụ này. Mặc dù sự liên lạc trực tiếp và sự truy cập thông tin do kỹ nghệ hiện đại cung cấp rất có nhiều sức cám dỗ, bạn cần phải cân nhắc nó với tính thâm nhập cố hữu của các dụng dụ này có thể đi sâu vào đời sống riêng tư của chúng ta và thu thập dữ kiện về hoạt động của bạn và mạng lưới bạn bè.

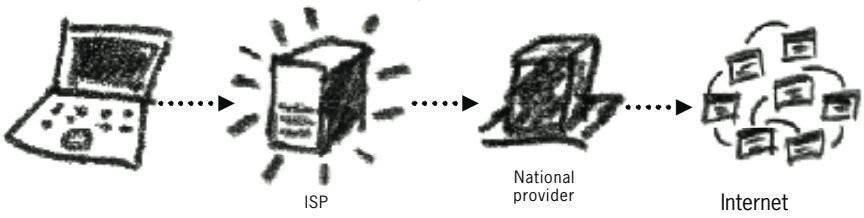
Khả năng tình báo mạng không phải chỉ hiện hữu tại các nước tân tiến và ưa dùng kỹ thuật. Xu hướng thường gặp trong giới buôn bán võ khí trên toàn cầu – có nhiều nước sẵn sàng bán kỹ thuật đã lỗi thời cho bất cứ ai mua được – là họ cũng áp dụng kỹ thuật theo dõi và bảo an. Sự tập trung các cơ sở dữ liệu công cộng và tư nhân về một nơi, dưới chiêu bài an ninh quốc gia và thế giới thường được dùng nhằm vượt qua các trở ngại về luật pháp và tài chính, cũng như việc tất cả chúng ta phổ biến và đón nhận các dụng cụ và chức năng truyền thông, tạo ra hậu quả làm suy giảm đi và thường là xóa đi sự kín đáo và ẩn danh của danh tính chúng ta – một quyền lợi bẩm sinh và được bảo vệ bởi nhiều hiệp ước và tổ chức quốc tế.

Danh Tính Điện Tử

Trong thực tế của thế giới, mỗi người được nhận dạng nhờ vào hộ chiếu của chính phủ cấp và người quen biết mặt. Ngoài ra, còn có nhiều tài liệu và thông tin khác như là bằng lái xe, số an sinh xã hội và số khai thuế và tiếng tăm là những đặc tính nổi bật cho danh tính và đoàn thể của ta.

Kỹ nghệ thông tin hiện đại có khả năng xâm nhập và lấy nhiều chi tiết tỉ mỉ hơn so với thế giới ta thường biết đến. Có nhiều cách nhận dạng của đời sống cá nhân, thói quen, lãnh vực hoạt động và đoàn thể xã hội bạn đang sinh hoạt, được thu thập và giữ lại. Nghiên cứu các thông tin và giả thuyết về lối sống tại nhà và tại sở làm được gọi là phác thảo và được trình bày sau trong chương này.

Danh tính điện tử của bạn có thể được thu thập từ nhiều mẫu thông tin, thường do chính hành động của ta tạo ra hoặc báo ra, hoặc do hành động của bạn bè và đồng nghiệp ta. Mỗi khi liên kết vào mạng, bạn được nhận dạng bởi địa chỉ IP ấn định cho máy bạn (xin xem thêm tại Chương 2.5 và Phụ Lục B). Trường hợp bạn làm việc từ nhà hoặc sở làm, có thể dùng địa chỉ IP này để dễ dàng suy ra danh tính thật của bạn – vì bạn đã đăng ký và mua dịch vụ truy cập mạng từ một nhà cung cấp tại địa phương đã biết được tên và địa chỉ của bạn.



Minh Họa 26: Quá trình truy cập mạng có thể dùng để liên kết trực tiếp đến máy bạn.

Một nguyên tắc tương tự cũng được áp dụng cho điện thoại di động. Nếu bạn đã đăng ký số điện thoại dưới tên bạn, thì mọi cuộc gọi tại số này có liên quan đến bạn. Ngoài ra, địa điểm của mỗi điện thoại di động đều có thể tính được bằng kỹ thuật gọi là phép đo tam giác – khi một số đài điện thoại nằm gần nơi điện thoại của bạn có thể tính toán được nơi bạn đang ở, chính xác đến độ vài mét. Còn có thể phức tạp hơn. Mỗi cái điện thoại được nhận dạng bằng một số IMEI duy nhất. Con số này được ghi lại mỗi khi bạn dùng điện thoại để gọi. Dù thay đổi thẻ SIM của điện thoại đã có gắn liền với danh tính của bạn (qua số IMEI) cũng chưa chắc làm cho bạn được ẩn danh.

Điện thoại di động thế hệ thứ 3 – loại điện thoại cung cấp dịch vụ truy cập mạng và tọa độ định vị toàn cầu (GPS) tiết lộ địa điểm chính xác của bạn và thường thì tiết lộ danh tính của bạn cho hãng cung cấp dịch vụ. Ngay cả khi đã tắt đi, điện thoại cũng có thể tiết lộ tọa độ của nó: nó vẫn tiếp tục liên lạc với các đài điện thoại bằng cách gửi đi một tín hiệu hoạt động ngắn[63]. Vì lý do này, nên nhà cung cấp phục vụ có thể mở điện thoại di động lên từ xa. Có giải pháp là tháo pin ra hẳn khỏi điện thoại, và như vậy sẽ làm điện thoại mất đi khả năng cung cấp điện cho bất cứ chức năng nào.

Trương mục và địa chỉ email cũng có thể dùng để nhận dạng bạn. Khi trương mục được đăng ký dưới tên thật thì nhận dạng thật dễ dàng, và khi trương mục được ẩn danh nhưng được truy cập từ một địa điểm mà địa chỉ IP có gắn liền với bạn thì bạn cũng có thể bị nhận dạng.

63
ZDNet, cơ quan FBI dùng mic của điện thoại di động để nghe lén, Declan McCullagh, ngày 1 tháng 12 năm 2006, http://news.zdnet.com/2100-1035_22-150467.html

Cùng một nguyên tắc được áp dung khi bạn viết blog và sử dụng trương mục chat trên mạng, đăng nhập mạng xã hội, đăng ký diễn đàn và tiểu sử trò chơi mạng. Như đã trình bày trước đây trong sổ tay này, nhà cung cấp dịch vụ mạng và điện thoại thu thập lại tài liệu liên lạc. Khi có đủ thông tin về hoạt động mạng của bạn, có thể nhờ vào dụng cụ truyền thông điện tử mà suy ra danh tính xác thực của bạn.

Máy đã bị nhiễm malware cũng có thể vạch trần chi tiết bí mật của người dùng máy, tiết lộ thông tin về hoạt động của người dùng cho một kẻ thứ ba. Nếu muốn biết thêm chi tiết về cách đối phó với những mối đe dọa này, xin xem thêm ở Chương 2.9.

Thiết Lập Hồ Sơ Điện Tử (Digital Profiling)

Khi danh tính của một hồ sơ điện tử trên mạng (digital profile) chủ ý hay vô tình có liên hệ với một cá nhân thì quyền riêng tư của cá nhân ấy trở thành một quan tâm lớn. Bởi vì những lần truy cập vào những trạng mạng trên Internet, hoặc những trao đổi, liên lạc qua email có thể làm lộ những tin rất quan trọng về một người, ví dụ như thói quen và những mối quan hệ của người ấy với những tổ chức, cá nhân cụ thể khác. Cho nên, quan điểm chính trị và xã hội, cũng như sự liên kết với các tổ chức và đặc biệt là những hành động trong tương lai của cá nhân ấy có thể được giả định. Hiện nay, việc thu gom thông tin cá nhân trên mạng để lập thành hồ sơ cá biệt để xử sử dụng cho nhiều mục đích khác nhau rất phổ biến. Với tên gọi digital profiling, đây là cách thu thập thông tin từ các kho dữ liệu (database) mà người sử dụng mạng vô tình hay cố ý lưu lại. Dựa vào các hồ sơ ấy, người ta có thể phỏng đoán cá tính, xu hướng hành vi hay hành động của một cá nhân hay một tổ chức. Vi vậy profiling được các công ty tiếp thị, hoặc tài chính áp dụng để phân tích sở thích của người tiêu dùng, cũng như sự tác động của một mặt hàng hoặc dịch vụ lên người tiêu dùng. Profiling cũng là cách thông dụng để cơ quan công quyền có thông tin về những suy tính gây ra tội ác để suy đoán, và nhận diện nhằm ngăn chặn kẻ gian trước khi họ gây ra tội ác. Cụ thể, profiling hiện nay rất phổ biến trong kỹ nghệ hàng không. Cách này được áp dụng để ngăn chặn kẻ có tiềm năng gây ra tội ác, hay khủng bố ngay trước khi họ bước chân lên phi cơ.

Ngoài việc thu thập hồ sơ về tội ác, tiềm năng tín dụng, việc làm, và dữ liệu y khoa, profiling ngày nay bao gồm thu thập luôn danh tính điện tử trên mạng (digital identity) để nâng cao mức xác thực và mức độ chi tiết của mỗi hồ sơ. Cụ thể, tất cả các email gửi đi và nhận được, những cú điện thoại, và các trang mạng bạn truy cập đều được lưu lại. Để khi cần, người ta mang ra phân tích. Các ví dụ phổ biến là Google Email và các ứng dụng (applications) của Google. Google cung cấp dịch vụ miễn phí cho hàng triệu khách hàng. Nhưng, Google vẫn kiếm được lợi nhuận là nhờ vào quảng cáo. Các phầm mềm được cài sẵn trong những dịch vụ của Google sẽ rà soát email và những mối liên lạc qua ngã Google để tìm thông tin và đối tượng tương xứng để quảng cáo. Điều đáng ngại là khách hàng phải đồng ý với chính sách này khi ghi danh tạo trương mục (account).

Tuy rất khó để biết Google sẽ phản ứng và sử dụng các thông tin nêu trên ra sao dưới sức ép của luật pháp Mỹ, nhưng chúng ta cũng hình dung ra được những mối nguy ngại từ việc nhận dạng (profiling) này. Tương tự như vậy, ta sẽ còn gặp khó khăn nữa để có thể đoán trước đại công ty này sẽ tuân thủ và hành động như thế nào nhằm tôn trọng các luật về quyền riêng tư của chính quyền nước ngoài. Ví dụ, tại Hoa Lục, Google đã lắp đặt những hệ thống sàng lọc kết quả truy cập (results of searches) Internet do người dân Hoa Lục tìm khi Google phải tuân thủ theo luật pháp nơi này.

Cũng xin nói thêm là, cứ vài năm một lần, các công ty viễn thông hàng đầu và nhiều chính phủ các nước họp mặt để thảo luận về các tiến trình cũng như cập nhật các kỹ thuật kiểm soát Internet và truyền thông. Mong rằng quyền riêng tư sẽ được phần nào bảo đảm.

Thông tin cá nhân của một người và rồi danh tính của người đó không chỉ bị lộ (hay bóp méo) qua những hoạt động hằng ngày, mà còn phải chịu tác động bởi những gì người khác trao đổi hoặc bàn luận về người ấy. Ví dụ, một bức điện thư (email) gửi đến hộp thư với nội dung liên quan đến hồ sơ (profile) của một người. Căn cứ vào nội dung của bức thư ấy (qua Internet hôm nay), bất kể email kia được nhận hay không, người ta có thể đoán ra danh tính của người nhận thư. Vì thế, khi một email được gửi đến một nhóm địa chỉ, mối giao kết và liên hệ giữa các người trong nhóm tự nhiên thành hình, bất kể sự mong muốn của mỗi người nhận. Cho nên, hồ sơ cá nhân trên mạng của ta rất dễ, và thường chịu ảnh hưởng bởi những giao tiếp giữa ta, bạn bè và đồng nghiệp.

Vài ví dụ nhằm biểu thị tiềm năng việc bị thu thập thông tin khi sử dụng các dịch vụ liên kết mạng xã hội. Công chúng sẵn sàng tải lên Internet một khối lượng lớn thông tin cá nhân, tạo liên kết giữa bạn bè và đồng nghiệp, để lộ nơi ở, hình ảnh, và cả thông tin liên lạc, khi sức ép và sự thu hút tham gia vào "cách mạng truyền thông" này mỗi ngày một lớn. Chưa khi nào bằng lúc này, khi các nhà tiếp thị, chính phủ, và kẻ gian có thể thu thập thông tin cá nhân trên mạng dễ dàng để sử dụng cho nhiều mục đích khác nhau. Điển hình là các Vệ Binh Cách Mạng Iran đã tốn rất nhiều thời gian trên mạng Twitter để theo dõi tất cả các cuộc biểu tình cũng như chương trình hành động của đối phương, đôi khi còn mạo dạng người đấu tranh. Vì thế họ đã thành công trong việc ngăn chặn hành động của đối phương ngay từ khi còn trong trứng nước. Twitter cũng có thể đã giúp họ nhận diện hoặc xác nhận danh tính của những người biểu tình và những nhà lãnh đạo đấu tranh xã hội.

Một khi thông tin đã được lưu, rất khó xoá (**xem thêm chương 2.3**), và điều này cũng áp dụng tại các ứng dụng trên những mạng xã hội (social networking tools). Một trang Facebook hoàn toàn cá nhân có thể bị người chủ tương lai soi mói trước khi mướn bạn, bất kể công việc bạn xin làm là việc gì. Hoặc một cơ quan truyền thông, được sự bảo trợ của chính phủ, nếu muốn chế diễu hay tìm bẩn các thành viên của tổ chức nhân quyền như NGO, không những có thể điều tra các trang mạng xã hội của bất cứ thành viên nào, mà còn có thể đi sâu vào trang của bạn, và bạn của bạn họ nữa. Có thể nói, khi một quả táo hư, hay một chút bụi bẩn được tìm trong muôn vàn mối liên hệ trên toàn cầu của một người, nhiều chuyện có thể được thêu dệt để tác động đến danh tiếng và uy tín của người đó, và cả luôn tổ chức hay cơ quan người đấy làm.

Tóm lại, không ai có thể tránh khỏi việc bị thu thập thông tin cá nhân (profiling). Tuy nhiên, nhận thức ra và có những biện pháp đề phòng sẽ giúp ta giới hạn, hoặc có quyền chọn lựa những thông tin gì về ta sẽ bị thu nhặt. Xin kết luận rằng, sự tác động của kỹ thuật vào trong đời sống nghề nghiệp và đời sống cá nhân đồng nghĩa với việc phải ta đối diện với nguy cơ bị thu thập thông tin cá nhân!

Chính Danh và Sự Minh Danh (Authenticity and Authentication)

Tính chất toàn cầu và đại chúng của Internet đồng nghĩa với phải cần thêm nhiều phương pháp mới để thẩm định thông tin và chính danh của người dùng. Cho đến bây giờ, người sử dụng email được nhận dạng bởi tên người xử dụng (username) và mật khẩu (password). Mỗi trương mục gắn liền với danh tính, và tên liên hệ được hiển thị để minh chứng nguồn gốc tất cả tin nhắn gửi đến bạn bè và đồng nghiệp. Username cũng được xử dụng bởi các tham dự viên trên những phiên tán gẫu (chat), diễn đàn (forum), và các trang mạng liên kết xã hội trên Internet. Như đã được bàn luận trước đây và trong toàn tài liệu này, nhiều nội dung thông tin qua ngã Internet rất dễ bị giám sát. Thêm vào đó, rất nhiều danh tính mà ta dựa vào để nhận dạng nhân sự trong môi trường ảo, có thể làm giả được. Một kẻ gian đủ kinh nghiệm có thể ngụy tạo địa chỉ điện thư của họ giống hệt như của bạn (xem chương 2.5) để mạo danh bạn gửi thư. Bằng cách lần theo dấu vết của bức thư khi đã được mã hoá, ta có thể tìm ra người nặc danh, nhưng dường như rất ít trong chúng ta được chỉ dạy cách này (xem Phụ Lục B-Điện Thư).

Nguồn gốc của một email không thể tin cậy được nếu không thể xác định người đích thực gửi là ai. Ví dụ, tổ chức Ân Xá Quốc Tế, vì nhận thức vấn đề này, nên tất cả liên lạc qua điện thư của tổ chức này đều kèm theo thông điệp phủ nhận trách nhiệm sau đây:

"...Những giao tiếp qua Internet không an toàn, bởi vậy Ân Xá Quốc Tế không chấp nhận trách nhiệm pháp lý đối với nội dung của thư tín này. Nếu bạn không phải là người được nhận, bạn không được tiết lộ hoặc đặt niềm tin vào thông tin trong bức điện thư này."

Khi tán gẫu (trên MSN hay Skype), bạn đôi khi cho rằng đối phương đích thật là người họ tự nhận, mặc dù chưa có cách nào kiểm chứng được qua giọng nói hay qua thị giác. Cho nên một trương mục được thoả hiệp, hoặc một trương mục nặc danh có thể gây ra nhiều rủi ro đến sự riêng tư và an toàn cho những ai đặt hết niềm tin vào uy tính một trương mục khi trao đổi thông tin.

Những phương pháp điện tử (digital methods) thường không hiệu quả lắm trong việc nhận dạng chân dung kẻ gian trên Internet. Cho nên ta phải dựa vào một phương pháp cũ, nhưng thông dụng, là trao đổi ám hiệu cho nhau trước khi trò chuyện. Những ám hiệu này có thể là một ngôn từ bí mật, hoặc một câu hỏi với câu trả lời mật giành riêng cho các đương sự trước khi cuộc tán gẫu bắt đầu. Và những ám hiệu này được gắn bó với một trương mục hay username với người mà bạn thật sư quen biết. Chỉ có vậy mới phần nào bảo đảm được quyền riêng tư của bạn!

Nhận dạng danh tính trực tuyến tương đối rắc rối hơn khi xử dụng điện thư. Bởi vì người gửi có thể không gửi kèm bất cứ chi tiết gì để minh định danh tính của họ (ví dụ như giấu địa chỉ nơi gửi). Tương tự, bị đọc lén và thay đổi nội dung thư là những đe dọa có thật và thường có xác suất xảy ra rất cao. Những chữ ký điện tử (digital signatures) được tạo ra nhằm để đối phó với những khó khăn trong việc xác định danh tính thật trên môi trường ảo. Các chữ ký này sử dụng phương pháp mã hoá (encryption) để lưu lại hết nội dung của tin nhắn và danh

tính của người gửi, và được bảo an bởi một mật khẩu mạnh. Nếu bản tin nhắn ấy bị đột nhập, hay phá hoại, chữ ký kia sẽ bị làm hỏng, và người nhận sẽ được thông báo rằng tin nhắn kia không còn đáng tin cậy nữa. Cho nên một khi bạn xây dựng được một hệ thống mã hoá công cộng tốt, chữ ký điện tử của bạn sẽ trở thành một giá trị tối đa trong việc xác định danh tính của bạn và người nhận khi trao đổi tin nhắn.[64]

Hướng Đến Sự Ẩn Danh (Towards digital anonymity)

Khuất danh theo đúng nghĩa là điều có đạt được trong thế giới tân tiến của kỹ thuật trao đổi thông tin. Rất nhiều nhà đấu tranh đã và đang bị lộ và bị xét xử vì phát hành bài viết, gửi tin nhắn, hoặc gọi điện thoại cho nhau cho dù đã dùng bí danh. Có lẽ những thông tin trong bản tin ngắn hay những trao đổi qua điện thoại không hé lộ bất kỳ thông tin nào để có thể nhận dạng danh tính họ. Nhưng khi phải xử dụng đến những phương tiện giao tiếp kia, họ vô tình dùng đến các chức năng khác đã được cài sẵn, và các chức năng ấy hé lộ danh tính của họ!

Giải pháp là tìm hiểu một phương tiện cụ thể, một tin nhắn, hay một hành động trên mạng gắn liền với danh tính thật của bạn ra sao để tìm cách ứng phó. Mức độ khuất danh vừa phải có thể đạt được bằng cách ghi danh một địa chỉ email ảo với thật nhiều trương mục khác nhau. Tốt nhất là làm vậy trên máy điện toán công cộng (ví dụ, tại thư viện hay quán Café Internet) khi địa chỉ IP của máy không liên hệ đến bạn. Hãy chọn dịch vụ được biết đến rộng rãi, như Hotmail hay Gmail và tạo một địa chỉ điện thư không dùng tên bạn hoặc bất cứ từ khoá nào mà người ta có thể lần mò theo mà tìm ra danh tính thật của bạn. Phải quyết tâm không nhắc, không kèm theo bất cứ thông tin nào liên quan đến danh tính thật của bạn khi trao đổi tin nhắn nếu không cần, và phải hết sức thận trong khi tiết lộ địa chỉ điện thư ảo với người khác.

Khi lướt các trang mạng, hãy để ý các hành động của bạn bị giám sát ra sao. Nếu bạn muốn giữ trạng thái tương đối khuất danh khi phải lướt những trang mạng "nguy hiểm" thì nên làm chuyện này ở các máy điện toán công cộng. Còn những mạng lưới ẩn danh như Tor hay các proxy servers hỗ trợ ẩn danh[65] thì có thể giúp bạn ngụy trang điểm đến và nguồn gốc các thông tin bạn tìm. Hãy cố gắng không xử dụng cách này khi lướt những trang"nguy hiểm" qua đường kết nối Internet cá nhân tại nhà riêng, cho dù chỉ làm "một lần." Bởi vì một khi đầu mối về bạn đã được hình thành, nó có thể được lưu trữ tại các server của nhà cung cấp dịch vụ Internet.

Khi xử dụng điện thoại di động, đổi máy di động mới và thẻ nhớ mới (SIM) sẽ giúp bạn phần nào ẩn danh. Những thẻ nhớ trả tiền trước (Pre-paid SIM cards) và các máy không đăng ký có thể ẩn danh những người tham gia nói chuyện. Ở một số nước, bạn có thể mua thẻ nhớ và máy không cần phải đăng ký danh tính, hoặc mua với danh tính giả. Nhưng đấy có thể là một việc làm bất hợp pháp về mặt pháp lý. Chúng ta cần biết rằng, nguy cơ bị lộ danh tính sẽ giảm đi nếu bạn hạn chế sử dụng và thường xuyên thay đổi máy di động.

Có thể đã quá trễ để ẩn danh danh tính hiện giờ, dù là trên Internet hay qua các phương tiên truyền thông di động. Hãy tạo nhiều trương mục mới và hãy thay đổi số điện thoại nhằm phần nào giữ được ẩn danh trong trao đổi. Sau đó, hãy lưu tâm đến nơi và cách đăng ký, cũng như nội dung trao đổi qua phương tiện hay dịch vụ này với người khác.

Tóm lại, phải luôn luôn cẩn thận, cảnh giác, và thận trọng đối với những sinh hoạt trên Internet và điện thoại di động, nếu sự ẩn danh dính liền với sự an nguy của bạn!

64 Hãy xem Chương 4, phần Mã Hoá để biết thêm chi tiết.

65 Xem thêm chi tiết ở Chương 2.6.

3.0 NHỮNG BIẾN CHUYỂN VỀ MẶT PHÁP LÝ VỀ SỰ RIÊNG TƯ TRÊN INTERNET VÀ QUYỀN TỰ DO NGÔN LUẬN ẢNH HƯỞNG ĐẾN CÔNG VIỆC VÀ SỰ AN TOÀN CỦA NHỮNG NHÀ ĐẤU TRANH NHÂN QUYỀN TOÀN CẦU[66]

Phần này sẽ bàn đến những yếu tố pháp lý làm giảm đi sự chính đáng và tầm quan trọng trong các công việc mà các nhà bảo vệ nhân quyền (human rights defenders) làm, khi áp dụng vào trong thế giới ảo và kỹ thuật liên hệ. Chúng ta sẽ chú trọng đến các đạo luật có ảnh hưởng trực tiếp và gián tiếp đến an ninh và an toàn của những nhà đấu tranh bảo vệ nhân quyền.

Internet đã và và đang là một môi trường mới để trao đổi thông tin và kiến thức. Đại đa số các chính phủ trên thế giới biết được tiềm năng xã hội và kinh tế của nó. Nhưng trong khi hầu hết các chính phủ đã mạnh dạn dựa vào Internet để phát huy kinh tế, một vài chính phủ lại e dè, sợ sệt vì tầm ảnh ưởng của Internet có thể tác động đến sự ổn định và tồn vong của chính quyền đang cai trị. Bởi vì Internet vượt qua được những biên giới hành chính và địa lý thật dễ dàng và nhanh chóng chưa từng thấy. Nó cung cấp một phương pháp tiên phong mà qua đó tiếng nói của một người có thể đến tai tất cả những ai được kết nối cùng lúc. Không như trên các phương tiện thông tin truyền thống-khi thông tin có thể được trích nguồn, chia phân, biên tập, hay rút ngắn-thông tin trên Internet được chính bạn đọc, người xem tự chọn theo ý muốn. Cho nên người sử dụng không bị ảnh hưởng bởi các tuyên truyền chính trị, tin nóng về các nhân vật công chúng, hay thông tin thể thao tổng hợp, trừ khi người sử dụng muốn vậy. Vì thế bạn đừng ngạc nhiên rằng Internet đã tạo ra nhiều rắc rối ở những quốc gia nào muốn kiểm soát tự do chính trị, xã hội và tôn giáo.

Nguyên tắc hoạt động công khai của Internet là để thi hành theo bản Tuyên Ngôn Quốc Tế Nhân Quyền (Universal Declaration of Human Rights), đặc biệt là quyền tự do ngôn luận, nhóm họp, và lập hội (Điều 19). Trong bản báo cáo gởi đến Cao Ủy Liên Hiệp Quốc về Nhân Quyền ngày 20 tháng Giêng, 1999, Đặc Trách Viên về việc bảo vệ và quảng bá tự do ý kiến và ngôn luận là Abid Husseid nhận xét, "trong khi rất cá biệt vì tầm thẩm thấu và cách ứng dụng, Internet đơn thuần là một phương tiện truyền thông mới. Vì thế, bất cứ hành vi hạn chế hoặc quản lý nào cũng là vi phạm những quyền được đề ra trong bản Tuyên Ngôn Quốc Tế Nhân Quyền, đặc biệt là Điều 19." Ông lý giải thêm rằng:

66
Những dữ kiện và trích dẫn trong chương này đã được mượn từ Sự Riêng Tư Quốc Tế -- Báo Cáo về Sự Riêng Tư và Nhân Quyền năm 2004 – Mối Đe Dọa cho Sự Riêng Tư www.privacyinternational.org và trang nhà của Ký giả không biên giới www.rsf.org

"Về những ảnh hưởng của các công nghệ truyền thông mới, Đặc Trách Viên cho rằng đây là điều rất quan trọng để các kỹ nghệ truyền thông mới này được bảo vệ bởi các tiểu chuẩn quốc tế như những phương tiện truyền thống, và không bị bất cứ một phương pháp nào cản trở nhằm gây tổn hại đến tự do ngôn luận và thông tin; trong trường hợp phải phân vân trước một quyết định, quyết định ấy nên nghiêng về phía tự do ngôn luận và tự do trao đổi thông tin. Riêng về Internet, Đặc Trách Viện xin nhấn mạnh rằng những biểu lộ, trao đổi trên mạng nên được dìu dắt bởi các tiêu chuẩn quốc tế và phải được bảo vệ như bất cứ phương tiện thông tin truyền thống nào."[67]

Sự tăng trưởng của kỹ nghệ truyền thông Internet (Internet Communication Technologies) cũng đã và đang khiến cho nhiều khúc mắc về riêng tư thêm rõ nét. Khi chúng ta chuyển sang thế giới điện tử (digital world) để truyền thông, chúng ta phải đối phó với những mưu lược thu thập, giải mã, phân tích, và quản lý các nhu liệu này bởi những chính phủ và công ty kinh doanh. Nhu liệu này bao gồm luôn những dữ kiện về các trang mạng chúng ta vào, những điện thư, các nơi đến trong những chuyến du lịch, tài chính cá nhân và hồ sơ bệnh án, thành viên của các phong trào chính trị hoặc xã hội, liên hệ với các tổ chức tôn giáo, vân vân. Tất nhiên việc quyền riêng tư bị xâm phạm không có gì là mới lạ, nhưng nên nhớ rằng việc sử dụng những kỹ thuật thời đại và những chức năng giám sát căn bản của chúng đồng nghĩa với nguy cơ quyền riêng tư của ta bị xâm phạm ngày càng gia tăng. Ngay cả Liên Hiệp Quốc cũng đã trở thành nạn nhân của các vấn đề này. Ví dụ tại Hội Nghị Quốc Tế Thượng Đỉnh về Kỹ Thuật Truyền Thông lần thứ nhất (First World Summit on Information Technology) năm 2003, tất cả tham dự viên được trang bị thẻ nhận dạng danh tính. Bên trong các thẻ ấy, một thẻ nhu liệu (chip) phát ra sóng điện từ như của đài radio được cài sẵn. Qua thẻ nhu liệu đó, người ta có thể đã thâu lại tất cả cử chỉ, liên lạc của tất cả tham dự viên trong khi Hội Nghị Thượng Đỉnh diễn ra điều mà các tham dự viên không hề hay biết!

