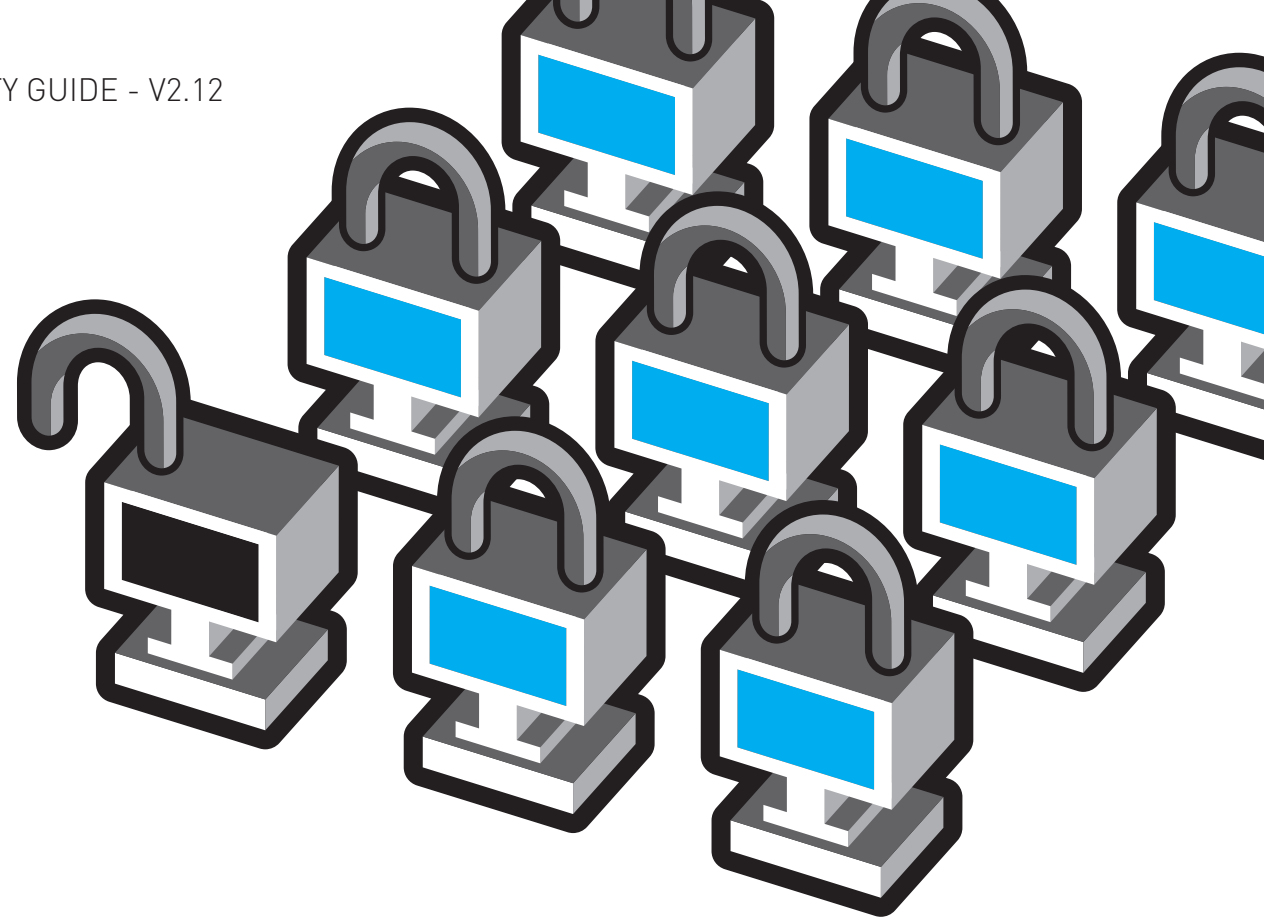


HƯỚNG DẪN THỰC TIỄN ĐỂ BẢO VỆ DANH TÍNH

VÀ AN NINH TRÊN MẠNG VÀ KHI SỬ DỤNG ĐIỆN THOẠI DI ĐỘNG

Hướng dẫn này được viết cho những người muốn sử dụng kỹ thuật một cách an toàn để liên lạc trao đổi, tổ chức, và chia sẻ dữ liệu (tin tức, thông tin, hình ảnh, âm thanh, v.v…) - nhưng nó cũng có thể được sử dụng bởi bất cứ ai muốn bảo vệ sự riêng tư và an ninh của mình khi vào mạng tại bất cứ nơi nào.

Tài liệu này nhắm đến đại khối quần chúng với trình độ sử dụng vi tính trung bình, muốn biết làm sao để an toàn khi lên mạng và khi dùng các thiết bị di động. Tài liệu này chỉ cách thức và các công cụ giúp làm giảm việc bị theo dõi và giám sát, bảo vệ sự riêng tư, và đối phó với kiểm duyệt. Nó bao gồm: Cách sử dụng email và chat (tin nhắn nhanh) cho an toàn, giữ mật khẩu tốt, làm thế nào để giữ cho máy tính không bị vướng vi-rút hay những phần mềm dọ thám, phương cách để vượt kiểm duyệt mà vẫn ẩn danh, kỹ thuật để sử dụng điện thoại di động an toàn, và ngoài ra có thêm các nguồn tài liệu chuyên môn khác. (Nếu bạn gặp khó khăn khi truy cập vào các đường dẫn nêu trong tài liệu này, vì bị chặn sau khi sử dụng các công cụ vượt thoát đề cập dưới đây, hãy email về info@accessnow.org và cho chúng tôi biết những gì bạn muốn để gửi qua email).

Trong khi tất cả các thông tin trong hướng dẫn này được xem là chính xác và đã được kiểm tra từ tháng 7 năm 2011, bảo vệ chính mình khi vào mạng là một quá trình phức tạp và thường thay đổi, khi các kỹ thuật mới và những kẽ hở về bảo mật xuất hiện. Không có một giải pháp toàn bộ nào nhằm bảo đảm an ninh và sự riêng tư của chúng ta, nhưng những công cụ này chắc chắn sẽ giúp bạn an toàn hơn.

Tài liệu này đã được soạn thảo và rà soát lại bởi một loạt nhiều các tổ chức và cá nhân chuyên về bảo mật trực tuyến và an toàn di động. Nếu bạn tìm ra được lỗi trong tài liệu này hoặc có ý kiến nhằm cải thiện, xin hãy email về info@accessnow.org.

