

## **Một số bí quyết khi truy cập, gửi, nhận thông tin trên internet**

Làm thế nào để truy cập, gửi, nhận, hay phổ biến thông tin trên mạng internet một cách an toàn? Một câu hỏi tuy đơn giản đơn giản nhưng được người dân ở các nước siết chặt quản lý internet như Việt Nam hết sức quan tâm, nhất là giới trẻ khao khát tự do thông tin, tự do tiếp cận với thế giới mở bên ngoài.

Để giúp quý vị và các bạn tìm lời giải đáp, Trà Mi có cuộc trao đổi với ông Ethan Zuckerman, chuyên gia của Trung Tâm Nghiên Cứu Về Internet Và Xã Hội Berkman, thuộc trường luật Harvard, tại Hoa Kỳ.

Ông Zuckerman là người góp mặt trong rất nhiều công trình nghiên cứu nhằm phát triển tính hữu dụng của công nghệ thông tin phục vụ xã hội dân sự và quyền tự do thông tin của con người. Ông đã được trao rất nhiều giải thưởng và danh hiệu cao quý về những cống hiến cho nhân loại trong lĩnh vực này. Trong số này có danh hiệu “Nhà lãnh đạo tương lai của toàn cầu” vào năm 2003 và “Nhà lãnh đạo trẻ của toàn cầu” vào năm 2005.

### **Gửi, nhận email ở Việt Nam**

Trà Mi: Các hoạt động trao đổi thông tin trên mạng có thể chia thành hai dạng chính như trao đổi, phổ biến thông tin, phát biểu ý kiến qua email hay blog, hoặc tìm kiếm, cập nhật thông tin bên ngoài bằng các công cụ vượt tường lửa. Trước hết, nói về phương tiện phổ biến nhất hiện nay là email, xin được hỏi ông làm cách nào để sử dụng email một cách an toàn nhất?

Ông Ethan Zuckerman: Tại một quốc gia như Việt Nam, nơi internet bị nhà nước quản lý chặt chẽ, thì các cư dân mạng, đặc biệt là những ai muốn tự do truy cập thông tin hay bày tỏ quan điểm trên mạng, phải đối diện với rất nhiều rủi ro và đàn áp từ phía chính quyền.

Vì vậy, đăng ký (ghi danh) sử dụng các tài khoản email từ các nhà cung cấp dịch vụ email miễn phí như yahoo hay hotmail chẳng hạn quả thật là không an toàn. Các nhà cung cấp này có thể giao nộp thông tin cá nhân và nội dung trao đổi thư từ của bạn cho an ninh mạng, nếu được yêu cầu.

Hiện nay có những nhà cung cấp email cung cấp công cụ hỗ trợ cho các dạng email mã hóa. Một ví dụ điển hình là Google, tức dịch vụ gmail. Nếu bạn vào đường link URL tên là: <https://mail.google.com/mail> để đăng ký (ghi danh) 1 tài khoản email với Google thì bạn sẽ có một địa chỉ email mà sử dụng nó thì nội dung email của bạn khi gửi đi sẽ được mã hóa.

Cho nên, trên đường thư tới tay người nhận, an ninh theo dõi trên mạng không thể biết được nội dung của lá thư. Thế nhưng, điều này không có nghĩa đây là cách an toàn tuyệt đối. Vì thư của bạn được tải về trạm chuyển thư là Google trước khi được gửi tới người nhận, thì cũng có khả năng là khi được chính quyền Việt Nam yêu cầu, Google có thể sẽ hợp tác bằng cách cung cấp cả nội dung email và thông tin của người gửi.

### **An ninh trong thế giới blog**

Trà Mi: Còn về việc sử dụng nhật ký điện tử Blog để trao đổi, phổ biến thông tin hay bày tỏ quan điểm. Ông có lời khuyên gì giúp những bloggers tại Việt Nam tự bảo vệ an toàn cá nhân?

Ông Ethan Zuckerman: Tôi có phổ biến những chỉ dẫn cụ thể về phương cách sử dụng Blog an toàn trên mạng. Bài viết nhan đề: “Blog ẩn danh với chương trình Wordpress và TOR” được lưu trữ trong phần Tools and Guides trên trang [www.advocacy.globalvoicesonline.org](http://www.advocacy.globalvoicesonline.org). Qua đó, tôi đề nghị người dân tại những nước kiểm duyệt internet:

Trước hết, bạn nên tải phần mềm (thảo trình, nhu liệu) TOR từ trang web:

[www.tor.eff.org](http://www.tor.eff.org) vào máy tính hoặc vào đĩa, hay USB của mình, làm theo hướng dẫn từng bước trong đó. TOR là một chương trình có chức năng xóa dấu vết, dấu địa chỉ xuất xứ của người truy cập khi họ gửi, nhận, hay đọc thông tin trên mạng internet bằng cách mã hóa nhiều lần những thông tin trao đổi trên net của người đó và chuyển qua nhiều máy chủ trung gian khác nhau trước khi gửi tới người nhận.

Sau khi đã có công cụ vượt tường lửa TOR trong tay, nghĩa là có thể yên tâm rằng mọi hoạt động của bạn trên mạng được bảo mật, bạn nên đăng ký một địa chỉ email với Gmail.

Kể đến, bạn cần tạo ra một tài khoản với WordPress Blog Tool and Weblog Platform, là một phần mềm trọn gói (thảo trình gồm đầy đủ mọi thứ) chỉ dẫn, hỗ trợ tạo blog rất phổ biến, tương tự như yahoo 360 độ.

Nhớ rằng khi tạo địa chỉ email với Gmail và mở blog với Wordpress, bạn đều phải sử dụng TOR để bảo mật an toàn. Có như vậy, cả Gmail và Wordpress đều không biết được những thông tin cá nhân của bạn. Họ chỉ thấy được là bạn sử dụng TOR để đến với họ, nhưng họ không biết được vị trí của bạn đang ở đâu, từ quốc gia nào.

Cho nên, cho dù có được chính quyền Việt Nam yêu cầu đi chẳng nữa, thì Gmail và Wordpress cũng không hề có được thông tin cá nhân của bạn để giao nộp hay tiết lộ.

Làm những việc này, bạn sẽ có được một địa chỉ email an toàn để mở blog và trang blog cá nhân để giao tiếp với mọi người trên khắp thế giới. Hơn nữa, mọi hoạt động trên blog bạn đều thực hiện với công cụ TOR thì công an mạng khó mà truy tìm được ra bạn là ai.

Đương nhiên cách này không phải là an toàn tuyệt đối, nhưng nó có tính bảo mật cao hơn và cũng dễ sử dụng đối với mọi người.

### **Những lưu ý khi vượt tường lửa**

Trà Mi: Một hoạt động khá phổ biến trên net là truy cập và tiếp cận thông tin toàn cầu. Việc này vốn bị cản trở rất nhiều ở các chế độ độc tài bằng những bức tường lửa, và công cụ ‘leo rào’ phổ biến hiện nay là dùng proxy. Theo ông, để vượt tường lửa an toàn, cần lưu ý những điều gì?

Ông Ethan Zuckerman: Chúng tôi không đề nghị sử dụng các proxy công cộng vì bạn không thể biết được người đang vận hành các proxy công cộng đó là ai.

Chúng tôi khuyên bạn nên dùng TOR hay JAP, tức những proxy ẩn danh có hỗ trợ Java.

Những cư dân mạng ở Việt Nam nếu có bà con, bạn bè định cư ở nước ngoài thì nên sử dụng Psiphon. Người thân của bạn ở hải ngoại chỉ cần cài đặt chương trình Psiphon vào máy và đưa cho bạn những thông tin kết nối như địa chỉ IP của máy chủ, tên đăng ký sử dụng, và mật khẩu.

Một người ở Việt Nam truy cập internet bằng Psiphon thì cũng giống như là người ấy đang dùng máy tính của người thân ở nước ngoài để vào mạng vậy. Bạn sẽ có thể tha hồ truy cập vào bất cứ trang web nào mà bạn thích, mà không để lại dấu vết gì có thể bị truy ra cả. Bạn có thể tải Psiphon về từ địa chỉ: [www.psiphon.civisec.org - Coming Soon](http://www.psiphon.civisec.org - Coming Soon) (hoặc chuyển thẳng về từ kho nhu liệu của thuvientoancau.com tại đây:

[http://tvvn.org/tvvn/index.php?categ...3&p13\\_fileid=5](http://tvvn.org/tvvn/index.php?categ...3&p13_fileid=5)). Đó là những cách vượt tường lửa an toàn nhất.

Tóm lại, bạn cần nhớ rằng khi đăng tải ý kiến cá nhân lên net hay lên blog, cần sử dụng các công cụ như TOR, Psiphon kèm theo để ‘ngụy trang’ và tăng cường tính bảo mật.

**Một vấn đề khác đáng lưu ý là tuyệt đối đừng bao giờ tiết lộ bất cứ thông tin nào liên quan đến cá nhân của bạn trên mạng hay trên blog.**

Trà Mi: Xin chân thành cảm ơn ông đã dành thời gian cho cuộc trao đổi này.

Trà Mi, phóng viên đài RFA

© 2007 Radio Free Asia

## **HÀNH TRANG CỦA CHIẾN SĨ DÂN CHỦ - Dùng secure mail để gửi e-mail**

Sống trong môi trường kiểm soát internet một cách nghiêm ngặt và hoàn toàn không có tự do thông tin, ngôn luận như ở Việt Nam, việc trao đổi thông tin liên lạc thật vô cùng khó khăn và thiếu bảo mật cho các anh em Chiến Sĩ Dân Chủ ở trong nước. Bằng kinh nghiệm của tôi, và tham khảo một số anh em IT bạn bè, tôi viết bài này để mong giúp thêm được phần nào

cho anh em Chiến Sĩ Dân Chủ một công cụ hỗ trợ đắc lực trong việc trao đổi tin tức trên mạng lưới nhện thông qua điện thư.

Nếu chúng ta chỉ trao đổi tin tức qua yahoo email, chắc chắn chúng ta sẽ thất bại, bởi vì cộng sản có thể đọc tất cả nội dung đó một cách dễ dàng bằng cách cut và paste nội dung đó vào một server khác trên đường truyền mà chúng ta không hề hay biết. Và cộng sản cũng chẳng cần mật mã để làm gì, một khi chúng đã biết chính xác địa chỉ điện thư. Cho nên đối với server địa chỉ điện thư quan trọng hơn là mật mã, đối với bạn bè bình thường thì mật mã quan trọng hơn địa chỉ điện thư.

