BẢO MẬT KỸ THUẬT SỐ THỰC HÀNH

Bảo mật ngoài công nghệ

practical**digital**protection.com

BẢO MẬT KỸ THUẬT SỐ THỰC HÀNH

Hướng dẫn về thực hành an ninh không gian mạng trong môi trường thù địch

practicaldigitalprotection.com

DANH MỤC

LỜI NÓI ĐẦU

Nếu bạn đang đọc cuốn này, bạn có thể đã nhận thức được các mối đe dọa an ninh mạng cơ bản. Hướng dẫn này được thiết kế để cho bạn thấy các vấn đề về an ninh mạng quan trọng và cách thực hiện các bước để ngăn chặn chúng. Nó cho thấy sự quan trọng của việc ngăn ngừa, với những trường hợp thật về an ninh mạng và sự mất an ninh mạng là sự khác biệt giữa tự do và tù đày của bạn, của bạn bè, nguồn tin hoặc người cùng làm việc. Không chỉ là hướng dẫn sử dụng kỹ thuật an ninh mạng, đó là hướng dẫn về hành vi số an toàn hơn.

Một trong nhiều lý do của cuốn cẩm nang này là cung cấp một nguồn đáp ứng các nhu cầu thực sự về an ninh mạng cho các nhà báo, luật sư, các nhân viên NGO và những người khác ở Việt Nam.

"Nhiều mối đe doạ mà bạn phải đối mặt có tính vật lý hơn là kỹ thuật số"

Mọi người đều nghe nói về Edward Snowden và những phát hiện của ông về NSA và UCHK của Anh quốc và có thể đã xem những bộ phim của Mỹ về giám sát bằng điện tử hoặc thảo luận về cách mật vụ chính phủ và hacker cá nhân bẻ mã hoá để ăn cắp dữ liệu. Thật không may, những việc này không thực sự có liên quan đến các nhà bảo vệ nhân quyền ở Trung Quốc, hoặc hầu hết trên thế giới. Những vấn đề chính mà bạn phải đối mặt không phải là Hoa Kỳ hoặc các chính phủ khác đang sử dụng các tài nguyên khổng lồ để phá vỡ mã hóa đi kèm với hầu hết tất cả các email hoặc các chương trình trò chuyện trên điện thoại di động vào những ngày này. Vấn đề thực sự nằm ở những gì xảy ra khi bạn bị giam giữ hoặc điện thoại hoặc máy tính bị tịch thu. Hướng dẫn này sẽ tập trung nhiều hơn vào một cách tiếp cận hành vi đối với an ninh kỹ thuật số.

Đây là một trong nhiều lĩnh vực mà mối đe dọa đối với hoạt động ở Trung Quốc rất khác so với những gì thường được nói đến về an ninh mạng. Nhiều mối đe doạ mà bạn phải đối mặt mang tính chất vật lý hơn là kỹ thuật số. Hướng dẫn này, dựa trên đầu vào và ý tưởng từ nhiều nhà báo, nhân viên NGO và những người khác ở Trung Quốc, nhằm khắc phục sự hiểu lầm bằng cách cung cấp một cuốn hướng dẫn để xác định và chống lại những rủi ro phổ biến nhất.

Thứ hai, hầu hết các tài liệu bạn sẽ xem trực tuyến hoặc được trình bày trong các khóa đào tạo bạn có thể đã tham dự, thường là một sự tổng hợp của các giải pháp kỹ thuật khác nhau, nhiều trong số đó không cần thiết nâng cao. Những điều này thường không có những cuộc thảo luận cẩn thận về việc làm thế nào để cải thiện tính bảo mật của bạn thường không phải là từ các giải pháp kỹ thuật tiên tiến (mặc dù đôi khi cần thiết), nhưng từ những thay đổi tương đối trong hành vi.

Cuối cùng, việc tạo ra một hướng dẫn về an ninh mạng mà không tính đến hành vi và giới hạn của người hoạt động sẽ là một sự lãng phí thời gian. Nếu hướng dẫn sử dụng tập trung vào các giải pháp bảo mật phức tạp nhất mà không tính đến tác động của nó đến việc sử dụng và hiệu quả hàng ngày, thì có thể nó sẽ bị bỏ rơi sau thời gian, thực hành an ninh mạng sẽ từ từ bị lờ đi và làm cho bạn ít an toàn hơn khi bắt đầu. Một hướng dẫn có tính thực tế cần phải có một mặt bằng trung bình.

> “... cải tiến về bảo mật của bạn thường không phải là từ những giải pháp kỹ thuật tiên tiến, mà từ những thay đổi tương đối trong hành vi.”

Hướng dẫn này được xây dựng từ ba vấn đề trên và trình bày thành một văn bản độc lập với từng bước tự hướng dẫn trong việc giải quyết các nguy cơ về bảo mật mà bạn thường gặp phải.

GIỚI THIỆU

Chào mừng bạn đến với cuốn cẩm nang thực tiễn, tự học về an ninh mạng. Trong một khoảng thời gian ngắn một ngày, nó sẽ giúp bạn hiểu rõ những rủi ro đối với sự an toàn của mình và cho phép bạn tăng đáng kể sự an toàn liên quan đến việc sử dụng máy tính và điện thoại. Chúng tôi khuyên bạn nên đọc hướng dẫn này theo từng chương, vì mỗi chương sau dựa trên kiến thức được trình bày trong phần trước.

Xin vui lòng có máy tính xách tay và điện thoại của bạn khi bạn đọc sách này. Trước khi bạn bắt đầu thực hiện thay đổi, đảm bảo bạn đã tạo một bản sao lưu hoặc lưu lại bất kỳ dữ liệu, tài liệu hoặc các tệp tin khác mà bạn muốn chắc chắn để giữ. Bạn có thể di chuyển chúng vào USB, ổ cứng hoặc bộ nhớ đám mây của bạn ngay bây giờ. Sau này trong sổ tay này chúng tôi sẽ đề cập đến việc bảo vệ lưu trữ dữ liệu di động như USBs.

Tất cả các chương được viết cho máy tính xách tay của bạn(Win10 và OSX), nhưng nhiều vấn đề cũng áp dụng cho điện thoại thông minh. Nhiều ứng dụng cũng có sẵn cho cả iOS (iPhone) và Android. Bảo mật điện thoại thông minh được trình bày trong chương của riêng mình.

Hướng dẫn được viết với sự dễ nhớ và hầu hết các chương sẽ giống nhau theo cách bố trí. Hầu hết các chương sẽ bắt đầu với một giới thiệu chung về các vấn đề và khái niệm của chương. Sau đó trình bày thay đổi hành vi để hạn chế những rủi ro này, và kết luận với các giải pháp kỹ thuật. Trong hầu hết các trường hợp, bạn sẽ có thể tìm thấy các câu trả lời kỹ thuật trực tuyến, do đó chỉ những khía cạnh khó khăn hoặc quan trọng hơn được trình bày từng bước với ảnh chụp màn hình.

Trong suốt cuốn sách này, cụm từ "đối thủ" được sử dụng. Đây là mô tả người, người hoặc tổ chức gây ra mối đe dọa cho bạn. Nó có thể bao gồm từ cá nhân, đến tội phạm có tổ chức, cảnh sát, các nhân viên nhà nước hoặc thậm chí các tổ chức bán quân sự hoặc khủng bố.

Các phần kỹ thuật của cuốn sách này được tô màu. Phần có nền màu xanh nhạt đằng sau văn bản và hình ảnh dành cho OSX (máy Mac) và iOS (iPhone). Các phần với nền màu tía nhạt liên quan đến máy tính Win10 (máy tính cá nhân) hoặc điện thoại Android.

Giữa các chương là những câu chuyện. Những câu chuyện này dựa trên những trường hợp thực sự và cho thấy cách sử dụng hay không sử dụng các giải pháp được đưa ra sẽ có tác động trực tiếp. Các trường hợp đó là của các nhà hoạt động NGO, các nhà báo và các luật sư nhưng tất cả các câu chuyện đều được trình bày dưới dạng nặc danh hoặc bằng bút danh.

Sổ tay được chia thành bốn phần, chia thành 12 chương.

Phần I tập trung vào việc nhận biết những rủi ro của bạn. Nó được thiết kế để cung cấp cho bạn những công cụ để phân tích tình hình của chính bạn và những gì có thể đe dọa nhất đối với bạn. Nó cũng bao gồm một số bước cần thực hiện với máy tính của bạn trước khi bắt đầu, chẳng hạn như thay đổi cài đặt cơ bản.

Phần II, phần cơ bản, từ chương 3 đến chương 7. Mỗi chương sẽ tập trung vào một vấn đề cụ thể, ví dụ như mã hóa ổ cứng, bảo đảm an toàn trình duyệt web, hoặc xóa. Mỗi chương bắt đầu với tổng quan về vấn đề. Tiếp theo là các đề xuất thay đổi, cả về hành vi và các giải pháp kỹ thuật của bạn và khi cần thiết, hướng dẫn từng bước về cách thực hiện những thay đổi đó.

Phần III, từ chương 8 đến chương 11, là về bảo mật dành riêng cho điện thoại. Phần lớn những gì đã nói về thực hành trên máy tính sẽ áp dụng cho điện thoại (và máy tính bảng), nhưng phần này đề cập đến các mối đe dọa và giải pháp cụ thể liên quan đến điện thoại.

Phần IV bao gồm những biện pháp phòng ngừa. Nó sẽ giúp bạn thực hiện các bước thiết thực, không liên quan đến không gian mạng để đảm bảo sự an toàn của bạn và cách chuẩn bị cho điều tồi tệ nhất.

PHẦN I
RỦI RO

CHƯƠNG 1
Hiểu về các mối đe dọa của bạn sẽ trình bày thông tin về các mối đe dọa đang tồn tại, và hướng dẫn bạn đánh giá rủi ro và nhu cầu của bạn, để cho phép bạn tập trung vào những gì là quan trọng nhất đối với bạn.

CHƯƠNG 2
Chuẩn bị máy tính của bạn sẽ hướng dẫn bạn thực hiện các bước đầu tiên hướng đến bảo mật kỹ thuật số tốt hơn, và hướng dẫn bạn cách cài đặt cơ bản của hệ điều hành và làm thế nào để thay đổi chúng để tương ứng với nhu cầu.

CHƯƠNG 1
HIỂU VỀ CÁC MỐI ĐE DỌA CỦA BẠN

Bằng cách đọc chương này, bạn sẽ làm quen với các loại mối đe dọa đang tồn tại đối với bạn liên quan đến an ninh mạng. Biết được những điều cơ bản này sẽ giúp bạn hiểu và sử dụng phần hướng dẫn tốt hơn

Có rất ít hữu ích trong việc thực hiện các bước để tự bảo vệ mình nếu bạn không hiểu những mối đe dọa mà bạn phải đối mặt. Chương này ngắn gọn vạch ra một số các mối đe dọa phổ biến nhất. Nếu bất kỳ mối đe dọa nào tấn công liên quan đến bạn hoặc làm bạn quan tâm, hãy dành thời gian để tìm kiếm thêm thông tin trực tuyến. Nếu bạn gặp sự cố khi tìm kiếm các nguồn lực tốt hoặc vấn đề không rõ ràng hoặc quá kỹ thuật, bạn có thể liên hệ với chúng tôi để được trợ giúp.

BỊ BUỘC PHẢI VÔ HIỆU HÓA BẢO MẬT CỦA CHÍNH BẠN

Đây là lý do đằng sau cuốn sách hướng dẫn này, vì những người làm việc tại Trung Quốc phải đối mặt với những mối đe dọa lớn hơn về an ninh không gian mạng của họ so với tấn công mạng. Mối đe dọa quan trọng là bị cảnh sát, nhân viên nhà nước, bọn tội phạm hoặc những người khác để vô hiệu hóa bảo mật của bạn bằng cách cung cấp mật khẩu cho email, lưu trữ trên đám mây hoặc lưu trữ dữ liệu được mật mã của bạn. Đây là sự quan tâm cho toàn bộ hướng dẫn sử dụng, và lý do hướng dẫn tập trung vào hành vi, chứ không chỉ là công nghệ, vì đó là cách duy nhất để chống lại mối đe dọa này. Tất nhiên, chúng tôi cũng xem xét các mối đe dọa kỹ thuật và cung cấp các giải pháp cho những người có nguy cơ này.

CHO PHÉP TRUY CẬP QUA CỬA SAU

Bạn sẽ không chi tiêu một tháng lương để mua một bộ cửa mới và sau đó quên mua một khóa? Hoặc lắp đặt một cửa trước an toàn cùng với khóa, nhưng lại để cửa hậu mở rộng? Thật không may, khi nói đến an ninh mạng thì đây chính là điều mà nhiều người làm. Sử dụng mật khẩu mạnh và lau dấu vết trình duyệt web của họ, nhưng lại cho phép một ứng dụng trên điện thoại thông minh của bạn truy cập trực tiếp vào cùng một dịch vụ, thậm chí không cần mã PIN. Hoặc bằng cách truy cập cùng một dịch vụ trên trình duyệt trên điện thoại của bạn, để nó mở rộng cho bất cứ ai có thể truy cập trực tiếp hoặc online vào điện thoại của bạn. Bảo mật thích hợp có nghĩa là bạn phải phân tích tình huống của mình và cách bạn sử dụng các dịch vụ và chức năng đúng và sau đó tắt các lỗ hổng của bạn.