Một số điều căn bản cốt yếu

Bảo vệ emails của bạn

Đối với những dịch vụ emails không tốn tiền, thì Hotmail và Gmail cung cấp phương pháp mã hóa khi giao dịch (HTTPS) trên mạng giữa bạn và công ty cung cấp dịch vụ.

Gmail hiện nay đã có HTTPS mặc định, nhưng bạn cần phải mở chức năng này lên cho Hotmail (Bạn hãy vào Tài Khoản>những chọn lựa khác>nối kết bằng HTTPS>Sử Dụng HTTPS tự động). Trong khi đó đến thời điểm này thì Yahoo Mail vẫn chưa được an toàn; cho nên tuy có thể phiền toái, chúng tôi khuyên bạn hãy nên thiết lập và sử dụng một tài khoản email có HTTPS trong việc nối kết mạng, đặc biệt là với những điều nhạy cảm cần bảo mật. Tuy nhiên hãy nhớ là HTTPS giữ an toàn giữa bạn và công ty cung cấp dịch vụ mà thôi, khi email được chuyển đến địa chỉ cuối cùng có thể không được mã hoá nếu người nhận không dùng HTTPS, hoặc họ dùng một công ty cung cấp dịch vụ khác. Ngoài ra, còn có những dịch vụ bảo đảm an toàn cho email khác như Riseup.net và Vaultletsoft. Thêm vào đó, một hệ thống hoàn hảo để mã hóa và ký tên điện tử cho email của bạn là PGP và GPG.

Nếu bạn sử dụng Gmail và muốn tìm hiểu thêm về những phương cách an toàn khác (như Khoá 2 chìa, Lịch sử IP) xin hãy vào phần Gmail Security Checklist. Nếu bạn sử dụng Hotmail, bạn có thể tìm hiểu thêm về những chức năng an ninh, kể cả chức năng mật khẩu tạm để dùng tại những máy vi tính nơi công cộng – Xin bấm vào đây.

Làm Mật Khẩu an toàn hơn

Một trong những điều tối quan trọng bạn có thể làm được là cấu tạo mật khẩu cứng cáp, chắc chắn và có những thoái quen tốt khi dùng mật khẩu. Đó là:

- Hãy nghĩ đến một nhóm từ, cụm từ thay vì chỉ một chữ duy nhất.
- Hãy dùng ít nhất 12 chữ và số cho mật khẩu; điều này sẽ làm cho việc bẻ khóa không dễ dàng.
- Hãy sử dụng một tổng hợp gồm có nhiều ký hiệu, số, chữ hoa, chữ thường với nhau. Một cách thường làm là hãy cho những ký tự (nằm trên nút của những con số trên bàn phím) và con số xen kẻ với chữ thường và chữ viết hoa, từ những lời nói hay một câu trong bài thơ hay bài hát.
- Không nên dùng một mật khẩu cho tất cả những tài khoản mình có; Nếu mật khẩu của bạn dễ dàng bị chận và đánh cắp khi sử dụng tại những nơi công cộng mà không có hệ thống HTTPS, thì điều đó sẽ khiến cho những tài khoản khác của bạn cũng sẽ bị xâm nhập.
- Nên thay đổi mật khẩu mỗi 3 tháng hoặc thường hơn nếu bạn sử dụng những dịch vụ Internet Café từ bên ngoài hay từ những computer nào không phải của riêng bạn.
- Nếu bạn không thể nhớ mật khẩu được, bạn hãy dùng một phần mềm có mã hóa như KeePass để giữ những mật khẩu này.
- Tài khoản có thể bị xâm nhập xuyên qua cách phục hồi mật khẩu. Do đó hãy cẩn thận đối với những câu hỏi và trả lời liên quan đến tài khoản của bạn, đừng quá thô sơ và dễ dàng phỏng đoán.

Chống vi-rút, mã độc, phần mềm dọ thám

Một vấn đề nguy hiểm cho nhiều người dùng máy vi tính là việc sử dụng phần mềm lậu, trái phép, đặc biệt là Microsoft Windows. Khi bạn mua hay lấy phần mềm bất hợp pháp, bạn tiết kiệm một ít tiền nhưng cũng sẽ đặt mình vào tình trạng có thể bị tấn công vì không nhận được các cập nhật và bản vá lỗi từ nhà sản xuất phần mềm. Nếu bạn không thể có được phiên bản chính thức, hợp pháp của các phần mềm và hệ điều hành, thì ít nhất là sử xử dụng phần mềm chống vi-rút và chống dọ thám để giảm thiểu rủi ro. Nhưng nếu có thể, cố gắng để có được các ấn bản chính thức của phần mềm này vì an ninh của chính bạn.

- Nếu bạn đang dùng phần mềm không tốt, một chương trình chống vi-rút miễn phí tuyệt vời cho Windows là Avast, nó giúp bảo vệ dữ liệu trên máy tính của bạn khỏi bị hư hỏng và bị nhiễm bệnh. Malwarebytes là một phần mềm chạy trong chế độ an toàn nếu máy tính của bạn đã bị nhiễm.
- Quan trọng không kém là phần mềm chống dọ thám, nó xác định và loại bỏ những mã độc có thể theo dõi tất cả hoạt động của bạn trên mạng hay ngoài mạng, một chương trình chống phần mềm dọ thám miễn phí và hiệu quả là Spybot.
- Để giảm xác suất gặp vi rút và các phần mềm dọ thám, không mở các email và tập tin đính kèm từ những nguồn không rõ hoặc không tin cậy. Nếu bạn không biết chắc nguồn gốc một tập tin đính kèm, hoặc trang web, bạn có thể tải lên để kiểm tra nó tại VirusTotal hoặc gởi email đến scan@virustotal.com với "SCAN" trong hàng tiêu đề (hoặc SCAN+XML nếu bạn muốn kết quả trong dạng XML.)
- Một cách xâm nhập thông thường khác của các mã độc hại là những bài vở, tài liệu mà bạn gặp được khi lướt mạng. Chúng tôi khuyên bạn nên dùng tiện ích NoScript để sử dụng với trình duyệt Firefox, nó cho phép bạn chặn hầu hết các đoạn mã và chỉ cho phép những đoạn mã nào bạn tin tưởng.
- Một cách xâm nhập thông thường khác của vi-rút và phần mềm dọ thám là thẻ USB và các thiết bị di động khác. Đừng gắn các thiết bị di động vào máy tính của bạn trừ khi nó đến từ một nguồn bạn biết và tin cậy. Ngoài ra cũng nên sử dụng phần mềm chống vi-rút và chống dọ thám như Spybot và Avast để quét các thiết bị di động.