Như vậy để bảo mật nội dung, chỉ có một cách duy nhất là mã hóa (encryption) nội dung trước khi gửi đi trên đường truyền, khi đó server Việt Nam sẽ không thể nào đọc được, dù biết chính xác địa chỉ điện thư. Chúng ta có 2 cách để mã hóa thông tin:

Một là mã hóa bằng một thảo trình trước khi gửi đi, và người nhận giải mã (decryption) cũng chính bằng thảo trình đó bởi mật mã đã biết trước.

Hai là dùng hệ thống secure mail. Có nhiều hệ thống secure mail, nhưng theo tôi cách thông dụng và dễ dàng nhất ở Việt Nam vẫn là HUSHMAIL.COM nếu người gửi và nhận đều dùng hushmail, việc này tương đối an toàn và có nhiều tính năng linh hoạt. HUSHMAIL KHÔNG NHỮNG CHỈ MÃ HÓA MÀ CÒN CÓ 3 CÁCH ĐỂ GỬI TIN TỨC KHÁC NHAU.

Chúng ta bắt đầu theo từng thứ tự cụ thể.

1- Việc tạo một hộp thư hushmail rất là dễ dàng và hoàn toàn miễn phí.

Đầu tiên chúng ta vào trang <https://www.hushmail.com> (chú ý rằng đây là trang <https://> chứ không phải <http://> như yahoo hay hotmail... SSL: viết tắt của Secure Sockets Layer, đây là 1 cách để chuyển tin cần độ an toàn cao)

Tiếp theo chúng ta vào trang ghi danh miễn phí (sign up for free email) và bắt đầu tạo một hộp thư.

Theo thứ tự 5 bước của nó chúng ta điền đầy đủ các yêu cầu. Và cách tốt nhất là tạo một "automatically email address". Ở bước thứ 4 chúng ta bấm vào phần "show advance option" để chấp nhận cho phép Java được chạy (Enable java). Điều này rất quan trọng về sau này, có nghĩa là chúng ta đang chọn "turn on java"... Ở bước thứ 5 chúng ta phải click vào terms of service để vào phần terms of service. Xong, chúng ta có quyền click vào Now created account.

Như vậy là chúng ta đã có một địa chỉ giống như thế này:

[auto175332@hushmail.com](mailto:auto175332@hushmail.com), [auto52608@hushmail.com](mailto:auto52608@hushmail.com).....

Chú ý, nếu sau 3 tuần không sử dụng địa chỉ này sẽ tự động deactivate và mỗi máy có thể tạo 4-5 địa chỉ hushmail.

2- Sign in vào địa chỉ email

Đề vào địa chỉ email chúng ta phải quay ngược lại trang chính hushmail đầu tiên, và enter full your address vào cột trống đầu tiên. Hushmail sẽ tự động chuyển tới trang thứ nhất, rồi trang thứ 2, chúng ta phải click chọn vào dòng chữ màu đỏ if you would like continue with a free account và hushmail sẽ tự động chuyển qua thứ 3 trang Password. Trang này rất quan trọng ở phần "enable java". Cả trang chỉ hiện lên ô trống passphase và dòng chữ màu xanh "enable java" hoặc "turn off java". Nếu chúng ta thấy dòng chữ "enable java" có nghĩa là chúng ta đang ở tình trạng "tắt java" và ngược lại.

Điều này RẤT quan trọng cho tính năng chia sẻ dữ liệu SHARE FOLDER sau này, Một cách gửi thông tin khác của hushmail.

Vì vậy cách tốt nhất là chúng ta phải luôn luôn mở java. Cho nên nếu thấy dòng chữ enable java chúng ta phải click chọn vào nó để chuyển đổi thành mở java trước khi enter passphase. Hushmail sẽ tự động chuyển thành "Enable java" sau khi bấm, hoặc có thể chúng ta phải quay lại từ đầu. Nghĩa là, nếu trang Passphase hiện ra dòng chữ "turn off java", là chúng ta đang làm đúng (không mở java chúng ta vẫn vào được trang inbox)

Cách thứ nhất để gửi tin tức:

Trang Inbox của hushmail cũng giống như mọi trang email khác. Chúng ta có thể tạo new mail ở compose và send một cách bình thường với nội dung đã được encryption. Chúng ta có thể đổi Passphrase ở phần Preference, và tìm hiểu thêm về turn on java ở phần Help.

Nhưng đặc biệt nhất có lẽ là tính năng SHARE FOLDER (chia sẻ dữ liệu) nếu chúng ta đang mở java, và người nhận lần người gửi đều dùng hushmail.com

Cách thứ hai để gửi tin tức:

Với tính năng SHARE FOLDER (không có hệ thống mail nào có) yêu cầu người gửi lần người nhận phải mở JAVA mới nhận diện lẫn nhau. Khi chúng ta turn on java ở trang Passphrase, vào đến trang inbox sẽ nhận diện thấy File Storage và Remote folder. Nếu không mở java chúng ta sẽ không thấy hai phần này.

File Storage dùng để upload những file mà chúng ta muốn lưu trữ trên hushmail server và có thể chia sẻ cho người khác nhận diện, download hoặc deleted nó. Nếu muốn share cho người khác, sau khi upload xong, chúng ta gõ địa chỉ người được share vào ô trống và click Add user, có thể chọn thêm các thuộc tính cho người nhận read or deleted ở dưới.

Remote folder cho chúng ta nhận thấy tài liệu được chia sẻ (share) từ một địa chỉ email khác, mà chúng ta sẽ được quyền mở (open) hay chuyển (download) nó.

Như vậy, thay vì send một điện thư bình thường, chúng ta có thể chia nhau coi (share) một tài liệu dạng .DOC .TXT .JPG .BMP.... cho người khác đọc mà không cần phải gửi tài liệu ấy đi. Nếu như tài liệu đó chúng ta đã mã hóa trước thì càng an toàn hơn.

Và càng bất ngờ hơn, nếu chúng ta tạo thêm một địa chỉ hushmail mới khác, và share folder cho người nhận thì làm sao server cộng sản nhận biết được mail nào đang gửi tin đi.

Cách thứ ba để gửi tin tức:

Ngoài việc có một account hushmail để gửi email, chúng ta vẫn có thể gửi secure mail thông qua hushmail mà chưa có account hushmail. Đó là cách gửi email thông qua HUSHMAIL EXPRESS.

Sau khi vào <https://www.hushmail.com> chúng ta click chọn hushmail express. Một trang mới hiện ra để chúng ta điền thông tin và nội dung muốn gửi.

Ở phần "your address", có thể chúng ta điền đúng địa chỉ điện thư của người gửi, (ở trang nhà yahoo, hotmail hay aol mail...). Hoặc có thể không đúng. Hushmail không quan tâm tới chuyện này, chỉ khi nào mail không gửi được, nó mới replay lại đúng địa chỉ này.

Cho nên nếu chúng ta ghi một địa chỉ email ảo khác thì server cộng sản không biết được địa chỉ mail nào đang gửi nội dung này.

Nhớ phải click chọn ở khung kiểm tra "I agree with term of sevice" mới có thể send được.

Có một giới hạn ở cách thứ 3 này là người nhận phải answer đúng câu answer của người gửi. Đó là password. Vì vậy cách này sẽ rất hữu dụng nếu người gửi và người nhận đã biết nhau từ trước, hoặc đã thỏa thuận trước một password nào đó. Tuy nhiên cách này độ bảo mật không cao. Nhưng trong rất nhiều tình huống đặc biệt chúng ta vẫn phải sử dụng nó.

Trên đây là sơ lược 3 cách sử dụng của hushmail, nếu chúng ta biết kết hợp với những software khác thì tính năng của nó sẽ đa dạng vô cùng. Giả sử chúng ta mã hóa dữ liệu trước, rồi dùng share folder để gửi cho người nhận thì server cộng sản bó tay, không thể đọc được nội dung (tùy thuộc vào software mã hóa). Có nhiều cách để mã hóa thông tin, nhưng có 2 cách thông dụng nhất là dùng software để mã hóa nội dung text, hoặc ẩn nội dung dưới một file hình ảnh.

Và cũng có rất nhiều thảo trình để mã hóa nội dung text. Thông dụng chúng ta có thể chuyển về ở những địa chỉ sau:

[http://www.songtoday.com/cgi-bin/nph-](http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s7072646s776r6p6s6164732r736s75726365666s)

[proxy.cgi/001100A/687474702s7072646s776r6p6s6164732r736s75726365666s](http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s7072646s776r6p6s6164732r736s75726365666s)

[7267652r6r65742s617863727970742s417843727970742q53](http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s7072646s776r6p6s6164732r736s75726365666s)

[657475702r657865](http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s7072646s776r6p6s6164732r736s75726365666s)

hoặc

<http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s7777772r63797068657269782r636s2r756o2s637279707461696r65725s6p655s646s776r6p6s61645s63656r7465722r68746q>

hoặc

software:ciphrtxt <http://www.roadkil.net>

Các thảo trình này hoàn toàn miễn phí và có dung lượng nhỏ, dễ gắn và rất dễ sử dụng có thể mã hóa một tài liệu, hoặc nguyên cả một hardrive v.v...

Software stephide dùng để ẩn dữ liệu dưới một file hình ảnh:

<http://www.songtoday.com/cgi-bin/nph-proxy.cgi/001100A/687474702s73746567686964652r736s75726365666s7267652r6r65742s>

Chúng ta có thể tìm thêm nhiều thảo trình khác ở trên mạng lưới nhện, có thể mỗi nhóm Chiến Sĩ Dân Chủ nên có những software riêng để trao đổi lẫn nhau. Với sự linh hoạt của mình, cộng với kiến thức về máy tính các Chiến Sĩ Dân Chủ sẽ có muôn vàn cách để tạo những hàng rào chắn chung quanh nội dung bí mật của mình.