XÁC ĐỊNH ĐỊA ĐIỂM / QUY TẮC TAM GIÁC / THEO DÕI

Những chiếc điện thoại thông minh ngày nay giống như máy tính, và máy tính giống như điện thoại thông minh. Thông qua GPS, kết nối không dây và tín hiệu radio (điện thoại), có nhiều loại kết nối để máy tính và điện thoại thông minh của bạn dễ bị theo dõi. Không có biện pháp phòng ngừa, luôn luôn giả định ai đó có thể dễ dàng theo dõi bạn, và các thiết bị được yêu cầu không tốn kém. Nó không cần phải là một chính phủ để làm điều này. Điện thoại của bạn không bao giờ dừng việc gửi tín hiệu vị trí, thậm chí không có thẻ SIM. Ứng dụng được cài đặt thường yêu cầu truy cập vị trí, mở ra nhiều cách để người khác theo dõi bạn.

TRUY CẬP SMS, CUỘC GỌI, CUỘC TRÒ CHUYỆN, EMAIL

Nếu không có mã hóa cho tin nhắn trò chuyện, email, cuộc gọi điện thoại và tin nhắn SMS, nội dung được gửi bằng văn bản thuần túy có thể bị đọc không chỉ bởi nhà cung cấp dịch vụ mà còn cho bất kỳ ai trong mạng của bạn. Hầu hết các dịch vụ ngày nay đều may mắn sử dụng mã hóa, và nếu bạn tránh xa các dịch vụ của Trung Quốc, các công ty này sẽ không cung cấp thông tin cho nhà nước Trung Quốc. Một lần nữa, vấn đề chính không phải là việc gửi email hoặc tin nhắn SMS, nhưng điều gì sẽ xảy ra khi điện thoại hoặc máy tính của bạn bị thu giữ và bạn bị buộc phải từ bỏ mật khẩu.

CÁC LỖ HỔNG BẢO MẬT KHI KHỞI ĐỘNG

Hầu hết các hệ điều hành (OS) cho máy tính và điện thoại đi kèm với các cài đặt được chọn để sử dụng dễ dàng, chứ không phải cho an ninh. Như vậy, bước đầu tiên là phải đi qua cài đặt cho thiết bị của bạn và thực hiện các thay đổi để cải thiện bảo mật.

PHÁ MẬT KHẨU

Chạy toàn bộ từ điển với mật khẩu có thể được thực hiện trong vài phút. Sử dụng brute force (chạy hàng triệu lần mỗi phút) thì việc phá mật khẩu 4-6 ký tự có thể được thực hiện trong một giờ. Xem xét điều này khi chọn mật khẩu cho những dịch vụ đó thực sự quan trọng đến sự an toàn của bạn, như email công việc hoặc bộ nhớ được mã hóa. Một mật khẩu ngắn có thể ngăn chặn một người ngẫu nhiên nhặt được điện thoại của bạn trên đường phố trong việc truy cập, nhưng sẽ không có ích nếu bạn trở thành mục tiêu cho cảnh sát hoặc tội phạm có tổ chức. Phải sử dụng cụm từ mật khẩu, mật khẩu ngẫu nhiên dài hơn.

VI RÚT, HACKER, ROOTKIT VÀ HƠN THẾ NỮA

Hướng dẫn này sẽ không tập trung vào các mối đe doạ hacking tiên tiến, bởi vì nó ít xảy ra. Tuy nhiên, hãy hiểu rằng các vi-rút và rootkit (các vi-rút ẩn với bạn nhưng cho phép người khác truy cập vào máy tính của bạn) là những mối đe dọa phổ biến. Đảm bảo rằng bạn đã kích hoạt Tường lửa của bạn và có một chương trình chống vi-rút chạy dưới nền và chúng được thiết lập để cập nhật tự động. Cập nhật thường xuyên đảm bảo rằng ứng dụng được trang bị để nhận ra các mối đe dọa mới nhất. Các chương trình diệt vi rút đã hết hạn hầu như không đảm bảo an toàn.

MẠNG

Nếu ai đó không muốn bắt giữ bạn hoặc tịch thu thiết bị của bạn, nhưng thay vào đó bí mật truy cập thông tin của bạn, mạng của bạn là điểm tấn công tự nhiên. Bạn đã bao giờ thay đổi mật khẩu và tên người dùng để truy cập bộ định tuyến (router) của bạn ở nhà? Có nhiều khả năng, giống như hầu hết mọi người, bạn không làm. Đăng nhập và mật khẩu cho các bộ định tuyến được đăng trực tuyến và giống nhau cho hầu hết các bộ định tuyến. Nếu ai đó có thể truy cập router của bạn, họ có quyền truy cập vào máy tính của bạn. Cũng cần phải lưu ý rằng mạng wifi công cộng vốn có thể bị theo dõi và bạn nên thận trọng hơn khi làm bất cứ điều gì qua mạng công cộng.

PHỤC HỒI TẬP TIN

Khi bạn xóa một tệp tin, hoặc làm trống thùng rác, hoặc di chuyển một tệp từ máy tính của bạn sang USB hoặc ổ đĩa ngoài khác, sẽ không có gì bị xóa. Không có gì. Phần đó vẫn ở đó và có thể vẫn ở đó trong nhiều năm tới. Nó dễ dàng được truy cập bởi bất cứ ai với thậm chí chỉ với ít kỹ năng CNTT. Các chương trình miễn phí có thể được tải xuống và những chương trình này có thể tìm thấy mọi thứ trên máy tính mà bạn đã xóa trong quá khứ chỉ với một cú nhấn chuột. Phần xóa các tập tin trong sổ tay này có thể là một trong những điều quan trọng nhất

Bạn có hiểu các khái niệm chung này và cách chúng có thể gây ra vấn đề? Nếu không, vui lòng truy cập trực tuyến và tìm kiếm thêm thông tin trước khi bạn tiếp tục. Một khía cạnh quan trọng để hiểu là vị trí trên điện thoại của bạn (hoặc máy tính) có thể cho phép những người khác theo dõi bạn và cách phục hồi tệp tin có thể là một trong những mối đe dọa nghiêm trọng nhất đối với máy tính của bạn nếu nó rơi vào tay kẻ xấu.

ĐÁNH GIÁ RỦI RO VÀ NHU CẦU CỦA BẠN

Trước khi bạn tiếp tục với cuốn cẩm nang này, bạn cần phải hiểu nó áp dụng như thế nào đối với bạn và tình huống của bạn. Những câu chuyện được trình bày trong cuốn cẩm nang này sẽ cho bạn rõ rằng với tư cách là luật sư, nhà báo hoặc nhân viên của tổ chức phi chính phủ, bạn đối mặt với những rủi ro đáng kể. Ngay cả khi công việc của bạn không dẫn đến bị truy tố hoặc bắt bớ nghiêm trọng, bạn vẫn bị theo dõi vào những thời điểm và nếu có chuyện gì xảy ra với người khác, chẳng hạn như đồng nghiệp hoặc bạn bè, bạn có thể bị đưa ra thẩm vấn, hoặc máy tính và điện thoại của bạn bị theo dõi. Nếu bạn chưa thực hiện các bước để tự bảo vệ mình, điều này có thể tạo ra một vấn đề bảo mật hoàn toàn mới cho bạn. Như vậy, đừng để việc bạn thiếu tư duy bảo mật dẫn đến một vấn đề nhỏ để trở thành một vấn đề lớn.

"Tư duy an ninh hợp lý sẽ giữ những vấn đề nhỏ bé."

BƯỚC MỘT. BẠN CẦN GÌ ĐỂ BẢO VỆ?

Bạn làm việc với loại thông tin nào, và nếu bị tiết lộ hoặc cung cấp cho tội phạm hoặc cảnh sát, nó có thể ảnh hưởng đến bạn như thế nào. Quan trọng hơn, nó có thể ảnh hưởng đến người khác như thế nào? Nếu bạn toàn bộ ổ đĩa cứng bị xâm hại, thông tin nào về bạn và công việc

của bạn sẽ bị rò rỉ? Những thông tin bị lộ có thể là về nguồn tin, nhà tài trợ, đồng nghiệp hoặc đối tác? Hãy biết rằng việc lơ là bảo mật của bạn có thể ảnh hưởng đến bạn và nhiều người khác.

BƯỚC HAI. THIẾT BỊ NÀO CÓ NGUY CƠ?

Bạn chỉ có một điện thoại? Có lẽ bạn đã đưa hoặc bán một điện thoại khác cho một đồng nghiệp. Bạn chỉ truy cập một máy tính riêng của bạn, hay sử dụng một máy tính khác ở văn phòng? Có lẽ bạn sử dụng máy tính của bạn bè để đọc email của mình đôi khi? Lập danh sách tất cả các thiết bị mà bạn sử dụng hoặc gần đây đã sử dụng cho bất kỳ công việc nào.

BƯỚC THỨ BA. TẠI SAO BẠN LÀ MỘT MỐI ĐE DỌA?

Bạn là một nhà báo? Có khả năng hoạt động chống lại bạn nhằm vào việc tìm nguồn tin của bạn? Bạn có phải là nhân viên của tổ chức phi chính phủ, và cảnh sát có thể hành động chống lại bạn để lập bản đồ hoạt động của bạn, hoặc ai là người cung cấp tài chính cho bạn? Một luật sư cung cấp trợ giúp pháp lý cho khách hàng là nhà nước sẽ không nhận được tư vấn pháp lý phù hợp?

BƯỚC BỐN. MỐI ĐE DỌA CỦA BẠN LÀ AI?

Có phải là cảnh sát địa phương, hay nó là mafia? Có lẽ đó là cảnh sát an ninh quốc gia? Tìm hiểu xem ai là kẻ đe dọa có thể là sẽ đi một chặng đường dài để bạn quyết định về chính sách bảo mật của mình. Có lẽ bạn không phải là một mục tiêu chính, nhưng bạn làm việc cho một tờ báo thường là một mục tiêu. Nếu vậy, ai là kẻ tấn công, và làm thế nào bạn có thể bị liên lụy ngay cả khi bạn không phải là một mục tiêu chính?

Đây là một số câu hỏi bạn cần phải suy nghĩ trước khi tiếp tục đọc hướng dẫn sử dụng này. Những câu hỏi này cũng được phát triển hơn nữa trong Chương 12: An toàn phòng ngừa, chương cuối cho sách hướng dẫn này. Bắt đầu suy nghĩ về điều này bây giờ sẽ làm cho cuốn cẩm nang này có ý nghĩa hơn đối với bạn, và làm cho nó dễ dàng hơn cho bạn để hiểu tại sao và như thế nào các chương khác nhau áp dụng cho bạn.

HÀNH VI BẢO VỆ CƠ BẢN

Một khi đã bị bắt bởi cảnh sát, an ninh hoặc bọn tội phạm, bạn có rất ít khả năng để bảo vệ mình. Sự bao che cho cảnh sát và quan chức chính phủ ở các nước như Việt Nam, Trung Quốc, Pakistan và nhiều nước khác sẽ khiến bạn ít được bảo vệ. Có nhiều khả năng mà họ buộc bạn phải làm những điều họ muốn, bằng cách đe dọa bạn, bạn đồng nghiệp hoặc những người thân yêu, hoặc thông qua tra tấn trực tiếp về thể chất hoặc tinh thần. Cách duy nhất để tự bảo vệ mình là thực hiện các bước để tự bảo vệ mình. May mắn thay, có những cách dễ dàng để đạt được điều này, và những bước này có thể có ý nghĩa lớn, là sự khác biệt giữa tự do và giam cầm cho bạn, hoặc làm cho người khác gặp nguy hiểm.

Có quá nhiều dịch vụ, email, và các hệ thống trực tuyến khác để cảnh sát sử dụng có hiệu quả các phương pháp ngẫu nhiên để lấy thông tin của bạn. Họ cần có ý tưởng về những gì họ đang tìm kiếm, hoặc bắt đầu từ đâu. Nếu họ buộc bạn từ bỏ thông tin đăng nhập hoặc mật khẩu, hầu hết thời gian, họ cần phải biết yêu cầu gì. Ở Trung Quốc, họ có thể cho rằng bạn có tài khoản WeChat, ở Việt Nam họ sẽ cho rằng bạn có Facebook. Tuy nhiên, bên cạnh một vài dịch vụ được sử dụng rộng rãi như vậy, họ cần phải tìm ra những gì cần tìm kiếm.

Các giải pháp cho các vấn đề phổ biến nhất được trình bày dưới đây được cung cấp trong hướng dẫn sử dụng.

HẠN CHẾ THIỆT HẠI CÓ THỂ XẢY RA BỞI BÊN THỨ BA VÀ NGƯỜI KHÁC

Thứ nhất, tài khoản của bạn có thể bị lộ vì những gì xảy ra với người khác. Các đối tác, đồng nghiệp hoặc các nguồn mà bạn liên lạc có thể đã bị giam giữ và cung cấp thông tin đó hoặc họ có thể đã phản bội bạn. Điều này có nghĩa là, đối với những giao dịch và hoạt động nhạy cảm, bạn cần phải xem xét không chỉ những gì bạn nói và cách bạn lưu trữ thông tin. Để bắt đầu, luôn có email chuyên biệt hoặc tài khoản chat cho công việc nhạy cảm nhất của bạn. Đây không phải là email hoặc tài khoản làm việc thông thường của bạn.

Các tài khoản này không được sử dụng tên đầy đủ của bạn, cũng như những thông tin cá nhân (về danh tính và vị trí) của bạn khi bạn là một phần của trao đổi email hoặc trò chuyện. Tránh điều này ít nhất sẽ cho phép bạn tránh khỏi những rắc rối, ngay cả khi một bên thứ ba tìm thấy một trao đổi từ tài khoản này trong giao tiếp của người khác và người này nói rằng tài khoản này thuộc về bạn.