Suy tính đến việc chuyển sang hệ điều hành Linux như Ubuntu trừ khi có một lý do quan trọng để tiếp tục phải sử dụng Windows. Ubuntu cho phép mã hóa ổ đĩa cứng và căn bản là không gặp vi-rút và mã độc. Nếu đừng tính việc tấn công có chủ đích, một người dùng Ubuntu sẽ an toàn hơn nhiều so với một người sử dụng một ấn bản lậu, chưa được vá, hoặc đã lỗi thời của Windows. Linux Mint là một hệ điều hành khác dựa trên Ubuntu có nhiều phần mềm ứng dụng để dùng.

Tin nhắn nhanh an toàn

Skype và Google Chat bên trong Gmail với HTTPS là lựa chọn tốt nếu bạn tin rằng tài khoản của bạn sẽ không là mục tiêu của tin tặc. Một lựa chọn an toàn hơn là sử dụng Pidgin để vào các chương trình chat (Google Talk, ...) cùng với Off The Record (OTR) plug-in - điều này bảo đảm rằng ngay cả có chìa khóa mã hóa, bất kỳ dữ liệu ghi nhận trước đó sẽ trở nên vô giá trị. Tìm đọc thêm về đặc tính an ninh của OTR để hiểu về một ví dụ của Bảo Mật bằng cách thiết kế (Privacy by design).

Những cách khác để giữ an ninh khi ở trên mạng:

- Để giữ bí mật danh tính của bạn khi tham gia vào các hoạt động trên mạng, bạn có thể dùng bí danh để xác định danh tính của mình khi vào các trang mạng xã hội

An Ninh Trên Mạng

và các trang truyền thông. Mức độ ẩn danh tùy thuộc chính bạn: dùng bí danh trên Twitter là chuyện thường, nhưng đa số dùng tên thật của họ cho các tài khoản mạng xã hội như Facebook. Việc này tùy bạn và tùy linh tính của bạn về xác suất bị theo dõi. Điều cần lưu ý cho Facebook là bạn phải chọn một tên giả nhưng nhìn như thật thay vì chọn một cái tên đọc lên thấy là giả mạo ngay và sẽ bị Facebook loại bỏ vì vi phạm giao ước dịch vụ.

- Nếu bạn quyết định sử dụng tên thật của bạn trên Facebook và sử dụng HTTPS để truy cập và sử dụng các trang web, điều quan trọng là bạn không cung cấp những thông tin cá nhân nhạy cảm như số điện thoại của bạn.
- Hiện nay đang có khuynh hướng gia tăng việc sử dụng kỹ thuật GPS để xác định vị trí của bạn khi lên mạng. Đây có thể là một chức năng hữu ích khi được sử dụng như là một nỗ lực gôm góp dữ kiện qua điện thoại di động trong một cuộc khủng hoảng hoặc một biến cố quan trọng, nhưng nó cũng đưa ra thông tin vô cùng nhạy cảm về vị trí và hoạt động của bạn. Chúng tôi đề nghị bạn tắt GPS cho các chương trình như Twitter và Bambuser trừ khi đó là tạm thời và quan trọng đối với một dự án mà bạn đang làm việc. Ngay cả nếu GPS không hiển thị, cũng cần phải tắt không cho thu thập các thông tin này trong trình duyệt hay các ứng dụng khác.
- Khi bạn gửi thông tin nhạy cảm cho người khác, hãy nhớ rằng họ có thể không được an toàn, danh sách liên lạc, email, và thông tin liên lạc khác có thể bị theo dõi. Hãy đặc biệt cẩn thận khi liên lạc với những đối tượng mà bạn chưa xác minh được danh tính của họ. Ngoài ra, bất kỳ tin nhắn trực tiếp khi bạn gửi đến cho một người nào đó (đã biết hoặc không biết) thông qua Facebook và Twitter có thể đọc được nếu họ không thực hiện các bước cần thiết (xem chi tiết về HTTPS và các công cụ gian lận bên phải).
- Hãy hạn chế việc sử dụng ở mức tối thiểu những phần mềm phụ trội hoặc hoàn toàn không nên sử dụng chúng (ví dụ như các ứng dụng truy cập tài khoản của bạn cho Twitter, Facebook, Gmail, v.v..) Chúng thường có nhiều kẽ hở an ninh và được sử dụng để xâm nhập vào những tài khoản được bảo vệ an toàn.

Internet bị kiểm duyệt nặng nề ở nhiều quốc gia trong vùng, chẳng hạn như Bahrain, Kuwait, Oman, UAE, Qatar, Syria và Ả-rập Xê-út. Internet cũng bị giám sát, mặc dù ở một mức độ không rõ. Nếu bạn có khả năng vượt thoát kiểm duyệt, điều đó không có nghĩa là bạn qua mặt sự giám sát vì việc này khó hơn nhiều. Bạn phải sử dụng proxy nặc danh an toàn với giả thiết rằng hoạt động của bạn có thể bị theo dõi và ghi lại. Ngoài ra, chúng tôi đề nghị rằng bạn không sử dụng trình duyệt Internet Explorer, vì nó có một số lỗ hổng an ninh, đặc biệt là trong các phiên bản lậu. Một trình duyệt khác thay thế vừa miễn phí vừa tốt hơn với một số tiện ích hữu dụng là Firefox của Mozilla.

Mã Hóa những hoạt động trên mạng của bạn bằng HTTPS

Nếu bạn đang tham gia hoạt động trên mạng, điều quan trọng là phải bảo vệ danh tính và mật khẩu cho an toàn. Chúng tôi vừa mới nhìn thấy Tunisia thực hiện một chiến dịch lừa đảo quy mô khi họ khai thác một lỗ hổng an ninh để thu thập log-in và mật khẩu của công dân nào truy cập vào Facebook. May mắn thay, Facebook phản ứng bằng cách cho phép dùng HTTPS và đã giúp chống lại được. Khi có thể, bạn nên luôn luôn sử dụng HTTPS. Điều rất quan trọng nếu bạn không thể sử dụng HTTPS được thì bạn phải sử dụng một hệ thống proxy an toàn khác hoặc tương tự. Giới kiểm duyệt có thể nhắm vào một nhóm người sử dụng hoặc một số trang web để không cho truy cập vào trang HTTPS. Nếu bạn sử dụng một proxy ẩn danh như Tor, sẽ rất khó khăn nếu không nói là không thể thực hiện các cuộc tấn công như vậy.