Trong thời đại hiện nay, mỗi Chiến Sĩ Dân Chủ đều phải sử dụng internet để tấn công cộng sản vì vậy chúng ta phải luôn luôn trang bị cho mình những kiến thức đầy đủ về vi tính và cập nhật thường xuyên. Chắc chắn cộng sản sẽ thất bại bởi internet, cho nên chúng tìm mọi cách để trấn áp trong lãnh vực này. Mỗi Chiến Sĩ Dân Chủ cần phải có 4-5 địa chỉ email cùng một lúc, trong đó chắc chắn phải có 2 hushmail, 2 hotmail và 1 yahoomail để liên lạc bạn bè cho vui... **Hotmail an toàn hơn yahoo vì trong history, hotmail không để lại dấu vết của người gửi. Khi sử dụng hushmail chúng ta sẽ nhận thấy cộng sản luôn tìm cách xâm nhập vào inbox của chúng ta, tìm mọi cách phá hoại như là không đổi password được, không replay được, không new mail được.... Chúng ta có thể cảm nhận được sự rình mò của cộng sản ở bên cạnh, trong khi đó ở yahoo mọi việc đều êm xuôi, suông sẻ, ngọt xót, bởi vì cộng sản đã đọc được tất cả thông tin của chúng ta ngay từ lúc mới khai trương, nếu chúng ta luôn sử dụng một máy tính tại nhà và một mạng ADSL cố định. Chính mạng ADSL là mạng dễ quản lý nhất.**

Trong bóng tối cộng sản sẽ chiến thắng, cộng sản đang sợ ánh sáng, và sẽ thất bại bởi ánh sáng. Vì vậy tôi rất thật tình mong muốn những người am hiểu nhiều về network, cung cấp thêm những kiến thức và kinh nghiệm về lãnh vực này cho anh em Chiến Sĩ Dân Chủ dùng làm hành trang trên con đường đấu tranh đầy gian khổ này. Bài viết của tôi có những điểm sai hãy cứ thẳng thắn nêu lên để chúng ta cùng nhau rút kinh nghiệm. Đừng nghĩ rằng cộng sản không biết, cộng sản đang nắm server, cộng sản đang lưu manh nhất thế giới. Vậy thì chỉ có một phương pháp đấu tranh mở chúng ta mới chiến thắng cộng sản mà thôi.

Sài Gòn

Nguyen Van IT

## **Làm thế nào để công an Việt Nam không đọc được email của bạn?**

**2007.11.23**

### **Đỗ Hiếu, phóng viên đài RFA**

Với sự phát triển nhanh chóng của mạng thông tin toàn cầu Internet, tại Việt Nam, hiện giờ các nhà đấu tranh cho dân chủ cũng triệt để khai thác phương tiện thông tin hữu hiệu này.

Để kiểm soát nguồn thông tin từ trong nước với hải ngoại, nhà nước đã cho thành lập lực lượng công an Internet nhằm theo dõi, ghi nhận, thu thập, gạn lọc và phát hiện những email bất lợi cho chế độ, đồng thời truy bắt những nhân vật vận động cho dân chủ, nhân quyền.

Ủy Ban Bảo Vệ Người Lao Động vừa phổ biến cách thức có thể vô hiệu hóa hoạt động của lực lượng công an Internet.

Mời quý vị theo dõi thêm chi tiết qua cuộc trao đổi giữa phóng viên Đỗ Hiếu của RFA với ông Đoàn Việt Trung, Tổng Thư Ký, Ủy Ban Bảo Vệ Người Lao Động Việt Nam, hiện định cư tại Úc Châu.

Đỗ Hiếu: Thưa ông, mới đây chúng tôi được biết là Ủy Ban Bảo Vệ Người Lao Động Việt Nam mới phổ biến cách thức làm sao có thể giữ an toàn cho email, xin ông cho biết trong bối cảnh nào Ủy Ban Bảo Vệ Người Lao Động Việt Nam có nhu cầu viết bài này và phổ biến đến tất cả người Việt toàn thế giới?

Ông Đoàn Việt Trung: Từ Khi Ủy Ban Bảo Vệ Người Lao Động Việt Nam chúng tôi được thành lập cách đây khoảng hơn một năm thì chúng tôi đã bắt đầu làm việc nhiều với một số người trong nước mà cũng cùng một chí hướng, tức là tranh đấu cho người lao động có thể lập được công đoàn để bảo vệ cho quyền lợi của họ.

Khi chúng tôi làm việc với nhau, chúng tôi nhận thấy qua kinh nghiệm làm việc thực tiễn thì nhận thấy là có nhu cầu cần phải giữ cho công an tin học của nhà nước không thể nào đọc lén email của chúng tôi được, tại vì nếu họ đọc lén được thì từ đó họ có thể truy ra những anh em làm việc với chúng tôi ở trong nước và từ đó sẽ gây hại cho họ.

Qua kinh nghiệm làm việc thực tiễn đó chúng tôi có được một số phương pháp, nhưng khi nghĩ rộng ra thì thấy không phải chỉ có chúng tôi mới có nhu cầu đó mà có rất nhiều người khác những người tranh đấu trong nước về đủ mọi đề tài, nhiều tổ chức khác ở hải ngoại này nếu có liên lạc với họ, cũng như là những thân hữu bạn bè của họ ở ngoài này, vì thế chúng tôi thấy có lẽ bài này nên được phổ biến cho thêm nhiều người biết về cách làm sao giữ cho liên lạc qua lại ra vào Việt Nam hay ngay bên trong Việt Nam để giữ được an toàn.

Đỗ Hiếu: Làm sao ông có thể biết được là nhà nước Việt Nam tuyển dụng một lực lượng công an tin học để chuyên theo dõi và ghi nhận hầu như là tất cả các nội dung email trao đổi giữa những nhà tranh đấu cho dân chủ, nhân quyền trong nước với nhau và với người hải ngoại?

Thứ nhất là thỉnh giả nên có một địa chỉ mà phổ biến bao nhiêu cũng được. Dĩ nhiên là địa chỉ đó thì không có viết gì cần phải phải bảo mật. Thứ nhì là nếu mà có viết gì cần phải bảo mật với một số người thì hãy có một số địa chỉ email riêng. Mỗi một địa chỉ đó chỉ nói cho một hoặc một số người nào đó mà mình tin cậy, mình liên lạc với họ và chỉ có họ mới biết địa chỉ email này mà thôi.

Ông Đoàn Việt Trung: Thưa anh, tôi có thể đưa ra vài thí dụ. Cách đây khoảng một năm có một nhà tranh đấu cho dân chủ trong khi đang ngồi ở một quán cafe internet thì đã bị công an ập đến bắt. Sở dĩ anh bị bắt như vậy là tại vì địa chỉ email của anh đã bị phát hiện bởi hệ thống và những công an tin học của nhà nước.

Một thí dụ khác là hồi gần đây có một người tị nạn chính trị bên Campuchia, thân nhân của họ ở Việt Nam đã bị công an kêu lên, và khi thẩm vấn người thân nhân đó thì công an đã đưa ra cho người đó thấy những email qua lại giữa người đó và thân nhân của người đó ở bên Campuchia. Điều đó chứng tỏ cho thấy là công an đã đọc lén email giữa hai người này, mặc dù là email riêng. Tuy họ đọc lén như vậy nhưng họ vẫn ngang nhiên ngạo nghễ đưa cho người ở Việt Nam coi cái email riêng mà họ đã in ra như vậy đó anh.

Đó là hai thí dụ trong số nhiều việc mà chúng tôi có thể kể ra để cho thấy việc công an tin học nhà nước có theo dõi các địa chỉ email và các cách đọc lén email qua lại là chuyện có thật. Tôi xin thưa là những email đó không phải là chỉ có email của người trong nước ra ngoài hay từ ngoài vào mà cũng có thể là email giữa những người tranh đấu sống tại Việt Nam họ viết cho nhau cũng có thể bị công an theo dõi nữa.

Đỗ Hiếu : Thưa ông, như vậy là công an tin học của nhà nước Việt Nam không có mật mã thì làm sao họ có thể vào đọc được tất cả những email mà các nhà đấu tranh dân chủ trong nước trao đổi với nhau, hoặc là liên lạc với thế giới bên ngoài?

Ông Đoàn Việt Trung: Vâng, thưa ông, chuyện đó thực ra không khó tí nào. Muốn đọc email thì công an tin học của nhà nước họ chỉ cần có 2 thứ: Thứ nhất là cái địa chỉ email của người gửi và người nhận, và thứ nhì là họ cần phải làm sao đi vào được nội dung của email, nắm được cái email đó.

Thế thì, cái thứ nhất, thưa anh, thật là quá dễ bởi vì có một số nhà dân chủ trong nước có thể nói là không cẩn thận cho lắm về việc phổ biến địa chỉ của mình. Có nhiều người họ chỉ dùng có một địa chỉ thôi để liên lạc, không những liên lạc với những người mà họ cần bảo mật mà cũng dùng cái địa chỉ đó để liên lạc với những người một cách tổng quát nữa. Thành ra với những địa chỉ được phổ biến nhiều như vậy thì công an họ dễ dàng theo dõi.

Còn về nội dung của email làm sao công an có thể nắm được thì tôi xin thưa như thế này. Với một người trong nước thì có hai trường hợp, trường hợp thứ nhất họ dùng cái web server, tức là nơi chứa thư từ của họ, cái web server Việt Nam nếu mình dùng địa chỉ email của mình tận cùng bằng **.vn** thì trong trường hợp đó tức là máy computer chứa email của mình nằm ở trong Việt Nam, những máy computer đó không phải do nhà nước làm chủ thì nhà nước cũng đều có thể quản trị cả, họ có thể đòi hỏi nội dung cả, vì thế mà họ dễ dàng đọc email của mình mà không cần mật mã. Đó là trường hợp thứ nhất, tức là dùng địa chỉ email có tận cùng bằng **.vn**.

Cũng có những người dùng địa chỉ như gmail, hotmail, yahoo! v.v... thì trong trường hợp đó thư của họ không chứa trong web server trong nước mà giữ ở cái server của những hãng như là gmail, hotmail, yahoo! ở tuốt bên Mỹ, thế nhưng trong những trường hợp đó khi họ dùng những program để đi vào website của yahoo!, gmail, v.v... để đọc email của họ thì họ phải đi qua web server, tức là máy computer mà nó nối giữa hệ thống internet trong nước với hệ thống internet trên thế giới tự do bên ngoài, và ngoài ra những nội dung đó cũng chạy qua những đường dây cáp ở trong nước, những đường dây cáp nối tỉnh này qua tỉnh khác, những đường dây cáp đó thì chủ cũng là nhà nước.

Vì thế cho nên nhà nước có thể đọc được nội dung của email đó mà không cần có mật mã, bằng hai cách, hoặc là họ chặn email tức là những tín hiệu qua lại giữa những web server, hoặc họ chặn lại trên đường dây cáp đó để họ đọc lén.

Nhưng nếu trong quý thính giả có một số người là những người tranh đấu cho Việt Nam thì vì tầm mức nguy hiểm cho nên quý vị phải làm thêm một số điều khác nữa như thế này, là khi mình viết email thì nội dung **email nên viết vô trong một tài liệu của Microsoft Word**, xong rồi khóa nó lại, dùng một mật mã (tiếng Anh gọi là encryption) khóa nó lại, xong rồi thì mình **zip bằng Winrar hay winzip**, rồi cho nó vào bên trong attach vào email thay vì thư của mình trong email.