Vấn đề này là một trong những mối quan tâm lớn nhất, nhưng cũng là vấn đề bạn không thể kiểm soát hoàn toàn, bởi vì nó phụ thuộc vào người khác.

Cách an toàn nhất để hạn chế nguy cơ này là, đối với các cuộc trao đổi nhạy cảm nhất của bạn, sử dụng email và các chương trình trò chuyện với chức năng tự động hủy. Chức năng như vậy có nghĩa là các bản ghi hoặc email bị tự động bị hủy, trên cả hai đầu (người gửi và người nhận) dựa trên một khoảng thời gian đã thỏa thuận, bị phá hủy sau một giờ hoặc một

ngày. Danh tính của người dùng vẫn có thể bị tổn hại, nhưng bất kỳ thông tin thực tế hoặc "bằng chứng" nào được chia sẻ sẽ không có sẵn cho bất cứ ai, kể cả bạn và người khác, vì nó sẽ được tự động hủy một cách tự động mà không cần hồi phục.

Email tự động hủy đặc biệt hữu ích khi giao tiếp với người mà bạn không tin tưởng hoàn toàn hoặc người mà bạn biết có rất ít kỹ năng về các vấn đề về CNTT. Nó cũng rất dễ sử dụng. Tương tự với các chương trình trò chuyện nhất định.

THIỆT HẠI DO VẾT TÍCH VÀ BẰNG CHỨNG TRÊN MÁY TÍNH CỦA BẠN.

Ngay khi bạn bị giam giữ hoặc thiết bị của bạn bị tịch thu, chính quyền có thể bắt đầu phân tích pháp y kỹ thuật. Đây là cách cảnh sát có thể theo dõi bạn sử dụng những tài khoản nào và với kiến thức đó, dễ dàng buộc bạn từ bỏ quyền truy cập vào các tài khoản đó. Một khi họ đã thành công, thông tin mà họ tìm thấy có thể và có thể sẽ được sử dụng chống lại bạn, cũng như chống lại những người khác. Điều quan trọng của việc này không thể được nhấn mạnh đủ. Có nhiều cách để giải quyết vấn đề này.

Ví dụ, trình duyệt của bạn sẽ lưu và lưu trữ nhiều dữ liệu. Loại rõ ràng nhất là dấu trang đến nhà cung cấp dịch vụ email, hoặc các cookie hiển thị trang web bạn truy cập, mà còn dữ liệu quan trọng hơn, cũng như thông tin đăng nhập và thậm chí mật khẩu.

Bạn có thể thiết lập trình duyệt để tự động xóa các thông tin đó nhưng điều đó có nghĩa là bạn cần phải đăng nhập lại mọi thứ trong mỗi lần mở trình duyệt, bao gồm phương tiện truyền thông xã hội, các trang web mua sắm, vv Bạn cũng sẽ không thể lưu dấu trang. Điều này làm cho việc sử dụng máy tính nói chung là không hiệu quả. Nó cũng có vẻ nghi ngờ.

Thay vào đó, điều đầu tiên bạn cần làm là sử dụng chiến lược trình duyệt kép. Một trình duyệt cho ngày bình thường của bạn để lướt ngày và sử dụng. Một trình duyệt khác để truy cập email nhạy cảm nhất của bạn và các tài khoản khác hoặc sử dụng cho nghiên cứu nhạy cảm hơn. Trình duyệt thứ hai này nên được đặt để xóa mọi dấu vết tự động khi bạn đóng nó. Nó cũng nên thêm các phần mở rộng bảo mật nhất định bổ sung cho các trình duyệt quét sạch, để loại bỏ tốt hơn dấu vết.

DẤU VẾT HỆ THỐNG ĐIỀU HÀNH VÀ BẰNG CHỨNG.

Giống như trình duyệt của bạn, hệ điều hành của bạn thu thập các dấu vết trên mọi thứ bạn làm. Điều này bao gồm truy cập Internet. Nó cũng bao gồm các tài liệu word được mở và chỉnh sửa, các bản sao dữ liệu và tài liệu tạm thời, và các bản ghi ít hoặc nhiều thứ. Truy cập thông tin như vậy đòi hỏi nhiều kỹ năng kỹ thuật hơn là phân tích trình duyệt của bạn, nhưng không phải là rất khó khăn cho cảnh sát hoặc các chính phủ có nhiều nguồn lực.

Để giải quyết vấn đề này, bạn cần phải sử dụng một chương trình được thiết kế để xóa các dấu vết và dữ liệu tạm thời này khỏi máy tính của bạn. Một lần nữa, may mắn, nó rất dễ sử

dụng.

TÀI LIỆU "ĐÃ XÓA"

Một trong những khái niệm bị hiểu nhầm nhất là xóa mọi thứ từ máy tính. Cảnh sát biết điều này, và sử dụng nó. Nói tóm lại, khi bạn "xóa" một cái gì đó, hoặc rỗng thùng rác, không có gì là thực sự bị xóa. Sự khác biệt duy nhất là máy tính hoặc điện thoại đánh dấu nó là "không gian sẵn có", sau này có thể được ghi đè bằng các dữ liệu mới. Nó vẫn ở đó. Trong nhiều trường hợp, nó vẫn tồn tại trong nhiều năm tới. Trong các trường hợp khác, chỉ một phần dữ liệu "đã xoá" được ghi đè bằng nhạc, tệp, video hoặc bất cứ thứ gì khác, trong khi phần còn lại vẫn còn.

Mặc dù bạn không thể nhìn thấy nó hoặc tìm kiếm nó, hiện có nhiều chương trình dễ và hiệu quả để khôi phục tất cả các dữ liệu như vậy như là nó đã không bao giờ được "xóa". Các chương trình như vậy rất dễ sử dụng - trên thực tế, ngay cả những người không có kỹ năng sử dụng máy tính cũng có thể làm được, chỉ trong 5 phút. Nếu bạn bị giam giữ, điều này sẽ được sử dụng trên USBs, điện thoại, máy tính và thiết bị của bạn. Hãy ghi nhớ điều này.

DỮ LIỆU CỦA BẠN.

Dữ liệu là tất cả các tệp tin, từ tài liệu đến video, ảnh mà bạn lưu giữ và lưu trữ trên USB, điện thoại, ổ cứng gắn ngoài hoặc máy tính của bạn. Cách duy nhất để thực sự bảo vệ thông tin như vậy là lưu trữ nó ở một nơi an toàn cao. Đây phải là ổ cứng được mã hóa, khó tìm trên máy tính của bạn.

Tuy nhiên, nếu được mật mã, cảnh sát sẽ thông báo, trực tiếp hoặc thông qua các dữ liệu pháp y. Với ý nghĩ đó, để thực sự bảo vệ thông tin như vậy, bạn cần phải sử dụng mã hóa "ẩn", do đó, họ thậm chí không thể thấy rằng bạn đang mã hóa thông tin ở nơi đầu tiên. Họ không thể đòi hỏi, đe dọa, hoặc tra tấn bạn về những thứ mà họ không biết có sự tồn tại.

MỘT LẦN NỮA, ĐIỀU NÀY THỰC SỰ DỄ DÀNG HƠN.

Bạn cũng nên đơn giản hóa mọi thứ. Điều này có nghĩa là không chỉ lưu trữ tất cả các tệp công việc liên quan ở một nơi mà chỉ lưu trữ những thứ cần thiết. Xem nhanh các tệp công việc cũ của bạn có thể cho thấy rằng hầu hết các tệp đó không cần nữa. Bản nháp, các phiên bản trước, các tệp được hỗ trợ sau được kết hợp với các tài liệu chính, v.v ... chúng có thể và tất cả sẽ bị xóa. Chỉ lưu trữ những thứ mà bạn thực sự cần.

Bạn cũng có thể di chuyển các tệp cũ mà bạn cần phải lưu giữ, nhưng không chắc sẽ cần phải sử dụng, để lưu trữ an toàn trong đám mây. Lưu trữ đám mây như vậy cần được an toàn và bạn cần sử dụng bộ nhớ không có máy chủ ở quốc gia của bạn. Bạn cũng cần xem xét các điểm về các trình duyệt, để đảm bảo cảnh sát không thể xác định việc sử dụng lưu trữ đám mây của bạn hoặc truy cập nó một cách dễ dàng.

ĐIỆN THOẠI, PADS VÀ CÁC ỨNG DỤNG.

Bạn cần tách riêng việc sử dụng máy tính và điện thoại. Bạn không nên để nó chồng lên nhau. Tất cả các bước bạn thực hiện vì sự an toàn và bảo mật có thể trở nên vô nghĩa khi sử dụng điện thoại bất cẩn. Việc áp dụng các biện pháp an toàn ở máy tính có còn ý nghĩa nếu cảnh sát có thể tìm thấy thông tin đó thậm chí còn dễ dàng hơn trên điện thoại của bạn?

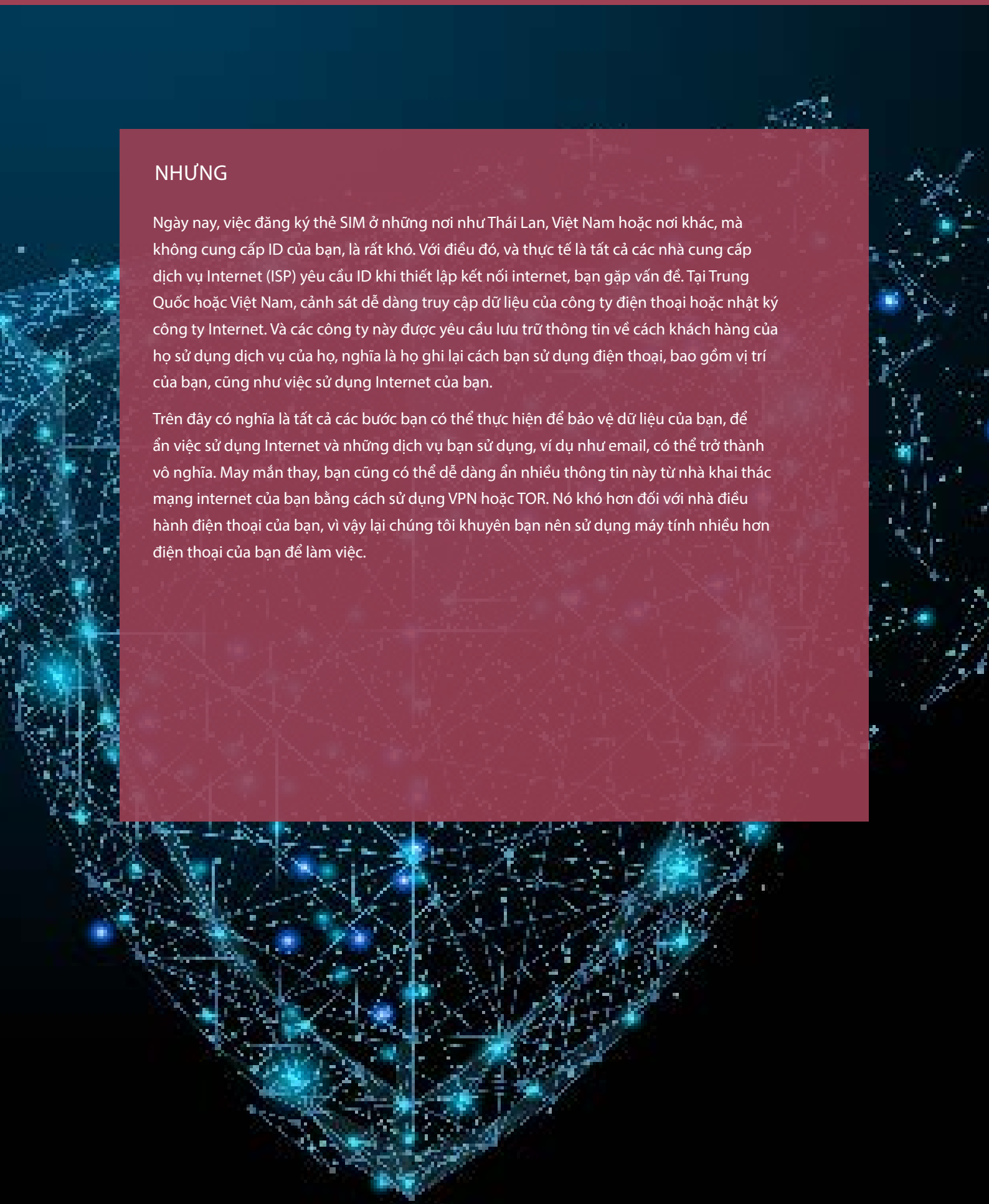
Mọi người đều sử dụng các ứng dụng trên điện thoại để truy cập các tài khoản và dịch vụ. Ứng dụng di động không chỉ cho phép cảnh sát truy cập trực tiếp, mặc dù có hạn chế, vào tài khoản của chúng ta, ví dụ như email ngay cả khi bạn bảo vệ các ứng dụng đó bằng mật khẩu khác, cho phép họ biết bạn sử dụng dịch vụ nào. Điện thoại của bạn có thể xóa bỏ hoàn toàn tất cả an ninh máy tính của bạn. Điều này đã xảy ra nhiều lần.