HTTPS

Một phần mềm tiện tích rất tốt và dễ dùng là HTTPS Everywhere (Khắp mọi nơi). Đây là một tiện ích của Firefox để "buộc" một trang web phải sử dụng HTTPS nếu có chức năng này. **Tải phần mềm này về là một trong những điều đầu tiên khi bạn bắt đầu sử dụng để có thể mã hóa toàn bộ việc truy cập vào các trang Facebook, Twitter, Google Search, v.v....** Nó cũng sẽ làm giảm sự thiệt hại của bạn trong việc mật khẩu bị đánh cắp khi vào mạng wifi mở rộng, không an ninh.

- Nếu chưa làm, thì hãy tải về phiên bản mới nhất của Firefox. Sau đó tải HTTPS Everywhere và / hoặc Force TLS, rồi khởi động lại Firefox, và cấu hình các chọn lựa. Lưu ý: HTTPS Everywhere có một số các trang mặc định có thể chỉnh sửa được. Force TLS cần phải cấu hình lại, đòi hỏi người dùng tạo ra danh sách các trang dùng HTTPS.
- Nếu bạn dùng Google Chrome, hãy tải về KB SSL Enforcer Extension. *(Lưu ý: nó không hiệu quả như các tiện ích của Firefox đã đề cập ở trên. Vẫn còn một số lỗi với SSL Enforcer, mặc dù chúng tôi nghĩ sẽ được cải thiện theo thời gian)*

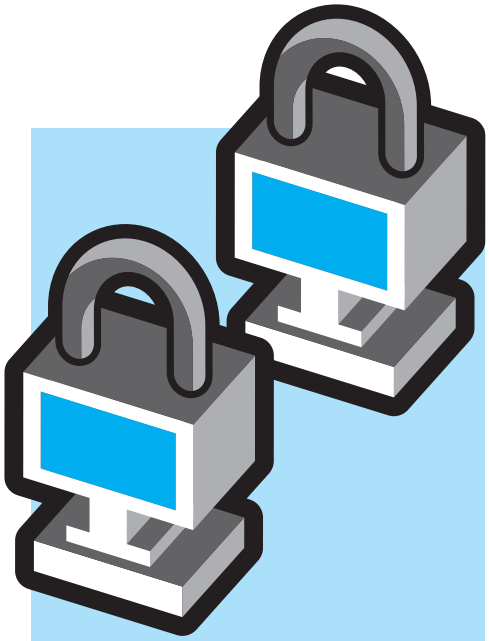
Facebook: Mặc dù tiện ích cho Firefox đề cập bên trên buộc HTTPS cho một số trang web, nhưng nếu bạn sử dụng Facebook thường xuyên, điều chỉnh để Facebook dùng HTTPS mặc định thì tốt hơn hết, đặc biệt là nếu bạn truy cập vào từ nhiều máy tính.

- Để kích hoạt HTTPS cho Facebook, hãy đến Account ở góc trên bên phải > account settings > trên bảng settings, chọn account security <"change"> đánh dấu vào hộp bên cạnh <"secure browsing (HTTPS)">
- Dùng một số games hay những tiện ích phụ trội khác của Facebook sẽ vô hiệu hóa việc sử dụng HTTPS.
- Facebook cũng có chức năng bảo mật khác mà bạn có thể sử dụng, bao gồm việc đăng xuất từ xa và thông báo đăng nhập (remote log-out and log-in notifications) cho phép bạn giới hạn các máy nào có thể truy cập vào tài khoản của bạn. Một đoạn video xem xét lại các chức năng bảo mật có thể được tìm thấy trên trang web của Facebook. Một hướng dẫn toàn diện về cách sử dụng Facebook an toàn có thể được tìm thấy ở đây (here).

Twitter: Mặc dù tiện ích cho Firefox đề cập bên trên cũng bắt buộc HTTPS cho Twitter, tuy nhiên điều chỉnh lại để Twitter dùng HTTPS mặc định thì tốt hơn hết, đặc biệt là nếu bạn truy cập vào từ nhiều máy tính.

- Để kích hoạt HTTPS cho Twitter, nhấp chuột vào tên gọi Twitter của bạn ở góc trên bên phải > chọn settings > sau đó di chuyển đến dưới cùng của trang và đánh dấu vào ô "Always use HTTPS".
- Lưu ý: Thay đổi thiết trí trong tài khoản Twitter của bạn "Always use HTTPS" không có hiệu lực trên các thiết bị di động. Cho đến khi nào có được, bạn nên vào trang https://mobile.twitter.com.

Vượt thoát: Truy cập vào các trang web bị chặn



Một số quốc gia trong vùng kiểm duyệt gắt gao nhiều trang web và blog và việc này cũng có thể cho thấy có một nỗ lực giám sát nào đó tùy mức độ của mỗi quốc gia. Để truy cập và tải bất kỳ bản tin nào lên các trang web bị chặn, bạn có thể sử dụng các công cụ vượt thoát kiểm duyệt. Điều quan trọng cần lưu ý là có một sự khác biệt giữa mã hóa và bảo mật /ẩn danh: các công cụ vượt thoát tốt sẽ mã hóa thông tin giữa người dùng và trạm trung gian, nhưng không thể mã hóa thông tin giữa trạm trung gian và trang web được truy cập. Đây là lý do quan trọng tại sao phải dùng HTTPS bất cứ khi nào có thể được, vì nó cung cấp mã hoá từ đầu đến cuối. Nhưng nếu chỉ sử dụng HTTPS một mình, thì nó sẽ không giúp bạn truy cập vào một trang web đã bị cấm, đó là lý do tại sao vai trò của công cụ vượt thoát rất quan trọng. Địa chỉ IP của bạn luôn luôn được ghi lại bởi các dịch vụ truy cập - chỉ với proxy ẩn danh (ví dụ như Tor) địa chỉ IP của bạn mới thực sự được giấu một cách an toàn. Nhiều dịch vụ sẽ tiết lộ thông tin đăng nhập cuối cùng của bạn và do đó nếu tài khoản của bạn bị xâm nhập, địa điểm trước đây của bạn sẽ được tiết lộ.