Hai cuộc khủng bố ngày 11 tháng 9 năm 2001 ở Hoa Kỳ đã gây ảnh hưởng xấu lên các đạo luật về quyền riêng tư, vì chúng khiến những quốc gia nào chưa (ngay cả chưa bàn đến) có những biện pháp giám sát thông tin truyền thông cũng phải làm vậy. Tháng Mười năm 2001, Hạ Viện Mỹ phê chuẩn "Đạo Luật để Cung Cấp Những Phương Tiện Cần Thiết nhằm Đánh Chặn và Ngăn Cản Khủng Bố" (Act to Provide Appropriate Tools to Required to Intercept and Obstruct Terrorism, hay còn gọi nôm na là "the USA-Patriot Act). Đạo luật này cho phép Cơ Quan Điều Tra Liên Bang (FBI) lắp đặt một hệ thống giám sát Internet, với tên DCS 1000 (hoặc nôm na là CARNIVORE), ở tất cả trạm cung cấp dịch vụ Internet cấp quốc gia.[68] Năm 2003, Quốc Hội Hoa Kỳ bãi bỏ việc phải xin giấy phép từ toà án (warrants) trước khi các toán điều tra công quyền truy tìm dữ liệu về người xử dụng Internet, hoặc khi họ truy cập các trang mạng để lấy tin. Ref. Sau đó, bộ trưởng tư pháp là ông Aschcroft đã cho phép cơ quan FBI mọi quyền hạn cần thiết để xúc tiến việc giám sát trực tuyến để thu thập thông tin về người sử dụng Internet, dù họ chưa bị tình nghi hoặc không liên quan gì đến các cuộc điều tra công vụ. Lúc đầu, đạo luật nêu trên được dự tính tồn tại tạm thời, nhưng đạo luật đó đã trở thành vĩnh viễn sau những cuộc khủng bố bằng bom ở London, Anh Quốc xảy ra vào tháng Bảy, 2005.

Sau những cuộc tấn công ở Bali năm 2003, chính quyền Úc Đại Lợi đã ban hành nhiều đạo luật để bắt buộc tất cả các nhà cung cấp dịch vụ Internet (ISPs) phải tích

67
Báo cáo của Hội Đồng Nhân Quyền LHQ về vấn đề nhân quyền và tự do ngôn luận January 29, 1999, E/CN. 4/1999/ 64.

68
Tháng Giêng năm 2005 FBI không còn dùng hệ thống Carnivore nữa mà chuyển qua một hệ thống khác.

trữ và giám sát dữ liệu truyền tải qua server của họ, và đồng thời khuyến khích bạn dùng chia sẻ khoá mã hoá (encryption key) cũng như tham gia vào dự án giám sát ECHELON do Hoa Kỳ điều khiển.

Sau đó, chính quyền Úc cũng cho phép các cơ quan công quyền chặn bắt và đọc điện thư, tin nhắn dạng ngắn (SMS, như trên Twitter) và tin nhắn miệng mà không cần giấp phép của toà án, với lý giải rằng những thông tin này thuộc loại "lưu trữ" chứ không phải là loại thông tin sống (real-time)!

Colombia và Zimbabwe và nhiều nước khác đã hợp thức hoá chuyện chặn đầu và nghe lén những trao đổi thông tin tư mà không cần toà án chấp thuận; Ấn Độ đã ban hành Đạo Luật Chống Khủng Bố (Prevention of Terrorism Act) nhằm cho phép cảnh sát quyền truy tìm những trao đổi thông tin trên Internet; Jordan đã sửa lại bộ luật hình sự bao gồm Điều 150 là "xử tù" bất cứ ai "lưu hành, phát ngôn, hay hành động nhằm đả kích đoàn kết quốc gia, kích động xung đột, truyền đạt hận thù, kích động kỳ thị chủng tộc, quảng bá tin đồn ngụy tạo, kích động bạo lực, tham gia và tổ chức các cuộc nhóm hội họp bị luật pháp ngăn cấm."; Quốc Hội Hoà Lan đã đồng ý với dự luật cho phép công tố viên chính phủ đòi hỏi nhu liệu liên quan đến vi phạm giao thông từ các nhà cung cấp dịch vụ truyền thông công cộng và đồng thời đã thông qua sắc lệnh cá biệt cho phép cơ quan công quyền nghe lén những trao đổi giữa luật sư và thân chủ của họ. Còn Singapore thì đã tu bổ Đạo Luật về Lạm Dụng Điện toán (Computer Misuse Act) để cho phép các cơ quan công quyền nước này xúc tiến những biện pháp chống lại những đối tượng mà theo những "thông tin đáng tin cậy" là những kẻ bị tình nghi tấn công (hack) vào những trang mạng chứa đựng thông tin nhạy cảm. Những hình thức pháp lý này là để gia tăng khả năng giám sát và thu thập thông tin cá nhân của chính phủ với chiêu bài chống khủng bố. Điều quan trọng là những đạo luật này bao gồm những cách hoạt động của các cơ quan tình báo mà luật pháp không bao quát, như nghe lén, chặn điện thư, hay là trộm thông tin từ máy điện toán cá nhân. Ví dụ, vào Tháng Ba năm 2006, chính quyền của tổng thống Bush bị phát hiện cài đặt hàng nghìn dụng cụ nghe lén tại những đường điện thoại tư mà không xin phép quốc hội. Lời biện minh cho việc làm này là "quyền Tổng Thống" và sự an ninh cần thiết quan trọng hơn nhu cầu hoạt động trong vòng pháp luật!

Chuyện lạm dụng quyền lực, khi được củng cố bởi các thay đổi pháp lý, thường xảy ra ở các nước không có nền luật pháp công bằng và không có những tổ chức điều phối độc lập. Đa số công dân các nước này biết rõ nhu cầu chống khủng bố, tuy nhiên họ dâng nạp những quyền cá nhân và những quyền riêng tư, bảo mật mà không nghĩ đến hậu quả sâu xa. Xin trích dẫn một nhận xét chung về quyền riêng tư của Hội Đồng Nhân Quyền Liên Hiệp Quốc, tức tổ chức được ủy nhiệm giải thích trách nhiệm cấp quốc gia của những quốc gia ký vào Công Pháp Quốc Tế về Quyền Dân Sự và Chính Trị (International Covenant on Civil and Political Rights):

"Khi tất cả công dân sống trong xã hội, sự bảo vệ quyền riêng tư là điều cần thiết tương đối. Tuy nhiên, các cơ quan công quyền chỉ nên đòi hỏi những thông tin liên quan đến quyền riêng tư khi nào những thông tin ấy nằm trong quyền lợi xã hội, như được hiểu trong bản Công Pháp. [...] Ngay cả khi những can thiệp vào quyền riêng tư phù hợp với Công Pháp, một bộ luật phù hợp phải ghi rõ thật tỉ mỉ phạm vi của bộ luật và những can thiệp cụ thể nào được cho phép. Khi một quyết định được ban hành để can thiệp thì quyết định ấy phải xuất phát từ cơ quan công quyền được bộ luật kia ủy nhiệm, hoặc được ủy nhiệm theo từng trường hợp. [...] Thông tin lấy được từ mỗi lần can thiệp phải được bảo mật. Ngoài những trường hợp này, những sự giám sát, theo dõi và nghe lén qua phương tiện điện tử, điện từ hay những phương pháp giao tế khác phải tuyệt đối bị cấm."[69]

Các chính phủ của Bangladesh, Pakistan, Trung Quốc, Việt Nam và một số quốc gia khác đã và đang cho phép các cơ quan chính phủ quyền xâm phạm mọi thông tin trao đổi trên Internet và thư điện tử. Các công ty cổ phần Internet đa quốc gia đang làm ngơ với những tiêu chuẩn quốc tế về quyền riêng tư. Họ hợp tác với các chính phủ này trong việc cung cấp thông tin cá nhân của những khách hàng lưu ở các server. Chuyện phủ định quyền riêng tư và quyền tự do ngôn luận đang trở thành một xu hướng chung tại nhiều nơi trên toàn cầu. Các phương tiện kỹ thuật đang góp phần vào khả năng giám sát mỗi cá nhân-cho dù ở trên đường phố hay trên Internet. Xin bạn hãy thật thận trọng!

69
Phát biểu từ Hội Đồng Nhân Quyền LHQ số 16. Quyền bảo vệ đời tư (điều luật 17), 08/04/88, paras. 7 and 8.

3.1 KIỂM KHẢO NỘI DUNG TRÊN MẠNG (CENSORSHIP OF ONLINE CONTENT)

XUẤT BẢN TRÊN MẠNG

Những nhà bảo vệ nhân quyền đã và đang có được nhiều lợi điểm từ Internet bởi vì Internet giúp họ dễ dàng liên lạc với cộng đồng toàn cầu. Những bản tin về vi phạm nhân quyền được lưu hành trên mạng và có thể kích động ngay một cuộc lên án từ bên ngoài, đặc biệt bên ngoài một quốc gia hay một vùng. Những vùng mà lúc trước các phương tiện truyền thông quốc tế không thể với tới nay đã khác. Những chính phủ nào muốn bịt miệng các nhà đối kháng tại quê hương họ, nay phải đối đầu với nhiều thử thách có tầm vóc quốc tế. Nhưng, bởi vì khuôn khổ cấp quốc tế không cung cấp chuẩn mực để biện minh hoặc cho phép chuyện kiểm khảo nội dung, nên đại đa số các quốc gia dựa vào luật pháp của nước họ. Thường, Internet được cho là nằm trong phạm vi của các đạo luật quản lý truyền thông. Thế nhưng, điều này rất khó thể biện minh được bởi vì những gì xuất bản trên mạng, không giống như trên phương tiện thông tin truyền thống địa phương, được xuất bản cho khán giả toàn cầu và có thể xuất phát duy nhất tại một quốc gia, nhưng vẫn truy cập được trên toàn cầu. Trong trường hợp của nhóm truyền thông Dow Jones và Gutnick tại Úc Châu, Joseph Gutnick kiện tạp chí trên mạng là Barrons (1) của Canada tội phỉ báng. Toà thượng thẩm Úc đã tái khẳng định quyết định của toà tối cao bang Victoria rằng bài báo trên Barron phải được xem qua các máy điện toán đặt tại bang Victoria mới có giá trị pháp lý! Nói một cách khác, khi suy rộng ra, một xuất bản không chỉ được pháp luật bảo vệ tại nơi được đọc, mà luôn cả nơi biên tập.

Những nhà bảo vệ nhân quyền đã và đang có được nhiều lợi điểm từ Internet bởi vì Internet giúp họ dễ dàng liên lạc với cộng đồng toàn cầu. Những bản tin về vi phạm nhân quyền được lưu hành trên mạng và có thể kích động ngay một cuộc lên án từ bên ngoài, đặc biệt bên ngoài một quốc gia hay một vùng. Những vùng mà lúc trước các phương tiện truyền thông quốc tế không thể với tới nay đã khác. Những chính phủ nào muốn bịt miệng các nhà đối kháng tại quê hương họ, nay phải đối đầu với nhiều thử thách có tầm vóc quốc tế. Nhưng, bởi vì khuôn khổ cấp quốc tế không cung cấp chuẩn mực để biện minh hoặc cho phép chuyện kiểm khảo nội dung, nên đại đa số các quốc gia dựa vào luật pháp của nước họ. Thường, Internet được cho là nằm trong phạm vi của các đạo luật quản lý truyền thông. Thế nhưng, điều này rất khó thể biện minh được bởi vì những gì xuất bản trên mạng, không giống như trên phương tiện thông tin truyền thống địa phương, được xuất bản cho khán giả toàn cầu và có thể xuất phát duy nhất tại một quốc gia, nhưng vẫn truy cập được trên toàn cầu. Trong trường hợp của nhóm truyền thông Dow Jones và

Gutnick[70] tại Úc Châu, Joseph Gutnick kiện tạp chí trên mạng là Barrons (1) của Canada tội phỉ báng. Toà thượng thẩm Úc đã tái khẳng định quyết định của toà tối cao bang Victoria rằng bài báo trên Barron phải được xem qua các máy điện toán đặt tại bang Victoria mới có giá trị pháp lý! Nói một cách khác, khi suy rộng ra, một xuất bản không chỉ được pháp luật bảo vệ tại nơi được đọc, mà luôn cả nơi biên tập.

Nhiều quốc gia hiện nay đã ban hành nhiều luật cụ thể để hoạch định tính hợp pháp của những thông tin được phát hành trên mạng. Điển hình, luật pháp Iran "…cấm và cho rằng phạm pháp nếu phát hành trên Internet bất kể tài liệu nào trái ngược hay lăng mạ giáo pháp Hồi Giáo, giá trị cách mạng, tư tưởng của Imam Khomeini, Hiến Pháp, hoặc gây tổn hại đến đoàn kết quốc gia, cấy sự mất lòng tin vào khả năng lãnh đạo của giới cầm quyền, tuyên truyền tốt cho những nhóm bất hợp pháp, khuyến khích những thói xấu như hút thuốc lá, hay lăng mạ viên chức chính phủ."

Thái Lan và Tây Ban Nha nghiêm cấm tất cả hành vi phạm thượng đến hoàng tộc, trong khi tại Thổ Nhĩ Kỳ thì cấm tất cả nội dung có mục đích lăng mạ chủ nghĩa quốc gia, nói xấu cha đẻ của nước này thời hiện đại là Kamal Attaturk, hoặc đề cập đến cuộc thảm sát chủng tộc Armenia.

Trong khi đó, Đức và Pháp tích cực theo đuổi và dẹp bỏ (hoặc kiểm khảo nội dung) bất cứ bài viết, tài liệu nào phủ định cuộc diệt chủng người Do Thái (Holocaust) hoặc trợ giúp tìm kiếm những kỷ vật thời Đức Quốc Xã trong Đệ Nhị Thế Chiến.

Tại Ai Cập, trong những đạo luật về tình trạng khẩn trương quốc gia (Emergency Laws) có đoạn nghiêm cấm "kêu gọi bằng truyền miệng, viết, hoặc bất cứ cách nào khác nhằm cản trở hiến pháp hoặc luật pháp; tàng trữ tài liệu kêu gọi các hành động vừa nêu, bóp méo tin tức hoặc những tuyên bố của chính phủ, phát tán và khuyến khích tin đồn nhằm phá rối an ninh trật tự, hoặc làm tổn lại đến công chúng và lợi ích chung."

Vào năm 2002, người sử dụng Internet tại Ai Cập được cảnh báo phải tránh xa những vấn đề cấm kỵ (như quan hệ giữa người Thiên Chúa Giáo và người Hồi Giáo, xuất bản ý tưởng khủng bố, vi phạm nhân quyền, chỉ trích tổng thống, gia đình tổng thống và quân đội, hay quảng bá phiên bản mới của đạo Hồi Giáo) và được mách bảo rằng việc bày tỏ ý kiến công khai không được hoan nghênh. Từ đó, vài nhà dân báo (bloggers) đã bị tù đày chỉ vì bày tỏ ý kiến, tư duy trên mạng.

Các trường hợp pháp lý khác đã tác động đến việc truy cập thông tin điện tử bao gồm:

70
(2002) 210 CLR 575.

- Chính Án về Phát Sóng Úc Châu (dịch vụ mạng) 1999 đã tạo và trao quyền kiểm soát nội dung Internet cho Ủy Quyền Truyền Thông và Thông Tin Úc Châu (Australian Communications and Media Authority). Nội dung trên các website đăng bởi các server tại Úc hoặc tại nước ngoài được phân loại bởi Phòng Phân Loại Phim và Văn Phẩm (Office of File and Literature Classification). Tất cả nội dung trên trang web nào bị liệt kê vào loại "cấm" có thể bị lệnh gở xuống nếu ở Úc, còn nếu ở nước ngoài thì sẽ bị cho vào danh sách sàng lọc (filtering).
- Bên Hoa Lục, Điều Khoản về Quản Lý Thông Tin và Dịch Vụ Internet (Chinese Provisions fo the Administration of Internet News Information Services) định nghĩa nội dung của những thông tin trên mạng là "...tin tức, phúc trình, và bình luận thời cuộc, chính trị, kinh tế, quân sự, ngoại giao, ngụy kịch quốc gia, và những chuyện thời sự khác..."Ref. Điều 5 trong Điều Khoản trên bắt buộc bất cứ website hoặc bản thông cáo này muốn phát hành bất cứ nội dung gì không có trên các website chính thức của chính phủ phải được duyệt xét và chấp thuận bởi Phòng Thông Tin của Hội Đồng Nhà Nước.
- Tại Việt Nam, nghị định Văn Hoá và Thông Tin Truyền Thông (Decree on Cultural and Information Activies) sẽ phạt 30 triệu đồng Việt Nam (khoảng 1 500 USD) đối với những ai phát tán tư tưởng "phản động" bao gồm cả thố lộ bí mật (của đảng, nhà nước, kinh tế, và quân sự), những ai không nhìn nhận thành tích cách mạng, và những ai không nạp những bài viết để được duyệt xét trước khi lưu hành.
- Ân Độ bắt buộc những công ty cung cấp dịch vụ Internet (ISP) được phép hoạt động tại nước này phải "bảo đảm không được lưu hành bất cứ điều gì có nội dung chống đối, khiêu dâm, chưa được chính phủ ủy thác, hoặc bất cứ nội dung khác, cũng như tin nhắn hay những thông tin truyền thông vi phạm bản quyền, quyền sở hữu trí tuệ và các luật về mạng ảo của quốc tế lẫn quốc nội, bằng bất cứ hình thức nào hoặc không phù hợp với luật pháp Ấn Độ, trên mạng lưới của mình, và ISP phải có biện pháp ngăn chặn những nội dung nêu trên.."

3.2 SÀNG LỌC TRANG WEB (WEBSITE FILTERING)

Các quốc gia trên thế giới đang áp dụng kỹ thuật sàng lọc Internet. Việc này cho phép họ ngăn chặn nhiều trang web hoặc một trang web cụ thể trong phạm vi lãnh thổ của mình. Trong thực tế thì việc này đồng nghĩa với kiểm khảo nội dung đối với Internet. Chuyện sàng lọc này xảy ra hầu hết tại mỗi quốc gia, và thường đối tượng là những thông tin được phân loại trước. Đối tượng thông tin bị phân loại trên Internet để được kiểm khảo bao gồm thông tin về: tôn giáo, chính trị, khiêu dâm, tình dục vị thành niên, nhân quyền, v.v.

Hai phương pháp căn bản để kiểm khảo thông tin quen thuộc là: (1) Tất cả những gì không được phép lưu hành rõ ràng là bị cấm; và (2) Tất cả những gì không bị cấm được phép lưu hành. Hai cách này thường được đề cập là "sổ đen" và "sổ trắng" và cách sau cùng là cách nổi trội được dùng ở các cở sở hạ tầng Internet cấp quốc gia. Cuba, Miến Điện và Việt Nam khởi đầu ngăn chặn toàn bộ mạng Internet, và chỉ cho phép công dân truy cập một vài trang web.

Sự khó khăn khi duy trì "sổ đen" và "sổ trắng" thường khiến công tác này được giao phó lại cho nhà cung cấp dịch vụ Internet (ISP), và ISP phải chịu trách nhiệm đối với những nội dung bất hợp pháp mà công dân của một nước truy cập được tại nước đó. Trong hoàn cảnh này, các công ty kinh doanh phần mềm sàng lọc nhân cơ hội thủ lợi. WebSense, Content Watch và Fortinet chỉ là một vài ví dụ các công ty sản xuất phần mềm sàng lọc nội dung Internet được sử dụng trên các mạng lưới của học đường, công ty thương mại, và của quốc gia. SmartFilter, một sản phẩm của Secure Computing, có thể tự phân loại các đường link URL theo tiết mục như "Phá Thai, Vật Liệu Người Lớn, Giáo Dục, Tin Tức và Truyền Thông, Bất Hợp Pháp, hoặc Nghi Vấn" và v.v. để người sử dụng có thể gửi vào các URL mà họ truy cập theo từng tiết mục. Sản phẩm này được nhiều chính quyền và các nhà ISP mua để thực hiện chính sách kiểm khảo nội dung Internet.

Các quốc gia thường mở rộng những quy định về truyền thông hiện hay để quản lý ấn phẩm trên Internet. Bất kỳ ai muốn tạo một trang dân báo (blog) tại một nơi nào đấy có thể, ví dụ, phải ghi danh như một công ty truyền thông theo các luật pháp hiện hành, dù chỉ quản lý loại truyền thông phát sóng và truyền thông in, cũng được áp dụng đối với môi trường blog. Trên bề mặt thì có lẽ cách này đơn giản hóa những pháp lý cần thiết để quản lý những ấn phẩm trên mạng, nhưng blog thường chỉ nêu lên ý kiến của một người, không qua quy trình biên tập và thường được xuất bản bất chấp chuyện server của các website đặt tại nơi nào (tức là luật quản lý nội dung tại một quốc gia) và những điều nhạy cảm

tác động đến người đọc. Cho nên dân báo (blog) không tuân theo mô hình truyền thông và báo chí truyền thống.

Nhiều quốc gia hiện nay đang tiến trước các thoả thuận quốc tế về tự do thông tin và ngôn luận, và tự quyết định nội dung nào công dân họ được phép truy cập. Việc này thường được xúc tiến với chiêu bài duy trì ổn định quốc gia, bảo vệ văn hoá, an ninh, và luật pháp. Những cách giải thích này đã và đang được sử dụng rộng rãi để cản ngăn các trang mạng dấn thân vào các vấn đề tự do ngôn luận, tự do chính trị, độc lập thông tin, và nhân quyền. Ví dụ, ngày 31 tháng Chạp năm 2002, chính quyền Iran ban hành "Sắc Lệnh Hiến Pháp của Hội Đồng Đương Quyền về việc Quy Định các Trang Websites bị Cấm"(Decree on the Consitution of the Committee in Charge of Determination of Unautorized Websites) khẳng định rằng, "Để bảo vệ văn hoá đạo Hồi và văn hóa quốc gia, một hội đồng gồm đại diện các bộ Thông Tin, Văn Hóa và Hướng Dẫn Hồi Giáo, Phát Sóng Cộng Hòa Hồi Giáo Iran, Hội Đồng Văn Hoá Cách Mạng, và Tổ Chức Tuyền Truyền Hồi Giáo được thành lập bởi bộ Thông Tin để thẩm định và báo cáo với bộ Kỷ Thuật Thông Tin Truyền Thông (Ministry of Information Communications Technology). Những trang web bị báo cáo đến bộ này đều được cho vào danh sách kiểm duyệt. Tại Singapore các trang web trên Internet bị quản lý và được cấp phép hoạt động bởi Ủy Quyền Phát Sóng Singapore (Singapore Broadcasting Authority) và phải tuân thủ theo các quy định gắt gao của cơ quan này. Những thông tin với nội dung "đồi trụy" từ khiêu dâm đến "những lãnh vực tác hại đến đạo đức công chúng, phồn thịnh chính trị và tôn giáo" phải được quản lý.

Thông thường thì ý định ngăn chặn các trang web từ một chính phủ không được công bố, và danh sách của các trang web bị chặn cũng không được công bố. Cho nên, các trang mạng Internet bị chặn thường thì không vì vi phạm một điều luật cụ thể, nhưng bị chặn bởi vì các giới chức cho rằng việc truy cập chúng sẽ tác động xấu đến những chính sách mà chính phủ muốn thúc đẩy. Một ví dụ cổ điển là tại Trung Quốc, nơi mà các ISP bị bắt buộc phải đồng ý "không truyền tải những thông tin có thể làm tổn hại đến những truyền thông tốt đẹp và đạo đức nước Hoa. 1". Kết quả, Trung Quốc đã triển khai được một hệ thống sàng lọc quy mô và phức tạp nhất thế giới, với hàng nghìn nhân viên ngày đêm rà soát và liệt kê các trang web vào "sổ đen" hay "sổ trắng."

Thông thường, việc một chính phủ kiểm khảo các trang web không được sự đồng thuận đa số từ công chúng, và có quy trình kiến nghị để gở bỏ các trang web khỏi danh sách bị chặn. Hậu quả của việc này là người dân tìm các kỹ thuật leo rào để thoát khỏi hệ thống sàng lọc do chính quyền thành lập. Quy trình này thường là yêu cầu máy điện toán tại một quốc gia khác (không có sự kiểm soát Internet) vào trang web mong muốn để lấy và truyền tải lại nội

dung theo yêu cầu. Từ khía cạnh kỹ thuật, người dùng chỉ truy cập thông tin từ máy tiếp vận chứ không phải từ trang web bị ngăn cấm.

Theo ông John Gilmore, người thành lập ra Electronic Frontier Foundation, thì "Hệ thống Internet xem đường vào các trang web bị kiểm khảo như bị hư hại, và tự tìm đường khác để vòng vào."

Tóm lại, sàng lọc Internet không những cản trở công việc của những nhà bảo nhân quyền mà đôi khi còn ngăn cản tin tức về vi phạm nhân quyền lan đến cộng đồng địa phương bạn và cộng đồng quốc tế. Các chính phủ có thể ngăn chặn truy cập đến một trang web tại nước họ, và vì vậy làm tê liệt khả năng truyền tải và cập nhập thông tin của những tổ chức đấu tranh. Bằng cách khác, các chính phủ cũng có thể ngăn cản công dân truy cập những trang web nhất định, và vì vậy hạn chế việc truy cập thông tin, tin tức, và khả năng bày tỏ ý kiến một cách tự do của những nhà bảo vệ nhân quyền.

3.3 SỰ GIAM SAT TRUYỀN THONG (COMMUNICATIONS SURVEILLANCE)

Sự giám sát truyền thông đã bắt đầu hiện diện khi thời đại điện tin chào đời. Nói chung, chúng ta có thể chấp nhận việc cảnh sát và các cơ quan tình báo được quyền nghe lén ai đó để bảo đảm quyền lợi và an ninh công cộng. Nhưng, vì nhiều kẻ gian đã bị bắt bởi vì bị phát hiện nghe lén điện thoại hoặc đột nhập để xem hồ sơ những cú gọi. Cho nên, quyền nêu trên phải được bảo đảm không được ủy nhiệm một cách dễ dàng và phải thông qua một quá trình pháp lý, hoặc một quá trình tương đương trước khi các hành động trên được ủy thác. Nếu không, người người sẽ đứng lên và la ó một khi họ biết rằng mỗi cuộc nói chuyện qua điện thoại của họ từ trước đến nay đều bị ghi âm và lưu giữ! Vì vậy, chúng ta đừng ngạc nhiên hoặc cảm thấy lạnh người khi biết rằng rất nhiều quốc gia đã ra tay một cách nhanh chóng và thầm lặng để ban hành những đạo luật để hợp pháp hoá sự giám sát và lưu trữ những giao tiếp trên Internet.

> *Ví dụ, vào năm 1996, Digicom, công ty cung cấp dịch vụ điện tử lớn nhất tại Pakistan, yêu cầu khách hàng ký bản giao kết nhằm áp đặt những hạn chế khi xử dụng Internet. Dưới các điều khoản của bản giao kết này, người xử dụng bị cấm không được mã hoá dữ liệu và phải chấp nhận những trao đổi, thông tin điện tử của họ được giám thị bởi các cơ quan nhà nước. Thêm vào đó, người xử dụng Internet phải cung cấp cho Digicon bản sao căn cước của thẻ chứng minh nhân dân, trong khi công dân ngoại quốc phải cung cấp bản sao của hộ chiếu. Những ai thiếu sót sẽ bị cắt đường nối kết, và mất dịch vụ Internet*[71].