Hãy đảm bảo cách bạn sử dụng điện thoại của mình và đảm bảo tránh sử dụng những chương trình cho phép xác định dịch vụ bạn sử dụng trực tuyến. Thông thường, khi tải xuống hoặc định cấu hình ứng dụng trên điện thoại di động của bạn, bạn sẽ được hỏi có cho phép nó truy cập về vị trí, máy ảnh hoặc danh bạ không. Hơn nữa, không sử dụng trình duyệt trên điện thoại của bạn để truy cập trang web nhạy cảm, vì không thể xóa dấu vết trên điện thoại. Đồng thời, việc xóa thích hợp cũng rất khó khăn trên điện thoại và bạn không nên sử dụng điện thoại để lưu trữ bất kỳ tài liệu công việc nào hoặc tải xuống bất kỳ tài liệu làm việc nào để chuyển sang máy tính sau này

NGƯỜI DÙNG

Cuối cùng, bạn là mối đe dọa lớn nhất đối với bản thân bạn, và cho người khác. Bảo vệ thông tin, kiến thức và dữ liệu của bạn đòi hỏi bạn phải lên kế hoạch trước. Ngoài việc thực hiện đánh giá rủi ro, bạn cần lập kế hoạch làm thế nào để hành động nếu có và chia sẻ kế hoạch này với nhiều người đáng tin cậy, những người không có khả năng thực hiện. Bạn có thể chia sẻ thông tin gì (và một số bạn phải chia sẻ, hoặc họ sẽ biết bạn đang giấu một thứ gì đó) và bạn phải bảo vệ thông tin gì? Tương tự như vậy, nếu bạn làm việc với các đối tác, bạn cần thảo luận và đưa ra các thỏa thuận để mọi người đồng ý về cùng một chiến lược. Bạn cần phải có một ý tưởng tốt những thông tin mà những người khác có thể sẽ tiết lộ?

Có một câu nói trong thế giới chính trị: Không bao giờ nói dối về một cái gì đó mà công chúng sẽ biết được. Đối với bạn, đừng giấu thông tin mà cảnh sát có thể sẽ tìm thấy. Không có giải pháp kỹ thuật cho điều này, chỉ có biện pháp phòng ngừa và trí thông minh của riêng bạn.



NHƯNG

Ngày nay, việc đăng ký thẻ SIM ở những nơi như Thái Lan, Việt Nam hoặc nơi khác, mà không cung cấp ID của bạn, là rất khó. Với điều đó, và thực tế là tất cả các nhà cung cấp dịch vụ Internet (ISP) yêu cầu ID khi thiết lập kết nối internet, bạn gặp vấn đề. Tại Trung Quốc hoặc Việt Nam, cảnh sát dễ dàng truy cập dữ liệu của công ty điện thoại hoặc nhật ký công ty Internet. Và các công ty này được yêu cầu lưu trữ thông tin về cách khách hàng của họ sử dụng dịch vụ của họ, nghĩa là họ ghi lại cách bạn sử dụng điện thoại, bao gồm vị trí của bạn, cũng như việc sử dụng Internet của bạn.

Trên đây có nghĩa là tất cả các bước bạn có thể thực hiện để bảo vệ dữ liệu của bạn, để ẩn việc sử dụng Internet và những dịch vụ bạn sử dụng, ví dụ như email, có thể trở thành vô nghĩa. May mắn thay, bạn cũng có thể dễ dàng ẩn nhiều thông tin này từ nhà khai thác mạng internet của bạn bằng cách sử dụng VPN hoặc TOR. Nó khó hơn đối với nhà điều hành điện thoại của bạn, vì vậy lại chúng tôi khuyên bạn nên sử dụng máy tính nhiều hơn điện thoại của bạn để làm việc.

CHƯƠNG 2:
CHUẨN BỊ MÁY TÍNH CỦA BẠN

Chương này sẽ cho bạn thấy một số cài đặt trên máy tính của bạn cần được xem xét. Bằng cách đi qua chương này, bạn sẽ có hiểu biết sâu hơn về cài đặt cơ bản và thiết lập máy tính của mình, cũng như cách bạn có thể thay đổi và kiểm soát được máy tính của mình.

Đối với phần còn lại của hướng dẫn này, về những hướng dẫn kỹ thuật, chúng tôi sẽ sử dụng các chức năng tìm kiếm. Do đó, khi những thay đổi về kỹ thuật cần được thực hiện, chúng tôi sẽ cung cấp cụm từ tìm kiếm để xác định cài đặt. Bạn có thể quen thuộc với các chức năng tìm kiếm, nhưng để đảm bảo, dưới đây là một ảnh chụp màn hình hiển thị vị trí của khu vực tìm kiếm.

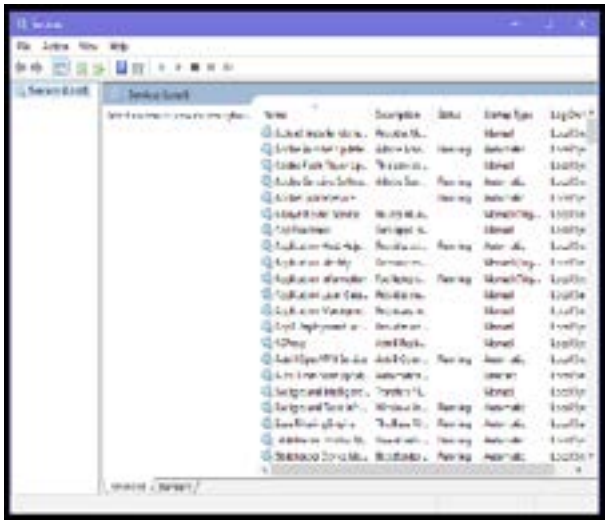
Các cụm từ tìm kiếm này sẽ được cung cấp bằng cả tiếng Việt và tiếng Anh vì bạn có thể sử dụng cả hai ngôn ngữ trên máy tính của bạn và các cụm từ tìm kiếm sẽ như sau: Search Term/Thuật ngữ tìm kiếm.

Đối với Win10, các vấn đề chúng ta cần phải xem trước khi bắt đầu với phần cốt lõi của cuốn sổ tay này, được chia thành ba khu vực: Dịch vụ, Chính sách an ninh cục bộ và Cài đặt.

"Nếu bạn đang sử dụng ấn bản Windows HOME, một số cài đặt này sẽ không có sẵn"

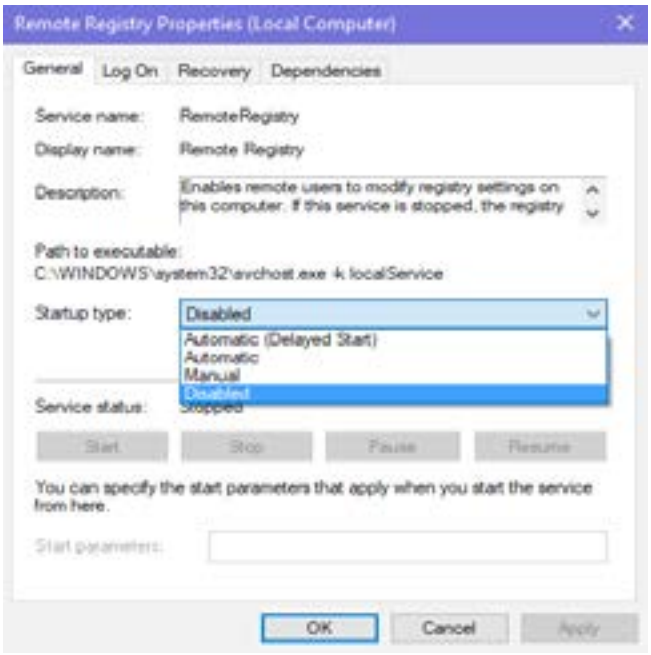
DỊCH VỤ (SERVICES)

Một số tính năng của Windows, chẳng hạn như Services/Dịch vụ và Local Security Policy/Chính sách an ninh cục bộ (cũng như BitLocker) chưa được bản địa hoá cho tiếng Việt và vẫn hiển thị bằng tiếng Anh.



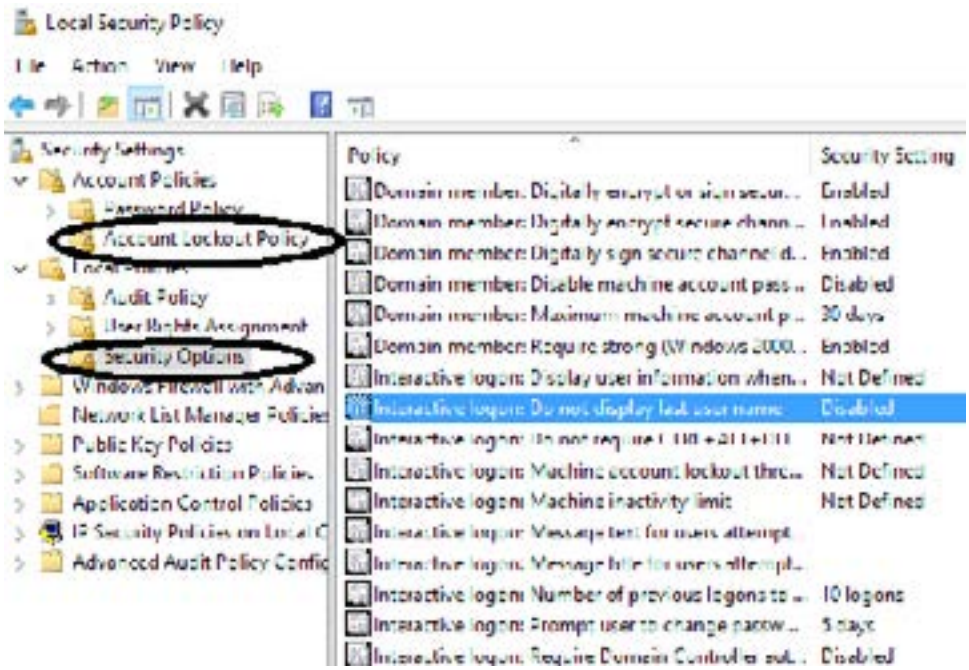
Dịch vụ chạy dưới nền máy tính của bạn và xác định máy tính có thể làm gì. Ví dụ, để từ chối truy cập từ xa vào máy tính của bạn, dịch vụ cho phép truy cập từ xa phải được tắt. Chúng tôi sẽ xác định một số dịch vụ chính mà bạn phải tắt (vô hiệu hóa) để cải thiện bảo mật.

Đối với Win10, mở cửa sổ dịch vụ bằng cách nhập Dịch vụ vào thanh tìm kiếm. Trong cửa sổ sẽ mở ra (WIN - XX), tìm các dịch vụ được liệt kê dưới đây bằng cách đi qua danh sách, và nhấp đúp vào mỗi một trong số chúng.

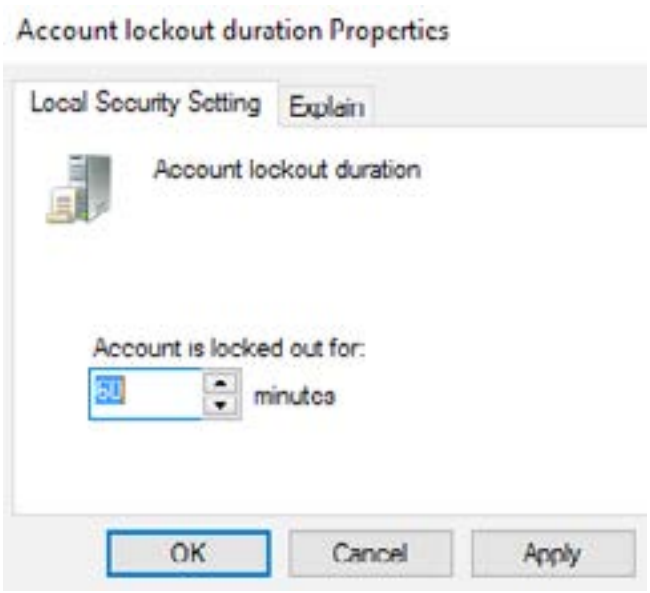


- Remote Desktop Configuration (Cấu hình máy tính từ xa)
- Remote Desktop services (Dịch vụ máy tính từ xa)
- Remote Registry (Đăng ký từ xa)
- Routing and Remote Access (Định tuyến và truy cập từ xa)
- UPnP Device host (Máy chủ lưu trữ UPnP)
- Volume Shadow Copy (Bản sao khối lượng)
- File History Service (Lịch sử dịch vụ tệp)

Trong cửa sổ nhỏ mới mở ra, tìm Startup Type, và thay đổi nó thành Disabled và nhấn OK hoặc Apply.



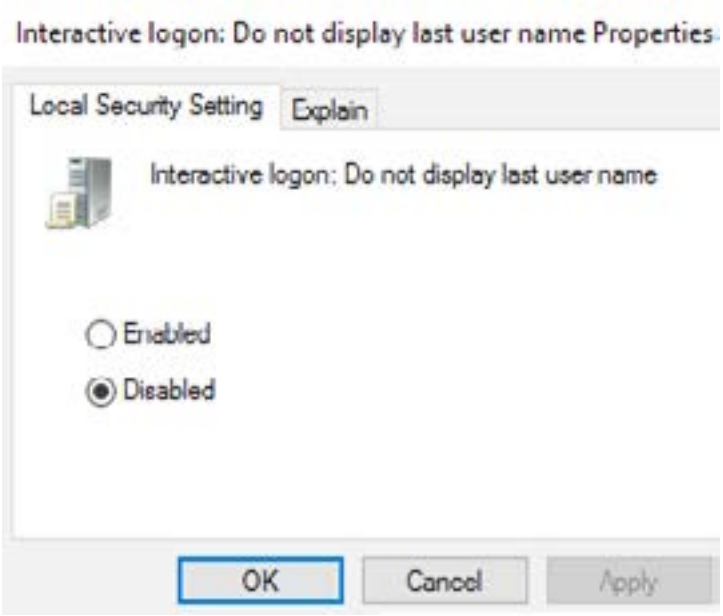
CHÍNH SÁCH BẢO MẬT (CHÍNH SÁCH BẢO MẬT CỤC BỘ)



Khu vực chính sách bảo mật cho phép bạn thiết lập một chính sách cho các vấn đề liên quan đến bảo mật. Ví dụ, bạn có thể thiết lập chính sách để nếu ai đó nhập mật khẩu sai nhằm mở hệ điều hành 5 lần liên tiếp, máy tính sẽ ngừng hoạt động trong 1 giờ. Bạn nên biết một số thay đổi của chính sách bảo mật. Mở cửa sổ Chính sách bảo mật cục bộ/Local Security Policy bằng cách viết trong cụm từ tìm kiếm Local Security Nhấn vào Account Policies > sau đó nhấn Account Lockout Policy. Nhấn đúp Account lookout duration và trong của sổ mới chọn mức thời gian, ví dụ 1 h rồi nhấn OK. Sau đó kích đúp vào Account lockout threshold và lựa chọn 3 hoặc 5. Điều đó có nghĩa nếu đánh sai mật khẩu 3 hoặc 5 lần liên tiếp, máy tính sẽ bị khóa 1 h hoặc bao lâu tùy theo bạn đã cài đặt trước đó.