Vượt tường lửa

Các trang web proxy đơn giản cho phép người dùng truy cập các trang bị ngăn chặn. Người dùng chỉ cần vào trang web proxy, điền vào địa chỉ trang web muốn truy cập để proxy truy tìm và hiển thị lại. Còn proxy loại HTTP/SOCKS thì chuyển thông tin qua các giao thức khác để đi lọt qua tường lửa. Để dùng các loại proxy này, chỉ cần điền vào địa chỉ IP và số cổng (được liệt kê trên các trang danh bạ proxy) vào trong cấu hình của trình duyệt.

Mặc dầu các loại proxy này thường được dùng để vượt tường lửa, chúng không có chức năng ẩn danh (hoạt động lướt mạng của bạn có thể bị thấy, bị theo dõi) và cũng không biết được chủ nhân các proxy này là ai. Có một số rủi ro khi sử dụng các proxy trên, thành ra nên dùng một dịch vụ như Tor vừa giúp vượt tường lửa, vừa giúp ẩn danh.

Một giải pháp proxy khác là Psiphon. Psiphon có nhiều dạng khác nhau. Psiphon 1 là một loại web proxy nhẹ ký chạy trên hệ Windows và Linux. Trạm Psiphon thường không phải là proxy công cộng. Ý muốn ở đây là cho những người bình thường không cần phải có thiết bị gì đặc biệt có thể tạo lập ra những trạm proxy để cho một số bạn bè ở vùng bị kiểm duyệt có thể vào các trang bị chặn. Đây là mô hình mạng-tín-cẩn, vì người bạn cung cấp dịch vụ proxy có thể xem được các thông tin đi ngang qua đó thành ra phải có sự tin tưởng giữa người dùng và chủ nhân của trạm proxy. **Psiphon có ghi lại dữ kiện của người dùng nhưng địa chỉ IP được ẩn dấu.** Phsiphon 2 là một giải pháp dựa trên « hệ thống mây “ (cloud-based) được quản trị một cách tập trung, điều hành bởi công ty Psiphon, bao gồm các proxy có đường nối được thay đổi. Psiphon 1 và 2 thường gặp khó khăn khi giao tiếp với giao trình HTTPS và các trang nhà Web 2.0. Những giới hạn này đã được giải quyết trong phiên bản mới PsiphonX.

Tor: ẩn danh trên mạng

Tor là một công cụ tinh vi và hữu ích cho nhu cầu vượt thoát kiểm duyệt và giúp bạn ẩn danh trên mạng. Tuy nhiên, trở ngại chính là Tor có thể chạy chậm hơn các giải pháp khác. Dùng gói Tor Browser (trình duyệt Tor) là đủ để sử dụng mà không phải cần cài đặt. Dùng cầu nối Tor để truy cập vào nơi bị kiểm duyệt gắt gao.

Trong lúc có nhiều cách để dùng Tor, chúng tôi khuyên bạn nên tải xuống gói Trình duyệt Tor, để dùng Tor trên hệ Windows, Mac OS hay Linux mà không cần phải cài đặt nhiều thứ. Chỉ cần cho chạy tập Tor Browser Bundle, và một phiên bản Firefox được chế tạo một cách đặc biệt sẽ chạy cùng với Vidalia, một ứng dụng để kiểm soát Tor, được cấu hình ngay từ đầu để nối và vận chuyển thông tin qua mạng Tor. Bạn có thể thiết trí Tor Browser Bundle trên một thẻ USB, như vậy bạn có thể sử dụng Tor trên bất cứ máy vi tính nào. Nếu cần Browser Bundles dù có hay không có dịch vụ an toàn IM với nhiều ngôn ngữ khác nhau (kể cả tiếng Ả Rập hay Farsi), bạn hãy viếng trang Tor download site. Khi sử dụng Tor, việc lướt mạng có thể sẽ bị chậm đi, do đó, chúng tôi khuyên nên dùng 2 trình duyệt khác nhau, một để sử dụng với Tor để truy cập các thông tin quan trọng bị ngăn chặn, cái còn lại để sử dụng cho tất cả những truy cập vào thông tin thông thường. Nếu bạn để Tor chạy thường xuyên, Tor sẽ cải tiến hiệu năng qua thời gian và bạn sẽ nhận thấy việc truy cập sẽ nhanh hơn. Nếu bạn cảm thấy việc truy cập vào các trang nhà với Tor quá chậm và những nội dung được biểu thị chỉ hiện dưới dạng chữ, bạn cần phải tắt việc tải hình ảnh và javascript qua trình duyệt. Như vậy việc tải xuống các trang mạng qua Tor sẽ trở thành nhanh hơn nhiều.

Điều không may là trang web chính của Tor thường bị chặn bởi đa số các quốc gia trong vùng. Bạn vẫn có thể có được phần mềm này bằng cách:

- Đến viếng trang nhà Tor qua địa chỉ HTTPS – https://www.torproject.org/
- Tìm một trang phụ (mirror) torproject.org qua việc tìm kiếm trên Google “tor mirror”. Bạn cũng có thể lấy được danh sách chính thức các trang nhà phụ nếu bạn tìm trên google “site: torproject.org mirrors” và duyệt qua kết quả của trang đệm “Tor Project Mirrors”
- Hay bạn có thể xin một tập bằng cách gởi một điện thư đến rô-bốt tự động “gettor” tại địa chỉ gettor@torproject.org. Ghi chú : nhằm có được mức độ an ninh và kết quả tốt nhất, nên sử dụng một tài khoản Gmail với giao trình HTTPS để gởi điện thư đến gettor@torproject.org. Lựa chọn tên trong những phần mềm sau đây và ghi tên tập vào bất cứ nơi nào trong phần nội dung của điện thư:
- tor-im-browser-bundle for Windows (Tor & instant messaging)

Những phương tiện liên lạc di động

- tor-browser-bundle for Windows OR Intel Mac OS X OR Linux (Tor browser)

Ít lâu sau khi bạn gởi điện thư đi, bạn sẽ nhận được một điện thư từ rô-bốt "gettor" với phần mềm bạn yêu cầu đính kèm dưới dạng Zip. Nếu bạn cần sự giúp đỡ liên quan đến Tor, gởi điện thư lại tor-assistants@torproject.org

Ghi chú : Tor được sử dụng trên điện thoại di động Android với tên"Orbot". Tìm kiếm ứng dụng này trong Chợ Android (Market) hay tải xuống trực tiếp từ trang nhà Tor hay các trang phụ (mirrors).