Đỗ Hiếu: Thưa ông, về cách thức mà Ủy Ban Bảo Vệ Người Lao Động Việt Nam muốn hướng dẫn những người sử dụng email để có thể bảo vệ an toàn cho họ thì gồm có những bước kỹ thuật như thế nào?

Ông Đoàn Việt Trung: Trước khi nói về kỹ thuật tôi xin thưa về lối suy nghĩ trong đầu của mình. Việc đầu tiên mình hãy nghĩ tới email của mình, cái địa chỉ đó giống như một nơi mình chôn giấu gia tài và cái nội dung bên trong email nó giống như là gia tài của gia đình mình. Mình hãy coi nó là quý, bởi vì nếu có ai nắm được thì có thể có một số người sẽ phải vô tù. Quý như vậy đó thì mình sẽ thấy là bỏ công ra một chút để khóa tay công an cũng rất là đáng.

Nói về chi tiết thì phương pháp đó có được đăng trong bài của chúng tôi ở trang web [baovelaodong.com](http://baovelaodong.com), nhưng tôi xin thưa sơ sơ như vậy: Thứ nhất là thính giả nên có một địa chỉ mà phổ biến bao nhiêu cũng được.

Dĩ nhiên là địa chỉ đó thì không có viết gì cần phải phải bảo mật. Thứ nhì là nếu mà có viết gì cần phải bảo mật với một số người thì hãy có một số địa chỉ email riêng. Mỗi một địa chỉ đó chỉ nói cho một hoặc một số người nào đó mà mình tin cần, mình liên lạc với họ và chỉ có họ mới biết địa chỉ email này mà thôi.

Xong rồi khi mình email cho họ, dĩ nhiên những điều gì không cần bảo mật thì cứ viết địa chỉ email bình thường, viết một cách bình thường như từ xưa tới nay. Nhưng nếu có gì cần phải bảo mật thì dùng địa chỉ email bí mật đó mà viết cho họ.

Khi viết cho họ thì cái địa chỉ của họ quý thỉnh giả đừng bỏ địa chỉ của họ vào hàng "TO", "CC" (tức người nhận) mà hãy bỏ vào hàng "BCC" tức là phần mà email vẫn đến người đó nhưng không ai có thể đọc được, biết được là email đó đã được gửi tới địa chỉ đó.

Như vậy công an sẽ không tìm ra được cái địa chỉ email của họ.

Đó là những phương pháp mà tôi nghĩ là đại đa số ai cũng có thể làm được.

Nhưng nếu trong quý thỉnh giả có một số người là những người tranh đấu cho Việt Nam thì vì tầm mức nguy hiểm cho nên quý vị phải làm thêm một số điều khác nữa như thế này, là khi mình viết email thì nội dung email nên viết vô trong một tài liệu của Microsoft Word, xong rồi khóa nó lại, dùng một mật mã (tiếng Anh gọi là encryption) khóa nó lại, xong rồi thì mình zip bằng Winrar hay winzip, rồi cho nó vào bên trong attach vào email thay vì thư của mình trong email.

Tại sao như vậy? Là tại vì công an mỗi ngày có cả triệu triệu email đi vào Việt Nam thì làm sao họ đọc được mọi email, cho nên họ rà, họ kiếm trong những email trong thân hay trong phần "To" hay "BCC" hay phần của người gửi những chữ gì mà họ muốn kiếm. Khi họ muốn kiếm trong thân mà những gì mình viết lại **không viết trong thân mà lại viết trong tài liệu đính kèm thì họ sẽ khó rà hơn nhiều.**

Và nhất là những tài liệu mình đã khóa lại thì nếu họ không có mật mã thì họ không có cách nào mà mở tài liệu đó. Để khóa và để mở tài liệu đó thì quý vị và người kia cần phải có mật mã. Mật mã đó nên cho nhau biết bằng điện thoại vì nếu họ đã đọc được email thì họ cũng có thể biết được mật mã đó luôn.

Và tôi xin nhắc lại là những chi tiết này có đăng trên trang web của Ủy Ban Bảo Vệ Người Lao Động Việt Nam, địa chỉ là [baovelaodong.com](http://baovelaodong.com).

Đỗ Hiếu: Chúng tôi xin cảm ơn ông Đoàn Việt Trung, Tổng Thư Ký của Ủy Ban Bảo Vệ Người Lao Động Việt Nam, đã dành thì giờ cho Đài RFA.

Ông Đoàn Việt Trung: Dạ, xin kính chào ông. Kính chào quý thỉnh giả.

Tiếng Việt

**Tin buồn: Công an muốn ăn cắp gia tài email của bạn. Tin vui: Có cách khoá tay họ**  
Ủy Ban Bảo Vệ Người Lao Động Việt Nam

**Trong nhiều lần thăm vấn những nhà tranh đấu hoặc thân nhân của họ, công an đã ngạo nghễ đưa ra email riêng của họ mà công an đã lén đọc. Việc công an lén lút đọc email là có thật. Việc công an dùng những người như bạn, tức không phải là nhà tranh đấu được nhiều người biết đến, để làm bàn đạp hãm hại những người tranh đấu trong nước, là có thật.**

Vậy, bạn hãy coi nội dung trong email như gia tài quý báu. Còn địa chỉ email, thì hãy coi như chỗ giấu gia tài. Đừng để công an lén lút ăn cắp, gây hại cho bạn VÀ cho những nhà tranh đấu trong nước. Bài này, có đăng trên [baovelaodong.com](http://baovelaodong.com), hướng dẫn một số phương pháp, dựa vào kinh nghiệm làm việc thực tiễn của một số thành viên trong và ngoài nước của Ủy Ban Bảo Vệ Người Lao Động Việt Nam.

### **1. Tin buồn 1: Công an biết địa chỉ email của bạn**

a) Nếu bạn là người đã công khai đứng lên tranh đấu (dù ở trong nước hay hải ngoại) thì công an internet của nhà cầm quyền Hà Nội dễ dàng biết địa chỉ email của bạn.

Bạn không phải là nhà tranh đấu nổi tiếng? Dù bạn chỉ vào các forum về xã hội hoặc chính trị, hoặc dù bạn chỉ nhận email từ hay có nhắc đến những người mà công an chú ý, thì công an vẫn muốn có địa chỉ email của bạn.

Vậy thì chính bạn (người đang đọc dòng chữ này) công an có biết địa chỉ email của bạn không? Nếu các spammer đã tìm được địa chỉ email của bạn, thì hãy coi như công an cũng có thể tìm được.

b) Bạn không phải là nhà tranh đấu, thì công an mất công tìm địa chỉ email của bạn làm chi? Công an có thể chỉ dùng email của bạn làm bàn đạp để theo dõi và hãm hại họ cũng giống như kẻ gian chui vào nhà bạn để từ đó chui qua nhà hàng xóm. Những email mà bạn gửi đi, nhận được, bạn chuyển đi, hay ai khác chuyển đến bạn, nếu email có liên quan đến người hoặc việc mà công an theo dõi, thì công an đều có thể dùng làm bàn đạp.

## **2. Tin buồn 2: Công an có thể đọc nội dung email của bạn**

a) Công an không có mật mã thì làm sao đọc email của bạn được? Nhà cầm quyền làm chủ hoặc kiểm soát mọi tổng đài email (mail server) trong nước. Họ cũng làm chủ mọi đường dây huyết mạch (internet backbone) nối các web server trong Việt Nam với nhau cũng như nối Việt Nam với thế giới tự do.

Do đó, nếu bạn ở Việt Nam và dùng các mail server trong nước (thí dụ, địa chỉ email của bạn tận cùng bằng @.vn), thì khi email ra, vào, hoặc luân chuyển trong Việt Nam, chúng sẽ chạy qua các mail server này, họ có thể lén đọc dù không biết mật mã. Còn nếu bạn dùng web mail (yahoo, gmail, v.v.), thì bạn không đi qua mail server nhưng lại đi qua web server và backbone, do đó công an vẫn đọc lén được.

Còn nếu bạn ở hải ngoại thì sao? Nếu 1 email gửi nhiều người, trong đó có ít nhất 1 người ở Việt Nam, thì công an có thể dùng cách nói trên để đọc email của bạn. Nếu trong nhóm không có ai ở Việt Nam, nhưng chỉ cần 1 người trong nhóm sơ hở, là công an có thể biết tất cả những người kia đã viết gì. ‘Sơ hở’ đây, có nghĩa là thí dụ họ dùng password quá đơn giản cho hộp thư và công an đã tìm ra được password.

b) Có cả trăm triệu email, họ đọc cái nào? Họ đọc những email mà phần **FROM, TO,** hoặc **CC** có chứa những địa chỉ email họ theo dõi. Ngoài ra, họ cài máy ở các mail server, web server, và các backbone nói trên, để rà tất cả những email nào có chứa những chữ họ muốn theo dõi.

## **3. Tin vui: Bạn có thể khóa tay kẻ trộm mà không tốn nhiều công sức**

Bạn có thể khóa tay kẻ trộm bằng cách có 1 địa chỉ email mà công an đến cũng không sao, chỉ phí công những kẻ trộm này, và có một số chỗ bí mật để chứa gia tài:

a) Dùng 1 địa chỉ email công khai, **không bao giờ viết gì cần bảo mật (cả trong phần TO, CC lẫn trong thân email)**. Địa chỉ này chỉ để dùng cho việc phổ biến tin tức rộng rãi hoặc để nói những việc vô thưởng vô phạt.

b) Làm ra một số địa chỉ email bí mật, và thường xuyên thay đổi mật mã. Mỗi địa chỉ này chỉ cho một thân hữu, hoặc một nhóm thân hữu, biết. Nếu không nhớ được các địa chỉ email hay các mật mã thì bạn viết xuống giấy, hoặc trong máy điện thoại di động, chứ đừng viết trong máy điện toán.