Theo lời đồn, các cuộc tấn công khủng bố 11 tháng Chín (Hoà Kỳ) đã được chuẩn bị phần lớn qua Internet. Giờ đây, các nhà chức trách trên toàn thế giới, với lý do an ninh, đã tự ý nới rộng những cơ sở pháp lý nhằm giám sát thêm những thông tin lưu chuyển trên Internet trong phạm vi lãnh thổ của nước họ. Như đã nói, những hệ thống giám sát Internet đã và đang được thiết lập ở cấp quốc gia. Ví dụ, Sở An Ninh Liên Bang của Nga Sô đã đặt một hệ thống hộp đen (black box) để giám sát tại mỗi ISP (dự án này được biết với tên SORM2). Thêm vào đấy, họ ép buộc các ISP phải chi trả chi phí cho hệ thống giám sát này. Tương tự, dự án "Khiên Vàng" (Golden Shield) của Trung Quốc được công bố năm 2001. Thay vì xử dụng một hệ thống Internet cấp quốc gia với nhiều tường lửa được lắp đặt, khác biệt với mạng lưới

71
Báo Cáo Kiểm Duyệt Internet - Uỷ Ban Bảo Vệ Ký Giả Của Canada.

toàn cầu, Trung Cộng đang chuẩn bị xây dựng một hệ thống giám sát tình báo dính liền vào hệ thống này để tiện cho nước này "thấy," "nghe" và "suy đoán".[71] Và một hệ thống giám sát toàn cầu được biết đến với tên ECHELON[72] đã được các nước Hoa Kỳ, Anh Quốc, Úc Đại Lợi, Tân Tây Lan, và sau cùng Đức đồng xúc tiến sau khi cuộc Chiến Tranh Lạnh kết thúc.

Những trao đổi qua Internet không những bị giám sát mà còn bị lưu lại, thường là trong một thời gian dài. Năm 2005, liên minh Châu Âu (EU), dưới áp lực từ ban hội đồng đã đệ trình một đao luật bắt buộc tất cả các nước thành viên phải lưu trữ dữ liệu Internet ít nhất là hai năm[100], mặc dầu thành viên có quyền chọn lưu trữ lâu hơn.

Điều 8 trong Công Ước Âu Châu về Nhân Quyền bảo đảm quyền được tôn trọng đối với đời sống riêng tư và đời sống gia đình. Điều này quy định cụ thể rằng các cơ quan công quyền có thể can thiệp vào các quyền này chỉ ở các trường hợp rất hạn hẹp đã được xác định. Cụ thể, bất cứ sự can thiệp nào vào quyền này phải hợp pháp và chỉ được thi hành để chống tội ác và bảo đảm quyền lợi an ninh quốc gia.

Sự giám sát và lưu trữ các dữ liệu riêng tư một cách tùy tiện và vô tội, bất kể lợi hại là một mối đe doạ đến công việc và sự an ninh của những nhà nhân quyền. Những thông tin mà họ trao đổi cũng có thể bị kẻ gian ngụy tạo, hoặc nặc danh nhằm phá hủy uy tín của họ, hay kết tội hình sự đối với họ. Cho nên, chuyện các công ty Internet đang hợp tác với những chính quyền độc tài là đang tiếp tay hủy hoại quyền riêng tư của các công dân đang bị các chính quyền đó cai trị.

Tóm lại, quốc gia nào đã và đang xúc tiến các biện pháp giám sát công dân tại nước mình trên Internet, với quy mô lớn, nên thành lập một cơ quan độc lập và ủy quyền cơ quan đó giám thị việc thu thập, lưu trữ và xử dụng những dữ liệu cá nhân như nêu trên. Những đạo luật gắt gao phải được ra đời để chống sự lạm dụng nhằm bảo vệ quyền riêng tư và danh tính của chúng ta!

71
G. Walton, "Khiên Vàng Của Trung Quốc", http://serveur.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html.

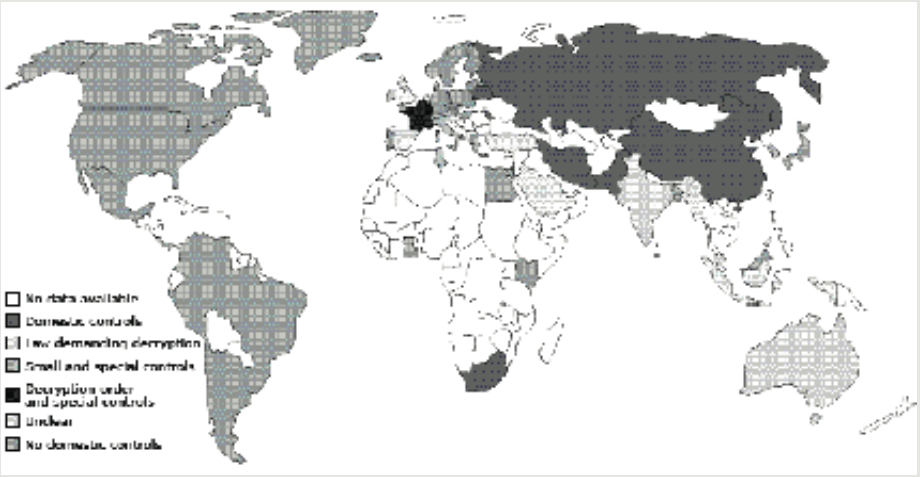
72
Trong một báo cáo năm 2003 một nhân viên của và một bộ trưởng Anh Quốc cho biết tình báo Hoa Kỳ và Anh Quốc dùng Elchelon để nghe lén liên lạc riêng tư của Tổng Thư Ký LHQ Kofi Annan.

3.4 KHOA MÃ HOA (CRYPTOLOGY)

Vì những chuyện theo dõi và giám sát trên Internet, như đã được mô tả ở phần trước, những người sử dụng internet rất cần có những phương cách để giành lại sự riêng tư cho mình khi truy cập vào Internet. Bởi vì nếu thông tin cứ tùy tiện được thu thập và lưu trữ bất kể nội dung và mục đích, thì người sử dụng có quyền hành động để bảo đảm sự riêng tư cho mình, và đương nhiên tránh khỏi nguy cơ bị những đôi mắt soi mói, hoặc bị giả mạo.

Bởi vì tính hữu dụng quan trọng trong việc mã hoá dữ liệu thông tin và truyền thông nhằm bảo mật, nên các chính phủ và tổ chức dân sự đã sử dụng nó một cách rất nhanh chóng. Sự ra đời của các chìa khoá mã hoá công cộng và vài dụng cụ mã hoá dễ dùng khác đã khiến việc mã hoá để bảo mật nằm trong tầm tay của mọi người. Công dụng của nó trong việc hóa giải thành công những khả năng giám sát của các cơ quan công quyền đã sớm được nhìn nhận. Từ đấy, một vài chính phủ đã phải chạy ngược chạy xuôi để hạn chế việc xử dụng khóa mã hóa công cộng, hoặc cấm luôn hoàn toàn.

Bản "Khảo Sát Chính Sách Mã Hoá Quốc Tế" do Electronic Privacy Information Centre (Trung Tâm Bảo Vệ Quyền Riêng Tư Thông Tin Điện Tử) năm 1999 bắt đầu với lời khẳng định này:" Hầu hết các quốc gia trên thế giới ngày nay không có biện pháp quản lý việc xử dụng phương pháp mã hóa. Tại đại đa số quốc gia, các phương tiện mã hóa có thể được tự do xử dụng, sản xuất, và rao bán không giới hạn. Đây là sự thật tại các quốc gia công nghiệp và những quốc gia đang phát triển."



Mười năm sau, chúng ta chứng kiến những biến chuyển pháp lý một cách quyết liệt nhằm quản lý viêc mã hóa nêu trên-như được Bert Jaap Koops thu thập trong bản Khảo Sát về Luật Mã Hoá (Crypto Law Survey)[73] của anh. Hầu như mọi quốc gia trên thế giới hôm nay đều quản lý sự mã hóa thông tin, buôn bán sản phẩm để mã hóa, nhập khẩu và xuất khẩu và đôi khi luôn cả chuyện chỉ dạy cách xử dụng các sản dùng để mã hóa. Điển hình là Kazakhstan, một quốc

73
http://rechten.uvt.nl/koops/cryptolaw/cls- sum.htm

gia miền núi thuộc miền trung bắc Á Châu, đã ban hành một sắc lệnh về việc này.

Mức độ bảo mật do mã hóa khiến việc này được phân loại là vũ khí quân dụng và bị liệt kê vào thoả ước Wassenaar[74]. Hoa Kỳ ban đầu cũng đã yêu cầu một hế thống chìa khoá mã hóa toàn cầu, và sau đó nhiều nước khác cũng đã làm theo. Bởi vì khi ấy, các chính phủ sợ sẽ mất khả năng thu thập tin tình báo, nên giới hạn việc mã hóa thông tin trừ khi họ có khả năng giải mã. Dần dần, các nhà đấu tranh cho quyền riêng tư đã thắng cuộc chiến chống lại việc giới hạn dùng phương pháp mã hóa nhằm bảo mật thông tin cá nhân.

Tiếc thay, một vài quốc gia hiện nay vẫn còn trực tiếp cấm việc xử dụng những phương tiện mã hóa, hoặc gián tiếp ngăn cấm bằng cách truy tố người sử dụng. Ví dụ, Trung Quốc, chỉ cho phép xử dụng những sản phẩm mã hóa được thiết kế và cấp phép tại nước này. Điều này khiến ứng dụng điện thoại Skype trên Internet được ưa chuộng và phổ biến, bởi vì nó mã hóa thông tin trao đổi giữa người xử dụng, nên đã được tái chế và tiếp thị với tên Tomskype ở nước này.

Sự Đàn Áp Đối Với Những Nhà Bảo Vệ Nhân Quyền

Những chế độ áp chế độc tài đã và đang truy bức một cách mãnh liệt đối với những nhà nhân quyền khi họ tỏ ý chỉ trích chính phủ và viên chức chính phủ. Dưới đây là bản danh sách, thu thập từ Front Line và các nguồn khác, về những nhà bảo vệ nhân quyền bị đàn áp và tù đày vì những hoạt động của họ trên mạng:

Mohammad Reza Nasab Abdullahi

Iran-Ngày 23 tháng Hai, 2005, sau phiên toà xử kín không có luật sư đại diên, Mohmammad Reza Nasab Abdullahi bị tuyên án sáu tháng tù giam vì, theo cáo trạng, nhục mạ Nhà Lãnh Đạo Tối Cao (Supreme Leader) của nước này và phát tán tài liệu tuyên truyền chống chính phủ. Ông bị tống giam năm ngày sau đó. Nhưng trên thực tế, Abdullahi là một sinh viên đại học, một nhà bảo vệ nhân quyền, một tổng biên tập của nhật báo sinh viên, và là chủ nhân của mạng dân báo Webnegar ("Nhà Văn Mạng") ở thành phồ Kerman thuộc miền trung Iran. Anh bị tống giam thật ra vì đăng bài viết có tưa Tôi Muôn Biết" trên mạng dân báo của anh để gợi chuyện với Nhà Lãnh Đạo Tối Cao Ayatollah Khamenei và chỉ trích chính quyền đàn áp "quyền tư do, dân sự, và cá nhân."

Arash Sigarchi

Iran –Bởi vì những sinh hoạt như một nhà dân báo và nhà báo, Arash Sigarchi đã bị tống giam từ ngày 26 tháng Giêng năm 2006, chỉ bốn ngày sau khi bị tuyên án ba năm tù vì "Nhục Mạ Nhà Lãnh Đạo Tối Cao"và "tuyên truyền chống chính quyền." Trước đó ông cũng đã bị bắt và bị giam hai tháng vào đầu năm 2005 và bị Toàn Án Cách Mạng Iran tuyên án 14 năm tù giam với tội danh trên vào tháng Hai, 2005. Sau khi trả 1 tỉ rials (tiền Iran, bằng khoảng 95 nghìn đồng Euro) tiền tại ngoại, ông được thả ngày 17 tháng Ba, 2005. Trước đó nữa, ông bị

74
Hiệp ước Wassenaar là một hiệp ước giữa 33 quốc gia phát triển để giới hạng xuất cảng vũ khí và kỹ thuật có thể được sử dụng hai chiều đến một số quốc gia bị xem đoe doạ thế giới.

bắt ngày 27 tháng Tám, 2004 và bị giam vài ngày bởi vì đăng một bài báo với hình ảnh, về cuộc xuống đường của các thân nhân của những tù nhân bị hành quyết năm 1989. Từ đấy, ông thường xuyên bị công an quấy rầy, trù dập. Là cựu biên tập viên của nhật báo Gylan Emroz, Sigarchi sở hữu một trang dân báo chính trị và văn hoá (www.sigarchi.com/blog) được ba năm, khoảng thời gian mà anh thường chỉ trích chính quyền. Vì vậy các cơ quan thẩm quyền đã cố sức ngăn cản độc giả truy cập vào trang dân báo của, và vì vậy trang dân báo của anh gần như không thể vào được trong phạm vi Iran.

Al-Mansuri

Li Băng –Al-Mansuri xuất bản bài báo cuối cùng của anh ta ngày 10 tháng Giêng, 2005. Bài báo ấy là một bản phân tích cuộc tranh luận giữa hai viên chức chính phủ, một người là Shukri Ghamin, nổi tiếng là một nhà cải cách, và người kia là Ahmad Ibrahim, nổi tiếng là một nhà bảo thủ. Al-Mansuri bày tỏ hy vọng rằng al-Saddafi, nhà lãnh đạo độc tài Li Băng, sẽ ủng hộ Shukri Ghamin. Ngày 19 tháng Mười, 2005, toà án thành phố Tripoli, Li Băng tuyên án Al-mansouri một năm rưỡi tù giam vì sở hữu vũ khí trái phép!

Ibrahim Lutfy, Mohamed Zaki, Ahmad Didi và Fathimath Nisreen Maldives-Tháng Giêng, 2002 Ibrahim Lutfy, cùng với Mohamed Zaki, Ahmad Didi và Fathimath Nisreen, phụ tá của Lutfy bị kết tội "phỉ báng" và "chủ ý lật đổ chính quyền" sau khi họ phát hành đặc san Sandaanu, phát tán qua điện thư, với hai đề tài chính là vi phạm nhân quyền và tham nhũng. Lutfy, Zaki and Didi bị tuyên án tù chung thân ngày 7 tháng 7, 2002. Nisreen, khi phiên xử diễn ra mới 22 tuổi, nhận bản án 5 năm tù giam. Ông được thả tháng Năm, 2005 sau 3 năm tù giam.

Ibrahim Lutfy thì trong lúc lãnh án, ông lén chuyền tay một ám hiệu đến vị công an viên canh gác khi Ông ở Sri Lanka để mổ mắt. Cũng nên nói thêm rằng Ông đã phải chịu nhiều khổ sở vì chứng sưng mắt kinh niên, và chứng bệnh này đã trở nên trầm trọng bởi điều kiện bần cùng của lao tù. Sau nhiều lần từ chối không cho Ông đi điều trị, các cơ quan thẩm quyền cuối cùng cho phép ông đi Shi Lanka để điều trị. Sau khi vượt thoát thành công, Ông đã phải lánh nạn tại Shri Lanka, với sự giúp đở của bạn bè. Sau đó UNHCR giúp đở ông đi tị nạn chính trị tại Thụy Sĩ, nơi mà ông hiện nay vẫn sống. Còn người công an viên được chỉ định canh gác Ông ở Sri Lanka thì đã bị tống giam sau khi trở về Maldives.

Còn ông Didi thì đã phải nhập viện tại thành phố Male vào tháng Hai, 2004 và sau đó bị quản chế tại gia. Ông bị các hội chứng tim rất nghiêm trọng và có lẽ cần phải mổ. Zaki thì sức khỏe cũng đã suy giảm trầm trọng khi bị tù, cũng được quản chế tại gia. Cả hai đã được giảm án từ chung thân xuống còn 15 năm tù giam năm 2003.

Bác Sĩ Nguyễn Đan Quế

Vietnam – Bác sĩ Nguyễn Đan Quế, 61 tuổi, một nhà đấu tranh cho quyền tự do ngôn luận, được thả năm 1998 sau 20 năm tù, và đã bị bắt giam một lần nữa tại tư gia ở Sài Gòn ngày 17 tháng Ba năm 2003. Các viên chức chính quyền không hề cung cấp lý do bắt ông, nhưng có thể suy luận rằng có liên quan đến việc ông đăng một bản tuyên bố trên mạng nhằm chỉ trích rằng ở Việt Nam thiếu tự do báo chí. Thật ra, ông chỉ đáp lại những nhận định mà một phát ngôn nhân bộ ngoại giao công bố rằng quyền tự do thông tin ở Việt Nam đã được bảo đảm. Mặc dầu ông đang phải chống chỏi với bệnh cao huyết áp và khối u bao tử, nhưng gia đình ông không được phép thăm ông hoặc gửi các loại thuốc chữa bệnh mà ông cần, khi ông chưa được toà án xét xử gì cả. Ngày 22 tháng Chín năm 2003, mười hai khôi nguyên của giải Nô Ben Hoà Bình đã viết thư đến Tổng Bí Thư Đảng Cộng Sản Việt Nam để nói lên sự quan tâm đối với sức khoẻ của bác sĩ Quế và đồng thời yêu cầu ông được chăm sóc y tế đúng mức và gia đình ông được thăm nuôi ông trong thời gian chờ đợi được phóng thích.

Nguyễn Vũ Bình

Vietnam – Cựu nhà báo này bị tuyên án bảy năm tù giam ngay 31 tháng Mười Hai năm 2003 bởi phiên xử ngắn hơn ba giờ đồng hồ. Toà Án Nhân Dân Hà Nội cũng tuyên án ông 3 năm quản chế tại gia sau khi mãn hạn tù giam. Các nguồn tin thân cận với những cơ quan công quyền Việt Nam nói rằng cáo trạng chính trong vụ xử nêu trên có liên quan đến việc anh Bình gửi một bức thư ngày 19 tháng 7, 2002 đến Ủy Ban bảo Vệ Nhân Quyền của Quốc Hội Hoa Kỳ để chỉ trích những vi phạm nhân quyền tại Việt Nam. Ông bị kết tội vì liên hệ đến những phần tử "phản động"như Lê Chí Quang và Phạm Hồng Sơn, cả hai cũng đang bị giam vào lúc đó. Hơn thế nữa, ông bị quy tội vì đã nhận 4,5 triệu đồng Việt Nam (khoảng 230 đồng Euros) "từ một tổ chức phản động hải ngoại", tham gia vào một tổ chức chống tham nhũng, và kêu gọi các cơ quan công quyền Việt Nam thành lập một đảng tự do dân chủ. Anh Bình cũng bị quy chụp tội đăng tải những thông điệp "phản động" trên Internet, đặc biệt là bài văn với tựa, " Nhìn Lại Những Thoả Ước Biên Giới Việt-Trung"mà trong đó ông chỉ trích hoả ước biên giới năm 1999 giữa hai nước.

Zouhair Yahyaoui

Tunisia – Zouhair Yahyaoui, nhà sáng lập và chủ biên của trang mạng tin tức TUNeZine, được phóng thích theo điều kiện ngày 18 tháng Mười Một năm 2003 sau khi thụ án hơn nửa bản án 28 tháng tù giam. Ông bị bắt tại một quán Internet công cộng ở thủ đô Tunis, ngày 4 tháng Sáu năm 2002 khi đang dùng trang web TUNeZine để phát tán tín tức về tình hình cuộc chiến đòi dân chủ và tự do tại Tunisia. Với bí danh "Ettounsi" (tức "Người Tunisia" trong tiếng Arab), ông viết nhiều phê bình và luận văn và là người đầu tiên phát hành một lá thư tay gửi đến Tổng Thống Ben Ali để chỉ trích hệ thống tư pháp của Tunisia thiếu công minh.

TUNeZine bị các cơ quan thẩm quyền chính phủ kiểm duyệt nội dung ngay từ ban đầu. Nhưng, những người hâm mộ được nhận một bản danh sách proxy hàng tuần để truy cập. Ngày 10 tháng Bảy năm 2002, ông Yahyaoui bị tuyên án mười hai tháng tù giam vì "đăng tải tin sai sự thật (theo điều 306-3 của bộ luật hình sự nước này) và 16 tháng tù giam vì tội "trộm bằng cách gian lận đường truyền tải thông tin"(điều 84 trong bộ luật thông tin), nghĩa là ông dùng đường nối kết Internet ở quán publinet nơi ông làm việc. Ông bị giam trong điều kiện rất khắc nghiệt và đã hai lần tuyệt thực đầu năm 2003 để kháng án. Ông được phóng thích hơn một năm rưỡi sau đó, vào tháng Mười Một năm 2003, và qua đời vì nguyên nhân tự nhiên vào tháng Ba năm 2005, hưởng dương 36 tuổi.

Mohammed Abbou

Tunisia - Mohammed Abbou là một luật sư nhân quyền nổi tiếng, hiện đang thụ án ba năm rưỡi tù giam vì phát hành những công bố trên Internet để kêu gọi sự quan tâm đến những vi phạm nhân quyền trong hệ thống ngục tù của Tunisia. Những công bố đó so sánh sự tra tấn và bạc đãi mà tù nhân Tunisia phải chịu đựng với những tù nhân ở trại tù Abu Ghraib (Iraq). Mohammed là thành viên của Ủy Ban Quốc Gia vì Tự Do tại Tunisia (National Committee for Liberties in Tunisia), một trong những vô số các tổ chức phi chính phủ mà chính quyền Tunisia không công nhận, và là cựu giám đốc của Hiệp Hội Luật Sư. Là một nhà chỉ trích tham nhũng lừng danh, ông là một trong số ít những luật sư tại Tunisia sẵng lòng bình luận và hành động công khai đối với những cáo buộc tham nhũng liên quan đến gia đình của tổng thống Ben Ali. Ông bị bắt giam vào trại tù El Kef ở thành phố Tunis, cách nhà và gia đình ông 170 kilomét, vào tháng Tư năm 2005, sau một phiên xử bị lên án rộng rãi là bất công và phi lý bởi những tổ chức phi chính phủ (NGO) của Tunisia và của cộng đồng quốc tế. Từ ngày 11 tháng Ba đến 21 tháng Tư năm 2006, để kêu gọi sự quan tâm về những điều kiện vô nhân và ngày càng tồi tệ mà ông phải chịu đựng nơi ngục tù, và những sự sách nhiễu mà các thành viên trong gia đình ông phải đối phó khi thăm ông, ông đã tuyệt thực lần hai kể từ ngày vào ngục.

Samia Abbou, vợ của Mohammed Abbou, bị hành hung dã man ngày 7 tháng Mười Hai năm 2006. Bà và ba nhà nhân quyền Tunisia hàng đầu khác bị tấn công và đánh đập ngoài trại giam El Kef, gần Tunis, bởi một nhóm mặc đồ dân sự gồm khoảng bốn mươi người đàn ông. Samia Abbou đến El Kef để thăm chồng bà bị giam, cùng tháp tùng là Oncer Marzouk, cựu chủ tịch Ủy Ban Quốc Gia vì Tự Do cho Tunisia , Salim Boukhdhir từ tổ chức Liên Minh vì Nhân Quyền Tunisia, và Samri Ben Armor, một ký giả rất quen thuộc và là thành viên sáng lập Hiệp Hội Tương Trợ Tù Nhân Chính Trị Quốc Tế. Theo các tường trình, cảnh sát đã chặn xe của bốn người nêu trên vài lần trên đường đến Elf Kef, và đã hiện diện bên ngoài nhà tù El Kef khi cuộc tấn công diễn ra.

Habib Salih

Syria – Ngày 29 tháng Năm, 2005, các sĩ quan tình báo quân sự bắt Habih Sali tại Tartus, khoảng 130 cây số phía bắc thành phố Damascus (ông vừa được phóng thích sau cuộc tống giam trước đó-vì tham gia vào phong trào dân sự "Mùa Xuân Damascus"). Lần này, ông bị bắt vì đăng lên hai trang web một loạt thư viết tay gửi đến các đại biểu đang dự buổi hội thảo tháng Sáu, năm 2005 của Đảng Baath, mà trong đó ông tỉ mỉ kể lại những kinh nghiệm ông đã trải qua trong tù. Trong những tháng sau khi được phóng thích, ông cũng đã viết bài chỉ trích tờ báo an-Nahar của Lebanon và trang mạng bị cấm http://www.elaph.com . Sau khi bị bắt, các cơ quan thẩm quyền liền chuyển ông vào phòng điều tra, nơi ông phải đương đầu với nguy cơ bị tra tấn. Hiện phiên toà xử ông vẫn chưa được định đoạt.

Huang Qi

Trung Cộng– Huang là một nhà bảo vệ nhân quyền, và là người thành lập trang web Tianwang (www.6-4tianwang.com) vào tháng Sáu năm 1999 để công bố thông tin về những người bị mất tích. Lần hồi, trang web này bắt đầu đăng những phê bình và bài báo về những tiết mục mà thông thường không được các báo đài do nhà nước quản lý nói đến.

Trang web này đăng những chuyện về vi phạm nhân quyền, tham nhũng trong chính phủ, và chỉ vài ngày trước khi Houang bị bắt giữ-một vài manh mối về cuộc thảm sát Thiên An Môn (năm 1989). Huang bị bắt ngày 3 tháng 6, 2000-một ngày trước lễ kỷ niệm thứ thứ 11 của những cuộc biểu tình rầm rộ (của sinh viện) năm 1989-và bị kết tội dựa theo hai điều 103 và 105 của bộ luật hình sự. Ông bị quy chụp tội đăng tải những bài viết, do các nhà bất đồng chính kiến đang sống ở hải ngoại viết, về các cuộc biểu tình năm ấy trên website của ông. Trong một cuộc phỏng vấn với BBC, ông Huang nói rằng trong vòng một năm đầu tiên ông thụ án tù, ông bị cưỡng ép phải ngủ dưới sàn nhà, ngay cạnh bên cầu xí. Và ông phủ nhận tội trạng về lật đổ và ông khẳng định tội ây không áp dụng cho mình. Ông nói: "Nếu một ai đó ở Trung Quốc đấu tranh cho dân chủ và tự do và sau đó bị kết tội tham gia vào Biến Cố 4 tháng Sáu, thành viên Pháp Luân Công, hoặc là một nhà đấu tranh dân chủ, thì tôi chắc chắn sẽ nói với chính quyền rằng tôi cũng là một trong những người ấy, và tôi rất hãnh diện về điều đó. Không có sự nghi vấn nào rằng tôi đang đeo đuổi theo dân chủ và tự do." Ngày 4 tháng 6, 2005 Huang Qi được phóng thích sau khi mãn án. Tổ chức Phóng Viên Không Biên Giới trao tặng ông giải thưởng Cyber-Freedom Prize (Tự Do Trên Mạng Ảo) năm 2004.

4.1 TRƯỜNG HỢP NGHIÊN CỨU I TẠO MỘT CHÍNH SÁCH AN NINH

Khi hoạch định một chính sách an ninh cho chính bạn hoặc tổ chức của bạn, bạn phải hiểu rành mạch những nguy cơ về an ninh cho máy điện toán và dữ liệu của bạn. Mức độ nguy cơ, và tức nhiên nguy hiểm, tăng theo tỉ lệ thuận với những hiểm họa (threats) và nhược điểm (vulnerabilities), như trong phương trình này:

Nguy cơ = Hiểm Họa X Nhược Điểm

Hiểm Hoạ ở đây nghĩa là khả năng một ai đó sẽ gây hại đến sự an ninh của máy điện toán của bạn, dữ liệu lưu trữ bên trong và những trao đổi qua mạng. Đánh giá mức độ đe doạ nghĩa là phân tích xu hướng một mối đe doạ nhất định được đưa vào hành động.

Những ví dụ bao gồm:

- Một cuộc tấn công bằng virút (A virus attack).
- Tịch thu những thiết bị trong máy ví tính (ví dụ như ổ cứng).
- Chặn một trang web.

Nhược điểm nghĩa là mức độ bạn có nguy cơ bị mất, bị phá, và bị thiệt hại trong trường hợp một cuộc tấn công xảy ra (nếu mối đe doạ được phát hiện) và nó biến đổi theo hoàn cảnh và thời gian. Nhược điểm luôn luôn tương đối, bởi vì tất cả mọi người và tổ chức đều chỉ có nhược điểm (bị tác hại) ở một phương diện nào đấy. Thông thường thì nhược điểm trong lãnh vực kỹ thuật là ở chổ thiếu hiểu biết hoặc không được huấn luyện đúng mức. Một nhược điểm khác nữa là sự dựa vào kỹ thuật (bảo hộ) quá mức khi chưa biết rõ kỷ thuật ấy vận hành ra sao.