Một cách khác để vượt qua kiểm duyệt là sử dụng đường liên lạc được mã hóa VPN nhằm bảo đảm không bị lộ danh tính của mình. Bạn có thể đọc cách thức thiết trí qua việc bấm vào đây, hay tải xuống phiên bản miễn phí của VPN Hotspot Sield tại đây hay gởi điện thư về hss-sesawe@anchorfree.com (trong tiêu đề cần có ít nhất một trong các chữ sau đây "hss", "sesawe", "hotspot", "shield").

Một số cách vượt kiểm duyệt thông dụng khác gồm Ultrasurf và Freegate. Tất cả 3 mạng ảo VPN này đều là công cụ tốt nhằm giúp truy cập các trang nhà đang bị ngăn chặn, tuy nhiên điều quan trọng cần biết là cũng giống các loại web proxies hay HTTP/SOCKS/proxies, chúng không có khả năng giúp ẩn danh. Ngoài ra, những dịch vụ này bị giới kiểm duyệt biết đến và có một số chủ nhân của trang mạng bị chặn không thích hay không hỗ trợ. Thêm vào đó, những trang nhà này thường được biết là ghi lại các dữ kiện liên quan đến tất cả người truy cập vào. Đó thường là các công ty thương mại và làm ăn qua việc giới thiệu quảng cáo đến bạn, dựa trên những dữ kiện cá nhân của bạn (trang nhà bạn viếng, những cụm từ tìm kiếm bạn thường dùng, …) – đây là điểm cần lưu tâm đối với những ai đang muốn dấu lý lịch của mình hay bảo vệ sự riêng tư qua việc sử dụng các phần mềm vượt kiểm duyệt.

Ghi chú quan trọng: Khi một chính phủ có khả năng kiểm soát các dịch vụ trên mạng Internet trong một quốc gia, họ có thể tiến hành một số biện pháp nhằm đe dọa an ninh của bạn và sự riêng tư qua mã độc và việc cài certificate giả. Nhằm đối phó lại việc này, hãy sử dụng các công cụ và chiến thuật được trình bày ở trên, và cố gắng theo dõi tin tức hay báo động đến từ các người hoạt động trên mạng tại quốc gia bạn, những người này có thể nhận diện ra những loại chiến thuật này và báo động nhanh chóng.

Để tham khảo thêm: Video tutorials để học hỏi cách sử dụng nhiều công cụ vượt tường lửa bằng tiếng Anh hay tiếng Ả Rập (12 pm Tutorials).

Nhiều nhà hoạt động đã bị truy lùng qua điện thoại di động của họ, và một số quốc gia đã tiến hành việc kiểm soát với một quy mô rộng lớn hơn so với những nơi khác. Những người hoạt động Ai Cập đã phải chịu một mức độ kiểm soát nặng nề về mọi mặt, và nhà cầm quyền Ai Cập đã dùng những kỹ thuật để có thể từ xa biến điện thoại thành những dụng cụ thu âm thanh tại chỗ, ngay cả khi những điện thoại này đã được tắt. Bạn cần thẩm định những rủi ro liên quan đến những hoạt động của mình dựa trên những gì đang được tiến hành tại quốc gia của bạn, những việc làm của bạn có tầm mức quan trọng như thế nào, và những kinh nghiệm mà những người hoạt động như bạn đã trải qua. Công ty điện thoại cũng có khả năng theo dõi và thu thập dữ kiện liên quan đến việc sử dụng điện thoại di động, kể cả nơi bạn đang ở, và có thể chia sẻ tin tức này với nhà cầm quyền nếu được yêu cầu.

Ngoài ra còn có việc cài đặt các phần mềm theo dõi trong máy điện thoại, phần mềm này sẽ chạy một cách kín đáo và im lặng mà ngay cả người sử dụng không biết được. Đây là một rủi ro có thể gặp phải nếu điện thoại không nằm trong tầm tay của bạn trong một khoảng thời gian.

Khi điện thoại chạy, máy sẽ liên lạc và cung cấp thường xuyên những dữ kiện sau đây với những trạm phủ sóng chung quanh.

- Số IMEI - mỗi thiết bị điện thoại đều được xác định bởi một số duy nhất
- Số IMSI - mỗi thẻ SIM đều được xác định bởi một số duy nhất - số này gắn liền với số điện thoại của bạn
- Số TMSI - một số tạm có thể được dùng lại nhiều lần để chỉ nơi bạn đang ở hay mỗi khi tầm bao phủ thay đổi, số này có thể bị lấy trộm bởi những dụng cụ thương mại dùng thu lén dữ kiện
- Ô khoanh vùng (cell) của nơi điện thoại đang chạy. Vùng này có thể bao trùm từ vài thước cho tới vài cây số, với những ô khoanh vùng nhỏ tại các vùng đô thị và ngay cả rất nhỏ trong các cao ốc, các ô rất nhỏ này dùng các máy tái phát trên không nhằm gia tăng sức mạnh của tín hiệu trong nhà
- Vị trí người sử dụng trong một ô, vị trí này được định bởi phép đặt tam giác các tín hiệu từ các trạm phủ sóng chung quanh. Một lần nữa, sự chính xác của vị trí tuỳ thuộc vào kích thước của ô. Nơi nào càng có nhiều trrạm phủ sóng, thì nơi đó, mức độ chính xác của vị trí được định càng cao hơn.