## **4. Nếu là người tranh đấu, bạn nên làm thêm một số điều dưới đây**

Trên đây là những việc mà ai cũng nên làm. Còn nếu bạn là người tranh đấu và đang sống trong Việt Nam, hoặc nếu bạn ở hải ngoại nhưng liên lạc bằng email với những người nói trên, thì:

### **\*4A- Những cách để giữ an toàn cho địa chỉ email**

a) Khi viết email, **đừng dùng phần TO hay CC, hãy dùng phần BCC**. Trong hàng **TO**, chỉ biên địa chỉ của chính mình (tức là mình gửi cho mình), hoặc biên địa chỉ nào đó không có thật. Nếu thân hữu của bạn cho bạn địa chỉ bí mật của họ mà bạn lại cho vào phần **TO** hay **CC**, thì .. bật mí. **Dùng phần BCC thì công an bí**.

b) Không chuyển (forward) email nào có địa chỉ email của thân hữu mình, vì làm vậy sẽ lộ địa chỉ email của họ. Nếu phải chuyển, thì nhớ xóa các hàng **FROM, TO, và CC**.

### **\*4B- Những cách để giữ an toàn cho email**

a) Xóa email đi sau khi đọc (Xóa ở hộp Inbox, hộp Sent, VÀ thùng Trash). **Nếu cần giữ thư thì in ra, hoặc cho vào đĩa cứng**. Như vậy, nếu công an có tìm được mật mã để vào ngòi lén trong thùng thư của bạn, kẻ trộm sẽ phải ra về tay không, hậm hực.

b) **Không viết những điều cần bảo mật trong thân của email**, mà viết trong một hồ sơ, zip nó, rồi đính kèm. Tại sao? Vì công an rà các email ra vào Việt Nam để tìm những email có chứa chữ gì đó mà họ muốn theo dõi, nhưng rà **tài liệu đính kèm thì mất công hơn nhiều**. Và rà tài liệu đã zip thì còn mất công hơn nữa. **Để đánh lạc hướng công an, bạn có thể viết vài câu vô thưởng vô phạt vào thân của email**. Để zip, bạn có thể dùng WinZip hay RAR.

c) Bạn hãy khóa (encrypt) hồ sơ thư nói trên. Chia khóa thì nói cho nhau nghe trên điện thoại hay viết trong SMS, chứ không tiết lộ qua email. Và để nhớ thì viết trên giấy, đừng viết trong máy. Việc khóa tài liệu, mới nghe thì tưởng khó và tốn thời giờ lắm. Nhưng bạn hãy thử, sẽ thấy rất dễ. Trong Microsoft Word 2007, bạn bấm Alt-F rồi Prepare (thứ 7 từ trên xuống) rồi Encrypt Document (thứ 4 từ trên xuống). Sau đó đánh máy chia khóa vào.

\*\*\*

Vậy tốt nhất là viết bài trong Microsoft Word, sau đó gửi đính kèm, và không bao giờ viết bài trong thân email. Cũng như không bao giờ copi những bài mình đã nhận được, dán vào trong thân email. Rồi gửi trở lại người nhận.

Tóm lại, nội dung email là gia tài, và địa chỉ email là chỗ cất gia tài. Xin bạn cẩn thận để chính mình khỏi bị kẻ gian quấy phá, và nhất là để bảo vệ những nhà tranh đấu trong nước.

### **Cấm Nang Vượt Tường Lửa (FIREWALL) vs Việt Nam An Toàn**

Internet Guide for Vietnam -August 2002

Cấm nang Internet cho Việt Nam -Tháng Tám,2002

**Tóm lược:** Chính quyền nhà nước Việt Nam đã hình thành một bức tường lửa trên mạng Internet toàn quốc để cản trở nhiều người trong nước vô các trang nhà nước kiểm duyệt và cảm đoán. Các trang web sites nói về vấn đề dân chủ và nhân quyền là những trang bị cấm và bị bưng bít nhiều nhất. Cấm nang này vẫn tắt tìm hiểu bức tường lửa và quan trọng hơn cùng cố căn bản với kiến thức để vượt khỏi hàng rào cản thông tin đích thực của thế giới.

**Lời mở đầu:** Nhà nước cộng sản Việt Nam hiểu rằng mạng lưới Internet có lẽ là một phương tiện truyền thông tự do nhất. Khi mạng lưới Internet được mở ra rất trễ ở Việt Nam vào cuối thập niên 90, nhà nước đã dùng bức tường lửa, một công cụ bằng phần mềm để che dấu và chặn tin tức trung thực từ bên ngoài. Bức tường lửa của Việt Nam cản trở và che đậy những thông tin trung thực của các trang diễn đàn điện tử thế giới nói về vấn đề dân chủ và nhân quyền. Thật không phải là điều ngạc nhiên gì cho lắm, cộng sản Việt Nam là một trong số ít 21 quốc gia trên thế giới đang phải vật lộn để cấm đoán dân chúng không được đọc những thông tin dân chủ. Chẳng hạn,nếu người sử dụng muốn vô trang [www.lmvntd.org](http://www.lmvntd.org), trang của Liên Minh Việt Nam Tự Do, thì bức tường lửa sẽ tức khắc không cho vô và đồng thời cho hiện lên những hàng chữ vô hại như "The page cannot be displayed" hoặc "Access Denied" làm người sử dụng ngây thơ tưởng rằng trang đó không hiện hữu nữa. Thật ra, những trang này đa số vẫn còn truy cập rất dễ dàng tới các nước tự do. Vì vậy, cấm nang này sẽ gồm 3 phần để giúp bạn tìm hiểu thêm và để không chế lại tình trạng che đậy sự thật của tập đoàn lãnh đạo độc tôn cộng sản Việt Nam. Trong phần đầu tiên, phần kỹ thuật, bức tường lửa sẽ được giải thích. Trong phần thứ hai, một số cách để vượt khỏi bức rào cản của tường lửa sẽ được trình bày cùng các bạn. Trong phần thứ ba, những huyền thoại, sự thật và những mảnh khốe để giúp người sử dụng mạng internet sẽ được trình bày. Nếu bạn đã hiểu được về bức tường lửa thì phần thứ nhất cũng có thể bỏ qua. Và cuối cùng,bài viết cấm nang này đã được viết bằng cả hai thứ tiếng, Anh và Việt cho tất cả đồng bào Việt Nam.

Cấm nang này sẽ được tác giả cập nhật hóa mỗi khi có tin tức và kỹ thuật mới. Các bạn hãy cùng với những người yêu chuộng tự do, dân chủ phân phát cấm nang này đến thật nhiều người sử dụng mạng internet ở Việt Nam cũng như ở hải ngoại. Các bạn có thể đăng nó lên những diễn đàn thảo luận trên mạng internet hoặc gửi bằng email đến cho bạn bè. Thêm nữa, những đóng góp về bài viết này xin được gửi tới:

\*<http://us.f206.mail.yahoo.com/ym/Compose?To=ig4vn@yahoo.com> cùng với những kinh nghiệm của bạn về bức tường lửa Việt Nam. Nhưng vì lý do an ninh, bạn sẽ KHÔNG nhận được hồi âm của chúng tôi. Nếu email của bạn không bị trả lại, điều đó có nghĩa là email bạn sẽ được đọc.

\*\*\*

## Phần 1-Bức Tường Lửa

Con đường vào mạng Internet thế giới của Việt Nam được đặt tại Hà Nội. Điều này có nghĩa tất cả mọi giao dịch trên mạng internet phải bắt buộc thông qua con đường độc đạo kiểm soát tại Hà Nội trước khi tới được mạng internet của thế giới. Trụ sở thông tin này được gọi là proxy.Proxy là một hệ thống của nhiều máy điện toán được nối lại với nhau để giúp nối bạn vô mạng internet. Chẳng hạn bạn đang ngồi ở quán internet café tại Sài Gòn và ra lệnh cho máy truy cập trang của hãng thông tấn [www.cnn.com](http://www.cnn.com). Khi mà nhấn nút để gửi lệnh đi, thì lệnh của bạn sẽ được chuyển tới trụ sở kiểm soát proxy ở Hà Nội. Sau khi đó thì lệnh sẽ được gửi tới máy chính của hãng thông tin ở Atlanta, Tiểu Bang Georgia, nước Mỹ. Sau đó trang của Hãng thông tin CNN sẽ được gửi tới Hà Nội và sau cùng tới máy của bạn ở Sài Gòn. Sự kiểm soát mạng lưới internet từ một điểm ở Hà Nội cũng bao gồm thư điện tử email cũng như nói chuyện trên mạng như là chatting rất phổ biến hiện nay.

Với một điểm kiểm soát proxy tại Hà Nội, chính quyền bưng bít cộng sản Việt Nam rất dễ dàng kiểm soát tất cả những nội dung của các trang trên mạng internet mà bạn coi được. Nhà nước đã dùng công cụ phần mềm để cấm đoán các trang trên mạng internet không có lợi cho độc đảng cộng sản Việt Nam. Một bộ phận mềm như trên đã giúp nhà nước tạo nên một bức tường lửa không lồ bao trùm cả đất nước Việt Nam. Từ xưa khi mạng internet mới ra đời, bức tường lửa thông thường được các công ty lớn dùng đến để bảo vệ thông tin nằm trong những máy điện toán của mình. Nhưng nhà cầm quyền cộng sản Việt Nam đã đã man dùng biện pháp này để khống chế và những tin tức dân chủ, nhân quyền thật sự tại Việt Nam. Những trang dân chủ như [www.lmvntd.org](http://www.lmvntd.org) đều bị bức tường lửa cản, không cho qua khỏi cổng proxy tại Hà Nội tới người đọc.

Bức tường lửa hoạt động bằng cách dùng một danh sách có địa chỉ của những trang internet không có lợi cho đảng và không cho phép các máy điện toán truy cập những trang này. Chỉ có những trang internet không bị cấm trong danh sách mới được điếm proxy tại Hà Nội cho thông qua. Những phương cách trong cẩm nang này sẽ tìm cách khắc phục và vượt qua cấm đoán của bức tường lửa quái đản của một chế độ độc tài có một không hai trên thế giới này.

## Phần 2- Để vượt bức tường lửa.

Có một số cách để vượt khỏi bức tường lửa của Việt Nam. Đa số các cách nằm trong bốn loại sau đây:

- 1) Giấu tung tích của địa chỉ.
- 2) Dùng những trang đã được lưu trữ sẵn.
- 3) Dùng máy điện toán của những người yêu dân chủ và nhân quyền làm điếm truy cập thay vì điếm proxy của Hà Nội.
- 4) Dùng dịch vụ của công ty chuyển thư WebMailer.