Lưu ý: trước bước tiếp theo, hãy chắc chắn rằng bạn đã nhớ tên người dùng/tên để truy cập cho Win10, viết lên giấy nếu cần, cùng với email gắn liền với tài khoản Win10 của bạn. Bạn sẽ cần phải biết tài khoản đăng nhập/mã đăng nhập để đăng nhập sau khi thực hiện thay đổi này.

Vào Local policies > Security Options. Kích đúp Interactive login: Do not display last user name và chọn Enabled. Kích đúp vào Interactive login: Display user information when the session is locked và chọn Do not display username.



Điều này có nghĩa là tên người dùng của bạn sẽ không được hiển thị khi máy tính khởi động, và để mở Windows, bạn cần phải nhập tên đăng nhập và mật khẩu. Điều này tăng tính bảo mật, vì cả hai đều cần thiết cho việc mở, chứ không chỉ mật khẩu của bạn.

Cuối cùng, và cũng quan trọng, tìm cửa sổ Local Security Policy như trên (Local policies > Security Options) Shutdown: Clear virtual memory pagefile và chọn Enable rồi nhấn Ok. Lý do cho việc này sẽ được thảo luận ở Chương 7: Xóa thông tin

CÀI ĐẶT (SETTINGS)

Các cài đặt cơ bản này liên quan đến, chẳng hạn như cho phép các ứng dụng và chương trình sử dụng dịch vụ định vị hoặc để cho phép webcam hoặc micrô hoạt động. Nó cũng cho phép chúng tôi thực hiện một số thay đổi khác để tăng cường bảo mật của bạn.

Các cập nhật (Windows Update settings). Nhấn vào Advanced Options, chọn Automatic updates, và Give me updates for other Microsoft products when I update Windows.

Bảo vệ cửa sổ (Windows Defender). sử dụng bảo vệ hiện thời và dựa trên đám mây. Nếu bạn sử dụng chương trình chống virus khác thì Windows Defender sẽ tự động đóng và bạn có thể bỏ qua bước này.

Backup (Backup Settings). Hãy nhớ không lựa chọn Back up using File History is not selected.

Địa điểm/Location (Cài đặt cá nhân về địa điểm): Hãy để Location ở chế độ tắt. Khi bạn ở đây, nhấn Clear history on this device. Không như điện thoại thông minh, máy tính không cần thiết phải sử dụng địa điểm.

Webcamera (Webcam privacy settings). Nếu bạn ít sử dụng webcamera (WIN – XX), tắt dịch vụ này. Nếu bạn sử dụng thường xuyên, hãy để nó bật, nhưng cuộn xuống và đi qua từng chương trình và tắt tất cả mọi thứ, ngoại trừ chương trình bạn sử dụng nó (ví dụ như Skype) (S-W8).

Cũng giống như với cài đặt Webcamera, nơi bạn có thể tắt dịch vụ hoàn toàn hoặc cho phép nó, nhưng sau đó chọn chương trình nào được phép sử dụng, cũng được cung cấp cho nhiều khía cạnh khác của khu vực cài đặt được hiển thị bên dưới, như cho Microphone, Danh bạ, v.v.

Microphone (Cài đặt cá nhân cho micrô). Nếu bạn hiếm khi sử dụng micrô, hãy tắt dịch vụ này. Nếu bạn sử dụng thường xuyên, hãy để nó bật, nhưng cuộn xuống và đi qua từng chương trình và tắt tất cả mọi thứ, ngoại trừ chương trình bạn sử dụng nó (ví dụ như Skype).

Cortana (Cortana & Cài đặt tìm kiếm). Tắt tất cả tùy chọn. Đây là chức năng tìm kiếm của Win10 và nó thu thập rất nhiều thông tin về những gì bạn làm. Do đó, tốt nhất là tắt chức năng này.

Tài khoản (Cài đặt bảo mật thông tin tài khoản). Tắt Thông tin Tài khoản/Account Info.

Danh bạ (Cài đặt danh bạ). Xem lại tất cả các chương trình có quyền truy cập vào Danh bạ của bạn và tắt mọi thứ không cần thiết hoặc không sử dụng.

Dưới cùng một khu vực (Cài đặt bảo mật/ Privacy settings), nhấp vào General, Calendar, Call History, Email, Messaging, Radios and Other Devices. Tắt tất cả, trừ khi bạn biết chắc chắn bạn cần sử dụng chúng, mà điều này ít khi xảy ra.

Trong Cài đặt phản hồi và chẩn đoán (cài đặt phản hồi), hãy đặt chế độ Never/Không bao giờ về yêu cầu phản hồi của Windows và Send you device data to Microsoft to Basic.

Xem lại đăng nhập của bạn (sign-in options) và đảm bảo rằng mật khẩu là cần thiết để đánh thức máy tính từ chế độ ngủ.

Kiểm tra cài đặt bắt đầu của bạn (start setting) và tắt Show most used apps, show recently added apps and show recently opened items trong Jump Lists on Start o hoặc thanh tác vụ.

Mở cài đặt Bluetooth (Bluetooth Setting) và tắt Bluetooth trừ khi bạn sử dụng. Nếu bạn quyết định sử dụng Bluetooth, hãy nhấp vào liên kết More Bluetooth options. Trong cửa sổ mới bật lên, hãy tắt Allow Bluetooth devices to find this PC. Then select/enable Alert me when a new Bluetooth device wants to connect.

Tìm kiếm Allow remote access to your computer và đảm bảo rằng nó không được phép (Remote Assistance and Remote Desktop).

Cuối cùng, trong phần cuối của Background apps, xem lại những ứng dụng nào được phép chạy và loại bỏ tất cả những gì mà bạn không muốn chạy

ẩn hoặc những gì bạn không sử dụng. Các chương trình trò chuyện sẽ cần chạy dưới nền nếu bạn sử dụng chúng trên máy tính của bạn (nhưng bạn nên tránh sử dụng các chương trình trò chuyện trên máy tính).

Chúc mừng, phần tẻ nhạt nhất của hướng dẫn này đã hết và chúng ta có thể chuyển sang những phần thú vị hơn.

v

LƯU Ý VỀ MẬT KHẨU

Chúng tôi sẽ bắt đầu phần này bằng cách không nói về mật khẩu. Bảo vệ lớn nhất mà bạn cần đối với cảnh sát hoặc bọn tội phạm là chúng không biết điều chúng cần là gì. (Chương 4: Lấy thông tin). Đó là lý do tại sao bạn phải sử dụng mã hoá ẩn để lưu trữ các tài liệu của bạn (Chương 5: Lưu trữ thông tin). Và đó là lý do tại sao CCleaner nên được sử dụng để xóa tất cả dấu vết công việc của bạn khi bạn tắt máy tính (Chương 7: Xóa thông tin).

Đơn giản chỉ cần đặt, nếu họ không biết những dịch vụ bạn sử dụng, họ không thể yêu cầu mật khẩu cho chúng. Đây là cách bạn tự bảo vệ mình. Đó là một phần cốt lõi của bất kỳ hành vi an toàn. Đảm bảo người khác không biết tài liệu gì bạn có.

Mật khẩu đôi khi được gọi là cụm từ mật khẩu. Cả hai cái tên đều tồi tệ, bởi vì chúng cũng không phải là từ hay cụm từ. Để hiểu tại sao, hãy xem bên dưới ba cách chính để phá vỡ chúng.

Hình thức đầu tiên là kỹ thuật xã hội, để tìm ra mật khẩu của bạn có thể dựa vào người hoặc bối cảnh của bạn như kiểm tra số kết hợp ngày sinh của mẹ, tên vật nuôi hoặc thể thao ưa thích của bạn, v.v ...

Để bảo vệ kỹ thuật xã hội, đừng bao giờ sử dụng tên, số kết hợp dựa vào ngày sinh nhật hoặc lễ kỷ niệm của chính bạn, người thân, bạn bè ...

Hình thức thứ hai là một cuộc tấn công từ điển, nơi mà một máy tính có thể chạy qua một từ điển chỉ trong vài phút, cũng như sự kết hợp của các từ. Nếu bạn sử dụng từ, thậm chí trong một câu dài, nó sẽ bị phá rất nhanh, và có thể được thực hiện trong vòng vài giờ.

Để bảo vệ từ một cuộc tấn công từ điển, mật khẩu của bạn sẽ không bao giờ chứa từ, ngay cả khi kết hợp với nhau như một câu dài. Điều này bao gồm tiếng lóng. Điều này đặc biệt quan trọng để tránh những từ tiếng Hoa và tiếng Anh.

Hình thức thứ ba được gọi là một cuộc tấn công tàn bạo, với một máy tính chạy hàng triệu thử nghiệm kết hợp các nhân vật khác nhau mỗi phút. Mã PIN chỉ sử dụng 4- hoặc 6. Số lượng cuộc tấn công bruteforce có thể phá vỡ mật khẩu ngắn rất nhanh, ngay cả khi mật khẩu đó là ngẫu nhiên.

Để bảo vệ chống lại một cuộc tấn công tàn bạo, mật khẩu không được quá ngắn, và nên bao gồm tất cả bốn loại ký tự khác nhau.

Bàn phím được thiết kế bằng cách có 4 loại khóa khác nhau. Đây là những chữ in hoa (ABC), chữ cái nhỏ (abc), số (123) và ký tự đặc biệt (?! @).

Một mật khẩu tốt phải chứa ít nhất một chìa khóa từ mỗi nhóm, và có ít nhất 10 phím dài. Đối với các tài khoản nhạy cảm, bạn cần sử dụng một mật khẩu nâng cao theo tất cả các quy tắc này.

Bạn có thể kiểm tra sức mạnh tương đối của các cụm từ mật khẩu khác nhau với các dịch vụ trực tuyến như How Secure is My Password. Trang web sẽ cho bạn biết thời gian bao lâu để phá vỡ mật khẩu của bạn, từ vài giây đến hàng triệu năm.

26

(https://howsecureismypassword.net/)

Đồng thời đảm bảo rằng các mật khẩu mà bạn sử dụng cho bảo mật liên quan đến công việc không liên quan đến mật khẩu của bạn cho các dịch vụ cá nhân. Không nên có sự tương đồng giữa mật khẩu cho công việc và việc khác. Nếu bạn sử dụng Innoj-A7 cho tài khoản cá nhân, không sử dụng InnojH * ASH-B7 cho tài khoản làm việc. Nó quá giống nhau. Đảm bảo rằng không có sự giống nhau về kiểu dáng hoặc cấu trúc giữa các mật khẩu khác nhau của bạn.

Chúng tôi không khuyên bạn nên sử dụng phần mềm quản lý mật khẩu, như KeePass, trừ khi bạn lưu trữ chương trình và cơ sở dữ liệu bí mật và mã hóa trong USB. Nếu bạn có chương trình quản lý mật khẩu trên máy tính, chỉ cần nhìn thoáng qua là cảnh sát hoặc bọn tội phạm sẽ biết bạn có dung và sẽ ép bạn phải cung cấp mật khẩu. Chúng tôi cũng khuyên bạn không nên lưu trữ những chương trình như vậy trong phần không gian mã hóa giấu (xem Chương 10: Lưu trữ thông tin). Lý do cho điều này là chúng có thể thấy thấy không gian giấu và bẻ gẫy nó và sẽ lấy được hết những mật khẩu của bạn cho những tài liệu mà bạn muốn bảo mật.

Nhận dạng bằng mắt hoặc vân tay

Không bao giờ sử dụng nhận dạng võng mạc, vân tay, hoặc các thông tin sinh trắc học khác. Nó có vẻ như là công nghệ tiên tiến nhưng nó ít an toàn hơn, theo các bước trên.

Dữ liệu sinh trắc như vậy một khi nó được tiết lộ, không giống như mật khẩu, nó không thể thay đổi. Nếu mật khẩu của bạn bị xâm nhập bạn có thể dễ dàng tạo một mật khẩu mới. Bạn không thể có được đôi mắt mới hoặc dấu vân tay khác.

Quan trọng hơn, nếu bạn đã thiết lập võng mạc hiển thị hoặc dấu vân tay để mở điện thoại hoặc giải mã một tập tin, và bạn đang bị bắt giữ này, cảnh sát thậm chí không cần phải bắt bạn tiết lộ mật khẩu của bạn. Tất cả những gì họ cần làm là giữ điện thoại lên mặt hoặc buộc ngón tay lên cảm biến. Bạn thậm chí không cần phải tỉnh táo. Để bảo đảm an toàn, không sử dụng!