Những phương tiện liên lạc di động

Vì những lý do nêu trên, khi điện thoại bạn chạy và liên lạc với hệ thống các trạm phủ sóng, điện thoại có thể được sử dụng như là một dụng cụ để theo dõi cho những người có khả năng truy cập những dữ kiện mà công ty viễn thông đang thu thập, gồm có:

- Nội dung những cú điện thoại của bạn nhận và gọi đi
- Nội dung những SMS bạn nhận và gởi đi, kể cả những dữ kiện liên quan đến người nhận và người gởi
- Tất cả những dịch vụ về thông tin bạn dùng (thí dụ như hoạt động truy cập vào mạng nếu không sử dụng HTTPS, chuyển và nhận tin nhắn nhanh không mã hóa, cũng như khối lượng thông tin lưu chuyển (tải lên youtube chẳng hạn)
- Địa điểm (phỏng chừng) bạn đang đứng (từ vài thước tới vài cây số tùy theo mật độ các trạm phủ sóng)

Bạn cần ghi nhớ là nếu bạn nghĩ bạn đang bị theo dõi, thay đổi thẻ SIM chưa đủ vì bạn vẫn có thể bị theo dõi bằng số căn cước của thiết bị điện thoại.

Có nhiều dữ kiện trên máy điện thoại có thể được dùng để chống lại bạn, nếu điện thoại bị tịch thu hay bị lấy khỏi tay của bạn. Tất cả máy điện thoại cầm tay đều có một phần bộ nhớ nhỏ trong thẻ SIM, cũng như bộ nhớ bên trong của điện thoại (thêm vào đó, một số máy điện thoại có thẻ nhớ SD (hay microSD) để chứa phim ảnh, âm thanh. **Một cách tổng quát, chứa dữ kiện trong thẻ SIM hay thẻ nhớ tốt hơn là chứa trong bộ nhớ bên trong máy điện thoại, vì bạn có thể mang đi hay hủy dữ kiện trong thẻ SIM hay thẻ nhớ.**

Dữ kiện chứa trên thẻ SIM, bộ nhớ bên trong của điện thoại, và thẻ nhớ SD bao gồm:

- Danh bạ điện thoại- với tên và số điện thoại
- Lịch sử điện thoại - những người bạn gọi, ai đã gọi bạn và giờ gọi
- Những tin nhắn mà bạn nhận hay gởi đi
- Dữ liệu của bất cứ chương trình ứng dụng bạn dùng, như là lịch hay danh sách những việc cần làm
- Hình hay phim ảnh mà bạn đã thu hay quay từ máy điện thoại. Đa số máy điện thoại đều ghi thời điểm các hình được chụp và cũng như nơi chụp.

Đối với các máy điện thoại có khả năng truy cập vào mạng, bạn cần biết quá trình lướt mạng được giữ lại bao nhiêu. Và nếu được thì đừng lưu lại quá trình lướt mạng. Email cũng là một mối đe dọa tiềm tàng khác nếu một kẻ có ý xấu vào được thẻ SIM hay bộ nhớ của máy điện thoại.

Giống như bộ đĩa cứng của máy vi tính, bộ nhớ thẻ SIM của máy điện thoại di động giữ các dữ liệu được lưu trữ cho đến khi nào bộ nhớ không còn chỗ để chứa nữa, khi các dữ liệu cũ bị xoá và được thay thế bằng các dữ liệu mới. Điều này có nghĩa là ngay cả khi bạn xóa các tin ngắn SMS, lịch sử các cú điện thoại và danh bạ người liên lạc vẫn có thể thu hồi lại được từ thẻ SIM (có một chương trình miễn phí để làm chuyện này). Điều này cũng được áp dụng cho máy điện thoại có những bộ nhớ phụ trội, bên trong máy hay xử dụng một thẻ nhớ bên ngoài. Bạn cần ghi nhớ, nếu một máy điện thoại càng chứa nhiều dữ liệu, thì việc thu hồi dữ liệu bị xóa sẽ càng lâu.

Vậy những việc đó có ý nghĩa gì đối với bạn

Điện thoại di động có thể là một dụng cụ tối tân cho những người hoạt động, nhưng cũng có thể là những nguy cơ vô cùng, nếu nhà cầm quyền hay công an hợp tác chặc chẻ với công ty điện thoại để truy lùng bạn. Nếu bạn đang ở một quốc gia đang dùng những phương tiện liên lạc di động để kiểm soát, nhất là nếu bạn nghĩ bạn bị theo dõi sát vì những hoạt động nổi trội của bạn, bạn không nên dùng điện thoại di động để liên lạc. Mà nên tổ chức các cuộc gặp gỡ trực tiếp.

Cuối cùng lại, mức độ rủi ro tùy theo bạn chọn: nếu bạn không nghĩ là bạn đang là đích nhắm như một nhà hoạt động có tên tuổi hay là bạn đang bị nhắm tới trong một chiến dịch theo dõi quy mô và bạn muốn dùng điện thoại để liên lạc với các cộng sự viên, thu hình và video, hay chuyển đi thông tin, bạn có thể dùng những biện pháp sau đây:

- Tạo ra và sử dụng một loại mật mã dạng riêng để liên lạc với những người bạn hoạt động
- Sử dụng "réo gọi" như một phương tiện liên lạc với những người bạn hoạt động

(gọi một hay hai lần rồi tắt, để nhắn lại những người quen bạn là bạn đã đến một nơi an toàn, …)

- Không xử dụng tên thật của những cộng sự viên trên cuốn sổ địa chỉ, cho họ một con số hay một bí danh nào đó. Làm như vậy để trong trường hợp điện thoại của bạn hay thẻ SIM bị lực lượng công an lấy đi, họ không thể truy ra được các đường giây hoạt động của bạn.
- Mang theo thẻ SIM dự bị khi tham dự một hành động phản đối nếu bạn biết là thẻ sẽ bị tịch thu và bạn cần phải có điện thoại để liên lạc. Nếu bạn phải bỏ một thẻ SIM, bạn nên tìm cách phá hủy thẻ này.
- Nếu điện thoại bạn có thể khoá bằng một mật khẩu, nên làm việc này. Việc này cũng liên quan đến số PIN của thẻ SIM: thẻ SIM lúc đầu chỉ có một số PIN (Personal Identification Number) có sẵn, nếu được, bạn cần thay số PIN lúc đầu bằng một số PIN chỉ một mình bạn biết và sử dụng chức năng khóa thẻ SIM bằng PIN. Như vậy bạn sẽ cần phải đánh vào một mật khẩu (số PIN) mỗi lần bạn sử dụng điện thoại di động.
- Nếu bạn nghĩ hành động phản đối sẽ gặp một sự trấn áp mạnh mẽ hơn của lực lượng công an, bạn có thể nghĩ tới việc chuyển điện thoại di động vào trạng thái "trên máy bay" (tức không liên lạc với các trạm phủ sóng), bạn sẽ không gọi hay nhận điện thoại được nữa, nhưng bạn vẫn có thể thu video và hình ảnh và tải lên các trang mạng sau đó. Biện pháp