Tóm tắt những cách vượt bức tường lửa:

1.- Giấu tung tích của địa chỉ muốn tới: Đây là cách nhanh nhất để truy cập những trang bị cấm. Có nhiều trang trên mạng internet giúp chúng ta giấu địa chỉ truy cập để qua mặt được Hà Nội. Giả thử bạn muốn truy cập trang của Liên Minh Việt Nam Tự Do, [www.lmvntd.org](http://www.lmvntd.org), bạn sẽ chẳng thấy gì trên màn hình bởi trang này bị bức tường lửa chặn. Nhưng khi muốn giấu tung tích của nơi bạn muốn tới, trang [www.anonymizer.com](http://www.anonymizer.com) sẽ giúp bạn. Từ ngay trong trang [www.anonymizer.com](http://www.anonymizer.com), bạn có thể đánh chữ [www.lmvntd.org](http://www.lmvntd.org) vào để giấu tung tích. Khi địa chỉ [www.lmvntd.org](http://www.lmvntd.org) đã bỏ dấu, điếm proxy ở Hà Nội sẽ không chặn được.

Nhưng, bạn có thấy một điểm nhỏ cần chú ý không? Nhà cầm quyền cộng sản Việt Nam cũng có thể chặn không cho chúng ta truy cập [www.anonymizer.com](http://www.anonymizer.com). Nhà nước đã cho [www.anonymizer.com](http://www.anonymizer.com) vô danh sách đen, vì vậy, không thể truy cập trang internet này ở Việt Nam nữa. Sau đây là danh sách của một số trang internet cũng có chức năng giống như [www.anonymizer.com](http://www.anonymizer.com). Một số đã bị vô sổ đen của nhà nước:

<http://www.anonymizer.com/>  
<http://www.phantomip.com>  
<https://proxy1.autistici.org/>  
<http://www.the-cloak.com/login.html>  
<http://www.guardster.com/>

Ngoài những trang này ra, bạn có thể vô [www.google.com](http://www.google.com) và đánh vô chữ **web anonymizer** hoặc **web mailers** để tìm thêm những trang tương tự. Mong bạn có thể tìm thấy những trang chưa hân hạnh được vô sổ đen bức tường lửa của nhà nước.

2.- Dùng những trang đã được lưu trữ sẵn: Những trang được lưu trữ cũng giống như một cuốn sách lịch sử. Dịch vụ lưu trữ những trang internet được miễn phí tại các địa chỉ sau đây: [www.archive.org](http://www.archive.org) và [www.google.com](http://www.google.com). Cũng giống như phần trên, khi bạn truy cập [www.archive.org](http://www.archive.org), bức tường lửa sẽ không biết bạn đang truy cập những gì. [www.archive.org](http://www.archive.org) rất dễ xài, bạn chỉ việc vô đó và đánh tên địa chỉ mình muốn tới, chẳng hạn như [www.lmvntd.org](http://www.lmvntd.org) thì dịch vụ này sẽ cho bạn thấy trang [www.lmvntd.org](http://www.lmvntd.org) được lưu trữ. Dịch vụ lưu trữ này thường không cho ta thấy trang internet trực tiếp nhưng cho ta thấy trang này trong tình trạng được lưu trữ, có thể đã có một vài tuần hoặc vài tháng. Còn [www.google.com](http://www.google.com) thì cũng một phần tương tự. Google cũng lưu trữ toàn thể các trang của internet. Thí dụ để coi trang [www.lmvntd.org](http://www.lmvntd.org), bạn truy cập trang [www.google.com](http://www.google.com) và đánh vô [www.lmvntd.org](http://www.lmvntd.org). Google sẽ hiện ra những gì kiếm được, bạn chỉ bấm vô "Show Google's cache of [www.lmvntd.org](http://www.lmvntd.org)" thì sẽ thấy được trang lưu trữ cách đây vài tháng. Với cách này, nhà nước Việt Nam không dám chặn những trang internet nổi tiếng như google vì có quá nhiều người xài, kể cả khách ngoại quốc.

3.- Dùng máy điện toán khác để tránh điểm proxy bùng bít của Hà Nội: Bây giờ bạn hãy tưởng tượng nếu chúng ta dùng một loại kỹ thuật mới tránh né proxy của Hà Nội. Điều gì sẽ xảy ra nếu chúng ta nối cả triệu máy điện toán cá nhân trên thế giới lại? Câu trả lời như sau: Nối hàng triệu máy điện toán cá nhân của tất cả thế giới tự do là mục đích của hai chương trình Peekabooty và Six/Four. Khi bạn ra lệnh truy cập [www.lmvntd.org](http://www.lmvntd.org), thì điểm proxy của Hà Nội sẽ phải gửi lệnh tới một trong hàng triệu máy điện toán cá nhân. Một máy cá nhân này sẽ lập tức giúp và gửi lệnh cho bạn xem nội dung của [www.lmvntd.org](http://www.lmvntd.org). Proxy của Hà Nội sẽ tưởng rằng địa chỉ của máy cá nhân này là địa chỉ vô hại. Đây sẽ là một vấn đề nhức đầu cho chính quyền Việt Nam vì rất khó cảm đoán. Thứ nhất, đây là tập hợp của hàng triệu máy điện toán và địa chỉ của mỗi máy (IP address) đổi từng giây từng phút, không thể kiểm soát nổi. Thứ hai, cả triệu máy điện toán được tập hợp của toàn thế giới, cộng sản Việt Nam sẽ phải bó tay vì không thể biết hết ai là ai. Vấn đề này y hệt như những gì đã xảy ra cho kỹ nghệ âm nhạc và phim của Hoa Kỳ, khi các chương trình nổi tiếng như Napster, Kazaar, AudioGalaxy, Morpheus và iMesh đã dùng hàng triệu máy trên thế giới để trao đổi dữ liệu nhạc và phim. Hai chương trình Peekabooty ([www.peek-a-booty.org](http://www.peek-a-booty.org)) và Six/Four ([www.hacktivism.com](http://www.hacktivism.com)) sắp sửa được ra đời vào mùa Thu năm 2002. Bạn hãy theo dõi.

3.- Trang internet nằm trong Thư Điện Tử-Webmailer: Kỹ thuật thư điện tử này rất khác với 3 cách trên. Thư điện tử webmailer cũng là một phương cách hữu hiệu để xem tin tức dân chủ. Thư điện tử sẽ giúp bạn coi trang internet bị cấm trong thư email của bạn. Dùng một địa chỉ điện thư miễn phí như Yahoo hoặc Hotmail, bạn ghi địa chỉ muốn coi vô phần Subject: và gửi tới một địa chỉ dịch vụ internet miễn phí <http://us.f206.mail.yahoo.com/ym/Compose?To=www@web2mail.com>. Sau đó, dịch vụ này sẽ gửi trang internet mà bạn muốn coi tới hộp thư điện tử của bạn. Nhà nước không thể kiểm

soát nội cách này vì không thể nào chặn được hộp thư miễn phí của Yahoo hoặc Hotmail. Với dịch vụ này, bảo đảm bạn sẽ được coi các trang bị bức tường lửa cảm, nhưng bạn phải kiên nhẫn đợi cho dịch vụ gửi lại trang internet, có thể đợi 10 phút hoặc một ngày sau.

Phần 3-Thêu dệt, sự thật và mảnh khõe để sử dụng internet tại Việt Nam.

Nhà nước Việt Nam có thể chặn thư gửi và thư nhận trong hộp thư điện tử? Đúng và sai. Hộp thư với chữ .vn ở cuối (ví dụ như <http://us.f206.mail.yahoo.com/ym/Compose?To=tudodanchu@ftp.vn>) có thể bị nhà nước chặn và đọc và bị sửa chữa vì những hộp này do sự quản lý của nhà nước. Vì vậy, các bạn nên dùng địa chỉ như Hotmail hoặc Yahoo. Vì nhà nước Việt Nam không thể chặn những dịch vụ hộp thư điện tử miễn phí này (thư của bạn có thể bị nhà nước mở ra đọc)

Khi tôi sử dụng Yahoo hoặc Hotmail, nhà nước không đọc được hộp thư của tôi? Sai, tất cả giao thông của xa lộ internet vào Việt Nam phải qua cổng Hà Nội. Yahoo và Hotmail không mã hóa lần thông tin email. Vì vậy nhà nước có thể mở thấy được thư của bạn. Để an toàn, bạn có thể làm một hộp thư dùng riêng nhưng không có tin tức thật về bạn.

Như vậy có cách nào để không ai đọc được thư điện tử của tôi không? Nếu bạn không muốn ai đọc email của bạn, bạn hãy sử dụng kỹ thuật mã hóa gọi là encryption. PGP Encryption ([www.pgpi.org](http://www.pgpi.org)) sẽ giúp bạn sử dụng kỹ thuật này nếu xài đúng cách. Những trang internet này cũng hơi khó sử dụng. Cho nên cách thứ 2 là tại trang [www.hushmail.com](http://www.hushmail.com) để đăng ký sử dụng. Cách này an toàn khi cả hai, người gửi lẫn người nhận, đều dùng [www.hushmail.com](http://www.hushmail.com). Làm sao đây? Tôi muốn tẩy xóa dấu vết của tôi sau khi xài internet tại quán café? Đúng vậy, bạn có thể tẩy xóa dấu vết của bạn khi đã xài internet khi bạn dùng Internet Explorer. Để cho nhà nước khỏi được quyền quản lý quyền tự do của bạn, hãy bấm vô chữ Tools/Internet Options. Bấm vô nút "Delete all offline content" và sau đó, "Delete Files", rồi "OK". Nếu thấy nút "Delete Cookies" hãy bấm vô nút đó luôn. Sau đó, bấm vô "Settings" rồi bấm vô "View Files". Nếu mà còn một số file trong đây, bạn bấm Ctrl-A để chặn tất cả rồi bấm nút Delete trên bàn phím. Như vậy bạn đã xóa đi rất nhiều vết chân lang thang trên internet. Cho chắc ăn, bạn cũng có thể bấm nút "Clear History" và bấm "OK". Bây giờ, bấm vô nút "Content" và sau đó vô nút "AutoComplete". Sau đó bấm vô nút "Clear Forms" và "Clear Passwords" để xóa tất cả mọi ô mật mã. Chúc may mắn.