PHẦN 2
MÁY TÍNH

Phần máy tính của bạn, gồm 5 chương, cùng một số lưu ý ngắn

CHƯƠNG 3
Các quy tắc cơ bản có lẽ là chương quan trọng nhất vì nó cho thấy hành vi và quy tắc cơ bản có thể bảo vệ bạn tốt hơn nhiều so với các giải pháp kỹ thuật.

CHƯƠNG 4
Lấy thông tin thảo luận về kết nối internet, cách ẩn địa chỉ IP của bạn khi lướt web, sử dụng trình duyệt và làm thế nào để có được thông tin.

CHƯƠNG 5
Lưu trữ Thông tin là về cách lưu trữ dữ liệu của bạn và các tập tin một cách an toàn.

CHƯƠNG 6
Chia sẻ thông tin liên quan đến việc gửi email an toàn, sử dụng lưu trữ trên đám mây và các vấn đề khác liên quan đến cách chia sẻ dữ liệu và giao tiếp an toàn với người khác.

CHƯƠNG 7
Xóa thông tin liên quan đến nhiều hiểu sai về bảo mật CNTT, cụ thể là làm thế nào để xóa thông tin một cách hiệu quả.

CHƯƠNG 3
CÁC QUY TẮC CƠ BẢN

Phần lớn an toàn mạng không phải là kỹ thuật mà đó là về hành vi. Do đó, một số quy tắc cốt lõi sẽ được trình bày dưới đây. Đừng lo lắng nếu bạn không hiểu làm thế nào để kết hợp những điều này vào hành vi của bạn ngay lập tức. Chúng tôi sẽ thảo luận chi tiết các vấn đề này trong các chương có liên quan sau đây. Tuy nhiên, các quy tắc này có thể đảm bảo tính bảo mật cho máy tính và điện thoại của bạn và bạn nên rất chú ý khi đọc chương ngắn này, do đó, bạn cần ghi nhớ những điều này khi nghiên cứu cùng với hướng dẫn sử dụng này.

Sau khi đọc từng mô tả ngắn gọn về từng quy tắc cơ bản, hãy tạm dừng và tự hỏi mình cách áp dụng cho hành vi hoặc thói quen của bạn. Chúng không phức tạp nhưng hãy dành một chút thời gian để suy nghĩ về từng quy tắc cơ bản cụ thể sẽ đảm bảo bạn nắm bắt được cách chúng tương tác với nhau và với các thói quen của bạn. Bạn đã theo lời khuyên này trong hành vi trực tuyến và không trực tuyến của mình và nếu không nghĩ về những thay đổi bạn cần thực hiện để tuân theo các quy tắc cốt lõi này được an toàn hơn. Nếu bạn có thắc mắc hoặc nghi ngờ, hãy đánh dấu lại hoặc viết ra. Chúng có thể được giải quyết bởi các chương sau trong sách hướng dẫn này nhưng nếu không chúng tôi cũng sẽ cung cấp thông tin bổ sung.

BIẾT CÁC MỐI ĐE DỌA CỦA BẠN

Không thể tự bảo vệ mình chống lại tất cả các mối đe dọa ở bên ngoài. Thậm chí nếu bạn dốc toàn thời gian vào việc này, bạn vẫn không thể an toàn 100%. Thay vào đó, bạn phải tập trung vào các mối đe dọa chính. Hãy trở nên thực tế. Từ các mối đe dọa chính mà các nhà báo, luật sư, các nhân viên NGO và các nhà bảo vệ quyền tại Trung Quốc phải đối mặt, chúng tôi đã thu hẹp được những mối đe dọa chủ yếu làm cơ sở cho hướng dẫn này. Tuy nhiên, phải mất nhiều thời gian để bạn biết về những cách khác nhau mà công nghệ có thể sử dụng để chống lại bạn, đó là lý do tại sao bạn phải đọc kỹ Chương 1: Nhận thức các mối đe dọa của bạn. Điều quan trọng là bạn phải ngồi xuống và phân tích tình huống của mình, để quyết định trọng tâm của bạn là gì. Hiểu được nguyên nhân và hậu quả của các mối đe dọa mà bạn phải đối mặt, chúng đến từ đâu và làm thế nào để làm cho chúng mất đi hoặc ít nhất cũng làm cho chúng trở nên ít nghiêm trọng hơn. Trong Chương 12: Bảo mật phòng ngừa, bạn nên theo hướng dẫn để phác thảo các mối đe dọa và khả năng của bạn.

ĐƠN GIẢN HÓA, ĐƠN GIẢN HÓA, ĐƠN GIẢN HÓA

Ngay cả đối với một chuyên gia biết làm thế nào để sử dụng an toàn nhiều chương trình, sẽ khó khăn hơn là biết làm thế nào để sử dụng an toàn vài chương trình. Mỗi chương trình bạn có đi kèm với nguy cơ mất an toàn thêm. Điều đầu tiên bạn muốn làm là xem tất cả các chương trình bạn có trên máy tính và điện thoại của bạn. Bạn có sử dụng chúng? Nếu không, hãy loại bỏ chúng. Chúng có cần thiết không? Nếu không, hãy loại bỏ chúng. Những ngày này một điện thoại sẽ nhanh chóng lấp đầy với nhiều chương trình trò chuyện khác nhau nhưng bạn nên xóa những chương trình không cần thiết. Điều này có thêm lợi ích là làm cho máy tính hoặc điện thoại của bạn hoạt động nhanh hơn.

TRÁNH CÁC CÔNG TY VÀ CHƯƠNG TRÌNH CỦA TRUNG QUỐC

Không giống như các công ty nước ngoài hay ít nhất là các công ty, dịch vụ và chương trình của phương Tây, mã hóa hiệu quả không phải là tiêu chuẩn trong các ứng dụng của Trung Quốc. Các dữ liệu mà các chương trình Trung Quốc thu thập được từ bạn không được toà án bảo vệ và có thể được sử dụng bởi nhà nước và cảnh sát mỗi khi họ muốn. Tội phạm cũng dễ dàng truy cập dữ liệu do thiếu mã hóa. Các chương trình của Trung Quốc đã được chứng minh là cũng thu thập nhiều thông tin về người dùng chúng so với các chương trình nước ngoài tương đương (QQ có lẽ là tồi tệ nhất trong số đó). Chúng có thể chứa các "cửa sau" cho phép nhà nước truy cập trực tiếp vào điện thoại hoặc máy tính của bạn mà bạn không biết. Ngay cả một chương trình, như WeChat, cũng có thể đe dọa tính bảo mật của toàn bộ điện thoại hoặc máy tính của bạn. Hãy ý thức!

CHÍNH SÁCH HỘP THƯ ĐẾN TRỐNG KHÔNG

Phải thừa nhận rằng, mối đe dọa chủ yếu đối với email của bạn không phải là hacker hiện đại mà là cảnh sát bắt giữ bạn và buộc bạn cung cấp cho chúng mật khẩu của bạn. Nếu điều đó xảy ra, rất có thể là cảnh sát sẽ truy cập vào email của bạn. Cuối cùng thì bạn sẽ cung cấp cho họ mật khẩu hoặc thậm chí bạn không đồng ý, đồng nghiệp hoặc bạn bè có thể cung cấp cho cảnh sát quyền truy cập vào email của họ và với điều này cảnh sát có thể thấy bất kỳ thông tin liên lạc nào bạn đã có với họ. Do đó, tuân thủ Chính sách Hộp thư đến trống không rất có ích và là một trong những công cụ quan trọng nhất cho sự an toàn của bạn.

Giả sử rằng email của bạn sẽ bị truy cập nếu và khi bạn bị bắt. Chính sách Hộp thư đến trống không sẽ đảm bảo rằng không có gì để họ đọc. Tóm lại, làm cho hộp thư đến của bạn (và các thư mục khác) trống. Trong 99% trường hợp, điều này không phải là một vấn đề, vì hầu hết các email không cần lưu trữ lâu dài. Không thể nhấn mạnh đủ mức độ quan trọng này. Tương tự như vậy, đảm bảo rằng đồng nghiệp hoặc bạn bè của bạn cũng làm như vậy. Điều này được thảo luận sâu hơn trong Chương 6: Chia sẻ thông tin.

Chúng tôi cũng sẽ giới thiệu cho bạn một dịch vụ webmail an toàn, có mã hóa và có chức năng tự hủy, giống như chương trình chat Telegram và chương trình SMS Signal, cũng được đề cập sau.

KHÔNG SỬ DỤNG REPLY

Để an toàn thông tin, thay vì bấm vào nút Reply/Trả lời, bạn nên viết email trả lời bằng một email mới. Làm như thế thì cho dù email mới này bị lộ thì người đọc trộm cũng không thể biết hết những nội dung mà các email trước trao đổi. Bằng không, mọi thông tin trao đổi trước đó sẽ bị lộ vì email dựa trên Reply chứa những thông tin ở email trước đó.

Như vậy, khi bạn trả lời email cho đồng nghiệp hoặc bạn bè, hãy tránh sử dụng chức năng Reply, hoặc nếu bạn làm như vậy, hãy xóa văn bản gốc. Điều này đảm bảo rằng sau khi bạn bị bắt, cảnh sát có truy cập email của bạn, và chúng sẽ thu được ít thông tin nếu bạn và đối tác áp dụng chính sách Không sử dụng Reply.

Thông tin thêm về việc tách email công việc và email cá nhân và thói quen email an toàn bổ sung sẽ được đề cập đến trong Chương 6: Chia sẻ thông tin. Nói chuyện với đồng nghiệp hoặc bạn bè mà bạn giao tiếp nhiều nhất về áp dụng chính sách không dùng chức năng Reply.

BẢO ĐẢM NHỮNG ĐIỀU CƠ BẢN

Bạn sẽ không chi tiêu nhiều tiền để lắp một cửa an ninh tiên tiến và khóa và sau đó để lại các cửa sổ mở rộng, phải không? Tương tự như vậy đối với máy tính và điện thoại của bạn. Thật không may, điện thoại và máy tính của bạn đi kèm với một số cài đặt, và hầu hết các cài đặt này không an toàn. Như vậy, trước khi bạn bắt đầu bảo mật thiết bị của mình với các giải pháp kỹ thuật bổ sung và hành vi được cải thiện, bạn cần phải bảo đảm những điều cơ bản này. Điều này có thể là tẻ nhạt và bao gồm các hướng dẫn từng bước về một loạt các vấn đề nhỏ. Tuy nhiên, sẽ giúp bạn bảo vệ thiết bị của mình và an toàn cho chính mình. Những vấn đề khác nhau được đề cập trong Chương 3: Bảo mật máy tính của bạn và Chương 10: Thiết lập Điện thoại của bạn và chúng tôi khuyên bạn nên làm những điều đó sau khi hoàn thành chương này.

CẬP NHẬT, CẬP NHẬT, CẬP NHẬT

Tầm quan trọng của việc cập nhật thường xuyên không thể bị nhấn mạnh quá mức và đó là một trong những nguyên nhân thường xuyên bị bỏ qua nhất về vi phạm an ninh. Đừng phạm sai lầm này. Đảm bảo hệ điều hành (OS) của bạn được đặt để tự động cập nhật. Đảm bảo trình duyệt của bạn được đặt để tự động cập nhật. Tương tự với bất kỳ chương trình nào bạn sử dụng liên quan đến công việc của bạn. Bạn có thể thấy nó gây phiền nhiễu để tạm dừng và chờ đợi các cập nhật không thường xuyên, nhưng nó là chìa khóa để bảo vệ máy tính và điện thoại của bạn. Bạn có muốn chờ đợi vài phút để cập nhật hoặc một vài tháng bị tạm giam không? Các chương trình, hệ điều hành và dịch vụ trở nên an toàn hơn mỗi ngày vì những lỗ hổng bảo mật mới đã được gắn và các mối đe doạ mới được phát hiện và ngăn chặn và chỉ bằng cách cho phép cập nhật tự động thì bạn sẽ được hưởng lợi từ việc này. Các chương trình và ứng dụng lỗi thời cực kỳ dễ bị phần mềm độc hại và các cuộc tấn công khác. Cập nhật thường xuyên cho phép bạn tránh những rủi ro không cần thiết này.

CÁC KẾ HOẠCH KHẨN CẤP

Khi cảnh sát tạm giữ bạn bè hoặc đồng nghiệp của bạn hoặc tịch thu máy tính của họ, mọi việc đã quá muộn. Trên thực tế, nếu bạn đợi cho đến lúc đó để bắt đầu nói chuyện với đồng nghiệp về cách loại bỏ những tài liệu nhạy cảm, bạn có thể bị cáo buộc hủy bỏ bằng chứng. Bạn phải chuẩn bị trước cho những tình huống này, và bạn phải biết bạn phải làm gì trước, khi nào, và sau khi điều đó xảy ra. Ngoài ra, bạn phải biết những gì bạn đồng nghiệp và bạn bè của bạn sẽ làm. Bạn cần một kế hoạch. Cách duy nhất để đạt được điều này là nói về điều đó trước và thỏa thuận về cách bạn và người khác phải hành động như thế nào nếu có ai bị bắt, hoặc máy tính hoặc điện thoại của ai đó bị tịch thu. Các bạn có cài đặt lại điện thoại của mình? Bạn có kiểm tra lại để đảm bảo hộp thư đến của bạn trống không? Bạn có thay đổi tất cả mật khẩu, hoặc có thể bạn cài lại máy tính của bạn? Bất cứ điều gì bạn quyết định, điều quan trọng là bạn và bạn bè của bạn làm cùng một điều và bạn đều biết những gì người khác sẽ làm.