- Vị trí cũng có thể trở thành nhược điểm. Ví dụ, màn ảnh máy điện toán và những hoạt động của bạn trên máy có thể dễ bị nhìn thấy nếu bạn sinh hoạt tại quán café Internet. Nếu bạn sống tại một quốc gia bị hạn hán hoặc thiếu điện thì nhược điểm của bạn sẽ là thiếu điện (hoặc dấy điện, tức electrical surge) và vì vậy máy của bạn không thể vận hành và truy cập Internet.
- Nhược điểm cũng bao gồm sự thiếu phương tiện liên lạc, như điện thoại hoặc không có nối kết Internet.
- Nhược điểm cũng có thể gắn liền với công tác tập thể và sự sợ hãi: Một nhà bảo vệ nhân quyền nếu bị hăm hoạ có thể sẽ cảm giác sợ hãi, vì thế công việc của người ấy sẽ bị ảnh hưởng. Nếu ông/bà ấy không có biện pháp đúng để đối đầu với sự sợ hãi này (người để bày tỏ, đồng đội tốt, vân vân), ông/bà ấy sẽ có nguy cơ phạm sai lầm trong công việc, hoặc là yếu kém trong những quyết định. Mặc dù mối đe doạ này không liên quan đến máy điện toán, nhưng nó rất đáng kể đối với an ninh điện toán bởi vì nó làm gia tăng mối đe doạ đã tồn tại rồi.

Năng Lực là những khả năng và phương tiện mà một nhóm hoặc một người có thể sử dụng để đạt một sự an ninh (cho máy điện toán) hợp lý. Những ví dụ năng lực có thể là được huấn luyện trong các vấn đề liên quan đến điện toán, hoặc an ninh điện toán.

Kiến thức về môi trường điện toán/Internet là một năng lực rất quan trọng trong việc đối phó với những bất an. Cho nên, sự quen biết với một chuyên viên điện toán khả tín, hoặc được tiếp tay bởi một nhóm người có kỹ năng tốt là điều cần thiết trong việc:

- Thiết lập chính sách an ninh trong tổ chức: Ví dụ như lưu trữ dữ liệu phòng hộ (secure).

- Bảo đảm an ninh cho các ngõ vào phần mềm office, và lắp đặt những khoá vững chắc tại các cửa (doors) và cửa sổ (windows) của máy điện toán.
- Sao chép lại tất cả bảo đảm của thiết bị cứng và những giấy phép của thiết bị mềm (copies of all hardware warranties and licences for software) cho máy.

Sự thiếu kiến thức trong môi trường làm việc và kỹ thuật (mà bạn) vận hành là một nguy cơ bị xâm hại, trong khi có kiến thức trong lãnh vực này là một năng lực. Nguy cơ bị xâm hại, tạo nên bởi những hiểm họa và nhược điểm, có thể được giảm thiểu nếu người sử dụng điện toán có đủ năng lực (năng lực càng nhiều, nguy cơ bị xâm hại càng ít).

Nguy Cơ = (Hiểm Họa X Nhược Điểm) / Năng Lực

Bởi vậy, ví dụ, nguy cơ bạn bị mất dữ liệu điện tử do một virút tấn công bằng: Hiểm Họa bị virút tấn công, nhân cho Nhược Điểm vì không có phầm mềm và tường lửa chống virút, chia cho Năng Lực đạt được khi bạn có trong tay phương tiện Digital Security Toolkit (để bảo vệ an ninh điện tử). Lẽ đương nhiên đây không phải là một công thức toán học, nhưng công dụng chánh của nó là nhằm giúp bạn nhận diện những yếu tố có thể gây ra nguy cơ nói trên để bạn biết mà trừ khử chúng.

TẠO DỰNG MỘT KẾ HOẠCH AN NINH

Cấu Tạo của Kế Hoạch

Mục đích của một kế hoạch an ninh là giảm thiểu nguy cơ bị hại của bạn. Cho nên nó sẽ có ít nhất ba mục tiêu, dựa theo bản lượng giá nguy cơ của bạn:

- Cắt giảm mức độ hiểm họa mà bạn đang chịu đựng
- Cắt giảm những nhược điểm của bạn
- Gia tăng năng lực của bạn

Sẽ hữu dụng hơn nếu kế hoạch an nình của bạn bao gồm thêm:

- Các kế hoạch hoặc quy trình dự phòng để bảo đảm công việc hằng ngày được thực hiện trong tiêu chuẩn an ninh cố định. Ví dụ, cách trao đổi những chủ đề nhạy cảm qua email với một nhóm người (lạ hay quen) phải nằm trong khuôn khổ được quy định trước nhằm bảo vệ an ninh.
- Những kế hoạch để đương đầu với trường hợp cụ thể khẩn cấp, ví dụ như bị tịch thu phương tiện.

Những Trách Nhiệm và Tài Nguyên Để Thực Thi Kế Hoạch

Để bảo đảm kế hoạch được thực thi, các thói quen về an ninh phải được áp dụng vào công việc hàng ngày. Hãy:

- Theo thói quen mà liệt kê công tác lượng giá nguy cơ (bị hại) và những điểm về an ninh trong chương trình làm việc của bạn.
- Báo cáo và phân tích những sự cố về an ninh.
- Phân chia trách nhiệm.
- Phân chia tài nguyên, tức là thời gian, tiền tài, vân vân, cho sự an ninh.

Soạn thảo kế hoạch-Cách bắt đầu.

Nếu bạn đã làm xong một bản lượng giá nguy cơ (risk assessment) cho một nhà bảo vệ nhân quyền hoặc một tổ chức nào đấy, bạn có thể đã có một bản liệt kê thật dài các nhược điểm, vài loại hiểm họa, và một số năng lực. Bạn không thể, trên thực tế, bao quát hết tất cả mọi thứ cùng một lúc. Vì vậy, phải bắt đầu từ đâu? Điều đấy rất dễ. Hãy:

• Chọn một vài hiểm hoạ: Ưu tiên hóa những hiểm họa-dù thật sự hay chỉ tiềm ẩn-mà bạn đã liệt kê bằng một trong những tiêu chí sau đây: Hiểm họa siêu nghiêm trọng-ví dụ, mất tất cả dữ kiện trong máy điện toán; hoặc nguy cơ hiểm họa siêu nghiêm trọng: Nếu một tổ chức tương tự như của bạn bị tấn công thì bạn có nguy cơ siêu nghiêm trọng sẽ bị tấn công; hoặc là hiểm họa tương ứng nhất với những nhược điểm của bạn-bởi vì nguy cơ bạn bị hại cao nhất tại nhược điểm cụ thể đó.

- Liệt kê những nhược điểm nào tương ứng với những hiểm họa bạn đã liệt kê. Phải đối phó với những nhươc điểm này trước, nhưng hãy nhớ rằng không phải nhược điểm nào cũng tương ứng tuyệt đối với tất cả hiểm họa. Ví dụ, nếu bạn không biết chắc tất cả dữ liệu trong máy ví tính của bạn đã được lưu secure (backup) chưa, thì điều này đồng nghĩa với hiểm họa bị mất tất cả dữ liệu trong máy mà không thể phục hồi, hoặc tìm lại được.
- Liệt kê những năng lực tương ứng với những hiểm họa mà bạn đã liệt kê. Bây giờ, bằng cách sử dụng những năng lực, bạn đứng ở tư thế sẵn sàng đối phó với những hiểm họa trong danh sách, và có thể bảo đảm một cách hợp lý rằng bạn sẽ có khả năng giảm thiểu nguy cơ bị xâm hại ngay từ thời điểm thích hợp ban đầu.

Áp Dụng Trong Thực Tiễn

Mục đích của kế hoạch này là bảo đảo dữ liệu trong máy vi tính của chúng ta không bị đánh mất, trộm, hoặc bị hư hại mà không thể phục hồi bằng cách này hay cách khác.

Bây giờ chúng ta hãy bắt tay vào việc giảm thiểu những nhược điểm và đồng thời gia tăng năng lực của chúng ta trong việc đối phó với những hiểm họa này và những hiểm họa khác có thể xuất hiện trong tương lai. Giải pháp và tài nguyên của bạn có thể sẽ khác nhau tùy theo trường hợp. Lưu ý rằng sự việc không sao lưu dữ liệu (lack of information backup) là một nhược điểm thông thường, nhưng có thể gây ra hậu quả nghiệm trọng, sau khi hiểm hoạ được phát giác. Dưới đây là một bản liệt kê những động tác mà bạn có thể thi hành để giảm thiểu các nhược điểm (tất cả những thiết bị, dụng cụ và chú thích về cách thực hành những động tác này có thể tìm trong cuốn cẩm nang (thủ bản) này và trong quyển Digital Security Toolkit.

Để đối phó với nguy cơ bị virút tấn công thì hãy:

- Ban hành một chính sách cứng rắn cho việc mở email có nguồn gốc lạ, trả lời các thư rác (spam). Nói trắng ra là, phải ngăn cấm bất kỳ ai làm một trong hai, hoặc cả hai điều này. Những ai nhận được hàng trăm thư rác hoặc thư chứa virút thì nên đổi đia chỉ điện thư.
- Cài đặt phần mềm chống virút miễn phí (như Avast) ở tất cả máy vi tính và cập nhật thông tin, phần mềm chống virút từ Internet. Các chương trình và chỉ dẫn có thể tìm tại Digital Security Toolkit. Hãy bảo đảm mỗi máy vi tính trong văn phòng được bảo vệ toàn phần bởi hệ thống chống virút khi vận hành.
- Khi virút được trừ khử và máy ví tính không còn nhiễm virút nữa, hãy sao lưu (backup) tất cả dữ kiện quan trọng, và cất giữ nó nơi riêng biệt (đĩa CD, đũa nhớ USB) cách xa văn phòng. Nếu trong trường hợp bạn bị virút tấn công, bạn vẫn ít nhất cũng thu hồi lại được những hồ sơ chứa dữ kiện quan trọng

Máy vi tính bị đánh cắp hoặc tịch thu, hãy:

- Để đề phòng kẻ trộm, bạn phải bảo đảm an ninh cho văn phòng và phạm vi làm việc của bạn. Cửa phải vững chắc và các cửa sổ thì được nẹp song sắt (đặc biệt cần thiết nếu văn phòng của bạn ở tầng trệt). Bạn cũng có thể đặt thêm hệ thống giao tiếp intercom hoặc các hệ thống nhận diện khác. Lý tưởng nhất là văn phòng của bạn có một bàn tiếp tân, để khách đến viếng được chào đón trước khi được vào văn phòng chính.
- Sao lưu dữ liệu và gìn giữ an toàn ở một nơi khác.

Những Hiểm Hoạ	Những Nhược Điểm	Những Năng Lực
Virút tấn công	• Nhân viên mở email mà không dè chừng • Không ai biết thiết bị mềm rà soát virút đã được cài đặt hoặc cập nhật • Dữ liệu không được sao lưu (backup)	• Vừa nhận được bản copy 'Digital Security Toolkit' để bảo vệ thông tin điện tử từ trang http://security.ngoin-abox.org
Máy vi tính bị tịch thu	• Kẻ gian dễ dàng đột nhập vào văn phòng • Không sao lưu dữ kiện • Không kinh phí để mua thiết bị mới • Thông tin không được bảo mật	• Đội ngũ đồng sự tốt, mọi người hiểu nhau và hợp tác • Mối giao hảo tốt với nhà tài trợ kinh phí
Máy vi tính bị hư hại do thời tiết hoặc những yếu tố bên ngoài khác.	• Không sao lưu dữ kiện • Không có kiến thức bảo trì, bảo vệ trang thiết bị điện tử	• Mối giao hảo tốt với nhà tài trợ kinh phí • Một người thân của một trong những nhân viên là thợ sử điện tử.

- Bạn cũng nên chuẩn bị trướnguồn tài khoản khẩn cấp để mua thiết bị mới để thu hồi và tải lại những dữ liệu được sao lưu.
- Nếu máy ví tính bị tịch thu, ít nhất phải bảo đảm những dữ liệu trong máy được bảo vệ để tránh bị truy cập một cách tùy tiện. Xử dụng phần mềm mã hoá để bảo vệ một phần ổ cứng (hard drive) trong máy của bạn. Tương tự, hãy xoá bỏ tất cảc dữ liệu không cần thiết để tránh khỏi việc bị khôi phục bởi những người tịch thu. (Xem thêm ở chương Sao Lưu Dữ Liệu, Hủy Bỏ và Thu Hồi)
- Hãy biết rõ ai có chìa khoá vào văn phòng, và biết luôn bao nhiêu bản photo copy đang hiện diện. Nếu máy vi tính của bạn không được bảo vệ bởi phương pháp mã hoá, hoặc văn phòng bạn lữu trữ dữ kiện nhạy cảm trên giấy hoặc trong máy vi tính, thì nên bảo đảm rằng không ai được phép đơn phương đột nhập vào văn phòng của bạn, kể cả nhân viên quét dọn.

Máy vi tính bị hỏng do thời tiết hoặc những yếu tố bên ngoài khác:

- Lý tưởng nhất là phạm vi làm việc của bạn được một thợ ống nước hoặc thợ điện kiểm tra thường xuyên để báo cáo tính bền chắc của nó. Ví dụ như các vết nứt trên ống nước, đường điện bị hỏng, hoặc tình trạng của thiết bị phòng cháy. Tất cả đường giây điện nào bị hỏng nên được vứt bỏ và thay thế đường giây mới. Việc này có thể đắt tiền, nhưng rất cần thiết, vì các máy vi tính rất tinh vi và không chịu nổi nước hoặc hơi nóng kéo một cuộc hoả hoạn xảy ra!
- Sao lưu tất cả các dữ liệu và chúng phải được gìn giữ an toàn tại một nơi khác.
- Bạn nên trang bị loại pin Uninterrupted Power Supply (UPS) cho máy vi tính của bạn để đề phòng máy bị tắt ngang trong trường hợp cúp điện. Ổ cắm điện và bảng điện ở nhà bạn nên có một hệ thống phòng chống bội điện, để chúng có thể tự động cắt điện trong trường hợp điện thế tăng đột biến (electric spike). Những vùng bị cúp điện cả tháng mỗi lần nên tìm đến máy phát điện chạy bằng dầu hoặc các nguồn năng lượng khác để phục vụ cho nhu cầu của máy vi tính.

Từ các khía cạnh nào đó, thật là khó khăn khi phải ban hành những chính sách an ninh mà không ảnh hưởng đến hiệu quả công việc tại phòng làm việc của bạn. Sự chú tâm đến an ninh thường tốn thời gian và công sức để tập trung. Những bất cẩn, thời hạn, và sự thiếu nhân lực là những kẻ thù của an ninh. Cho nên điều ấy rất cần thiết để các nguyên tắc an ninh được chấp thuận và tuân thủ bởi tất cả mọi người. Mỗi người phải thực thi chúng, và các lãnh đạo trong một tổ chức cụ thể phải dẫn đầu làm gương. Một nền an ninh vững chắc cũng bắt buộc bạn phải chủ động, phải phát hiện ra những hiểm họa và phải tìm cách đương đầu với chúng trước khi chúng tấn công.

4.2 TRƯỜNG HỢP NGHIÊN CỨU II
CÁC KÊNH THÔNG TIN LIÊN LẠC

Sơ Lược

Tổ chức phi chính phủ toàn cầu 'Nhân Quyền Cho Mọi Người' (Trung Ương), trụ sở đặt tại Âu Châu, đã yêu cầu một trong những phân hội quốc tế của họ (Chi Bộ) mở một cuộc điều tra các trường hợp tra tấn trong lúc bị chính quyền địa phương bắt giữ. Quốc gia được chọn ,'N', từ lâu đã lừng danh trong việc sử dụng biện pháp tra tấn tù nhân và đặc biệt là các tù nhân đấu tranh nhân quyền. Các thành viên làm việc ở nhóm hoạt động của Chi Bộ tại thủ đô nước 'N' có rất nhiều kinh nghiệm lâu năm trong việc xử lý các tình huống khó khăn. Họ có thể đối chiếu các thông tin cần thiết trong bản báo cáo về việc tra tấn nhưng lo ngại chính quyền sở tại sẽ dùng mọi biện pháp để ngăn chặn họ. 'N' là một quốc gia có chính sách kiểm duyệt thông tin chặt chẽ nhất nhằm bảo đảm thế giới bên ngoài không biết gì nhiều về các chuyện xảy ra bên trong.

Trung Ương quyết định tự công bố bản báo cáo dựa vào những dữ liệu họ nhận được từ Chi Bộ. Họ cần phải thiết lập một kênh thông tin bảo mật với Chi Bộ để bảo đảm công cuộc điều tra được tiếp tục tiến hành cho đến khi hoàn tất, bất kể là bao lâu. An toàn bảo mật là tiêu chỉ hàng đầu ở đây và họ đã dự trù một ngân sách khoảng 5,000 USD riêng cho Chi Bộ sử dụng trong kế hoạch này. Kế hoạch điều tra cần phải vượt qua những nổ lực gây nguy hại từ các lực lượng an ninh địa phương nhằm ngăn chặn hoặc tiêu diệt họ tận gốc. Chi Bộ hiện đang trong quá trình xem xét lại cách thức thu thập, liên lạc thông tin cùng với việc thiết lập nội quy hoạt động nhằm bảo vệ an ninh cho tất cả các thành viên thi hành.

Họ quyết định rằng tất cả các thành viên phải tham dự lớp an toàn hoạt động được huấn luyện bởi các chuyên gia địa phương và tự nghiên cứu các vấn đề liên quan đến an toàn cá nhân tự mạng Internet. Các trường hợp nghiên cứu, những nhân chứng, và các bản báo cáo cùng tất cả các thông tin khác về các trường hợp tra tấn họ điều tra được sẽ được lưu trữ trong dạng văn bản in lẫn dữ liệu điện tử. Các phóng viên làm việc bên ngoài sẽ báo cáo về những gì họ tìm hiểu được bằng cách lưu trữ những mảnh giấy mà họ ghi chép lại và lập bản báo cáo thường nhật từ một quán càfé Internet. Nói một cách khác, tất cả các dữ liệu sẽ được sao chép trong dạng giấy viết và dạng điện tử.

Nơi làm việc của họ là một căn chung cư thuê mướn tại trung tâm thành phố. Họ có 2 máy điện toàn và một đường nối mạng. Các thành viên đều quen biết rõ những nhà hàng xóm và có được sự ủng hộ của họ. Nơi làm việc này đã từng bị kẻ khác đột nhập, nhưng không có gì quan trọng bị đánh cắp.

Các mối nguy

Để thấu hiểu các yếu tố họ sẽ cần đến để bảo toàn cho kế hoạch này, trước tiên Chi Bộ quyết định rằng họ sẽ ghi chép xuống các mối nguy mà họ có thể phải đối đầu. Phạm vi làm việc của họ được sử dụng chung bởi cả nhóm, bao gồm thành viên điều tra và thành viên thường trực tại nơi làm việc. Mỗi người đều có các mối nguy riêng biệt của họ và những mối nguy này cần phải được xử lý riêng rẽ. Tương tự như thế, chính những mối nguy đó cũng được phân loại thành những loại ảnh hưởng đến an toàn nơi làm việc, đến an toàn của dữ liệu thu thập được, và đến an toàn của việc thông tin với nhau[75].

Trung Ương
- Mối nguy nơi làm việc: tối thiểu
- Mối nguy dữ liệu: Các bản báo cáo bị mất bởi virút gây hại hoặc bị hack.
- Mối nguy thông tin: Nguồn liên lạc với Chi Bộ bị lũng đoạn, hoặc các bản báo cáo có thể bị đánh tráo (giả mạo trong những đợt xâm nhập gây nguy hại).

Chi Bộ
- Mối nguy nơi làm việc: máy móc và dụng cụ nơi làm việc bị phá hỏng, đánh cắp, hư hại, cháy.
- Mối nguy dữ liệu: Máy tính bị tịch thu, dữ kiện bị hỏng bởi virút tấn công hoặc bởi tin tặc.
- Mối nguy thông tin: Đường truyền mạng bị cắt, không thể gửi hoặc nhận điện thư, trang mạng của tổ chức và các địa chỉ điện thư bị ngăn chặn, thông tin có thể bị giám sát.

Thành viên làm việc bên ngoài
- Mối nguy dữ liệu: các bản báo cáo bị mất hoặc bị tịch thu.
- Mối nguy thông tin: thành viên làm việc bên ngoài không thể tiếp cận với các quán càfé nối vào mạng, các trang mạng của Chi Bộ và Trung Ương bị ngăn chặn từ trong N.

GIẢI PHÁP

Liên lạc thông tin

Thông tin giữa các thành phần khác nhau trong kế hoạch này rất tối cần cho quá trình và sự thành công của nó. Cho nên các thành viên tham gia đã nghĩ ra một vài tiêu chuẩn và phương pháp để thiết lập và bảo vệ việc liên lạc này.

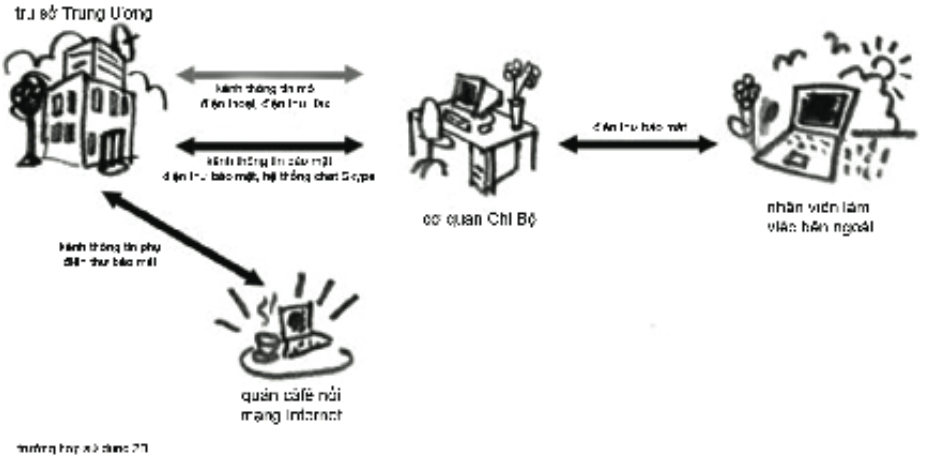
Có 3 kênh thông tin khác nhau để liên lạc với Trung Ương được thiết lập. Có một **kênh thông tin mở** mà trong đó, mọi dữ liệu được thông truyền một cách không bảo mật - bằng điện thoại, bằng cách đăng tin hoặc bằng điện thư thông thường. Duy trì một **kênh thông tin mở** rất quan trọng để khiến bộ phận giám sát hài lòng vì họ có thể tiếp cận những thông tin qua lại trong kế hoạch. Các dữ liệu qua lại trong kênh mở thuộc loại không nhạy cảm và bao gồm các thông tin về đặc trưng về quản lý và tổ chức.

Kênh thông tin mật được sử dụng cho các thông tin nhạy cảm và bảo mật. Nó sẽ được sử dụng để trao đổi tin tức về các trường hợp, các báo cáo của nhân chứng, và sách lược của tổ chức. Điện thư mạng với chức năng bảo toàn (Secure webmail) cùng hệ thống chat Pidgin với chức năng mã hóa OTR phụ để bảo mật các mẫu đối thoại[76]. Các thông tin nhạy cảm sẽ không được truyền qua điện thoại, fax hoặc điện thư chưa được bảo mật. Không nên sử dụng kênh thông tin mật thường xuyên để tránh gây chú ý.

Kênh thông tin phía trên đòi hỏi một đường truyền mạng còn hoạt động để liên lạc. Mọi người đều đồng ý rằng Trung Ương không nên bị ảnh hưởng trong trường hợp đường truyền mạng không hoạt động hoặc bị cắt nên một **kênh thông tin phụ** được thiết lập cho Chi Bộ và thành viên của họ làm việc bên ngoài sử dụng. Kênh thông tin phụ này là do thành viên Chi Bộ sử dụng một quán càfé

75
Có một yếu tố khác liên quan đến an nguy của thành viên, nhưng tốt hơn hết là yếu tố này được giải thích trong 'Cẩm Nang Bảo An cho Các Nhà Tranh Đấu Nhân Quyền' của Binh Đoàn Hòa Bình tại http://www.frontlinedefenders.org/manuals/

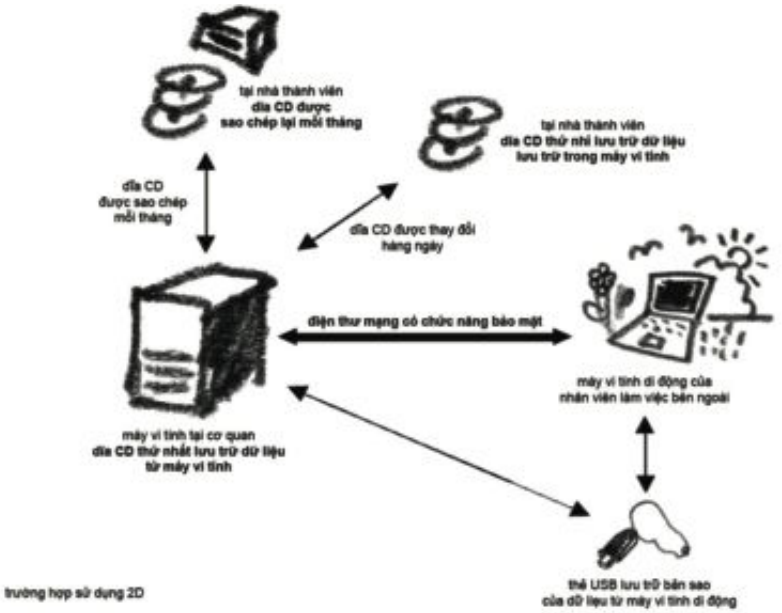
76
Bạn có thể tìm thấy Pidgin và OTR plugin trong Hộp Đồ Nghề An Ninh Kỹ Thuật Điện Tử (Digital Security Toolkit).



kết nối mạng ở gần đấy. Họ sẽ dùng đến các phần mềm cần thiết trong dạng lập trình di động, có thể truy cập được trong Hộp Đồ Nghề An Ninh Kỹ Thuật Điện Tử và lưu trữ trong các thẻ USB. Họ đã được chủ quán càfé mạng bảo đảm rằng các máy tính trong quán không nhiễm virút. Dù sao đi nữa, các thành viên sử dụng các máy tính công cộng cũng nên đề cao cảnh giác.

Dữ liệu, thông tin

Tất cả các dữ liệu thu hoặc gom nhặt được bởi các thành viên sẽ được giữ trên giấy và trong dạng điện tử. Điều này đòi hỏi những biện pháp an ninh cần thiết để bảo đảm rằng dữ liệu sẽ không bị mất, bị đánh cắp, hoặc bị hư hỏng. Thiết lập và duy trì một phương pháp để lưu trữ bản phụ có thể tồn tại mọi trường hợp tấn công có thể xảy ra là một việc rất quan trọng. Tương tự như thế, phương tiện lưu trữ của bản sao chính nó cũng phải được bảo toàn vì đó là bản sao của những tài liệu nhạy cảm.



Nhằm đảm bảo các bản báo cáo bên ngoài không bị mất trước khi được truyền đến Chi Bộ, cần phải mua một máy điện toán di động. Thành viên làm việc bên ngoài sẽ ghi chép thông tin trên giấy và sao chép lại trong máy tính di động. Họ sẽ thường xuyên chuyển các thông tin này đến Chi Bộ trong một tiệm càfé mạng mỗi ngày (hoặc thường xuyên hơn nếu khả năng cho phép).

Nơi làm việc

An toàn cho nơi làm việc bao gồm một nội quy nghiêm ngặt đối với thành viên để củng cố các điểm ra vào của tòa nhà và việc bảo toàn máy móc để giảm thiểu sự cố máy điện toán bị đứng.

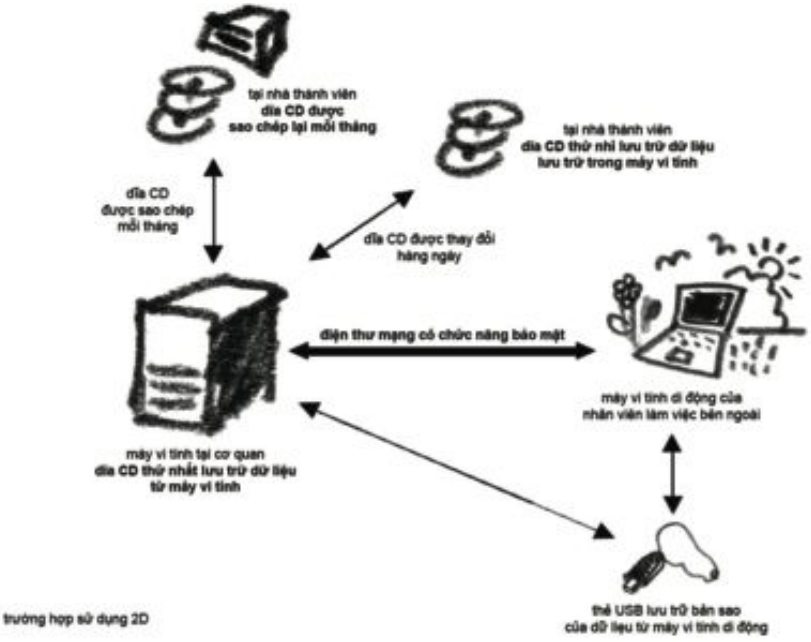
Các tài liệu giấy tờ cần thiết phải được giữ trong tủ sắt và nên được hủy bỏ đàng hoàng khi không cần đến chúng nữa. Cũng nên phòng ngừa khả năng máy điện toán và các văn bản, tài liệu của nơi làm việc có thể bị hư hỏng hoặc bị tịch thu, cho nên một ngân quỹ phụ cũng nên được duy trì để phòng khi phải mua sắm các máy móc để các thành viên có thể tiếp tục hoạt động trong trường hợp bị tịch thu.