Người Việt hải ngoại nhiều thời gian rảnh quá, làm những chuyện bôi nhọ cộng sản Việt Nam? Thật ra, ít ai ở hải ngoại có nhiều thì giờ. Nhưng vì người Việt hải ngoại rất quan tâm về vấn đề dân chủ và nhân quyền của Việt Nam, nhưng điều hiển nhiên trong đời sống của các nước tôn trọng tự do, nhân quyền. Tiếc thay, đất nước của chúng ta vẫn còn bị cai trị bởi bọn quý đồ độc tài cộng sản, việt cộng. Tiền đồ đất nước, Ải Nam Quan, cũng bị dấu nhem và bị việt cộng cắt đất cho Tàu vào năm 1999 và 2000. Còn tự gửi địa chỉ của những trang internet bị cấm đến với hộp thư Yahoo hoặc Hotmail của chính tôi. Làm như vậy thì lệnh truy cập của tôi qua Yahoo hoặc Hotmail chứ không phải proxy Hà Nội phải không? Sai. Nhưng đây là ý rất hay. Khi tác giả thử phương pháp này tại Việt Nam, phương pháp đã không hiệu nghiệm. Lý do là sao? Bởi vì proxy Hà Nội cũng có thể đánh hơi được nội dung của trang internet và bức tường lửa sẽ hoạt động trở lại.

Khi dùng những chương trình chat như AOL Instant Messenger (AIM) hoặc MIRC, nhà nước không kiểm soát nổi? Sai, nhà nước không có chặn khi bạn chat, nhưng có thể thấy những gì bạn viết.

Nhiều quán internet café dựng nên một trang chính giúp bạn truy cập những trang như Hotmail và Yahoo cho nhanh chóng. Nguy hiểm không? Vấn đề là, những trang chính có thể giữ lại tên và mật mã của bạn, nên họ có thể vô lại hộp thư điện tử của bạn. Nên coi chừng. Câu cuối là: Tôi sẽ không dám gửi cảm nang này tới bạn bè, tôi sợ. Thật ra, cảm nang này sẽ được quảng bá mạnh mẽ. Bạn và những người quen biết chỉ là một trong số rất lớn nhận được cảm nang này qua mạng các diễn đàn (forum), thư điện tử, trang chính và nhiều phương tiện truyền thông nữa. Để an toàn, bạn hãy mở những hộp thư giả của Yahoo hoặc Hotmail ra cho

bạn bè, người thân mình vô đọc những tin tức tự do thế giới. Nhưng dưới mắt của lãnh đạo cộng sản độc tài tham nhũng già nua là phản động.

Bây giờ là câu hỏi chốt. Có trang internet nào đó tôi vô tìm hiểu và đọc được những bài về tin tức về dân chủ và nhân quyền Việt Nam không? Tôi cũng muốn thử tài vượt bức tường lửa hiệu nghiệm đến cỡ nào sau khi đọc bài này.

Sau đây là các trang internet hay bị nhà nước bưng bít:

- www.lenduong.net - www.lmvtnd.org - www.saigonbao.com - www.vietland.net -  
www.vietquoc.com - www.daiviet.org - www.lephai.com - www.danchu.net -  
www.conong.com - www.ykien.net - www.thongluan.org - www.shcd.de -  
www.nsvietnam.com - www.tudotgvn.org - www.vietnamvietnam.com - www.fva.com -  
www.hannamquan.com

## KẾT LUẬN

Trong chế độ cộng sản độc tài Việt Nam, nhà nước phải vật lộn để bưng bít những thông tin đích thực ngoài nước. Đây nhằm chiêu bài tuyên truyền và xuyên tạc của cơ quan chức năng quản lý thông tin của nhà nước. May mắn thay, rất nhiều người xài internet tại Việt Nam đã nhận ra được điều cảm đoán bất công này, vì đa số tất cả mọi người trên thế giới ít ai bị kềm kẹp như Việt Nam. Chỉ có những chế độ hay nói dối, hay vẽ vờ, và độc tài mới sợ sự thật, ánh sáng của dân chủ và nhân quyền. Các bạn hãy quảng bá và giúp người dân biết cách vượt rào cản thông tin mà việt cộng đã bao trùm lấy đất nước Việt Nam. Như vậy, ta đã làm một điều quý giá cho đất nước mai sau để ta không phải hộ thân với lương tâm. Hãy cho mọi người thấy rằng chủ nghĩa cộng sản đã sắp đổ toàn cầu nhưng vẫn ngự trị tàn bạo trên đất nước của chúng ta. Nếu có ý kiến và đóng góp, xin cho chúng tôi biết qua thư điện tử, chân thành cảm ơn.

**BẠN NÊN LÀM NHỮNG GÌ SAU KHI TRUY CẬP INTERNET Ở NƠI CÔNG CỘNG ?**

Nguyễn An, phóng viên Đài RFA

Thường thì bạn không muốn danh tính, và từ đó, nhân thân của mình lưu lại trên máy vi tính nếu bạn sử dụng máy tại các nơi công cộng chẳng hạn như tiệm cho thuê máy, hay các cybercafes.

Nếu muốn như thế, bạn sẽ phải xóa ID của mình sau khi sử dụng xong, nhất là sau khi truy cập vào Internet. Bạn sẽ phải làm những gì? Sau đây là một số điều được các chuyên viên Internet đã nghĩ.

Trước khi rời khỏi nơi mà bạn vừa sử dụng máy vi tính để truy cập Internet, bạn nên làm lần lượt những việc sau đây:

**TOOLS**

**INTERNET OPTIONS**

**CLEAR HISTORY-DELETE FILES-DELETE COOKIES-TEMPORARY INTERNET FILES**

**GENERAL. CLEAR PASSWORDS-CLEAR FORMS-AUTOCOMplete-PERSONAL INFORMATION -CONTENT**

Bây giờ thì bạn có thể rời khỏi tiệm cho thuê máy vi tính được rồi.

Chúc các bạn may mắn.

## **Internet Protocol**

IP là chữ tắt của Internet Protocol (không phải là địa chỉ nhà mình ở). IP address là địa chỉ của IP mà khi mua dịch vụ internet được cung cấp qua máy **modem** (dùng cable TV hay cable điện thoại), gọi là WAN ( wide area network) IP address ví dụ: 99.230.221.231. Thường thì dịch vụ cung cấp linh động dynamic IP address thay đổi liên tục trong vài ngày, vài tuần...

Khi mình muốn dùng nhiều máy điện toán 1 lúc thì xài router có dây hoặc wireless không dây thì router cho mình LAN (local area network) IP address, ví dụ 192.168.1.1... mỗi

1 computer trong 1 nhà có 1 LAN IP address riêng, ví dụ: 192.168.1.2, 192.168.1.3... nhưng đều có chung 1 WAN IP address ra ngoài thế giới.

Câu hỏi: Như vậy nếu họ dùng wireless internet lấy IP của hàng xóm, hay xách laptop đi ra ngoài quán cafe, vào office thì IP đó có bị nhận diện không?

Trả lời: Tất cả những IP đó đều được nhận diện khi vào Internet. Khi xài 1 trương mục của 1 trang nhà nào đó thì khi vào thăm trang nhà đó, hệ thống của trang nhà sẽ tự động tạo 1 bản ghi nhận tất cả các WAN IP address mà bạn đã dùng account với user name và password bạn đã log in vào. Khi muốn block account này thì dựa vào bản ghi nhận này mà block tất cả các IP đã log in.

Tất nhiên là cũng có cách gỡ. Người này chỉ cần tạo 1 trương mục, biệt danh khác, mật mã khác, điện thư ghi danh khác, đổi dịch vụ internet khác để có WAN IP address khác hoặc gọi cho công ty dịch vụ yêu cầu thay đổi WAN IP address hoặc chờ cho dynamic WAN IP address tự thay đổi WAN IP Address khác, hoặc qua quán cafe internet khác hoặc dùng wireless internet câu trộm nhà khác thì cũng vào trang nhà đó được thôi !

Ở các nước ngoài Việt Nam thường thì ít (hay không có) ai thuê bao cung cấp dịch vụ Internet với số IP cố định thường là mắc hơn. Còn ngoài ra toàn là số IP không cố định nghĩa là số IP này bị công ty cung cấp dịch vụ **Internet thay đổi mỗi lần tắt Modem** hay để lâu không dùng. Nếu Dial-up miễn phí như Netzero hay Juno thì chỉ khi nào vào mạng nhập nhập đường Internet của họ, họ mới cung cấp số IP mà thôi. Nếu cho ghi danh như vậy thì người dùng (user name) khi trình thẻ hội viên sẽ không được cho phép vì 2 dãy số sau cùng của số IP bị thay đổi.

### **Làm sao để đọc thư chữ "Miên" trên điện thư? ..**

“CHÃ°c em má»™Mt ngÃ y em Ä‘á°p vÃ há°nh phÃ°c bÃ°n Gia Ä‘Ä¬nh”

Làm sao để đọc email có font bị mã hóa?

Bài viết ở sau sẽ đưa ra một giải pháp hiệu quả, giúp bạn đọc được một e-mail tiếng Việt font Unicode nhưng bị biến dạng thành những ký tự như #&1234...

Khi soạn và gửi email, trình mail client của người gửi sẽ mã hóa email theo một chuẩn đã quy định của trình soạn thảo. Thư gửi đến máy chủ, trình mail client của người nhận tải thư về rồi mã hóa ngược lại thì người nhận mới xem được email. Cho nên, nếu có lỗi xảy ra trong quá trình mã hóa xuôi hoặc ngược, hoặc bị lỗi trên đường truyền thì người nhận không xem được email. Khi gặp trường hợp này, nếu email được mã hóa theo chuẩn UTF-8, bạn có thể tự mã hóa ngược để xem. Nhưng trước hết, nếu bạn đang dùng Outlook Express thì hãy vào View > Encoding > More, chọn Unicode UTF-8 (hoặc Unicode UTF-7) xem có được không, nếu không thì thực hiện mã hóa ngược theo cách sau đây:

- Chạy chương trình thiết kế web Microsoft FrontPage, mở một trang mới, bấm nút HTML để hiện phần source của trang này, tìm dòng charset=windows-1252, sửa lại thành charset=UTF-8.

- Chạy chương trình Notepad (Start > Programs > Accessories > Notepad hoặc Start > Run, gõ notepad, bấm OK).

- Quét chọn nội dung email, bấm Ctrl+C để copy, dán vào cửa sổ Notepad, bấm Ctrl+A để chọn toàn bộ nội dung vừa dán vào, bấm Ctrl+X để cắt.

- Trở lại cửa sổ FrontPage, đặt con nháy ở giữa cặp thẻ <body> </body>, bấm Ctrl + V để dán vào. Cuối cùng, bấm nút Preview để xem.