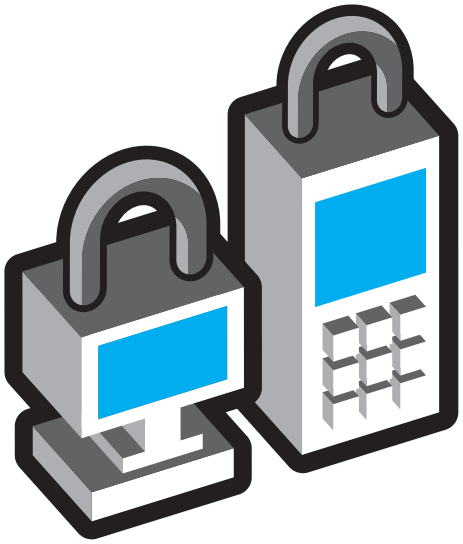
Những phương tiện liên lạc di động

này hữu dụng nếu bạn nghĩ công an đang trấn áp tất cả những ai có điện thoại di động trong một buổi tổ chức. Vì sau đó, nhà cầm quyền yêu cầu có được các cú điện thoại/tin ngắn SMS hay hồ sơ dữ liệu của tất cả những ai đang ở một nơi đặc biệt trong một khoảng thời gian nào đó để tiến hành việc bắt giữ đồng loạt.

- Tắt chức năng định vị và đánh dấu vị trí (geotagging) của tất cả các chương trình ứng dụng. Nếu bạn sử dụng điện thoại di động để thu trực tiếp video, bạn cần tắt chức năng GPS/geotagging (Xem Bambuser.)
- Nếu bạn sử dụng điện thoại với hệ thống điều hành Android, bạn cần sử dụng một số ứng dụng để mã hóa việc truy cập vào mạng, trao đổi tin trực tiếp, SMS và nội dung điện thoại qua những công cụ của dự án Guardian Project và Whispersys.
- Khi bạn dùng điện thoại di động để truy cập vào mạng, nên sử dụng HTTPS khi có thể.

Để tìm hiểu thêm:

- Tactical Tech's Mobiles in a Box (bằng tiếng Anh)
- MobileActive's Mobile Security Risks Primer (bằng tiếng Anh)



Ghi chú cho người sử dụng Blackberry

Hãng chế tạo ra điện thoại hiệu Blackberry là công ty Research In Motion (RIM) cung cấp hai loại trương mục với mức mã hóa khác nhau. Liên quan đến người tiêu thụ bình thường, không bao giờ có mã hóa thật sự từ đầu này đến đầu kia cho những liên lạc qua máy Blackberry của bạn – RIM hay hãng cung cấp dịch vụ điện thoại di động lúc nào cũng có thể nghe chặn bắt điện thoại, điện thư, SMS, truy cập trang web, ...). Ngược lại, nhân viên các hãng xưởng dùng Blackberry Entreprise Server (BES) hưởng được mức mã hoá từ đầu này đến đầu kia cho điện thư, thông điệp (BBM) và truy cập mạng. Tuy nhiên, nếu bạn là nhân viên hãng, nên nhớ rằng những người quản trị máy chủ hãng bạn, nhất là quản trị viên hệ thống điện toán, có khả năng giải mã tất cả những liên lạc của bạn, và có nhiều cách trong khuôn khổ luật pháp (và ngoài luật pháp) một chính quyền có thể sử dụng để giải mã liên lạc của bạn.

Gần đây, quốc gia UAE cố gắng thuyết phục Researh In Motion đưa cho họ cách thức giải mã tất cả các dữ liệu thông tin qua máy Blackberry, nhưng RIM đã từ chối. Người sử dụng Blackberry cần quan tâm đến tất cả tin tức liên quan đến các cuộc thương thuyết giữa chính phủ của họ và RIM liên hệ đến các vấn đề trên. Họ cần lưu tâm đến những toan tính chặn bắt và giải mã các liên lạc Blackberry. Năm 2009, cơ quan Etisalat của UAE đã gởi đến người dùng Blackberry một cập nhật "không chính thức" cho phép hãng cung cấp dịch vụ viễn thông nhận bản sao của tất cả các điện thư của người dùng. Ngay sau đó, RIM đã chuyển đến người dùng một cập nhật nhằm giải trừ phần mềm trái phép trên, nhưng người dụng Blackberry cần quan tâm đến tất cả mọi cập nhật nhu liệu không được tán phát ra trực tiếp từ RIM.

Dữ liệu khác

Làm blog

Nếu bạn có blog hay muốn làm blog, sau đây mà một số tài liệu để giúp thiết trí một blog. Điều chính bạn cần quan tâm để việc bảo đảm lý lịch bạn cho an toàn và làm sao cho những người sử dụng có thể đọc blog của bạn trong trường hợp bị ngăn chặn bởi nhà cầm quyền. Dưới đây là một số tài liệu khác về vấn đề thiết trí và thực hiện trang nhà phụ (mirror) trong trường hợp địa chỉ trang nhà chính bị ngăn chặn:

- Anonymous blogging with wordpress and Tor (Global Voices)
- Mirroring a censored wordpress blog (Global Voices)
- Tips on how to blog safely (EFF)
- Handbook for Bloggers (Reporters Without Borders)

Thu video

Sách: Video for Change in Arabic & Video: How to Create Videos for Change with Arabic subtitles (Nhân chứng).

Để tìm hiểu thêm những dữ liệu về an ninh và hoạt động trên mạng :

Tactical Tech & Frontline
Security in a Box:
Arabic tiếng Ả Rập, English tiếng Anh

The Electronic Frontier Foundation
In-depth guide (tài liệu hướng dẫn chi tiết): Surveillance Self-Defense (Theo dõi Tự Vệ) & Briefer International edition of SSD (tài liệu đúc kết ấn bản quốc tế của Surveillance Self-Defense) (cả hai tài liệu đều bằng tiếng Anh).

Tài liệu này được dịch bởi Blog No Firewall, www.nofirewall.blogspot.com.