Chi tiết về cách đối phó với các mối nguy

Sau khi thiết lập một khái niệm tổng quát về phương thức hoạt động nhằm đối phó với các tình huống có thể xảy ra, nhóm hoạt động sẽ tìm cách đối đầu với từng mối nguy được liệt kê trong biểu đồ. Qua mạng Internet, họ sẽ tham dự các lớp huấn luyện và tự nghiên cứu về an ninh điện toán.

Các mối nguy đối với dữ kiện, thông tin

Các dữ liệu hoặc các bản báo cáo có thể bị mất hoặc bị tịch thu: Để tránh trường hợp dữ liệu bị mất xảy ra, cần phải thường xuyên sao chép các dữ liệu vào các máy điện toán hoặc máy điện toán di động. Một máy sao chép dĩa CD loại có thể tái sử dụng (CD-RW) hiện nay có thể mua với giá 200 USD và cài vào 1 trong các máy điện toán. Dữ liệu được sao chép lại bằng cách sử dụng phần mềm sao chép Cobian có thể truy cập trong Hộp Đồ Nghề An Ninh Kỹ Thuật Điện Tử và các dữ liệu sẽ được ghi vào dĩa CD bằng phần mềm DeepBurner[77]. Cứ mỗi 2 ngày thì các dữ liệu cá nhân của người sử dụng sẽ được sao chép lại và cất giữ ở nơi khác. Người phụ trách việc bảo trì tài liệu sao chép lại thay phiên sử dụng 2 dĩa CD, một dĩa lúc nào cũng được lưu trữ ở nơi làm việc và 1 dĩa lúc nào cũng được lưu trữ ở nơi khác – có thể là nhà của thành viên phụ trách. Mỗi cuối tháng, một bản phụ khác được sao chép và trao cho một người thứ 2 giữ tại nhà anh ta. Theo phương pháp này, nếu máy tính ở nơi làm việc bị hư hỏng và hệ thống sao chép đồng thời cũng bị phá hoại (rất khó có thể xảy ra cùng lúc), sẽ có một bản phụ thứ 3 sao chép lại kể từ tháng trước đó. Thành viên hoạt động bên ngoài sẽ lưu trữ bản sao vào thẻ USB. Thẻ USB này chứa đựng một bản sao của tất cả các tài liệu mới nhất từ các điều tra viên tính cho đến lần cuối cùng họ trở về nơi làm việc. Nếu máy điện toán di động của họ bị lưu giữ, các tài liệu ít ra cũng sẽ được chuyển đến nơi làm việc.



Bi

trường hợp sử dụng 2D

77 http://www.deepburner.com

virus tấn công hoặc bị tin tặc xâm nhập (hack): Để tránh tình trạng dữ liệu bị mất qua các đợt tấn công của virút hoặc tin tặc, Chi Bộ cần phải cài đặt hệ thống phòng chống virút Avast4 vào tất cả các máy điện toán. Phần mềm phòng chống virút này miễn phí cho các tổ chức bất vụ lợi và tự động cập nhật khi máy điện toán được nối vào mạng Internet. Họ cũng đã cài đặt phần mềm Spybot vào máy điện toán để nhận diện và tiêu diệt các trojan. Tường lửa Commodo cũng được cài đặt vào các máy này để phòng chống tin tặc đột nhập vào. Tất cả các phần mềm đề cập đến đều có thể tìm thấy được trong Hộp Đồ Nghề về An Ninh Kỹ Thuật Điện Tử. Một nội quy khắc khe về virút phải được tuân thủ để đảm bảo không ai mở những điện thư lạ hoặc sử dụng một dĩa mềm trong máy điện toán trước khi sử dụng phần mềm thăm dò virút để khám xét.

Máy tính bị tịch thu: Nếu các máy điện toán bị tịch thu, tổ chức cần phải có cách để tiếp tục hoạt động. Cần phải có khả năng mua máy điện toán mới, và ngân sách phải dự trù khoản tiền cần thiết này. Nếu gặp khó khăn thì chỉ cần một máy điện toán thôi cũng đủ để tiếp tục hoạt động. Nhóm hoạt động sẽ mua một máy điện toán mới với giá 1000 USD từ một đại lý bán lẽ. Tất nhiên là những phần mềm cần thiết và bản sao của những dữ liệu chủ yếu sẽ được cài lại trong máy để tổ chức có thể tiếp tục hoạt động.

Văn kiện và máy móc bị đánh cắp: Một nội quy về chìa khóa văn phòng được thiết lập và tuân theo bởi những thành viên trong nhóm. Chỉ có những ai cần giữ theo chìa khóa bên mình mới có 1 chìa khóa phụ. Không nên làm thêm chìa khóa phụ khác mà không có sự đồng ý của cả nhóm. Khi đêm đến, tất cả các máy điện toán đều phải được rút điện (tắt) và tài liệu, văn bản phải được khóa trong tủ sắt bảo an có thể mua với giá 300 USD. Tất cả các dĩa CD, dĩa mềm, và giấy tờ có thông tin quan trọng trong đó cần phải được khóa lại trong tủ sắt. Cần ghi rõ trong nội quy là những người không liên quan không thể ra vào văn phòng. Các cửa kính ở tầng trệt của tòa nhà cần phải được gắn thêm song sắt bên ngoài. Cửa ra vào cũng phải kiên cố và có lỗ quan sát trên đó. Một công ty tại địa phương có thể nhận làm 2 việc này với giá 500 USD.

Đường nối mạng không hoạt động: Đường truyền mạng có thể sẽ bị cắt. Điều này sẽ xảy ra khi chính quyền tạo áp lực đối với nhà cung cấp dịch vụ mạng hoặc một lỗi kỹ thuật nào đó xảy ra trong hệ thống kết nối mạng. Kế hoạch B sẽ là sử dụng một quán càfé mạng. Nếu đường truyền mạng sẽ bị mất dài hạn, một khoản tiền nhỏ khoảng 500 USD sẽ được dự trữ để trang trải cho chi phí sử dụng mạng Internet tại quán càfé. Thẻ USB sẽ được sử dụng để tải và truy cập thông tin giữa văn phòng và quán càfé.

Thông tin liên lạc bị giám sát: Nếu hệ thống kiểm soát của nước N có trang bị kỹ thuật tối tân, chính quyền sẽ giám sát được các điện thư gửi vào quốc nội hoặc gửi ra quốc ngoại. Vì nghi ngờ thông tin của Chi Bộ sẽ bị giám sát, cho nên chỉ có hệ thống điện thư mạng với chức năng bảo mật SSL mới được sử dụng. Chi Bộ đăng ký hai hộp thư tại https:/mail.riseup.net[78] và sử dụng một trong hai hộp thư để liên lạc với Trung Ương và hộp thư còn lại được sử dụng để liên lạc với các thành viên hoạt động bên ngoài. Tất cả các thông tin sẽ được truyền đến trụ sở hàng ngày bằng điện thư. Thành viên của Chi Bộ sẽ dò xét khả năng các cuộc tấn công bởi kẻ trung gian mạo nhận có thể xảy ra bằng cách kiểm soát kỹ càng chứng chỉ điện tử (certificate) của các trang mạng.

Trang nhà và điện thư bị chặn: Nếu chính quyền quyết định ngăn chặn đường truyền mạng dẫn đến trang nhà của Trung Ương và hệ thống điện thư mạng bảo mật (secured webmail) RiseUP, vẫn còn giải pháp khác. Thành viên của Chi Bộ có thể sử dụng các hệ thống điện thư mạng bảo mật khác hoặc sử dụng các phương pháp khác để lòn lách qua các nẻo bị chặn. Họ đã yêu cầu chi bộ cài đặt bộ phận Psiphon vào máy điện toán tại gia đình của các thành viên. Địa chỉ IP và cách đăng nhập vào các máy điện toán này (mật mã và biệt danh) sẽ được truyền đến Chi Bộ. Cách này giúp họ có được một biện pháp để đối phó với tường lửa của chính quyền vì Psiphon sẽ giúp họ dùng các máy điện toán từ nhà thành viên ở nước khác làm khởi điểm để truy cập thông tin từ các máy chủ của Trung Ương.

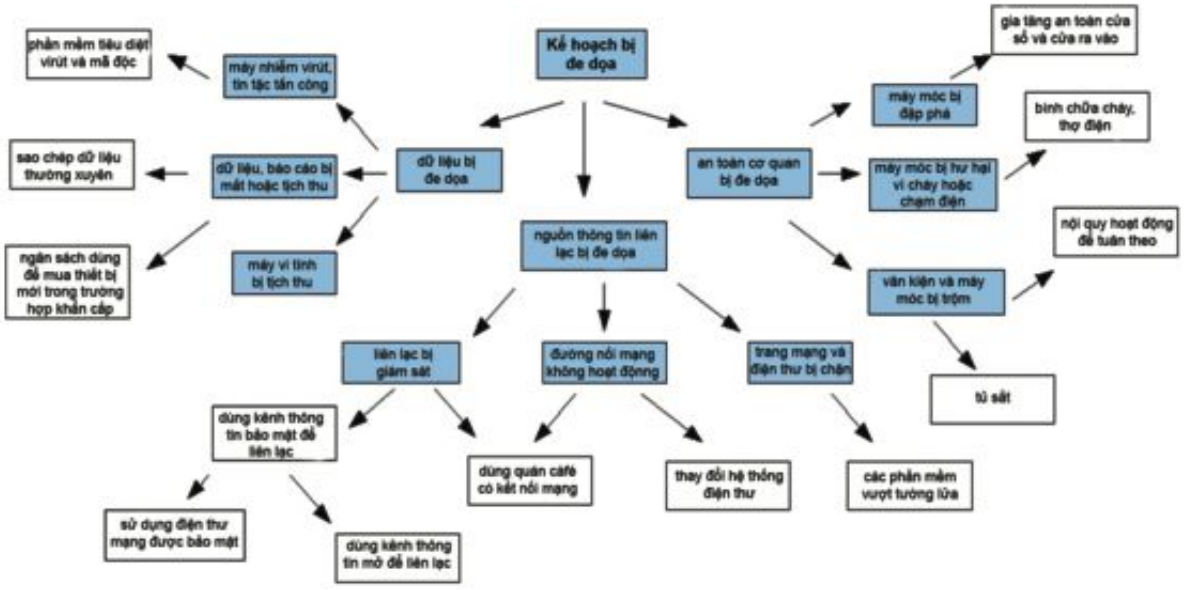
Kỹ thuật viên điện toán: Một kỹ thuật viên từ một công ty cung cấp dịch vụ máy điện toán đã từng giao dịch với nhóm trong quá khứ (và được tín nhiệm) sẽ đến văn phòng 2 lần mỗi tháng để quản lý và bảo trì máy móc. Chuyên viên này cũng sẽ được gọi đến trong trường hợp khẩn cấp với giá hợp đồng là 1000 USD cho mỗi 6 tháng.

Ngân sách

• Song sắt gắn trên các cửa sổ	500 USD
• Máy sao chép dĩa CD và 10 dĩa CD	200 USD
• Tủ sắt	300 USD
• 2 thẻ USB	100 USD
• Một máy điện toán di động	1000 USD
• Hợp đồng với chuyên viên kỹ thuật	1000 USD
Tổng cộng	**3100 USD**

Tiền dự trữ đề phòng trường hợp khẩn cấp : 1000 cho máy điện toán mới, 500 cho chi phí sử dụng mạng ở nơi công cộng - tổng cộng là 1500 USD.

Tổng số ngân sách	**4600 USD**



78
Các dịch vụ điện thư bảo mật khác gồm có https://bluebottle.com và https://www.fastmail.fm.

4.3 TRƯỜNG HỢP NGHIÊN CỨU III
BẢO TOÀN VÀ LƯU TRỮ DỮ LIỆU

Sơ Lược

Một tổ chức nhân quyền phi chính phủ, trụ sở đặt tại một quốc gia đang phát triển, đang cung cấp và giúp đỡ dịch vụ pháp lý miễn phí cho nạn nhân của các trường hợp vi phạm nhân quyền. Họ đã nhận nhiều trường hợp và giúp đỡ người dân địa phương tại đó trong 5 năm nay. Gần đây, họ bắt đầu gửi đơn đến tòa án nhân quyền trong vùng để kiện một trường hợp phức tạp và nhạy cảm về việc cảnh sát hành hung một thân chủ của họ. Tuần vừa qua, đã hai lần họ bị những kẻ lạ đe dọa - một lần qua điện thoại yêu cầu họ lập tức ngưng ngay những việc họ đang làm và lần khác từ một cảnh sát an ninh. Cảnh sát an ninh này nói rằng những tang chứng mà tổ chức này đang thu thập được xem như ảnh hưởng đến an ninh quốc gia và có thể bị tịch thu bất cứ lúc nào. Các luật sư của tổ chức phi chính phủ này tin rằng điều này không có thật và đây đơn giản chỉ là một thủ đoạn dọa dẫm. Họ tin chắc rằng vụ kiện hợp với luật pháp của quốc gia và những hiệp định quốc gia này đã ký kết với quốc tế. Tổ chức này muốn theo đuổi vụ kiện này đến cùng và đã đăng ký xin một nhà tài trợ một khoản tiền để giúp họ gia tăng mức độ an toàn và thu thập thêm tin tức.

Văn phòng của tổ chức này được đặt tại một tòa nhà kiên cố với lối ra vào đối diện với một con đường đông người qua lại. Tổ chức này cũng đã có được tiếng tăm tốt trong cộng đồng địa phương và các viên chức trong hàng ngũ cán bộ. Hàng xóm của họ lúc nào cũng vui lòng giúp đỡ và xem chừng kẻ lạ ra vào cho họ. Trong 5 năm họ hoạt động, chưa có chuyện gì không tốt xảy ra, nhân viên của họ tin tưởng vào địa điểm nơi họ đặt văn phòng làm việc và cũng đã thiết lập một nội quy nghiêm ngặt về việc xử lý chìa khóa văn phòng và các thân chủ tới lui. Những thay đổi trong chính quyền địa phương gần đây đã khiến tổ chức phi chính phủ này lo ngại vì họ e rằng cảnh sát an ninh sẽ có quyền bố ráp văn phòng của họ và tịch thu tài liệu liên quan đến các trường hợp thưa kiện. Họ đã chuẩn bị đầy đủ để thử thách và đối phó với mọi hành động trước tòa án nhưng lo ngại rằng tài liệu có thể bị tịch thu sẽ ảnh hưởng đến an nguy của nhiều người khác. Họ quyết định bảo toàn tài liệu trước những tình huống có thể xảy ra này. Họ cũng quyết định sẽ bảo toàn tất cả các tài liệu liên can đến những vụ kiện từ trước đến nay kể từ khi họ bắt đầu hoạt động.

Văn phòng có một máy điện toán và tất cả các nhân viên đều có kinh nghiệm kỹ thuật điện toán. Máy điện toán này được nối vào mạng qua một bộ phận modem gọi qua đường dây điện thoại. Họ sử dụng các thẻ nối mạng có in sẵn đầy đủ chi tiết để gọi số và đăng nhập với các khoản đăng nhập tạm thời. Máy điện toán này từ lâu đã không hoạt động vì bị nhiễm virus. Các ngăn tủ của văn phòng chứa đầy giấy tờ liên quan đế các vụ kiện mà họ đã giải quyết trong thời gian qua. Nhà bảo trợ đồng ý ủng hộ họ với số tiền tổng cộng là 1500 USD.

Các mối nguy và yếu điểm

Nhân viên của tổ chức phi chính phủ này nhận thức được rằng mối nguy chính họ phải đối diện là việc đơn kiện của họ bị tổn hại nếu tài liệu về vụ kiện bị

cảnh sát thu giữ. Điều này có thể gây nguy hại đến những thân chủ và nhân chứng của họ. Mối nguy này có thể xảy trong hai trường hợp:

1. Tài liệu bị tịch thu với trát lệnh của tòa án.
2. Tài liệu bị tịch thu trái với luật pháp bằng vũ lực.

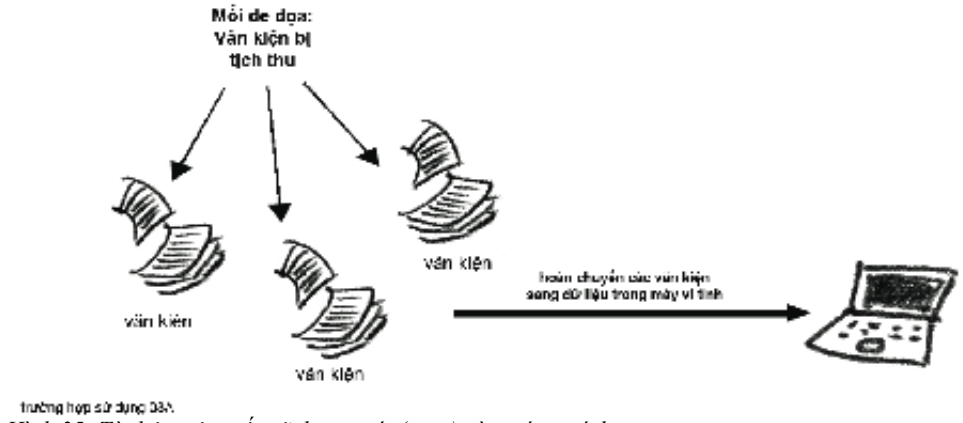
Bất cứ trong trường hợp nào, kết quả cũng sẽ như nhau và tài liệu cần phải được bản toàn để cả hai trường hợp sẽ không xảy ra. Tổ chức phi chính phủ này không những phải bảo toàn các tài liệu này mà còn phải bảo đảm họ sẽ giữ được mọi chi tiết về vụ kiện để có thể tiếp tục làm việc. Họ đã liệt kê tất cả những yếu điểm của tổ chức nhằm giúp cho họ biết cần phải quan tâm thêm về những lĩnh vực nào.

- Ghi nhận những vụ kiện với tài liệu chỉ được lưu trữ trên giấy tờ sẽ không an toàn.
- Máy điện toán không hoạt động vì bị nhiễm virút.
- Các phần mềm sử dụng lậu có thể sẽ được sử dụng làm lý do tịch thu máy điện toán.
- Dữ liệu chứa trong các máy điện toán có lẽ sẽ không được an toàn, tin tặc có thể đột nhập.
- Không có hệ thống sao chép và lưu trữ bản phụ của những tài liệu, văn kiện liên quan đến các vụ kiện đã bị tịch thu hoặc bị mất.

GIẢI PHÁP

Tiếp cận thông tin

Tổ chức đã quyết định nhằm để loại trừ nguy hiểm đem đến khi thông tin chỉ được lưu trữ trên giấy tờ, chúng sẽ được chuyển vào máy tính. Tất cả các giấy tờ đã được lưu trữ trong dạng điện tử sẽ bị hủy bỏ, khi cần có thể in ra sau.



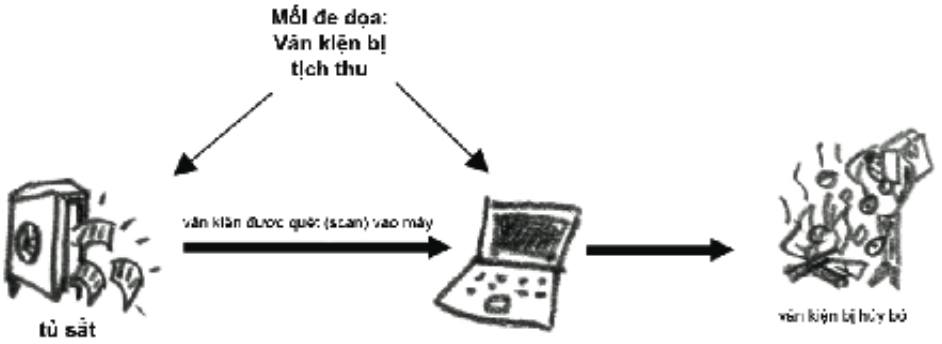
Hình 35: Tài liệu trên giấy sẽ được quét (scan) vào máy vi tính

Những tài liệu hiện đang được lưu trữ trong dạng giấy in cần phải được giữ an toàn trong lúc chúng được chuyển dần vào máy điện toán. Vì lý do này, họ sẽ mua một tủ sắt và khóa tất cả các tài liệu chưa được sao chép sang dạng điện tử vào trong tủ sắt đó. Các tài liệu này sẽ bị hủy bỏ sau khi được chuyển sang dạng điện tử. Cách hữu hiệu nhất để hủy bỏ giấy tờ là dùng lửa đốt cháy.

Máy tính

Tổ chức này cũng đã quyết định rằng máy điện toán của họ đã quá cũ và có thể sẽ không đủ khả năng chứa đựng một số dữ kiện nhiều như thế. Sau khi tìm kiếm trên mạng và trao đổi với bạn bè, họ thấy rằng cần phải mua một ổ cứng di động (removable drive) với

khả năng chứa được nhiều dữ liệu. Cần thiết nhất là một ổ cứng tiện lợi có thể gắn vào bất cứ máy điện toán nào. (thiết bị ổ cứng USB không cần điện là tiện nhất).

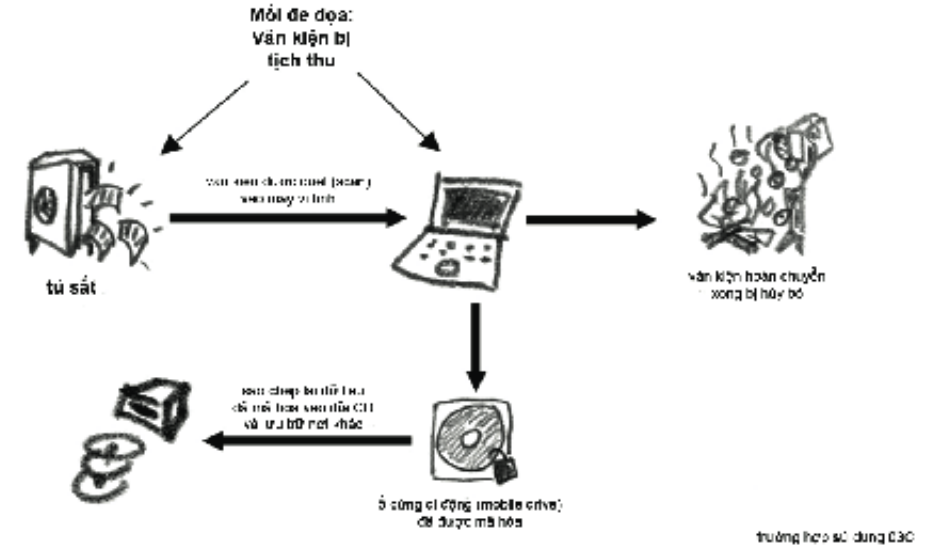


Hình 36: Lưu trữ văn kiện trong tủ sắt và hủy bỏ sau khi hoán chuyển vào máy

Để bảo vệ dữ liệu được chứa trong máy tính, tổ chức này cũng đã sử dụng hình thức mã hóa (encryption). Mặc dù không ai biết cách mã hóa tài liệu, họ có thể sử dụng một phần mềm trong Hộp Đồ Nghề An Ninh Kỹ Thuật Điện Tử. Phần mềm TrueCrypt có khả năng mã hóa toàn bộ ổ cứng mà không ai có thể sử dụng được nếu không có mật mã. Tổ chức phi chính phủ này đã quyết định mã hóa cả ổ cứng di động bằng phần mềm TrueCrypt. Nếu ổ cứng di động này bị tịch thu, dữ kiện chứa trong đó sẽ không ai đọc được.

Vì tất cả tài liệu được gom về chứa trong một thiết bị, cần phải lập một bản sao để phòng khi thiết bị chính bị tịch thu hoặc hư hỏng. Thiết bị của bản sao sẽ là một máy sao chép dĩa DVD. Mỗi ngày, tài liệu lưu trữ trong ổ cứng di động sẽ được sao chép lại trong dĩa DVD và được cất ở một nơi khác. Vì dữ liệu trong ổ cứng đã được mã hóa, chúng sẽ vẫn ở trong dạng mã hóa khi được sao chép vào dĩa DVD.

Một máy quét ảnh (scanner) sẽ được sử dụng để chuyển tài liệu từ dạng giấy in sang dạng điện tử. Tổ chức này dự đoán một nhân viên sử dụng một máy quét ảnh có thể quét (scan) khoảng 100 trang mỗi ngày. Nếu đúng như vậy, quá trình hoán chuyển



Hình 37: Ngăn ngừa dữ liệu điện toán bị mất bằng hệ thống sao chép và lưu trữ bản phụ

tài liệu từ dạng in sang dữ liệu điện tử sẽ được hoàn tất trong vòng 2 tuần.

Phần mềm

Tổ chức phi chính phủ này cũng quyết định mua một bản hợp pháp của Windows XP phiên bản sử dụng trong gia đình (WinXP Home Edition). Lý do là để cho mọi phần mềm thuộc quyền sở hữu trí tuệ cài trong máy điện toán có thể sử dụng một cách hợp pháp. Thay vì sử dụng bản sao chép lậu của phần mềm MS Office, họ chọn sử dụng phần mềm OpenDisk và Open Office cùng với lập trình GIMP để quét (scan) tài liệu trên giấy. Tất cả những phần mềm cần thiết như phần mềm phòng chống virus, tường lửa, mã hóa, và sao chép DVD đều có trong Hộp Đồ Nghề và hoàn toàn miễn phí vì chúng là những phần mềm lập trình mở (open source). Do đó, tổ chức phi chính phủ này không thể bị trở ngại pháp lý với tội danh sử dụng các phần mềm bất hợp pháp.

Những phản ứng cụ thể trước các mối đe dọa

Phần cứng: Một nhân viên đảm trách chuyến đi đến thành phố để mua về một máy scan, một ổ cứng di động và một ổ DVD. Những thiết bị này thuộc dạng trứ danh, đắt tiền và có mặt hầu hết khắp nơi trong các cửa tiệm kinh doanh vi tính. Cụ thể những thiết bị này gồm một cái máy scanner hiệu A4 trị giá 150USD, ổ cứng di động 100 gigabyte với giá 250USD, và một thiết bị làm DVD 250USD.

Phần mềm: một bản Microsoft Windows XP Home edition đáng giá 96USD tại các cửa tiệm buôn bán vi tính. Người nhân viên muốn biết cửa hàng này có cử một kỹ thuật viên để lắp đặt tất cả những phần cứng và mềm hay không. Người nhân viên được biết rằng muốn có một kỹ thuật viên đảm nhận chức vụ này họ cần phải trả 100USD. Phụ tùng an toàn kỹ thuật được đặt trên trang mạng http://orders.ngoinabox.org. Hộp phụ tùng này còn bao gồm cả hình tròn mở đĩa (OpenDisc).

Sau đó kỹ thuật viên lắp đặt một bản Windows XP mới in trong máy của bạn và xóa đi hết những dữ liệu cũ. Đây là một phương thức lý tưởng để dẹp hết những con vi-rút và những sự lỗi đã từng hiện diện trong máy. Đồng thời anh ta không quên gắn vào thiết bị viết DVD,

Phần mềm	Công năng	Nguồn
Open Office	Word processing, spreadsheets, presentations, database (hoàn toàn phù hợp với những dữ kiện Microsoft Office)	Hình tròn mở
GIMP	Tu sửa và scan hình ảnh	Hình tròn mở
Avast 4	Phòng chống virus	Phụ tùng an toàn kỹ thuật
Comodo (máy Internet)	Tường lửa	Phụ tùng an toàn kỹ thuật
TrueCrypt (máy dành cho dữ liệu)	Mã hóa đĩa	Phụ tùng an toàn kỹ thuật
DeepBurner (máy dành cho dữ liệu)	Phần mềm được dùng để chép DVD	Internet

máy scan và ổ cứng di động. Sau đó anh ta lắp đặt những phần mềm được liệt kê dưới đây:

Cài mã: Chương trình TrueCrypt là một chương trình chuyên mật mã hóa ổ đĩa cứng di động và cho phép nó được sao chép lại trong đĩa DVD sau khi mọi hoạt động đã hoàn tất. Người

nhân viên liền thiết lập một khối lượng TrueCrypt trong ổ đĩa cứng di động nặng 4 gigabyte (đi đôi với lưu lượng của đĩa)

Người duy nhất có thể biết được mật mã của phần đã được mã hóa là người nhân viên đảm trách mật vụ. Mật mã này sẽ được sử dụng một lần nữa để mở ra bộ phận được mã hóa trong DVD. Mật mã này gồm 12 ký tự và gồm cả số lẫn chữ. Một khi những người cần truy cập phần được mã hóa đã thuộc lòng mật mã, họ sẽ không cần phải viết nó xuống nữa.