- Hoặc:

<http://www.enderminh.com/minh/vnconversions.aspx>

## Một số lưu ý cơ bản để sử dụng Internet an toàn

Khi dùng email:

1. Khi vào một webmail, nếu chương trình webmail hỗ trợ giao thức bảo mật HTTPS, thì bạn dùng phương thức này thay vì giao thức HTTP thông thường. Gmail là một trong các webmail có HTTPS. Bạn có thể vào Gmail qua:

<https://gmail.com> thay vì <http://gmail.com>

2. Khi đăng nhập hòm thư, nếu máy tính hỏi có ghi nhớ password tự động hay không, bạn trả lời KHÔNG

3. Khi dùng hòm thư, bạn không nên lưu trữ các thông tin về danh tính hay thông tin mật trong hòm thư, mà nên xóa hoàn toàn (sau khi đã ghi nhớ hoặc cất giấu ở một nơi an toàn). Để xóa hoàn toàn, sau khi dùng chức năng Delete thư cần xóa, bạn vào thùng rác (trong Gmail có tên là Trash, trong các webmail khác có thể có tên khác) để xóa hẳn thư đó.

4. Ngoài ra, để gửi những thông tin mật một cách an toàn, bạn có thể sử dụng một chương trình mã hóa tài liệu và email là PGP. Cách sử dụng chương trình này có trong phần “Bảo mật thật sự cho thư điện tử cá nhân” của “Cẩm nang blogger & người bắt đầu chính kiến” do Tập Hợp Thanh Niên Dân Chủ chuyển ngữ. Bạn có thể download cẩm nang từ địa chỉ:

[http://thtndc.com/index.php?option=com\\_docman&task=cat\\_view&gid=49&Itemid=72](http://thtndc.com/index.php?option=com_docman&task=cat_view&gid=49&Itemid=72)

5. Thận trọng với những bức thư không rõ người gửi, không nên nhấp vào các link trong thư lạ cũng như mở các file đính kèm một khi bạn không chắc chắn về sự an toàn của chúng.

Khi duyệt web:

6. Khi rời khỏi một trình duyệt, các dấu vết duyệt web còn được lưu trong thư mục:

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files

Bạn có thể xóa các dấu vết bằng cách vào đường dẫn trên, chọn tất cả các file và xóa chúng.

Hoặc một cách khác:

Từ menu của cửa sổ trình duyệt Internet Explorer nào đó đang mở, bạn vào Tool/Options..., một cửa sổ cho phép thiết lập các tùy chọn khi dùng Internet sẽ hiện ra. Ngay tại Tab đầu tiên, như hình dưới đây:

[http://www.tufat.com/docs/gallery/images/internet\\_options.gif](http://www.tufat.com/docs/gallery/images/internet_options.gif)

Bạn chọn Delete Cookie, Delete Files và Clear History.

7. Khi duyệt web, tốt nhất bạn dùng một trình duyệt vượt tường lửa có chức năng che và xóa dấu vết các trang web được duyệt qua, như trình duyệt OperaTor, mà bạn có thể download từ:

<http://archetwist.com/en/opera/operator>

Trên trang này, bạn tìm đến link:

[OperaTor 2.6b - PBwiki](#)

[OperaTor 2.6b - WikiSend](#)

Download và giải nén file vừa download. Sau đó chạy file OperaTor.exe trong thư mục vừa giải nén, trình duyệt OperaTor sẽ mở ra như một trình duyệt Internet Explorer, và bạn có thể dùng bằng cách nhập địa chỉ trang muốn vào vào ô địa chỉ.

8. Thận trọng khi nhấp vào các link trên các trang web hay cài đặt các file mà bạn không rõ về sự an toàn.

Lưu ý khác

9. Máy tính của bạn nên được cài đặt phần mềm anti virus, anti spyware hay những chương trình bảo vệ khác. Ngoài ra, hãy cẩn thận khi trao đổi với người lạ không quen biết trên Internet.

## **Bảo Mật: Đặt bẫy bắt kẻ xem trộm hộp thư!**

Bạn có thể kiểm tra xem hộp thư của mình có bị ai đó xem trộm hay không bằng cách đặt một cái “bẫy” khá hữu hiệu.

Người sử dụng email nay không chỉ dùng hộp thư của mình để gửi email đơn thuần. Với việc các nhà cung cấp dịch vụ ngày càng mở rộng không gian lưu trữ (hơn 6 GB của Gmail, 5 GB với Hotmail và không giới hạn của Yahoo), hộp thư còn được dùng với mục đích lưu trữ thông tin cá nhân, lưu trữ mật khẩu, số tài khoản ngân hàng, tài khoản sử dụng, thư từ cá nhân và nhiều thứ khác nữa.

Vì thế hộp thư trở thành một mục tiêu béo bở cho hacker. Một khi hacker đánh cắp được mật khẩu email của bạn, họ dễ dàng đọc được nội dung mail của bạn và “Unread Again” để bạn không thể biết được là mail đã bị đọc. Để ngăn chặn tình trạng này, cách tốt nhất là bạn làm một “bẫy chuột” để nếu có ai đó xem trộm email của bạn là bạn sẽ bắt được ngay “con chuột” đó. Việc tạo bẫy rất đơn giản, chỉ mất chưa đến 5 phút:

1. Đăng ký một tài khoản miễn phí tại trang [www.onestatfree.com](http://www.onestatfree.com) bằng cách bấm vào dòng Register now for your free hit counter, bấm Accept để chấp nhận các điều khoản. Sau đó điền các thông tin bắt buộc vào các dòng và chú ý ở dòng thứ 10 (URL) bạn điền địa chỉ của hộp thư (ví dụ với tài khoản Gmail là google.com), bấm Next và Finish.

2. Bạn sẽ nhận được một email từ OneStat kèm theo một file đính kèm có tên là OneStatScript.txt. Tải file đính kèm này về máy và xóa email này đi nếu như đây là hộp thư bạn muốn đặt bẫy. Nhưng trước khi xóa hãy ghi nhớ số và mật mã đăng nhập của tài khoản OneStat vì bạn sẽ cần dùng nó sau này.

3. Thay đổi tên của file trên thành một cái gì đó rất hấp dẫn kiểu như “danh sách mật khẩu” (password list) cũng như thay đổi định dạng của nó thành htm khi đó tên file sẽ là passwordlish.htm.

4. Gửi một thư đính kèm theo file mới này tới tài khoản email của bạn.

5. Thế là bẫy của bạn đã hoàn thành. Khi một ai đó mở thư và file đính kèm, OneStat sẽ ghi nhớ nó, và khi đăng nhập vào tài khoản OneStat bạn sẽ được thông báo là mỗi ngày nó được mở bao nhiêu lần, kèm theo đó là thông tin chi tiết về “vị khách không mời” như thời gian ghé thăm, và đặc biệt là địa chỉ IP của họ.

Để xem thông tin này bạn vào Visitor Info > Last 20 visitors. Thông tin này sẽ giúp ích gì cho bạn? Đầu tiên là bạn phải ngay lập tức đổi mật mã hộp thư của mình. Kế đó, dựa vào địa chỉ IP bạn có thể xác định những người đã theo dõi hộp thư của bạn là ai.

Theo LBVMT

### **Bảo Vệ Email Address Book**

Phương cách bảo vệ sổ địa chỉ (email addressbook)

Một nhân viên kỹ thuật về điện toán đã cho biết rằng đây là một cái mồi quý như vàng! Và là một cái mồi rất hay!

Hôm nay tui (một thằng dân ngu cu đen) học được một cái mồi về điện toán vô cùng đơn giản về tính cách kỹ thuật. Như quý vị đã biết là một khi mà các chú “virus” chui vào máy computer thì nó sẽ chạy thẳng đến cái sổ địa chỉ (email address book) của quý vị, và tự gởi đi một cái email đến tất cả những người ở trong cái danh sách ấy, Vậy là tất cả các bạn bè của quý vị và những người liên hệ sẽ bị dính chấu.

Cái mồi này không ngăn cản được những tai hại mà các chú “virus” này sẽ gây ra cho máy “computer” của quý vị, nhưng sẽ chặn đứng được việc sử dụng cái sổ địa chỉ này để truyền đi và gieo rắc thêm tại họa, và đồng thời cũng sẽ giúp quý vị nhận biết được rằng các chú đang ẩn núp trong máy của quý vị.

Và đây là việc mà quý vị cần phải làm, rất đơn giản như đang giỡn dzậy đó:

Trước hết, hãy mở cái sổ địa chỉ (có chỗ gọi là “Contacts” có chỗ là “Address book” rồi bấm vào “New Contact”, làm giống như là quý vị đang bỏ thêm tên của một người bạn vào vào cái sổ địa chỉ của quý vị.

Ở “cái khung cửa sổ” nơi mà để điền tên (của người bạn vàng) thì quý vị hãy đánh vào chữ (mẫu tự) “A”.

Về phần địa chỉ (email address) thì hãy đánh vào “0000000@000.000”. Và đây tôi xin giải thích là cái địa chỉ trên đây sẽ có tác dụng và đem lại ích lợi gì cho máy “computer” của quý vị.

Cái tên “A” sẽ được sắp đứng đầu danh sách trong cái sổ địa chỉ của quý vị, như thể là cái tên này đã được gán cho số “năm-bờ-woanh” dzậy đó. Và chính đây cũng là cái địa chỉ đầu tiên (trong danh sách) mà các chú “virus” mon men đến để bắt đầu gửi email đi, để rồi từ đây các chú sẽ lần lượt gửi đến cho tất cả mọi người có tên nằm trong cái sổ địa chỉ của quý vị. Nhưng (ở đời luôn luôn có những chữ “Nhưng” bắt hủ), khi mà các chú gửi đi cái email có địa chỉ “0000000@000.00” thì cái email này sẽ bị dội ngược trở lại vì cái địa chỉ đó là một địa chỉ ma mà lị. Và một khi mà đã bị thất bại méo mặt (như trong trường hợp này đây) thì các chú “virus” sẽ chào thua và không thể nào truyền bệnh cho máy của các thân hữu của quý vị được. Hooray!

Và đây là sự hữu ích thứ hai của cái phương pháp đơn giản này:

Một khi mà một cái email bị dội ngược lại thì máy sẽ báo cho quý vị biết ngay. Do đó, nếu quý vị nhận được email (trả về) cho biết là địa chỉ “0000000@000.00” không có trên trần gian này (dưới âm phủ thì may ra) thì quý vị sẽ biết ngay là các chú đặc công, nằm vùng đảng ân núp trong máy của quý vị. Vậy là quý vị cứ tự tiện dùng những thứ vũ khí đang có trong tay để truy lùng và diệt địch. Đáng đời các chú nhé!

Đơn giản như đang giỡn phải không quý vị. Nếu tất cả các bạn bè của quý vị đều được bảo vệ bằng cách này thì kể từ đây quý vị sẽ chẳng có phải lo ngại gì khi mở email của bạn bè ra đọc...