Điều này được gọi là tuân theo 'một giao thức bảo mật' Nếu bạn tự thực hiện một số thứ để giữ an toàn nhưng một đồng nghiệp không làm thì các nỗ lực của bạn có thể trở nên vô nghĩa và khiến nhiều người gặp nguy hiểm. Hãy ngồi xuống với các đồng nghiệp của bạn và nói về điều này. Hãy nhớ rằng, nếu mạng lưới của bạn bao gồm nhiều nhóm đồng nghiệp hoặc những người bảo vệ nhân quyền làm việc trong nhiều vấn đề khác nhau và họ không biết nhau hoặc một số có liên quan đến các hoạt động nhạy cảm hơn những người khác, bạn luôn có thể tạo các kế hoạch khẩn cấp khác nhau với các nhóm khác nhau, và điều này nên thực hiện. Lập kế hoạch khẩn cấp và có một 'giao thức bảo mật' mà mọi người đều biết và sẽ tuân theo là cần thiết, và không phải là một điều xa xỉ. Điều này và các vấn đề liên quan sẽ được thảo luận trong Chương 12: Bảo mật phòng ngừa.

Trước khi tiếp tục chương tiếp theo, hãy đảm bảo bạn đã thực hiện các hướng dẫn trong Chương 2: Chuẩn bị máy tính của bạn. Bảo đảm các điều cơ bản trước khi tiếp tục là cần thiết để tận dụng tối đa các bước nâng cao kỹ thuật và hành vi bảo mật tiên tiến sẽ tiếp theo.

NHỮNG ĐIỂM QUAN TRỌNG

- Chính sách hộp thư trống không là gì và tại sao lại quan trọng?
- Tầm quan trọng của thoả thuận "không dùng chức năng Reply/Trả lời"?
- Các nguy cơ nếu không thường xuyên cập nhật phần mềm bảo mật là gì?
- Kế hoạch khẩn cấp là gì?
- Bạn sẽ làm những bước nào để xây dựng một kế hoạch khẩn cấp?
- Tại sao bạn cần phải đơn giản hoá và hạn chế số lượng chương trình mà bạn sử dụng?

CHƯƠNG 4
LẤY THÔNG TIN

Chương này sẽ hướng dẫn bạn cách lấy thông tin một cách an toàn. Phần này sẽ thảo luận cả phương pháp mà bạn tìm kiếm và nhận thông tin, trình duyệt sử dụng, và cả kết nối Internet mà bạn sử dụng khi mở trình duyệt. Để bảo mật, bạn cần phải xem xét cả trình duyệt cũng như kết nối mà nó sử dụng để lấy thông tin. Việc đảm bảo an ninh cho kết nối cũng sẽ cho phép bạn vượt qua những hạn chế do kiểm duyệt.

Các chương sau thuộc Phần III trên thiết bị di động sẽ thảo luận về việc sử dụng các ứng dụng và thiết bị di động nói chung.

Đôi mắt và tai của bạn với Internet có thể là trình duyệt của bạn. Hầu hết bạn sử dụng trình duyệt cho mục đích gửi email. Với quá nhiều công việc của bạn liên quan đến trình duyệt của bạn, điều quan trọng là phải sử dụng trình duyệt an toàn.

Khi bạn sử dụng một trình duyệt, có hai điều xảy ra. Các trang web bạn truy cập sẽ thu thập thông tin về bạn nhưng đồng thời máy tính của bạn cũng sẽ thu thập thông tin về những gì bạn làm với trình duyệt của bạn. Nó thực hiện việc này bằng cách thu thập "cookie", "LSO", mật khẩu bạn nhập, lịch sử sử dụng web của bạn và hơn thế nữa. Trên hết, để hoạt động tốt, hầu hết các trang web đều sử dụng các tập lệnh (lập trình JavaScript) và qua đó, trình duyệt và máy tính của bạn dễ bị lỗi web, vi rút lan truyền đến máy tính của bạn thông qua trình duyệt của bạn. Cả hai vấn đề này cần được giải quyết.

CHIẾN LƯỢC TRÌNH DUYỆT KÉP

Chúng tôi khuyên bạn nên sử dụng một trình duyệt có thể tự động xóa mọi thứ mỗi khi bạn đóng nó. Tuy nhiên, xét việc chúng ta sử dụng trình duyệt thường xuyên cho công việc cá nhân, chúng tôi cũng nhận ra rằng nếu bạn phải đăng nhập vào từng dịch vụ mỗi lần, nó sẽ không hiệu quả và bạn sẽ không sử dụng nó. Như vậy, chúng tôi khuyên bạn nên sử dụng một chiến lược trình duyệt kép. Chọn một trình duyệt để duyệt Internet cá nhân và một cho tất cả các công việc khác. Đối với công việc bạn nên luôn luôn sử dụng Firefox. Nó không phải là trình duyệt nhanh nhất

nhưng cho phép tinh chỉnh đáng kể, với phần mở rộng bảo mật quan trọng/tiện ích.

Để sử dụng việc cá nhân, chúng tôi khuyên bạn nên sử dụng trình duyệt nhanh như Chrome hoặc Opera. Sử dụng trình duyệt đôi sẽ có nghĩa là sử dụng cá nhân của bạn có thể tiếp tục như trước mà không bị chậm lại bởi tiện ích hoặc tiện ích mở rộng nhưng hành vi Internet liên quan đến công việc của bạn sẽ an toàn hơn đáng kể.

Một khi đã quyết định, hãy gắn bó với nó. Sử dụng Firefox cho tất cả các trình duyệt liên quan đến công việc, từ nghiên cứu, gửi email và bất cứ thứ gì khác, và trình duyệt khác của bạn cho tất cả các công việc cá nhân. Không cài đặt nhiều hơn hai trình duyệt, hãy chọn hai trình duyệt của bạn và giữ chúng. Chèn trên Firefox và các phần mở rộng bên dưới sẽ cho bạn thấy các chi tiết về cách sử dụng Firefox một cách an toàn.

LƯU CÁC TỆP Ở ĐÚNG NƠI

Việc chèn vào Firefox sau này sẽ cho bạn thấy làm thế nào để làm điều này. Bạn cần phải hiểu tại sao. Thư mục tải xuống / lưu mặc định của trình duyệt của bạn là một nguy cơ mất an toàn về bảo mật lớn mà ít người chú ý đến.

Nếu không có thay đổi nào được thực hiện, bất kỳ tệp đính kèm hoặc tài liệu bạn tải xuống thông qua trình duyệt của bạn sẽ được lưu trữ trên ổ cứng Hệ điều hành (OS). Tại sao điều này là một vấn đề? Như Chương 5: Lưu trữ thông tin, và Chương 7: Xóa thông tin, sẽ cho thấy việc xóa thông tin thực sự là khó khăn. Các chi tiết về điều này sẽ được đề cập sau. Bây giờ, điều quan trọng là bạn sử dụng trình duyệt và tải xuống theo cách mà bạn kiểm soát được việc lưu trữ các tệp mới.

Cách tốt nhất để quản lý việc này là tạo một thư mục trong ổ cứng đã mã hóa của bạn (chúng ta sẽ thiết lập trong Chương 5: Lưu trữ thông tin). Tuy nhiên, nếu bạn thiết lập đường dẫn tải xuống ổ cứng đã được mã hóa và sau đó cố gắng tải xuống một cái gì đó mà không cần giải mã cho ổ cứng đã mã hóa của bạn thì nó sẽ được lưu vào vùng mặc định mà không nói cho bạn biết. Như vậy, trong chèn bên dưới, chúng tôi sẽ cho bạn thấy làm thế nào để chọn Always ask me where to save files. Điều này có nghĩa là mỗi khi bạn tải xuống bất cứ điều gì, nó sẽ hỏi bạn nơi để lưu nó. Hãy chắc chắn rằng luôn luôn lưu trong cả a) cùng một nơi, và b) ổ đĩa cứng được mã hóa của bạn.

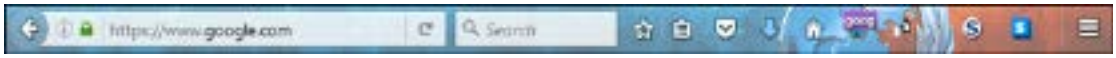
Đừng lưu tài liệu vào màn hình máy tính của bạn!

KẾT NỐI INTERNET

HTTP VS HTTPS

Ngày nay, hầu hết các dịch vụ yêu cầu mã hoá đăng nhập vào kết nối Internet giữa bạn và dịch vụ đó, như Facebook, Gmail, ngân hàng ... Có một cách rất dễ dàng để biết kết nối của bạn với một trang web được mã hóa hay không. Tất cả bạn phải làm là nhìn vào trường địa chỉ trong trình duyệt của bạn (S-W / O7).

Các kết nối không được mã hóa nói rằng HTTP (http: // www ...) ở đầu URL. Kết nối được mã hóa nói HTTPS (https: // www ...). Truy cập Gmail, Twitter hoặc Facebook và kiểm tra và xem. Bằng cách sử dụng trình HTTPS Everywhere trong Firefox, trình duyệt sẽ tự động sử dụng https nếu có thể với một dịch vụ.



INTERNET: BỘ ĐỊNH TUYẾN/ROUTER CỦA BẠN

An toàn khi nói rằng truy cập Internet của bạn là thông qua kết nối không dây, dù ở nhà, tại văn phòng của bạn, hoặc làm việc trong quán cà phê. Do đó, bạn cần phải có một số hiểu biết cơ bản về cách hoạt động của một bộ định tuyến không dây.

Để truy cập router của bạn, bạn sẽ cần một tên người dùng và mật khẩu. Đây thường là ghi trên một lưu ý ở mặt sau hoặc dưới cùng của router. Đây là những điều tương tự đối với hầu hết các bộ định tuyến, thường là "admin" và "password". Ngay cả khi khác nhau, mỗi router của thương hiệu hoặc mô hình đó sẽ có cùng một tên người dùng và mật khẩu, vì vậy rất dễ dàng tìm ra. Với thông tin này, mọi người bên ngoài, như một kẻ phạm tội hoặc cảnh sát hoặc những người khác, có thể vào router của bạn. Nếu họ có thể vào router, điều khiển internet của bạn, họ có thể dễ dàng cài đặt các chương trình để đăng nhập tất cả những gì bạn làm, hoặc thậm chí chặn Internet của bạn. Phần lớn mọi người không bao giờ vào router của họ để thay đổi tên người dùng và mật khẩu. Hầu hết các truy cập router là bằng cách mở một trình duyệt và viết trong địa chỉ IP của router, thường là 192.168.0.1. Địa chỉ cũng sẽ được in trên router. Sử dụng này, bạn có thể nhập router của bạn và thay đổi tên người dùng và mật khẩu.

Một vấn đề quan trọng cần xem xét là khi sử dụng linternet không dây, tín hiệu không dây cần phải được mã hóa, hoặc mọi thứ khác đều có thể được đọc bởi bất cứ ai ở gần đó. Nếu không được mã hóa, bất cứ ai cũng có thể kết nối và sử dụng tín hiệu không dây của bạn, và cũng có thể đăng nhập tất cả mọi thứ được thực hiện trên kết nối đó. Tín hiệu không dây của bạn sẽ có một tên, đó là tên bạn thường kết nối (gọi là SSID). Bạn biết mã hóa được sử dụng trên một kết nối không dây nếu nó yêu cầu một mật khẩu để kết nối. Không có mật khẩu có nghĩa là không mã hóa.

Khi bạn đã vào bộ định tuyến của mình, bạn có thể thay đổi tên mạng (SSID) và cũng có thể chọn để mã hóa tín hiệu. Mã hóa chuẩn được sử dụng trên router Wi-Fi hiện nay được gọi là WPA2. Các ứng dụng cũ được gọi là WEP. Dừng sử dụng những thứ đó. Để kích hoạt tính năng

mã hóa, bạn phải quyết định mật khẩu.

Do đó, có một tên người dùng và mật khẩu để vào router. Sau đó, có một tên và mật khẩu cho tín hiệu không dây thực tế mà bạn sử dụng. Hai việc không phải là giống nhau. Nếu bạn cần hướng dẫn để tìm ra cách để thực hiện những thay đổi này trong bộ định tuyến của bạn, bạn chỉ tìm tên router ở Google và số seria sản xuất, và sẽ có rất nhiều trợ giúp. Mặc dù giao diện cho bộ định tuyến của bạn có thể phức tạp, bạn chỉ cần thay đổi một vài điều và nó sẽ dễ dàng hơn nhiều so với giao diện đầu tiên.

INTERNET: ISP, ĐỊA CHỈ IP VÀ MAC

Tại Việt Nam, rất có thể bạn đang sử dụng kết nối Internet do một trong số ít nhà cung cấp dịch vụ Internet (ISP) cung cấp, hoặc nếu trên điện thoại của bạn, một trong những công ty điện thoại. Điều này đặt ra một nguy cơ lớn, bởi vì nhiều bước bạn thực hiện để bảo mật có thể bị vô hiệu hóa, bởi vì những người cung cấp sử dụng Internet cho bạn, cũng sẽ tự động đăng nhập tất cả mọi thứ được thực hiện với kết nối đó. Các nhà cung cấp khác nhau giữ thông tin như vậy với số lần khác nhau, nhưng tất cả đều ghi lại ít nhất việc truy cập Internet tạm thời của bạn.

Khi bạn kết nối Internet, router của bạn (hộp trong nhà hoặc văn phòng xử lý lưu lượng internet) sẽ liên lạc và sử dụng nhà cung cấp dịch vụ internet (ISP) để kết nối bạn với internet rộng hơn. Về cơ bản, bộ định tuyến ở nhà của bạn kết nối với internet đầu tiên thông qua các máy chủ của ISP, và từ đó ra trên internet rộng hơn. Đó là thông qua ISP của bạn mà kiểm duyệt được áp dụng, vì họ sẽ chặn các trang web và nội dung web.