Dự trữ: Vào cuối ngày, phần được tháo dỡ, nay đã chuyển thành một dạng tài liệu, được chép vào một chiếc DVD. Tốt hơn hết bạn nên chép lại tất cả nguyên bản của dữ liệu (bạn sẽ cần phải mua về những bộ phận ghi DVD và những chiếc đĩa DVD sao chép).

Đĩa DVD dự bị này sẽ được cất giữ trong nhà của một trong những người nhân viên thi hành công vụ. Cứ đến cuối tuần bạn sẽ làm một bản dự bị riêng và giữ nó tại một nơi bí mật. Đây là một phương pháp dự trữ bổ sung, phòng khi ổ đĩa cứng và những bản dự trữ hằng ngày bị tịch thu đi mất.

Ngân Khoảng Để Chi Tiêu:

Máy scan A4	150 USD
Ổ đĩa cứng di động	250 USD
Thiết bị chép DVD di động	250 USD
10 chiếc đĩa DVD sao chép	50 USD
Microsoft Windows XP	96 USD
Những dịch vi tính	100 USD
Két sắt	300 USD
Tổng cộng:	**1,145 USD**

Bạn còn một khoản tiền nhỏ trong ngân quỹ, phòng khi bạn cần mua thêm máy in hoặc vài chiếc đĩa DVD.

Điểm ích lợi của hệ thống này nằm ở chỗ nó gia tăng an toàn cho những tài liệu được thu thập bởi NGO. Sau khoảng thời gian đầu khi bạn đã thành công kỹ thuật hóa các văn kiện bằng giấy, tin rằng sẽ không còn dữ liệu nào có thể được tiếp cận bởi kẻ lạ. Tất cả các tập tài liệu sẽ được chuyển giao từ máy này sang máy khác. Vì thế nên cho dù tất cả các thiết bị có bị tịch thu hay chịu tổn thất, nhân viên vẫn còn một bản DVD dự trữ và một máy vi tính khác với chương trình TrueCrypt được gài sẵn. Dĩ nhiên là phải có một người biết mật mã của chiếc máy này!

4.4 TRƯỜNG HỢP NGHIÊN CỨU IV BẢO TOÀN EMAIL VÀ BLOG

4.4

Sơ Lược

Có một nhà làm báo tự do đảm trách nhiệm vụ báo cáo về những vi phạm nhân quyền trong đất nước của cô ta. Nhà báo này chuyên dùng một chiếc máy cầm tay để làm việc ở nhà và đồng thời cũng thường đem theo để hoàn thành công tác. Cô ta chủ yếu làm việc cho những nhà xuất bản nước ngoài và sử dụng bút hiệu thay vì tên thật, bởi vì việc công bố thông tin về quốc gia của cô ta là một việc khá nguy hiểm, nhất là khi giới truyền thông cũng như báo mạng trong quốc gia của cô luôn bị kiểm duyệt nghiêm ngặt bởi chính quyền. Những bài viết của cô ta thường được đăng tải trên blog.

Cô cảm thấy việc tiếp tục công việc càng lúc càng trở nên khó khăn. Những bài viết cô ta gởi qua email không đến nơi người nhận, cô không thể truy cập vào blog, và cô ta rất sợ sẽ gây nguy hiểm tới những người được phỏng vấn và đề cập tới trong hồ sơ. Cô ta rất lo sợ không biết chừng nào email của mình sẽ bị kiểm soát. Bất chợt một hôm chủ bút biên thư cho cô và tỏ ra hoảng hốt khi độc xong nội dung của một bài viết cô vừa đăng tải. Sau khi đọc lại, cô nhận ra rằng bài viết này đã bị thay đổi bởi một người nào đó trong quá trình nó được chuyển tới từ email cho đến tòa soạn.

Những mối đe dọa

Trước khi quyết định phải nên hành động ra sao, cô ta nêu rõ những mối đe dọa hiện nay:

- không thể gửi bài viết qua email
- không thể truy cập blog và cập nhật thông tin mới
- có người gây hại đến lý lịch tạm thời
- những bài viết trong lap top vào tay người ngoài
- những con virus hoặc hacker có thể hủy hoại những bài viết trong lap top

GIẢI PHÁP

Bảo đảm an toàn cho email

Như một việc làm tiền đề, cô ta quyết định bảo toàn hộp email làm sao cho những tin nhắn không thể bị đọc lén hoặc thay đổi bởi một người lạ. Cô ta gửi mail cho security@ngoinabox.org và xin họ cung cấp những mã truy cập cần thiết để đăng ký một tài khoản email mới qua RiseUp. Đây là một tài khoản webmail chỉ có thể được truy cập khi cô ta hoạt động trên mạng. Webmail này hoạt động thông qua SSL và được cài mã từ máy vi tính cho đến chủ máy webmail của cô ta. Cô ta đề nghị những người đồng nghiệp (những người nhận email) nên đăng ký một tài khoản miễn phí trên http://mail.riseup.net, để rồi những bài viết sẽ đến nơi họ thông qua đường hầm Internet đã được mã hóa. Cô ta tin

rằng những người sử dụng RiseUp này sẽ không gây hại đến hoặc truy cập vào email của cô.

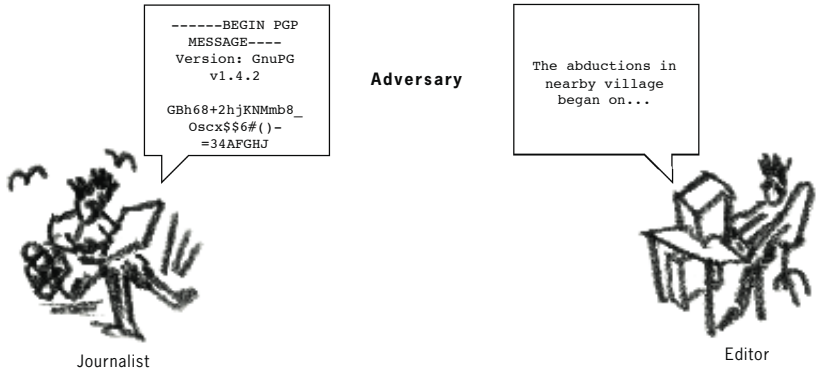
Đây có vẻ như một phương thức đơn giản và hiệu quả nhằm giảm đi những âu lo của cánh nhà báo. Chỉ cần có 'https:' xuất hiện trong thanh điền địa chỉ web, cô ta biết rằng hoạt động chuyên chở thông tin của mình được đảm bảo an toàn.

Để bước thêm một bước đảm bảo an toàn cho mình, cô ta gửi mail cho RiseUp và yêu cầu họ cung cấp vân tay chứng chỉ SSL. Họ chuyển cô tới một trang mạng có trình bày dấu vân tay. Cô ta đặc biệt lưu ý tới sự tấn công mang tính người-đứng-giữa-cuộc, trong đó kẻ thù đã ngăn chặn đường dây chuyển tới https://mail.riseup.net và cố tình gạt người sử dụng để cho họ nghĩ rằng họ đã thành công truy cập vào trang mạng mong muốn. Một bảng chứng nhận SSL được trình bày và một khi người sử dụng chấp thuận, họ được đem trở về trang mạng của kẻ thù. Tuy nhiên, chỉ cần nghiên cứu kỹ chứng chỉ SSL bạn hoàn toàn có thể biết được trang mạng này có khác với trang mạng chính thức hay không.[79]

Đảm bảo an toàn cho thông tin

Mặc dù cô ta đã thành công trong việc đảm bảo an toàn cho email, cô ta vẫn mong muốn những bài viết mình gửi đi sẽ không lọt vào nhận thức của ai ngoài người cô ta muốn gửi. Điều này có thể xảy ra trong trường hợp bị mất mật mã hoặc mật mã bị hủy hoại. Đây cũng là một bước đi an toàn để chống lại những trò tấn công dạng người-đứng-giữa-cuộc. Cô ta lắp đặt chương trình email Thunderbird và sắp đặt để cho phép cô đọc được tài khoản RiseUp. Cô ta thêm vào phần Enigmail mở rộng đến Thunderbird và làm theo chỉ dẫn trong Bộ Phụ Tùng An Toàn Kỹ Thuật để tạo nên một đôi khóa chung cô ta sẽ dung để cài mã cho những bài viết sang khóa công khai của người chủ bút1. Tất cả những đối tượng mong muốn giao lưu một cách an toàn với nhau khi dùng chế độ mật mã hóa khóa công khai cần phải lắp đặt phần mềm cần thiết và trao đổi khóa công khai với đối phương.[80]

Có đôi khi việc sử dụng mật mã hóa sẽ báo động đến phần chính đang được điều khiển. Cô ta không biết cài mã có phải là một hoạt động hợp pháp trong nước hay không và khi sử dụng nó khả năng thu hút sự chú ý không mong muốn là bao nhiêu. Cô ta quyết định dùng một phương pháp thay thế không lập



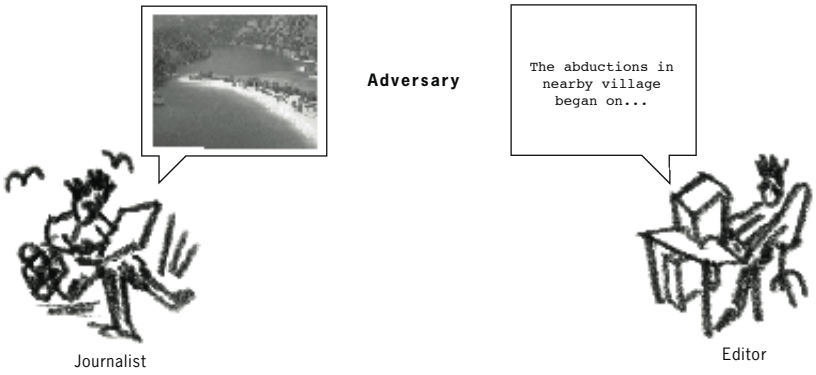
► Using **encryption** to secure sent messages

Ảnh minh họa 39: Cài mã để đảm bảo an toàn cho những tin nhắn đã gửi

79
For more info see chapter 'Encryption on the Internet'.

80
Thêm chi tiết, xem chương 'Mã hóa". Để download chương trình GnuPG, xem trang http://www.gnupg.org hay xem NGO in a Box – Security Edition CD.

tức khơi gợi sự nghi ngờ của người khác. Bằng cách sử dụng chương trình điện toán, cô ta có thể dính kèm một hình ảnh cùng với bài viết và đăng nó lên một trang mạng bí mật. Phương pháp này thật có thể qua mặt nhiều hệ thống quản đốc, chỉ cần bằng một cách nào đó người chủ bút có thể biết trước được tấm hình và bài viết này ở đâu. Phương pháp này nên được áp dụng bằng cách giữ đều một xu hướng hoạt động(đăng tải hình lên mạng) và không nên tách ra khỏi đường hướng hoạt động thông thường này.



►Using **steganography** to hide the presence of a message in your communications

Ảnh minh họa 40: Sử dụng điện toán để giấu đi tin nhắn trong các hoạt động truyền thông

Email nặc danh

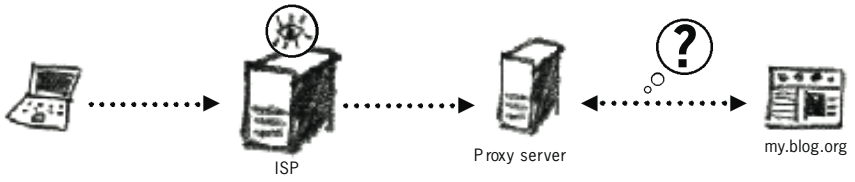
Một phương pháp khác để phòng ngừa sự ngăn chặn email và kiểm duyệt là sử dụng hàng loạt những dịch vụ webmail miễn phí chẳng hạn như Yahoo, Hotmail, Gmail—những website có hàng triệu người sử dụng. Bạn có thể đăng ký một tài khoản mail mới cho mỗi một email bạn gửi. Các chi tiết đăng ký có thể được điền vào một cách tùy tiện và nếu như bạn gửi email từ một nơi công cộng (quán café Internet), email này sẽ rất khó bị theo dõi hoặc kiểm duyệt.

Rất có thể những dịch vụ email an toàn (như RiseUp) sẽ bị ngăn chặn hoặc sẽ bị ngăn chặn trong trường hợp nó được sử dụng thường xuyên. Có một vài quốc gia cho phép ngăn chặn những hệ thống email miễn phí có quy mô lớn như Yahoo. Tuy nhiên, những dịch vụ quốc tế này đã từng hợp tác với chính phủ (chính phủ Trung Quốc chẳng hạn) để ban cho họ quyền hạn truy cập vào những trương mục email của người sử dụng. Nếu như cô nhà báo của chúng ta quyết định sử dụng email từ nhà cung cấp lớn, tốt nhất rằng cô ta nên truy cập vào nó từ một quán café Internet hoặc một nơi công cộng nào đó, nơi mà những chi tiết về cá nhân cô ta và hoạt động cũng như địa chỉ IP sẽ không vào bị lưu vào lược sử, và do đó không thể bị truy lùng. Cô ta còn có thể dùng tên giả khi mở trương mục, tuy nhiên điều này cần phải được sắp đặt trước với chủ bút.

Tránh khỏi tình trạng bị ngăn chặn trang mạng

Để có thể truy cập blog của mình, cô nhà báo này cần có nhiều biện pháp khác nhau để chống lại những nỗ lực ngăn chặn Internet trong nước của

cô ta. Còn về phải chọn công cụ kỹ thuật nào để thực hiện điều này tùy thuộc vào đường lối ngăn chặn của chính phủ. Cô ta có thể đăng ký để nhận được tin tức mới cập nhật về loại proxy nặc danh mà không có khả năng kiểm duyệt thông tin từ Peacefire1 hoặc yêu cầu một người bạn chung sống cùng nước sắp đặt Psiphon (xem chương 2.6 để có thêm chi tiết).



►With an anonymous proxy, the destination website will not know where your computer is really located

Ảnh minh họa 41: Bằng một proxy nặc danh, website bạn muốn truy cập sẽ không thể nào biết được vị trí của chiếc máy bạn đang dùng.

Bằng một biện pháp thay thế, cô ta lắp đặt chế độ trình duyệt Tor1 vào trong ổ flash USB, để có thể hoạt động mà không cần phải bị ngăn chặn. Trình duyệt Tor sẽ bảo mật các yêu cầu trên mạng của cô ta và có khả năng xuyên qua đa số các hệ thống kiểm duyệt trong nước.

Thường thường sẽ dễ dàng và thực tế hơn nếu bạn nhờ một người bạn nào ở trong nước đăng tải những bài viết của bạn trên blog. Những bài viết này có thể được chuyển bằng email an toàn.

Bảo vệ danh tánh

Hiện thời nhà báo này không muốn danh tánh của mình có dây mơ rễ má với bút hiệu. Cô ta cẩn thận không tiết lộ tên thật của mình trong email hoặc những bài viết được gửi qua Internet. Cô ta đồng thời cũng không sử dụng tài khoản email ISP vì nó được kết nối trực tiếp với cô ta. Cô ta chỉ sử dụng máy ở nhà để truy cập Internet và vào tài khoản webmail an toàn hoặc sử dụng một công cụ nặc danh để cập nhật blog để thực hiện những điều này.

Có những quán café có Internet tại nơi cô ta ở đã bắt đầu ghi lại tên những người sử dụng và giờ truy cập. Cô tạm né tránh những quán café này vì những hoạt động trên mạng cũng như email có thể được lần qua IP và truy đến cô ta.

Khi sử dụng máy ở quán net, cô ta vô cùng cẩn thận làm sao cho trình duyệt web không thể ghi lại tên và mật mã vào trong lược sử. Trước khi đến phiên mình sử dụng máy, cô ta dành một ít phút thiết lập cho trình duyệt Internet trở nên an toàn hơn và xóa đi mọi thông tin được lưu trữ trong máy sau khi đã hoàn tất công việc.

Bảo toàn laptop

Tất cả các bài viết đều được viết và lưu trữ trong máy laptop. Cô ta cần phải bảo vệ bản thân mình trước những mất mát, những bài viết không phải do chính mình viết và tổn thất được gây nên bởi virus và phần mềm gián điệp. Cô ta làm một mật mã BIOS để đề phòng người khác truy

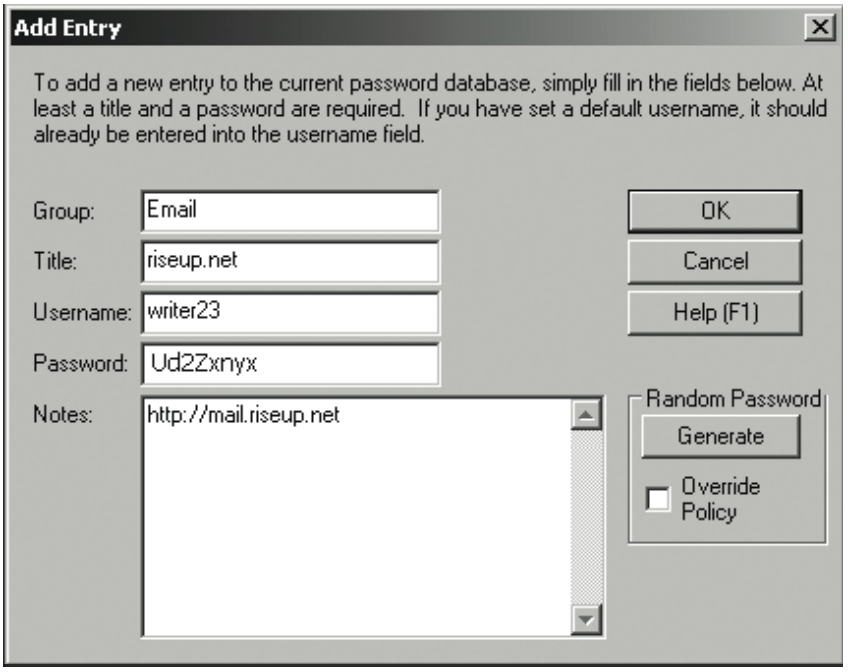
cập trực tiếp vào trong máy và lắp đặt những chương trình chống virus, chống phần mềm gián điệp và chương trình tường lửa từ Bộ phụ tùng an toàn kỹ thuật. Cô ta nâng cấp phần mềm Windows một khi có được những chỉnh sữa mới. Sẵn laptop cô ta đã có một ổ CD, cô ta mua thêm nhiều chiếc đĩa trống và tạo nên nhiều tài liệu copy dự trữ.

Mật mã

Laptop, BIOS, tài khoản email, blog, vv., của cô ta mỗi cái đều đòi hỏi phải có mật mã riêng. Những mật mã này thật cần thiết cho sự an toàn của cô ta, vì có những hệ thống an toàn hoàn toàn lệ thuộc vào sự vững bền của mật mã bảo vệ chúng. Bởi vì việc lưu nhớ tất cả các mật mã là bất khả thi, cô ta bèn sử dụng chương trình KeePass1 để lưu trữ những mật mã này. Cô ta có một bản copy của chương trình và tài liệu mật mã trong laptop cùng với ổ nhớ USB. Để gia tăng an toàn cho những mật mã này, chương trình KeePass đích thân tạo riêng một mật mã cho cô ta.

Tóm lại cô ta có rất nhiều nước bài và biện pháp để sử dụng một cách bí mật. Ban đầu có vẻ những chiêu thức này rất cực nhọc và tiêu hao nhiều thời gian, nhưng chí ít cô ta có thể bảo đảm an toàn tuyệt đối. Có lẽ một cái laptop và địa chỉ email an toàn sẽ có thể dư sức giúp cô ta tiếp tục hoàn thành suôn sẻ công việc. Tuy nhiên một khi những biện pháp bảo vệ này trở nên lỗi thời và không thể dùng được, cô ta sẽ phải chuyển sang những biện pháp mới. Internet là một không gian rất rộng với rất nhiều khả năng bị kiểm soát cũng như khả năng ẩn tánh.

► PasswordSafe



► Adding a new password entry

PHỤ LỤC A
GIẢI NGHĨA MÁY ĐIỆN TOÁN

A

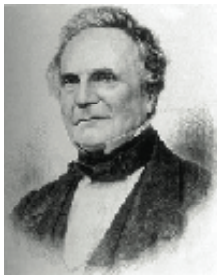
Hãy thử tưởng tượng trong tương lai sẽ có một thiết bị cá nhân, dạng một tài liệu hoặc thư viện cơ khí tư nhân. Nó cần một cái tên, và tạm thời ta có thể gọi nó là "memex". Memex là một thiết bị khi sử dụng cá nhân ta có thể trữ toàn bộ sách vở, kỷ lục, và các mối liên hệ, và được cơ khí hóa nhằm gia tăng tốc độ truy cập cùng với tính linh hoạt. Đây là một người bạn hỗ trợ gắn bó mật thiết với bộ nhớ của con người.

Nó bao gồm một cái bàn làm việc, và có thể được vận hành từ xa, và là một bộ phận trang bị cho phép ta hoạt động. Ở trên cùng là những màn che trong suốt, để chiếu những tài liệu nhằm tạo ích lợi cho việc tham khảo chúng. Rồi đây sẽ có một bàn phím với những cái nút và cần gạt. Chung quy, ngoài những đặc điểm đó ra, nó không khác gì một chiếc bàn làm việc bình thường.

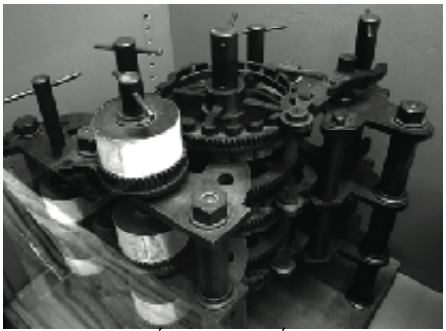
Vannevar Bush – Joint Research and Development Group, 1945

Lịch sử

Lý thuyết và phương trình toán học được dùng để chế tạo máy điện toán đã được thiết lập từ nhiều thế kỷ trước. Hệ nhị phân của số học (dùng '1' và '0' để thực hiện công thức số học) là phát minh của Gottfried Wilhem von Leibniz (1646-1716), người mà đồng thời đã cùng với Isaac Newton sáng chế phép tính. Charles Babbage cái tên lừng lẫy ấy đồng thời cũng là người sáng chế ra những phương thức tính toán khi xưa. Ông là người sáng tạo ra Cơ Cấu Phân Biệt và Phân Tích. Cơ Cấu Phân Tích sử dụng những tấm thẻ lỗ để đọc số nhập và số xuất, để làm sao cho sự tính toán vừa rồi có thể được giữ vào trong máy điện toán trong quá trình kế tiếp. Babbage miêu tả năm thành phần lôgic của cơ cấu này—thành phần dự trữ, thành phần máy cái, thành phần điều khiển, phần nhập và phần xuất (theo ngôn ngữ hiện đại: ổ cứng, đơn vị xử lý trung tâm (CPU), phần mềm, bàn phím/con chuột và màn hình). [81]



Charles Babbage (1791 – 1871)



1991 Sự tái thiết của Cơ Cấu Phân Biệt do Viện Bảo Tàng London Science thực hiện

George Scheutz, sau khi biết về Cơ Cấu Phân Biệt của Babbage, đã cùng con trai Edward chế tạo một phiên bản vi mô của nó. Đến năm 1853, họ đã chế tạo được một thiết bị có thể chế biến 15 chữ số và tính ra những khác biệt theo thứ tự số bốn. Cơ cấu của họ đã thắng giải vàng tại Triển Lãm Paris năm 1855, và họ đã bán nó cho Đài Thiên Văn Dudley ở Albany, New York, dùng để tính ra quỹ đạo của Hỏa Tinh. Một trong những nhà thương mại sử dụng những chiếc máy điện toán cơ khí đầu tiên là Cục Thống Kê dân số Hoa Kỳ. Họ đã sử dụng thiết bị thẻ lỗ được thiết kế

81
http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians

bởi Herman Hollerith để lập bảng kê cho tổng điều tra năm 1890. Vào năm 1911, công ty của Hollerith đã sáp nhập với một đối thủ cạnh tranh nhằm tạo thành một tập đoàn mà vào năm 1924 đã trở thành IBM, International Business Machines.

Hiện nay

Máy vi tính cá nhân hiện đại đầu tiên được sử dụng có tên 'Simon' và được chế tạo bởi một số học sinh tại trường đại học Columbia. Tuy nó không được hữu dụng với tư cách một cơ cấu chế biến, nó đã trở thành nguồn cảm hứng cho những kiểu mẫu khác. Chiếc máy vi tính cá nhân thương mại đầu tiên là IMB 5150, được công bố vào năm 1981.

Không ai biết chính xác có bao nhiêu chiếc máy vi tính được sử dụng hiện nay. Theo cuộc họp giới báo chí năm 2002 do hãng tư vấn công nghệ cao Gartner Dataquest[82] tổ chức, "…một tỉ chiếc máy vi tính cá nhân đã được bán trên khắp toàn cầu." Chưa kể con số này loại trừ các nhà tổ chức tư nhân, điện thoại di động, đồ điều khiển video game và một loạt những thiết bị đã trở nên quá quen thuộc trong cuộc sống hằng ngày của chúng ta. Xe hơi và đèn giao thông hiện nay đang được vận hành bởi máy vi tính, cũng như máy bay và dự báo thời tiết. Máy vi tính phát ra và lưu trữ âm nhạc, kiểm tra chính tả cho dữ liệu và trù bị thức ăn. Một hiện tượng tương tự truyện khoa học viễn tưởng 60 năm về trước nay đã trở thành một phần quen thuộc trong cuộc sống.

Máy vi tính ngày một trở nên nhỏ và tiện nghi hơn (trong khi vẫn không ngừng hoạt động nhanh chóng và lưu trữ được nhiều thông tin). Những chiếc máy vi tính cá nhân bình quân có thể thực hiện một tỉ hoạt động trong vòng một giây và lưu trữ được nhiều dữ liệu không thua gì một thư viện.

Máy điện toán vận hành ra sao?

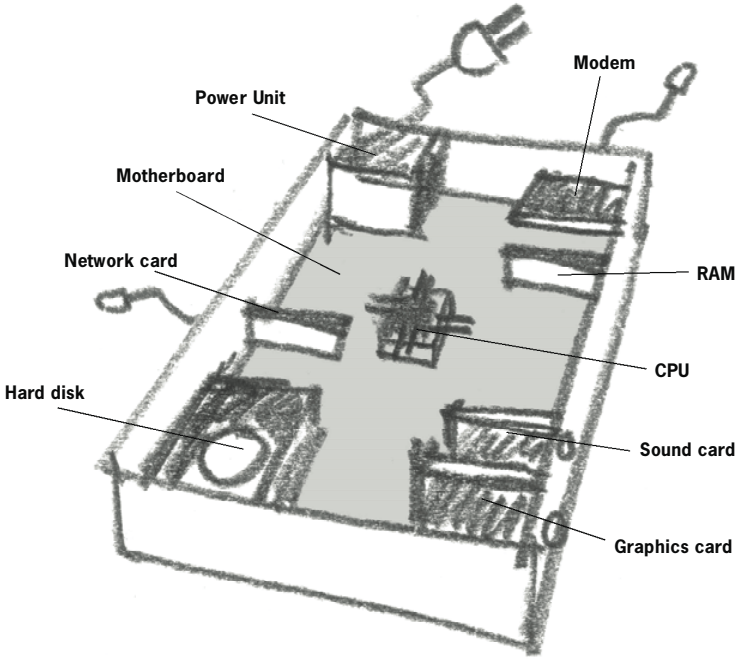
Dưới đây là lời miêu tả (cùng với biểu đồ) về những thành phần cốt yếu của một chiếc máy vi tính.

1. Đơn vị năng lượng—dự trữ và điều chỉnh dòng điện được chuyển tới máy. Máy cầm tay cũng có một nguồn năng lượng dự trữ trong pin.
2. CPU-Đơn vị xử lý trung tâm. Thực hiện những hoạt động của máy điện toán. Đây là một loạt những phương thức hoạt động toán học và lôgic được thực hiện ở một tốc độ cao. Một khi CPU bắt đầu nóng lên, nhiệt độ của nó cần phải được hạ xuống bởi một chiếc quạt.
3. Đĩa cứng—Đây là nơi lưu giữ những dữ liệu trong máy điện toán. Thường nó mang dạng một chiếc đĩa nam châm xoay chuyển. Thông thường ổ cứng rất nhạy cảm với từ trường, thành thử nó cần một vỏ bọc bảo vệ thật bền bỉ.
4. RAM – Bộ nhớ truy cập ngẫu nhiên. Đây là một đơn vị lưu trữ những dữ liệu bạn đang dùng tới. Khi bạn kích hoạt một chương trình, chẳng hạn như Microsoft Word, máy ví tính sẽ sao chép lại chương trình đó từ một chiếc đĩa cứng đến RAM. Khi bạn viết một tài liệu, nó cũng được lưu trữ trong RAM. Bằng cách lựa chọn 'save' dữ liệu này, bạn đã chuyển nó tới đĩa cứng.
5. Bộ mạch chủ - Một phần toàn bộ của máy điện toán cho phép tất cả những thiết bị tiếp xúc với nhau.
6. Card màn hình – chịu trách nhiệm trình bày thông tin trên màn ảnh.

82
Theo Gartner, số bán của năm 2005 là 285 triệu PCs and notebooks trên toàn cầu. Năm 2008 số bán sẽ lên tới 1 tỷ PCs. Nguồn:
http://news.bbc.co.uk/2/hi/science/nature/2077986.stm

và:
http://www.dailytimes.com.pk/default.asp?page=2006%5C01%5C23%5Cstory_23-1-2006_pg6_1

7. Card âm thanh – chịu trách nhiệm cho những âm thanh trong và ngoài máy.
8. Card mạng – chịu trách nhiệm kết nối đường dây mạng. Chỉ cần mạng bạn đang dùng có Internet, bạn có thể lên mạng thoải mái.
9. Modem – Nối đường dây mô hình điện thoại vào máy điện toán. Các thể loại gồm có ADSL và modem điện tử. Những thể loại này có thể được sử dụng để nối mạng với máy điện toán.
10. Màn hình – trình bày trên màn ảnh thông tin đến từ máy điện toán.
11. Bàn phím và con chuột – cho phép bạn nhập dữ liệu vào trong máy điện toán.



Bây giờ chúng ta sẽ nói tới chức năng vận hành của máy điện toán:

1 – Khi bạn kích hoạt một chương trình xử lý chữ và bắt đầu viết một tài liệu.

CPU --> tìm chương trình trong ổ cứng và chép nó vào trong RAM --> card màn hình trình bày chương trình trên màn ảnh --> bạn bắt đầu viết tài liệu và chọn 'save' nó --> tài liệu được sao chép từ RAM tới ổ cứng.

2 – Khi bạn kiểm tra và in ra email

CPU --> tìm chương trình duyệt web trong ổ cứng và chép nó vào trong RAM --> modem kết nối vi tính với www.riseup.net --> bạn đánh vào mật mã --> email được trình bày trên màn ảnh --> email được chép vào trong RAM --> bạn chọn 'in ra' --> bản mẹ tiếp xúc với máy in --> tài liệu đã được in.

Lưu ý: email của bạn đã được sao vào trong máy vi tính, mặc dù bạn không chọn lựa 'save' nó. Giờ đây bạn đã có một bản sao trong RAM. Đây là cách vận hành thông thường của máy vi tính, và nó cần phải được lưu ý tới khi truy cập hệ thống an toàn của máy (tham khảo những chương "An Toàn Windows' và 'Dự trữ dữ liệu, Phá hủy và Lấy lại').

Một chiếc máy vi tính đòi hỏi phải có tốc độ và lưu lượng. Sau đây là hướng dẫn sơ bộ

về các đơn vị đo lường tốc độ và lưu lượng của máy vi tính:

Ví dụ như ký tự 'A' đòi hỏi 1 byte lưu lượng.

```
        8 bits = 1 byte (B)
   1024 bytes = 1 kilobyte (kB)
1024 kilobytes = 1 megabyte (MB)
1024 megabytes = 1 gigabyte (GB)
1024 gigabytes = 1 terabyte (TB)
```

Lưu ý: đơn vị đo 1024 là kết quả của sự tính toán từ hệ số của 2. Quy định toán học này thật sự cần thiết cho một hệ thống kỹ thuật.

Cứ coi như mỗi một hoạt động vi tính một giây được gọi là hertz,

```
   1000 hertz = 1 kilohertz (kHz)
1000 kilohertz = 1 megahertz (MHz)
1000 megahertz = 1 gigahertz (GHz)
```

Vậy thì một chiếc máy vi tính với tốc độ 1.3GHz/giây có thể thực hiện 1,300,000,000 hoạt động mỗi giây. Chỉ với điều này thôi chiếc máy vi tính của ta đã nhanh hơn 'Si-mon' rất nhiều.

Các Hệ Thống Vận HànhTrong Máy Vi Tính (Operating System)

Tất cả các máy điện toán đều cần những sự chỉ dẫn để làm việc. Những nguồn chỉ dẫn chính, nhịp cầu nối những tất cả những bộ phận của máy điện toán, các chương trình ứng dụng và chúng ta - người sử dụng – là một hệ điều hành (operating system, OS).

Bạn có thể đã nghe đếnWindows, là hệ điều hành thông dụng nhất, được sản xuất bởi Microsoft. Sự phổ thông của nó là kết quả của của những cửa sổ hình ảnh dể hiểu, những giao kèo thành công với những nhà sản xuất máy điện toán và những chiến lược tiếp thị quyết liệt.

Nhiều phiên bản Windows đã được sản xuất. Khi bạn mua một máy điện toán, Windows có thể đã được cài sẵn trong máy rồi. Hệ điều hành Windows không miễn phí cho nên bạn phải có một giấy phép xử dụng. Đây không phải là trường hợp của mọi máy điện toán: rất nhiều máy có những phiên bản Windows 'đánh cắp' một cách bất hợp pháp. Nhiều người sử dụng máy điện toán và dân chuyên nghiệp không thích Windows vì các chiến lược tiếp thị của nó, những ứng dụng không hoàn hảo và việc độc quyền thị trường. Một số những người này cố khám phá những nhược điểm trong hệ điều hành hoặc là cảnh báo Microsoft để sửa sai hoặc tạo ra virus, lợi dụng vào những điểm sơ hở này, làm hư hỏng các dữ kiện trên máy điện toán và làm máy bị nhiễm virus.

Có nhiều cách khác nhau để thay thế cho hệ điều hành Windows. Thí dụ, công ty Apple có hệ điều hành riêng của nó. Rồi còn có Linux, là một hệ điều hành miễn phí mà đã trở nên rất thông dụng nhờ vào sự phân phối rộng rãi của nó trên Internet.

Linux được lập trình bởi rất nhiều người khác nhau mà không được trả lương bởi bất cứ công ty nào. Một sản phẩm của việc tham gia tình nguyện bởi nhiều chuyên viên, nó được phát hành miễn phí. Rất nhiều phiên bản khác nhau (gồm cả ngôn ngữ khác nhau) của Linux đã được đưa ra thị trường, và phần lớn là miễn phí. Phiên bản thông dụng nhất và cũng được tranh luận là dễ sử dụng nhất là Ubuntu[83].

Phần mềm - Phần mềm sở hữu đối lại Phần mềm miễn phí

Một chương trình ứng dụng được xem như sở hữu trí tuệ của người tạo ra nó (giống như một quyển sách hay một chuyện phim) Một giấy phép để sử dụng nó được bán chung với một mật mã (password). Việc đánh cắp phần mềm, xâm nhập mật mã hay chỉ đơn giản như sử dụng phần mềm không có bản quyền, đã xảy ra rất nhiều trên thế giới. Rất nhiều chính phủ đã đưa ra luật lệ bảo vệ các chương trình phần mềm dưới đạo luật về quyền sở hữu trí tuệ. Những hình phạt nặng nề được đưa ra cho những cá nhân và các tổ chức bị bắt quả tang sử dụng các phần mềm không có bản quyền.

Không phải mọi chương trình ứng dụng đều có sự giới hạn của bản quyền như được nói ở trên. Chỉ vì bạn có thể tình nguyện thời gian và năng khiếu cho một mục đích không có lời hay nhân đạo nào đó, vài người viết phần mềm rồi phân phát một cách miễn phí. Loại phần mềm này thường được viết sử dụng mã nguồn mở. Điều này có nghĩa là phần mềm ứng dụng được công khai cho mọi người khám xét, sửa đổi và cải thiện. Những người tình nguyện phiên dịch phần mềm này thành ngôn ngữ của họ và tung ra không lấy tiền. Loại phần mềm này được mô tả như là FOSS - Phần Mềm Mã Nguồn Mở Và Miễn Phí. Bạn có thể tìm được rất nhiều loại phầm mềm này trên thị trường.

Với một chương trình phần mềm Microsoft Office có bản quyền, bạn sẽ tốn từ 200-500 đô la[84] một bản, trong khi OpenOffice (có thể lấy xuống từ www.openoffice.org) thì được phát miễn phí. Cả hai đều rất giống nhau về hoạt động và tính năng: chúng tạo ra các loại hồ sơ giống nhau. Những vấn đề về sự vận hành được liên thông giữa một phiên bản 95 và các phiên bản trước đó của Microsoft Office và Open Office đã được lưu ý. Giải pháp là phải thay đổi sản phẩm văn phòng của bạn và của những người đồng nghiệp mà bạn đang liên lạc thành một sản phẩm độc nhất. Điều này có thể không phải là việc dễ dàng, nhưng nếu bạn quan tâm đến sự hợp pháp của phần mềm của bạn, bạn nên lưu ý đến việc tránh xa các sản phẩm của Microsoft, nếu không thì phải mua bản quyền của họ.

FOSS (phần mềm miễn phí và công khai) sẽ giúp bạn tránh khỏi các vấn đề luật pháp về đánh cắp tài sản phần mềm. Mặc dầu FOSS có thể không dễ sử dụng (nói về cài đặt, hướng dẫn và hình ảnh về cảm nhận) trong việc giúp đỡ bạn với phần mềm hay cho sự giúp đỡ tương tự như là phần mềm được trả tiền, nó có một số lớn cộng đồng người sử dụng, và họ đã lập ra rất nhiều diễn đàn để trả lời các thắc mắc chung của bạn và sẽ trả lời bất cứ những vấn đề mới mẻ nào bạn đưa ra. Với cách này, bạn sẽ nhận thấy một mạng lưới giúp đỡ trả lời nhanh chóng và nhiều chi tiết trong cộng đồng nguồn mở hơn là sự giúp đỡ kỷ thuật tốn tiền và thường xuyên 'phải đợi' cho phiên bản mới nhất của Microsoft Windows[85].

83
http://www.ubuntu.com

84
Giá cả khác nhau được tìm thấy bằng cách truy cập trên Internet vào tháng Chín 2006.

85
Thêm chi tiết hãy xem Hội Cho Phần Mềm Miễn Phí http://www.fsf.org and the Open Source Initiative http://www.opensource.org

PHỤ LỤC B
GIẢI NGHĨA MÁY VI TÍNH

Lịch sử

Sáng kiến nối kết các máy điện toán với nhau trên các địa điểm khác nhau về địa lý nẩy sinh ra sau Đệ Nhị Thế Chiến. Trong khi các máy điện toán vẫn còn trong thời kỳ phôi thai, khái niệm này chỉ hiện hữu trong suy nghĩ của những nhà tương lai học và triết học. Nước Liên Xô khởi thủy chiếc phi thuyền 'Sputnik' làm cho chính phủ Hoa Kỳ phải đầu tư nặng nề vào sự tìm kiếm và phát triển kỹ thuật tin học. Cơ quan Đề Án Tìm Kiếm Cấp Cao (ARPA) được thiết lập vào cuối thập niên 60, và khoảng 1969 bốn máy điện toán đã được nối kết với ARPANET. Vào năm 1972, Robert Kahn đã trình bày thành công về ARPANET ở Phiên Họp Truyền Thông Máy điện toán Quốc Tế và giới thiệu một sự áp dụng mới đến lãnh vực này – email. Mạng lưới ARPANET là tiền thân của Internet như chúng ta biết và sử dụng ngày hôm nay.


Illustration 49: Robert Kahn

Vào năm 1977 ARPANET nối kết 111 máy điện toán, và khoảng 1985 hệ thống mạng này đã với đến Âu Châu và Úc Châu. Hệ thống Internet này trở thành toàn cầu và không-quân-sự. Năm 1983 đã thấy sự ra đời của TCP/IP phiên bản 4 – là một sự nối kết mà với nó bất cứ máy điện toán nào trên thế giới, bất kể nhãn hiệu hay mô hình nào, cũng có thể truyền thông được với nhau trên cùng một hệ thống mạng. Sự ra đời kỷ thuật này được xem như sự ra đời của của Internet. Robert Kahn phát triển Hệ Thống Kiểm Soát Chuyển Tin/Hệ Thống Internet với 4 nguyên tắc căn bản:

- **Sự kết nối mạng.** Bất cứ hệ thống mạng nào cũng đều có thể nối được với một hệ thống mạng khác.
- **Sự phân phối.** Sẽ không có một hệ thống điều hành mạng trung tâm hay kiểm soát.
- **Sự phục hồi các lỗi.** Những túi dữ liệu sẽ được chuyển trở lại.
- **Phương cách hộp đen.** Không có sự thay đổi bên trong nào sẽ được thực hiện trong một hệ thống mạng để nối nó với các hệ thống mạng khác.

TCP/IP phiên bản 4 vẫn còn là một phương pháp nối kết thông dụng nhất của Internet ngày nay. Mọi cấu trúc của nó đã, cho đến bây giờ, đảm bảo rằng không có một người nào hay công ty đặc biệt nào điều hành Internet, và rằng tất cả người sử dụng kết nối với Internet được cung cấp sự truy cập không giới hạn đến nội dung của nó (chúng ta đã bàn về kiểm duyệt và thanh lọc trên Internet trước đây).

Hệ thống Mạng Toàn Cầu

Cách phổ thông nhất của việc sử dụng Internet ngày nay là qua Mạng toàn cầu (WWW). Hệ thống Internet chính nó là sự nối kết thực sự của những máy điện toán với các hệ thống mạng máy điện toán, trong khi WWW là một hệ thống chuyên biệt cho những máy điện toán này liên lạc qua nó. Khái niệm và kỹ thuật học của WWW được phát triển bởi

Tim Berners Lee và Robert Cailliau ở phòng thí nghiệm vật lý nguyên tử Conseil Européen pour la Recherche Nucleaire (CERN) và được công bố vào năm 1991. Những đặc tính của WWW là:

- Những điểm nối – (hyperlinks) nối một trang mạng đến một trang khác
- Phương thức liên lạc – HTTP (hypertext transfer protocol) - một ngôn ngữ điện tử được xử dụng bởi các máy điện toán trên Internet.
- Các trang mạng – HTML (Hypertext MarkUp Language) được dùng để vẻ mẫu các trang mạng và đối thoại với nhau bằng các phương tiện điểm nối. Những ngôn ngữ phổ thông khác dùng để viết các trang mạng là PHP và JavaScript.
- Địa chỉ - URL (universal resource locator) - một hệ thống gởi thư cho việc tham chiếu các trang mạng và những thông tin khác trên Internet.

Cùng với nhau chúng tạo ra những viên gạch xây dựng nên hệ thống Internet ngày nay. Sự truyền thông giữa những trang mạng được thực hiện bởi TCP/IP.

Internet Ngày Nay

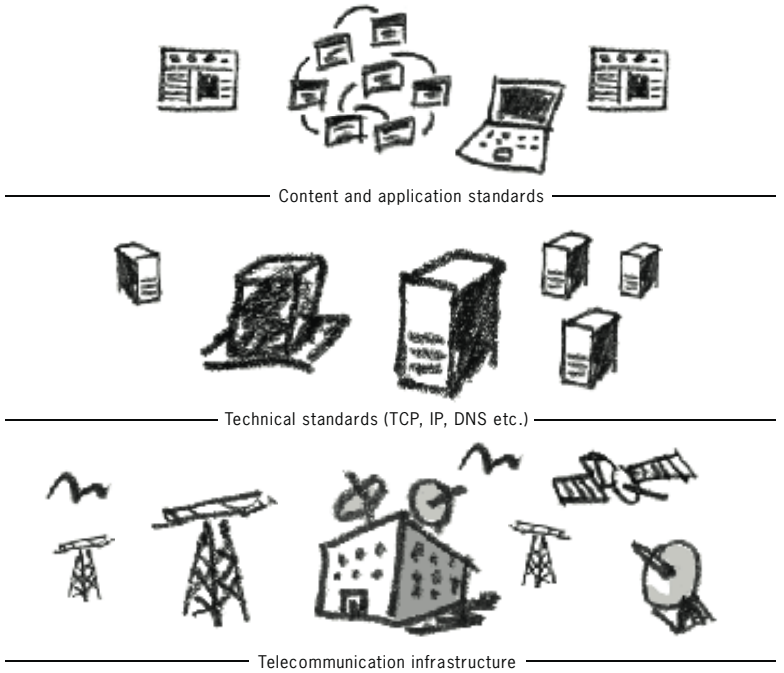
Theo như cuộc thăm dò của Thống Kê Internet, có trên 1 tỷ người sử dụng Internet trên toàn cầu trong tháng Giêng 2006. Đây là một con số kinh ngạc, so với việc không ai nghe về Internet vào năm 1990. Nó đã trở thành một phương pháp chính về lưu trữ và trao đổi thông tin cho nhiều người.

Một thí dụ gần đây về sức mạnh của Internet trên Wikipedia.org - một tự điển bách khoa trên mạng, với những bài viết được viết và sửa đổi bởi cộng đồng Internet. Chỉ trong 5 năm kể từ lúc nó ra đời, Wikipedia.org đã có 1 triệu 500 ngàn bài viết bằng tiếng Anh và ít nhất 100 ngàn trong 10 ngôn ngữ khác nữa. Sự phổ thông của nó dẫn đến một sự đánh giá độc lập của sự chính xác về thông tin của nó như được so sánh với Tự Điển Bách Khoa Britannica. Những kết quả cho thấy rằng cả 2 quyển tự điển này đều phỏng độ chính xác như nhau[86].

Cấu trúc hạ tầng căn bàn

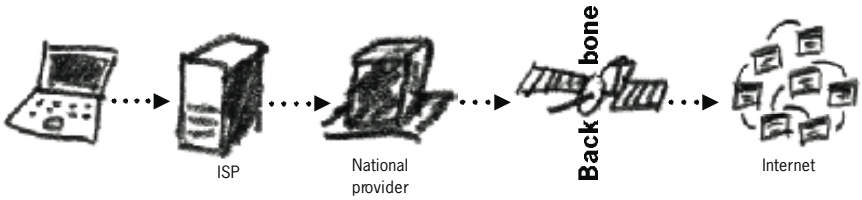
Hệ thống Internet là một hệ thống mạng được phân phối một cách toàn diện. Điều này có nghĩa là Internet không có cứ điểm trung ương hoặc một máy server. Tuy nhiên, internet áp dụng các tiêu chuẩn về phương diện điều hành (được gọi là nghi thức) cũng như những tổ chức phát triển những tiêu chuẩn này. Ngày nay Internet có 3 lớp vỏ bọc cho sự hoạt động của nó. Trước tiên, đó là cấu trúc hạ tầng truyền tin viễn thông. Là một sự kết hợp của các dây điện thoại, sợi quang, siêu sóng và vệ tinh - tất cả làm việc chung với nhau để đảm bảo sự lưu thông trên Internet được đi đến mọi ngỏ ngách trên thế giới. Cái vỏ bọc thứ nhì là các tiêu chuẩn và dịch vụ về kỷ thuật. Nó gồm có những nghi thức khác nhau, hướng dẫn sự lưu thông chung quanh cấu trúc hạ tầng và cho phép chúng ta thấy được các trang mạng và gởi email. Chính trên lớp vỏ bọc này mà chúng ta nối được vào Internet. Lớp vỏ bọc cuối cùng: nội dung và sự áp

86
http://news.bbc.co.uk/2/hi/technology/4530930.stm



dụng – là nơi mà tât cả các trang mạng và các dịch vụ vê Internet hoạt động. Một trong những sức mạnh của Internet là mỗi lớp vỏ bọc này đều hoạt động độc lập với nhau[60].

Hãy nhìn vào cách Internet hoạt động từ cái nhìn của người sử dụng. Trước tiên, chúng ta cần được nối với Internet. Việc này có thể được làm bằng cách mở một trương mục với công ty cung cấp dịch vụ Internet (ISP), mà sau đó, mua sự truy cập của nó từ một dịch vụ cung cấp quốc gia. Nhà cung cấp dịch vụ quốc gia nhận sự kết nối của nó từ một trong những công ty đa quốc gia bảo quản "cột sống" (backbone) Internet. "Cột sống" là một cấu trúc có công sức và chu kỳ cao, với những sự kết nối toàn cầu qua các đường dây cáp quang dưới nước và vệ tinh, làm cho các sự truyền thông giữa các quốc gia và lục địa có thể thực hiện được.



Cũng được biết như Tier1, nó được điều khiển bởi các công ty như MCI, AT&AT, Cable Wireless và Công ty viễn thông Pháp.

Khi bạn được nối kết với Internet, máy điện toán của bạn được cho một địa chỉ IP. Giống như một địa chỉ bưu điện, nó nhận diện độc nhất máy điện toán này trên hệ thống Internet. Tùy thuộc vào công ty cung cấp dịch vụ Internet của bạn, bạn có thể được cho các địa chỉ IP khác nhau ở các thời điểm nối kết khác nhau. Tất cả các hệ thống mạng và các máy server mạng đều có một địa chỉ IP.

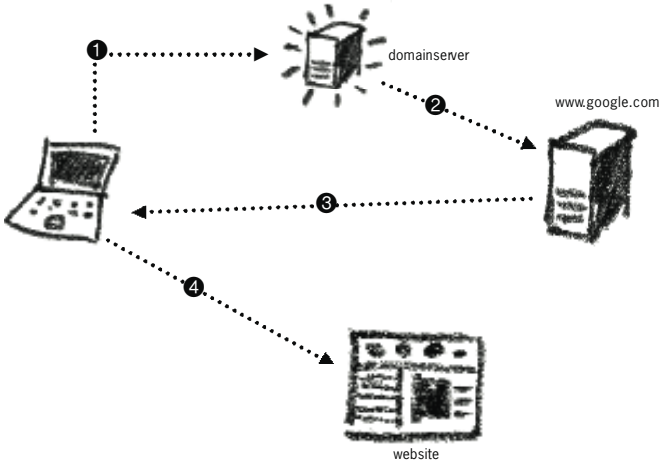
61
Sự quản trị về Internet – Giỏ cấu trúc hạ tầng và tiêu chuẩn hóa.

Tuy nhiên, khi chúng ta muốn thăm một trang mạng, chúng ta không yêu cầu số 217.67.142.198 mà đánh vào www.frontlinedefenders.org. Còn có một phương pháp để dịch các số IP thành tên trong những ngôn ngữ thông thường. Nó được gọi là Hệ Thống Tên Miền (DNS), và có những máy điện toán chuyên môn trên Internet mà nhiệm vụ của chúng là thực hiện những việc phiên dịch này. Vì vậy, chúng ta không phải nặng nhọc mà nhớ những con số phối hợp phức tạp này, nhưng chỉ cần phải nhớ sự mô tả bằng ngôn ngữ của cái tên mạng này.

DNS lệ thuộc vào máy server gốc. Những máy này được tuyển chọn để bảo trì một danh sách tên của những trang mạng quan trọng nhất và những căn cước thích ứng của chúng (.COM .ORG .NET .GOV, v.v).

Một vài những máy server gốc này của tư nhân và một số khác được điều khiển bởi các cơ quan chính phủ Hoa Kỳ. Đa số những máy server này được đặt ở miền duyên hải phía Đông Hoa Kỳ. Cấu trúc DNS được điều hành bởi công ty Internet dành cho Tên và Số được chỉ định, điều hành dưới đạo luật của Phòng Thương Mại Hoa Kỳ. Về thực tế, vài trong số những công ty lớn (những công ty mà làm chủ và điều hành các máy server gốc), như Versign (một công ty tư nhân của Mỹ), có quyền phủ quyết trong cơ quan quản trị này- sự thật mà đã trở thành một vấn đề trăn trở cho những người e sợ rằng Hoa Kỳ sử dụng quá nhiều quyền kiểm soát trên Internet.

Để thấy một trang mạng trên máy điện toán của bạn, bạn phải yêu cầu bằng việc đánh vào cái tên mạng ở phần địa chỉ của các trang mạng (URL). Hệ thống Internet lúc đó sẽ tìm địa chỉ của trang mạng (IP) bằng việc hỏi Hệ Thống Tên Miền (DNS). Cuối cùng, một lối đi từ máy điện toán của bạn đến điểm đến của trang mạng được vạch ra. Lối đi này có thể du hành qua nhiều quốc gia, đại dương và vũ trụ; nó có thể xa nhiều ngàn dặm và có thể đi qua vô số máy điện toán. Làm thế nào nó biết đi theo hướng nào, trong khi có hàng trăm triệu lối ra các trang mạng khác nhau? Công việc hướng dẫn thư tín đến trang mạng đó (và đi trở về) được thực hiện bởi những máy dẫn đường (routers), và cái phương pháp được biết như là chỉ đường (routing). Những máy chỉ đường này có thể được



Hình 2: Thí dụ về cách thư tín của bạn du hành trên Internet khi tìm một trang mạng qua Google.

điều khiển để ghi nhận hay hướng dẫn lại những túi dữ liệu hay ngăn chặn lối ra vào của các trang mạng.

Mọi máy điện toán hay máy chỉ đường, mà bạn đi qua để mang bạn đến điểm cuối cùng, được gọi là hop. Số lượng của hop là số lượng của máy điện toán/ máy chỉ đường mà thư tín của bạn đã tiếp xúc trong suốt cuộc hành trình. Phía dưới, là lối đi mà máy điện toán của tôi đã thực hiện trên Internet để đi đến www.google.com. Bạn có thể thấy rằng sự yêu cầu của tôi sẽ đi qua ít nhất là 13 máy điện toán (hop) để đến điểm cuối cùng.

```
lộ trình đến www.i.google.com (66.249.93.99), 64 hop tối đa, các túi dữ kiện 40 bytes
1 217.67.143.157 (217.67.143.157)  74.53 ms  30.910 ms  49.643 ms
2 217.67.140.61 (217.67.140.61)  29.780 ms  28.60 ms  29.628 ms
3 217.67.131.10 (217.67.131.10)  49.987 ms  29.872 ms  29.615 ms
4 217.67.131.6 (217.67.131.6)  40.267 ms  34.815 ms  40.219 ms
5 85.91.0.61 (85.91.0.61)  41.237 ms  39.192 ms  38.831 ms
6 208.50.25.109 (208.50.25.109)  31.452 ms  115.234 ms  37.396 ms
7 so0-0-0-2488M.ar3.LON2.gblx.net (67.17.71.25)  89.496 ms  44.303
  ms  46.455 ms
8 ldn-b1-pos2-0.telia.net (213.248.100.1)  47.497 ms  44.190 ms
  45.240 ms
9  google-104716-ldn-b1.c.telia.net (213.248.74.194)  52.678 ms
  89.984 ms  61.543 ms
10  72.14.238.246  (72.14.238.246)  69.863  ms  72.14.238.242
  (72.14.238.242)  59.778  ms  72.14.238.246  (72.14.238.246)
  75.364 ms
11 216.239.43.91 (216.239.43.91)  65.671 ms  61.264 ms  53.603 ms
12 72.14.232.141 (72.14.232.141)  55.727 ms  54.204 ms 216.239.43.88
  (216.239.43.88)  54.456 ms
13 64.233.175.246 (64.233.175.246)  72.265 ms  53.48 ms  55.586 ms
14 66.249.93.99 (66.249.93.99)  54.490 ms  113.495 ms 66.249.94.46
  (66.249.94.46)  57.798 ms
truy tìm chấm dứt
```

Nếu bạn đã dùng Internet trước đây, bạn biết rằng, mặc dầu Internet có vẽ là một cấu trúc phức tạp, Internet rất dể điều hành. Sự đơn giản này là kết quả của cấu trúc vững vàng của nó, như được cắt nghĩa bên trên. Nó cho phép chúng ta định vị trí nhanh chóng những gì chúng ta cần trong đại dương thông tin điện tử. Những máy server DNS (Hệ Thống Tên Miền) và các máy dẫn đường có trách nhiệm cho việc điều khiển tiến trình này. Nếu người nào đó có thể kìm hãm hay tạo được ảnh hưởng trên hoạt động của nó, khả năng sử dụng Internet của chúng ta sẽ bị hư hại hay bị giới hạn.

Email

Email điện tử gồm có những thông điệp điện tử và việc gởi chúng đi vòng quanh trên Internet. Bất cứ ai cũng đều có thể đăng ký một trương mục email trên Internet, hay nhận được một trương mục từ dịch vụ cung cấp Internet (ISP) của họ, và những người cung cấp dịch vụ này trở thành những người cung cấp dịch vụ email của chúng ta. Mọi trương mục email có một địa chỉ độc nhất (dmitri@email.com) nơi tên người sử dụng được cách biệt với địa chỉ của người cung cấp bằng chữ '@.'

Email được gởi vòng quanh Internet theo sau những nguyên tắc tương tự của

DNS và chỉ đường. Trước tiên, dịch vụ cung cấp email được tìm ra bằng tên khu vực của nó (thí dụ như email.com), kế đó dịch vụ cung cấp được hỏi về sự hiện hữu của một trương mục có tên đặc biệt đó (thí dụ như dmitri). Nếu thông tin này đúng, email được giao. Nếu không, email bị trả về (hay bị tưng) chúng ta với một lời giải thích là email không đúng.

Mọi thư từ email bạn gởi hay nhận chứa thông tin sau đây:

- Tên được đăng ký cho trương mục email (thí dụ Dmitri Vitaliev).
- Địa chỉ email.
- Số IP (địa chỉ) của máy xuất phát hay dịch vụ cung cấp email.
- Lộ trình được thực hiện bởi email để đi đến nơi cuối cùng.
- Ngày email được gởi đi và nhận được

Thông tin này được cất giữ trong phần đầu của thông điệp email và thường trong giống như vầy:

```
Nhận được: từ hotmail.com (bay17-f12.bay17.hotmail.com [64.4.43.62])
bởi mail2.frontlinedefenders.org (Postfix) with ESMTP id 5AB164F
for <dmitri@frontlinedefenders.org>; Thu, 20 Jan 2005 14:44:06 +0000 (GMT)
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
      Thu, 20 Jan 2005 06:44:04 -0800
Received: from 217.67.142.198 by by17fd.bay17.hotmail.msn.com with HTTP;
      Thu, 20 Jan 2005 14:43:58 GMT
Message-ID: <BAY17-F12DBF0F22EC08A06194JKDB9810@phx.gbl>
From: “Dmitri Vitaliev” <dmitri@hotmail.com>
To: dmitri@frontlinedefenders.org
Date: Thu, 20 Jan 2005 15:43:58 +0100
Content-Type: text/plain; format=flowed
X-Originating-IP: [217.67.142.198]
X-Originating-Email: [dmitri@hotmail.com]
X-Sender: dmitri@hotmail.com
```

Thí dụ này cho thấy phần đầu một thư tín cho email được gởi từ dmitri@hotmail.com to dmitri@frontlinedefenders.org. Bạn có thể thấy IP (địa chỉ) của các máy server Hotmail (64.4.43.62) và IP của máy mà email được gởi đi từ (217.67.142.198).

Tất cả email của chúng ta và sự lưu thông trên Internet đều được nhận diện và ghi nhận bởi địa chỉ (IP) của nơi đến/hay nơi xuất phát và ngày giờ mà nó được gởi đi hay nhận được. Thông tin này được dùng để ủy quyền thư tín của chúng ta và sự chuyển giao của nó. Đôi khi, nó cũng được dùng để theo dõi và hạn chế các sinh hoạt của chúng ta trên Internet. Hạ tầng cấu trúc Internet quan trọng, được mô tả bên trên, giúp ích khá nhiều cho việc quan sát và kiểm duyệt, chỉ vì yếu tố an ninh không có trong đầu của những nhà sáng lập Internet nguyên thủy.

Trang Mạng

Một trang mạng là một thu thập của nhiều trang được viết bằng HTML (và những ngôn ngữ khác cho Internet). Một trang mạng phải được cất trên máy server trang mạng (webserver), cũng được gọi là máy chủ (host). Máy chủ cung cấp một địa chỉ IP cho trang mạng, và bạn cũng phải đăng ký một tên DNS độc nhất cho nó, thí dụ như www.mywebsite.com. Một trang mạng có thể chia sẻ địa chỉ IP của nó với nhiều trang mạng khác được chứa trên cùng một máy chủ, tuy nhiên tất cả chúng sẽ phải có những tên DNS độc nhất.

VoIP

Tiếng nói trên IP là một tên kỹ thuật cho "viễn thông đặt trên Internet". Thay vì sử dụng hệ thống mạng lưới trao đổi điện thoại cổ điển, bạn có thể liên lạc qua tiếng nói trên Internet. Nó là một phương pháp truyền thông được ngày càng ưa thích, bởi vì sau khi trả tiền cho lần thiết lập đầu tiên, bạn không còn phải trả tiền gì nữa cho những cú điện thoại viễn liên: vị trí địa lý không có nghĩa đối với Internet. Skype có thể là một chương trình được biết đến nhiều nhất (với khoảng 100 triệu người sử dụng) đang dùng kỹ thuật này hiện tại[87]. VoIP đã trở nên một đối thủ lớn cho những công ty điện thoại thuần túy và đã gặp phải sự phản đối mạnh mẽ ở các quốc gia đang cố duy trì sự độc quyền về viễn thông.

Nhật ký điện tử

Đây có thể là một trong những áp dụng có ảnh hưởng nhiều nhất đến hệ thống Internet ngày nay. Một loại nhật ký mạng hay một cột báo về ý kiến trong ý nghĩa của nó, nó có thể được tạo ra bởi bất cứ ai trên bất cứ hệ thống Internet của những máy chủ chứa nhật ký mạng miễn phí. bạn không cần phải thiết lập một máy server mạng, cũng không tốn tiền gì hết. Đôi khi, cấu trúc trang mạng được làm sẵn rồi, và tất cả những gì bạn phải làm là trám nó đầy với nội dung của bạn. Viết nhật ký mạng cung cấp một cơ hội để bạn lên tiếng trên bất cứ lảnh vực nào do bạn chọn lựa.

Tương phản với nền truyền thông cổ điển là mong đợi người dùng chỉ tiêu hóa những thông tin mang đến cho họ, sự phát hành trên Internet là sự tiếp cận gần nhất có được cho một tiếng nói toàn cầu. Dân báo là một sự thu thập của mọi đề mục, ý kiến và nhật ký (hiện tại có khoảng 50 triệu người viết) về mọi vấn đề đang hiện hữu. Nó hoàn toàn đưa ra những thông tin không bị sửa chửa mà chỉ diễn đạt ý kiến của người đưa tin.

Tên 'Dân báo' được dùng để chỉ những người tường trình về tin tức, biến cố và các sự thay đổi trong quốc gia của họ qua nhật ký. Thường, dân báo là nguồn duy nhất về tin tức 'thật' từ một quốc gia. 'Dân báo' đã trở thanh một vũ khí rất mạnh trong việc đấu tranh cho tự do diễn đạt, và vì vậy nó bị theo dõi nặng nề và bóp nghẹn bởi các chế độ độc tài.

Mạng lưới Xã hội

Tên gọi này chỉ cái khả năng được giới thiệu bởi Internet và một loạt những phương pháp áp dụng mới cho việc tạo ra và bảo quản các mạng lưới của bạn bè và đồng nghiệp. Các dụng cụ cho phép bạn tiếp xúc với nhau bằng một loạt những phương pháp gồm có nhắn tin nhanh, hình ảnh và trao đổi video, cũng như nhắn gởi text bằng điện thoại di động. Mạng Lưới Xã Hội chịu trách nhiệm cho nhiều nguyên nhân xã hội được mang ra và quảng bá trên Internet cũng như cho các mối liên hệ giữa những người sống trong những phần khác nhau trên thế giới. Tuy nhiên, Mạng Lưới Xã Hội có nhiều bất lợi và mất an toàn mà người sử dụng cần phải đề phòng. Thông tin cá nhân về con người được mang ra trên mạng và trong lĩnh vực công cộng. Các mối liên hệ giữa những mạng lưới của những nhà đấu tranh bị phô bày, và có thể dễ dàng bị khai thác bởi một kẻ thù cương quyết.

87
Bạn có thể lấy xuống Skype từ http://www.skype.com hay xem Digital Security Toolkit CD. Đã có nhiều tranh luận như là sự an ninh của các sự truyền thông băng Skype. Mặc dầu Skype dùng phương pháp mã hóa để bảo đảm phần phiếm luận và di chuyển hồ sơ, mật mã của chương trình của nó thuộc loại đóng cửa và mức an ninh không thể được chứng minh bởi những chuyên gia bên ngoài. Xem tài liệu viết bởi by Simon Garfinkel về sự an ninh của Skype http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf.

PHỤ LỤC C
MẬT MÃ TÔI NÊN DÀI BAO NHIÊU?

Chúng ta hãy xem một người viết chương trình mất bao lâu để có thể đoán ra mật mã của bạn. Giả sử mật mã của bạn được làm ra với những chữ thường bằng tiếng Anh, chúng ta sẽ tính tối đa số lượng của sự khả thi mà người muốn phá mật mã cần để giải qua.

Chiều dài mật mã	**3**	**5**	**7**	**9**
Tính	*26 x 26 x 26*	*26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26 x 26 x 26*
Số lần khả thi	*17,576*	*11,881,376*	*8,031,810,176*	*54,295,503,678,976*

Bây giờ, chúng ta hãy cộng những con số và những chữ hoa vào mật mã chúng ta. Cái này gia tăng những sự khác biệt của những chữ cái đến 62 sự khả thi khác nhau.

Chiều dài mật mã	**3**	**5**	**7**	**9**
Tính	*62 x 62 x 62*	*62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62*
Số lần khả thi	*238,328*	*916,132,832*	*3,521,614,606,208*	*13,537,086,546,263,552*

Như bạn có thể thấy, sự khả thi tăng đáng sợ khi bạn cộng sự khác biệt vào những chữ cái của mật mã và khi bạn tăng chiều dài của nó. Nhưng các máy điện toán có thể phá những mật mã này nhanh như thế nào? Chúng ta sẽ xem như một máy điện toán đương đầu với 100.000 sự khả thi về mật mã mỗi giây (máy điện toán tân thời). Bản dưới đây cho thấy những chiều dài mật mã từ 3 đến 12 chữ cái. Những con số ở trên cao – 26, 36, 52, 68, 94 – cho thấy con số những chữ cái mà từ đó các mật mã được thành lập (giả sử bộ chữ cái tiếng Anh được dùng). 26 là con số chữ cái thường, 36 là chữ cái và số, 52 là những chữ thường và hoa trộn lại, 68 là những chữ đơn với số, mẫu tự và các dấu chấm[62].

62
Geodsoft.com – 'Mật mã xấu và tốt – làm thế nào để thực hiện'

	26	36	52	68
3	0.18 seconds	0.47 seconds	1.41 seconds	3.14 seconds
4	4.57 seconds	16.8 seconds	1.22 minutes	3.56 minutes
5	1.98 minutes	10.1 minutes	1.06 hours	4.04 hours
6	51.5 minutes	6.05 hours	13.7 days	2.26 months
7	22.3 hours	9.07 days	3.91 months	2.13 years
8	24.2 days	10.7 months	17.0 years	1.45 centuries
9	1.72 years	32.2 years	8.82 centuries	9.86 millennia
10	44.8 years	1.16 millennia	45.8 millennia	670 millennia
11	11.6 centuries	41.7 millennia	2,384 millennia	45,582 millennia
12	30.3 millennia	1,503 millennia	123,946 millennia	3,099,562 millennia

Đặt trên những con số này, người ta có thể cho rằng ngay cả một mật mã ngẫu nhiên dài 8 chữ dùng chữ thường và số cũng sẽ đủ làm phức tạp. Nếu mật mã của bạn hiện tại đã dài 5 chữ, có thể nó đã bị phá rồi, hay rất có thể bị phá, nếu mà có nhu cầu. Lưu ý: những con số bên trên chỉ áp dụng vào những mật mã ngẫu nhiên. Những sự tấn công bằng tự điển hay hồ sơ thì khác, bởi vì chúng chỉ hữu hiệu với những mật mã 'chữ thật'.

DANH TỪ KỶ THUẬT

Backdoor (cửa hậu)- trong một hệ thống điện toán, đây là một phương pháp đi tắt tránh được các phép tắc thông thường nhằm mở ra được một cổng ra vào từ xa đến một máy điện toán, trong khi vẫn tiếp tục ẩn trốn nhằm thoát khỏi sự truy xét bình thường.

Bcc - Blind carbon copy (**bản sao**). Nói về việc gởi đi một thông điệp, không có chứa danh sách người nhận đến nhiều người nhận, để họ không biết là ngoài họ ra, có những ai nữa đã nhận được thông điệp.

Có rất nhiều lý do cho việc sử dụng đặc tính này:

- Để gởi đi một lá thư của bạn đến một người thứ ba (thí dụ, một đồng nghiệp) khi bạn không muốn để những người nhận khác biết bạn đang làm việc này (hay khi bạn không muốn người nhận biết địa chỉ email của người thứ ba.)
- Khi gởi đi một email đến cho nhiều người, bạn có thể dấu địa chỉ email của họ từ người khác. Đây là một sự đề phòng thư rác có ý nghĩa, bởi vì nó giúp tránh được nhận một danh sách dài của địa chỉ email cho mọi người nhận (mà là những gì sẽ xảy ra, nếu bạn để email của mọi người trong phần Đến (To: hay CC). Vì lý do này, nó thường hợp lý để dùng phần Bcc để gởi danh sách email. Vài loại virus (vi khuẩn) thu lượm địa chỉ email từ những hồ sơ chứa địa chỉ của người gởi, và các danh sách lớn CC (bản sao) có thể phân tán xa hơn những virus không muốn, đây là một lý do thêm để sử dụng Bcc.

BIOS - viết tắt cho Basic Input/Output System (Hệ thống Xuất Nhập Cơ Bản) hay Basic Integrated Operating Systems (Hệ Thống Điều Hành Hội Nhập Căn Bản). Phần lập trình được điều khiển bởi máy điện toán khi máy vừa mới được mở lên. Nhiệm vụ chính của BIOS là chuẩn bị cho những chương trình thuộc phần mềm khác được cất giữ trong nhiều bộ phận truyền thông (như ổ cứng, đĩa mềm, và CD) có thể chạy được và tuân hành theo sự điều khiển của máy điện toán.

Blog- Nhật ký mạng - một trang mạng nơi những thông tin được viết vào như kiểu viết nhật ký và được trình bày theo thứ tự ngược. Nhật ký mạng thường cung cấp bình luận hay tin tức về một đề tài đặc biệt, như thức ăn, chính trị, hay tin tức địa phương; một vài nhật ký mạng hoạt động nhiều hơn là một nhật ký cá nhân. Một trang nhật ký mạng điển hình gồm có chữ, hình, và những nút nối vào những nhật ký mạng khác, những trang mạng, và những phương tiện truyền thông khác liên quan đến đề tài của nó. Các động cơ tìm nhật ký mạng phổ thông gồm có www.wordpress.com, www.livejournal.com, www.blogspot.com.

Nhiều ký giả và những nhà đấu tranh nhân quyền sử dụng nhật ký mạng như là để truyền tải những thông tin quan trọng, mà không thể có được từ giới truyền thông của chính phủ, trên Internet. Việc làm này được mệnh danh là 'dân báo' - một phương pháp đang phát triển được ưa thích

vì được dùng để phổ biến những thông tin thật sự về một biến cố hay về một quốc gia.

Control Panel - Hệ Thống Kiểm Soát – là một đặc điểm của Microsoft Windows mà cho bạn đi vào để sửa đổi những sự sắp đặt về hệ thống của máy điện toán của bạn, gồm có sự quản trị người sử dụng (user management), các đặc tính về năng lượng cho máy, các lối vào hệ thống mạng, những chương trình phần mềm cho các phần cứng (drivers) và nhiều phần điều hành khác của máy điện toán.

Circumvention -Mánh lới – trong tài liệu này, mánh lới liên quan đến việc đi tắt vào những nút chận của trang mạng trên Internet. Việc này có thể làm được bằng cách sử dụng kỷ thuật 'đi vòng qua' các chướng ngại vật.

Cryptanalysis(st) - Sự phân tích mã hóa (Nhà phân tích) - những khoa nghiên cứu về các phương pháp lấy được ý nghĩa của những thông tin được mã hóa, mà không cần phải đi vào phần thông tin được bảo mật đó. Một nhà phân tích mã hóa là một người thực hiện những việc nghiên cứu đó.

Cryptology - một môn học về toán, ngôn ngữ, và những mẫu mật hiệu khác và lịch sử của chúng.

Cyber-dissident(s)- Người chống đối trên mạng - một người hay một nhóm người đang tích cực hoạt động nhằm chống lại một thể chế chính trị đang cầm quyền qua việc bày tỏ quan điểm của họ qua phương tiện truyền thông trên Internet.

Denial of Service attack (DOS)- Tấn công bằng sự từ chối cung cấp dịch vụ - một loại tấn công bằng việc từ chối cung cấp dịch vụ được thực hiện bằng cách liên tục mở các yêu cầu truy cập vào một trang mạng. Muc đích của việc tấn công này là làm cho máy server mạng bị quá tải, bằng cách thực hiện hàng triệu yêu cầu tương tự trong một khoảng thời gian thật ngắn. Một cuộc tấn công dùng Distributed DOS (DDOS) sẽ điều khiển những máy điện toán bị nhiễm virus để cùng tấn công một trang mạng độc nhất.

Device drivers – Chương trình điều khiển thiết bị – là chương trình phần mềm mà cho phép một phần cứng (hardware) hoạt động trên máy điện toán của bạn.

Digital divide – lằn ranh phân chia điện tử - chỉ sự cách biệt giữa những người có được sự tiếp cận thường xuyên và hiệu quả đến kỹ thuật điện tử với những người không có.

DSL access - Tiếp cận DSL– kỹ thuật truyền thông dữ liệu làm cho sự vận chuyển dữ liệu (data) qua đường dây điện thoại bằng đồng trở thành nhanh hơn hàng chục lần so với một máy modem. Chữ viết tắt cho Digital Subcriber Line (Đường Dây Thuê Bao Mã Số) (với những sự khác biệt

của một đường dây ADSL – Asymmetric and SDSL – Symmetric)

ECHELON – mô tả một mạng lưới tình báo và phân tích ký hiệu toàn cầu cấp cao được điều khiển bởi cộng đồng UKUSA (mặt khác được biết như là "đồng minh Anh-Mỹ"). Echelon được đề cập tới bởi một số nguồn tin, trong đó có Quốc Hội Âu Châu. Theo một vài nguồn tin, ECHELON có thể bắt được các truyền thông bằng radio và vệ tinh, điện thoại, fax, email và những ghi nhận dữ liệu khác hầu như khắp mọi nơi trên thế giới. Hệ thống bao gồm có sự phân tích tự động bằng máy điện toán và xếp đặt những sự ngăn chận (intercept).

Encryption – Mã hóa -phương pháp che dấu thông tin bằng cách chuyển nội dung qua dạng ẩn ngữ với các phương pháp toán học, để người ngoài không thể đọc được nếu không có kiến thức chuyên môn hay khả năng kỹ thuật cao để giải mã.

Firewall (Tường lửa) - một bộ phận cứng (hardware) và/ hay phần mềm (software) được thiết kế hoạt động tại cổng ra vào mạng để bảo vệ hệ thống điện toán của hảng xưởng, tổ chức hay máy điện toán một cá nhân, nhằm phòng chống lại các cuộc tấn công, xâm nhập vào hệ thống điện toán, tạo an toàn cho sự thông tin theo một chính sách về an ninh được hoạch định.

Internet Service Provider (ISP)- Dịch vụ cung cấp Internet - một tổ chức hay cơ sở thương mại cung cấp cho người sử dụng sự truy cập vào Internet và các dịch vụ liên quan. Trong quá khứ, đa số ISP được điều hành bởi những công ty điện thoại. Ngày nay, ISP có thể được khởi đầu bằng bất cứ ai. Họ cung cấp các dịch vụ như truyền tải Internet, đăng ký tên miền (domain) và làm máy chủ, sự truy cập qua điện thoại hay DSL , đường dây thuê bao và cung cấp việc thuê bao máy chủ và các dịch vụ liên hệ tại cùng nơi (hosting services: giữ máy server của bạn ở công ty cung cấp dịch vụ, ISP)

ISP – xem Internet Service Provider

Secure Sockets Layer (SSL)- Lớp ổ cấm an toàn– một giao thức mã hóa bằng hình mà cung cấp những sự truyền thông an toàn trên Internet cho email, fax bằng internet, và những sự chuyển chở dử kiện khác.

Open encryption standards - Những tiêu chuẩn mã hóa công khai– những phương pháp hay toán đại số mà mật mã của nó được mở công khai đến công chúng cho việc sửa đổi và cải thiện. Những phương pháp này được coi như là loại đại số mã hóa được trắc nghiệm công khai an toàn nhất. Đại số mã hóa đóng cửa có thể có những khuyết điểm lớn (không được để ý bởi người viết chương trình), hay những "cửa hậu" (back door) được đặc biệt làm ra nhằm thu thập tiết lộ tất cả thông tin của bạn đến người thứ ba.

Partition (disk partition)- Sự phân chia ổ cứng– Sự phân chia (phân chia ổ cứng)- một sự phân chia về logic trên ổ cứng. Nó cho phép tạo ra

vài hệ thống hồ sơ trên một ổ cứng đơn và có nhiều lợi ích: cho phép sự thiết lập hai ổ cứng (thí dụ như bạn có thể sử dụng song song Microsoft Windows và Linux), chia xẻ những sự phân chia (sharing) được trao đổi nhau giữa những sự đa phân phối Linux, và bảo vệ hay cô lập các hồ sơ.

PKE – xem phần Public key cryptography

Proxy server - Máy server đại diện- một máy điện toán mà làm cho các máy khách có thể thực hiện những điểm nối gián tiếp trên mạng với những dịch vụ mạng khác (trang mạng)

Public key cryptography (encryption) – Chìa khóa mã hóa công– một hình thức của cryptography mà thường cho phép người sử dụng liên lạc một cách an toàn mà không phải tiếp cận trước với một chìa khóa bí mật chung. Việc này thực hiện được qua việc sử dụng một cặp chìa khóa mã hóa, được chỉ định là chìa khóa công và chìa khóa tư, mà có liên quan rất mật thiết với nhau về toán học.

SORM-2 – (Sistema Operativno-Rozysknykh Meropriyatii, đúng nghĩa là "System of Operational and Investigative Activities") - một đạo luật của Nga, được cập nhật năm 1998, mà cho phép FSB (Federal Security Service) Cơ quan mật vụ liên bang theo dõi các cộng đồng Internet

SSL – hãy xem Secure Sockets Layer

SSL Certificate- Chứng chỉ SSL– được tạo ra cho mọi trang mạng muốn được điều hành theo giao thức (protocole) SSL. Nó làm việc như là một hệ thống nhận diện độc nhất chứng minh sự nguyên thủy của trang mạng đó và cung cấp dữ kiện cần thiết cho việc thiết lập một kênh được mã hóa giữa máy chủ và khách

System registry - Danh sách Hệ thống – một danh sách của tất cả các chương trình thuộc phần mềm, các bộ phận thuộc phần cứng và những sự sắp đặt về hệ thống trên máy điện toán của bạn. Mọi chương trình thuộc phần mềm được cài đặt và các bộ phận của máy điện toán của bạn phải được ghi nhận vào danh sách này. Thường thì điều này tự động xảy ra. Đôi khi, khi một chương trình thuộc phần mềm chưa được cài đặt, nó không có gở bỏ sự ghi danh của nó vào trong danh sách này. Điều này có thể tạo ra một sự lo ngại về an ninh tương lai. Virus thường tấn công và làm hư hỏng danh sách này và có thể làm hư hại đến sự vận hành của máy điện toán của bạn.

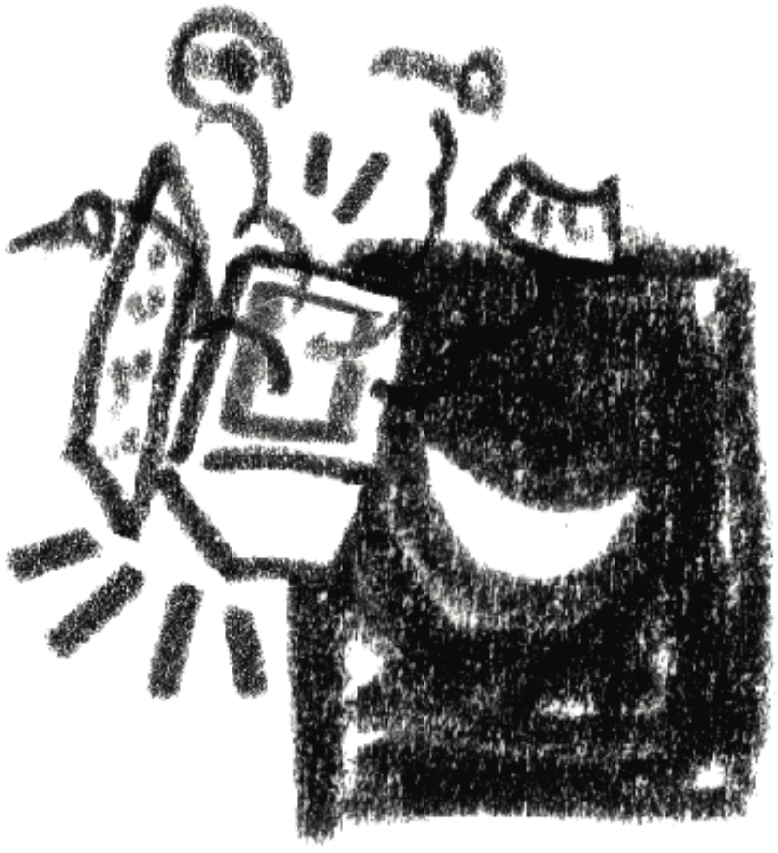
Webserver – Máy chủ mạng -Một máy điện toán mà làm chủ một hay nhiều những trang mạng. Cũng được gọi là máy chủ mạng (web host).

Wiping (file wiping) Lau hồ sơ – tiến trình của việc viết chồng lên trên một hồ sơ, đôi khi nhiều hồ sơ, để đảm bảo tất cả thông tin đều được hủy bỏ. Lau một hồ sơ tương đương với cắt vụn ra một tài liệu bằng máy cắt giấy.

Một sự đề nghị cho Bảng Các Quyền Về Internet

1. Quyền được truy cập hạ tầng cấu trúc Internet không kể bạn sống ở đâu
2. Quyền có khả năng và kiến thức giúp con người sử dụng và thay đổi cấu trúc Internet để đáp ứng cho nhu cầu của họ
3. Quyền được xử dụng phần mềm có nguồn miễn phí và mở rộng
4. Quyền được truy cập một cách bình đẳng cho nam và nữ
5. Quyền được truy cập và tạo nội dung đa dạng về văn hóa và ngôn ngữ
6. Quyền được tư do phát biểu
7. Quyền được tham dự vào việc phản đối trên mạng
8. Quyền được truy cập để nâng cao kiến thức
9. Quyền được tự do thông tin
10. Quyền được truy cập các thông tin được cung cấp công khai
11. Quyền được tự do không bị theo dõi
12. Quyền được sử dụng mã hóa
13. Quyền được giám thị tính chất dân chủ đa nguyên của Internet
14. Quyền được hưởng sự trong sạch và có thể tiếp cận được của bộ phận luật pháp Internet
15. Quyền được có địa phương phân quyền, cộng tác và có thể hoạt động liên đới trên Internet
16. Quyền được có sự bảo vệ về quyền lợi, ý thức và giáo dục
17. Quyền được cầu cứu khi quyền lợi bị vi phạm

(Để có nguyên bản xin hãy tham khảo nguyên bản từ trang mạng của Hội Cho Các Sự Truyền Thông Tiến Bộ http://rights.apc.org/charter.shtml).



FrontLine
INTERNATIONAL FOUNDATION
FOR THE PROTECTION
OF HUMAN RIGHTS DEFENDERS

81 Main Street
Blackrock Co. Dublin
Republic of Ireland
Tel: +35 3 1 212 3750
Fax: +35 3 1 2121001
info@frontlinedefenders.org
www.frontlinedefenders.org

Irish Aid
Department of Foreign Affairs
An Roinn Gnóthaí Eachtracha

NGO in a Box
security.ngoinabox.org