Việc theo dõi bạn, cho dù bởi ISP xử lý kết nối của bạn, hoặc các trang web bạn truy cập hoặc dịch vụ mà máy tính hoặc điện thoại của bạn kết nối, được thực hiện thông qua địa chỉ IP và địa chỉ MAC của bạn.

Địa chỉ IP của bạn là địa chỉ kết nối internet của bạn và có thể dễ dàng nhận diện và do đó được theo dõi lại bạn. Nếu bạn kết nối thông qua kết nối không dây, IP của bạn sẽ thay đổi (năng động) nhưng ISP của bạn sẽ luôn biết địa chỉ IP nào được gán cho kết nối internet vào thời điểm nào. Lưu ý: Tính năng này chỉ có sẵn trên một số phiên bản của WIN10.

Thiết bị hoặc máy tính của bạn cũng sẽ có một địa chỉ MAC. Mỗi thiết bị có kết nối sẽ có một địa chỉ MAC, và địa chỉ MAC duy nhất này được đặt cho phần cứng vật lý của chính nó. Địa chỉ MAC được đặt khi phần cứng được sản xuất, và MAC trông như sau: 00: 0a: 95: 9d: 68: 16. Khi bạn kết nối với Internet, địa chỉ MAC không được chia sẻ, vì vậy bạn không cần phải tốn quá nhiều thời gian để nghĩ về nó, tuy nhiên địa chỉ IP của bạn có thể gây ra vấn đề cho bạn.

Trong Win10 có một tùy chọn cài đặt để cho phép các địa chỉ phần cứng ngẫu nhiên (MAC), và nếu bạn có tùy chọn, hãy bật nó lên (S-WXX). Nếu bạn nhận thấy bất kỳ vấn đề nào với kết nối của bạn sau khi bật nó, khởi động lại máy tính của bạn. Nếu vấn đề vẫn còn, hãy tắt nó.

May mắn thay, có một số cách đơn giản để tránh ISP của bạn theo dõi hoạt động của bạn, hoặc có trang web theo dõi địa chỉ IP thật của bạn. Các giải pháp này được gọi là VPN và TOR, và

việc chèn trên VPN và TOR được cung cấp thêm dưới đây. Nói tóm lại, VPN hoặc TOR sẽ bỏ qua ISP, kết nối trực tiếp với các máy chủ bên ngoài của Việt Nam và trong nhiều trường hợp sẽ mã hóa lưu lượng truy cập của bạn, nghĩa là ISP của bạn không thể theo dõi việc sử dụng Internet của bạn. Sử dụng VPN hoặc TOR là điều cần thiết cho bảo mật và sự riêng tư của bạn.

VPN VÀ TOR

Sử dụng VPN (Virtual Private Network- Mạng riêng ảo) không chỉ bảo đảm rằng thông tin của bạn không bị ISP truy cập dễ dàng bởi vì nó mã hóa lưu lượng truy cập / kết nối, đồng thời ngăn cản việc kiểm duyệt ISP. Nó cũng làm cho khó hơn cho các trang web bạn truy cập muốn ghi lại địa chỉ IP thật của bạn. Nói chung, bạn nên luôn sử dụng VPN trên máy tính của mình và đặt nó để bắt đầu tự động khi bạn khởi động máy tính. Không có lý do gì để sử dụng Internet mà không cần bật VPN.

Một số VPN đi cùng kill switch, có nghĩa là nó tự động cắt đứt mạng Internet nếu VPN ngừng hoạt động (để ngăn IP thực của bạn hiển thị trên trang web hoặc dịch vụ bạn đang sử dụng khi kết nối VPN bị rớt). Đó là khuyến cáo sử dụng này. Ngày nay, nhiều VPN rất mạnh, và bạn sẽ không nhận thấy bất kỳ sự khác biệt về tốc độ. Có thể tốn một ít tiền để có được một khoản tiền lớn, nhưng đó là một trong những khoản đầu tư quan trọng nhất mà bạn có thể thực hiện.

Một VPN kết nối máy tính / router của bạn trực tiếp đến một máy chủ bên ngoài của Việt Nam (và bạn có thể chọn cái nào), bỏ qua ISP bằng cách tạo ra cái gọi là 'đường hầm'. Các trang web bạn truy cập sẽ thấy địa chỉ IP của máy chủ bạn đã kết nối (máy chủ VPN), chứ không phải địa chỉ IP của máy tính của bạn. Tương tự như vậy, ISP của bạn sẽ không theo dõi được sự truy cập Internet của bạn và do đó không thể ghi lại những gì bạn làm hoặc chặn các trang web mà bạn muốn truy cập. Một VPN cơ bản bỏ qua các ISP. Điều này có nghĩa là mặc dù bạn đang có mặt tại Việt Nam, nó có thể làm cho máy trông giống máy tính của bạn ở Hoa Kỳ hoặc Úc hoặc một nước thứ ba khác, nơi kiểm duyệt và những hạn chế trên web sẽ không áp dụng cho các hoạt động trực tuyến của bạn.

Astrill.com là nhà cung cấp VPN mạnh với các tính năng bảo mật bổ sung và các máy chủ trên toàn thế giới. VyprVPN và ExpressVPN là những lựa chọn phổ biến khác. Tìm kiếm trực tuyến cũng sẽ cho bạn thấy sự so sánh của các VPNs tốt nhất hiện có. Để có danh sách cập nhật về các VPN hoạt động tốt, chỉ cần Google và bạn sẽ tìm thấy nhiều thông tin và so sánh có liên quan.

Sử dụng VPN là sự bảo vệ mạnh mẽ địa chỉ IP của bạn, nhưng nó không hoàn toàn an toàn và với các nguồn lực thì có những thế lực có thể theo dõi bạn. Đối với các hoạt động thật sự nhạy cảm trực tuyến, bạn cần sử dụng TOR.

TOR được gọi là Onion Router (Onion- củ hành). Không giống như VPN, khi sử dụng TOR, dịch vụ miễn phí, nó sẽ kết nối bạn qua một đường dây dài các máy chủ khác nhau trên toàn thế giới trước khi đến trang web bạn đang tìm kiếm. Đó là phương tiện liên lạc an toàn nhất hiện có. Nó rất đáng tin cậy, nhưng cũng rất chậm. Hãy quên đi việc xem video trực tuyến trên TOR. Nếu bạn cần phải làm gì đó nhạy cảm, bạn nghĩ rằng có thể được sử dụng chống lại bạn nếu anh ninh thấy, hãy sử dụng TOR. Dễ dàng cài đặt trên cả máy tính và điện thoại.

Nó được gọi là bộ định tuyến củ hành vì thay vì sử dụng một máy chủ, giống như một VPN, nó nhảy qua nhiều máy chủ khác nhau, lên đến 20, như lột bỏ lớp hành tây trước khi kết nối với nội dung bạn đang truy cập. Bởi vì nó sử dụng nhiều máy chủ, nên gần như không thể tìm thấy IP của bạn.

DUCKDUCKGO.COM VÀ LƯỚT WEB AN TOÀN

DuckDuckGo là một công cụ tìm kiếm, giống như Google. Không giống các công cụ tìm kiếm khác, DuckDuckGo không tùy chỉnh kết quả tìm kiếm dựa trên vị trí của bạn, lịch sử trước và không lưu dữ liệu về những người sử dụng nó. Đó là một cách an toàn hơn để lướt web, nơi không có dữ liệu được thu thập theo thời gian. Điều đó có nghĩa là không có quảng cáo và không có quảng cáo tùy chỉnh dựa trên các tìm kiếm trước, vị trí và nhiều thứ khác. DuckDuckGo sử dụng giao diện tiếng Anh nhưng rất cơ bản, vì vậy ngôn ngữ sẽ không phải là vấn đề.

Nếu bạn sử dụng trình duyệt TOR / TOR và DuckDuckGo, nó có nghĩa là không có chút dấu vết nào của việc lướt web của bạn tồn tại, không phải với bạn ISP cũng như tại trang web mà bạn đang truy cập. Nếu cần thiết để tìm kiếm thông tin mà có thể, nếu được giám sát và lưu trữ, gây ra vấn đề cho bạn, hãy xem xét sử dụng DuckDuckGo trong khi truy cập với trình duyệt TOR. Để bảo mật tối đa, sử dụng trình duyệt TOR từ thanh USB, để hạn chế các dấu vết lưu trữ trên máy tính của bạn.

Khi nói đến lướt web, mức độ bảo mật có thể được tóm tắt như sau:

TOR cung cấp bảo mật tốt nhất, cao hơn trong khi sử dụng VPN, nhưng việc sử dụng VPN vẫn an toàn hơn nhiều so với kết nối 'bình thường'. Về việc chọn trình duyệt, sử dụng trình duyệt TOR trên USB là sự lựa chọn an toàn nhất của bạn. Sử dụng Firefox chính xác cấu hình vẫn còn an toàn hơn và tốt hơn so với việc sử dụng một thiết lập trình duyệt 'bình thường'.

NHỮNG ĐIỂM QUAN TRỌNG

- Bạn đã thiết lập một hệ thống trình duyệt kép và đã thực hiện những thay đổi cần thiết cho Firefox (hoặc trình duyệt công việc được chỉ định khác)?
- Bạn có hiểu các VPNs và TOR hoạt động như thế nào, và tại sao nó có thể giúp bạn, không chỉ vượt qua kiểm duyệt?
- Đảm bảo việc sử dụng VPN của bạn càng nhiều càng tốt, tốt nhất là luôn sử dụng nó, và tìm hiểu cách sử dụng TOR và trình duyệt TOR cho các hoạt động nhạy cảm nhất của bạn trên mạng.

CHÍNH SÁCH HỘP THƯ TRỐNG SẼ BẢO VỆ BẠN KHỎI TÙ ĐÀY

Một luật sư ở một quốc gia độc tài đã bắt đầu biện hộ trong những năm cuối của năm 2000, không chỉ bảo vệ những người hoạt độngchính trị mà còn hỗ trợ nhiều người trong số họ. Cùng với sự nổi tiếng của mình, ông và gia đình ngày càng đối mặt với gia tăng sách nhiễu, quấy rối và đe doạ từ phía chính quyền.

Để tránh nguy hiểm, ông nhận bào chữa ít hơn nhưng tham gia vào nhiều tổ chức NGO để cung cấp đào tạo và nhiều hình thức trợ giúp khác cho người hoạt động, đặc biệt là những luật sư trẻ hơn. Đồng thời ông cũng bỏ nhiều thời gian hơn để học về an ninh mạng để đảm bảo rằng những thong tin về hoạt động của mình không rơi vào tay kẻ xấu.

Khi chính phủ mởi rộng tấn công nhằm giới luật sư và những người lien quan, ông lo ngại rằng ông có thể là mục tiêu cho dù đã tham gia biện hộ ít hơn.

Thực tế, ông đã trở thành mục tiêu của an ninh và cảnh sát muốn thu thập thông tin về nhóm Luật sư Nhân quyền mà ông có tham gia. Nhóm này, trên thực tế, chỉ đơn giản là một nhóm trực tuyến của luật sư chi chia sẻ thng tin nhưng dưới con mắt của chính phủ thì nó là một tổ chức đối lập cần phải bị đàn áp.

An ninh không chỉ theo dõi ông mà còn theo dõi trợ lý của ông cùng hai luật sư khác cũng trong nhóm đào tạo. Ông nhầm lẫn khi nghĩ rằng cảnh sát chỉ quan tâm đến nhóm này, trong khi an ninh cũng nhắm đến những hoạt động của ông tại một tổ chức NGO chuyên cung cấp đào tạo và trợ giúp pháp lý cho giới hoạt động.

Ông lo ngại rằng những tài liệu về tập huấn có thể bị sử dụng để chống lại mình.

Cuối cùng ông bị bắt giam trong 17 ngày và bị đe doạ phải bị quản chế nửa năm.

Ông cho biết hai điều đã cứu ông rất nhiều trong quá trình giam giữ và thẩm vấn ông. Ông đã thực hiện chính sách hòm thư trống và liên lạc công việc qua những phương tiện bảo mật và thường xuyên xoá mọi nội dung sau khi chat.

Cảnh sát giam giữ ông chỉ vì họ khai thác được từ hòm thư của người trợ lý, người đã khai ra ngay mật khẩu khi bị cảnh sát đe doạ. Người trợ lý này không thực hiện chính sách hòm thư trống và cảnh sát biết rằng họ đã tham gia đào tạo và hỗ trợ người hoạt động nhân quyền.

Sai lầm của luật sư này là ông sử dụng ứng dụng email Tutanota trên điện thoại và cảnh sát biết ông có sử dụng dịch vụ này, do không lấy được mật khẩu của ông nên cảnh sách đã đe doạ người trợ lý.

Có vẻ như hai đối tác không thường xuyên của ông đã không nghiêm túc trong việc bảo mật các chương trình trò chuyện và email và do đó cảnh sát đã nắm được phần nào hoạt động của họ.

GIẢI PHÁP KỸ THUẬT: FIREFOX VÀ MỞ RỘNG

Firefox, như nhiều trình duyệt khác, thường xuyên thay đổi giao diện và kiểu trình bày. Nếu bạn thấy màn hình khác so với trình bày trong phần này thì hãy tìm trong phần cài đặt để lấy phiên bản thích ứng vì nội dung hướng dẫn vẫn như thế.

Khi Firefox cập nhập, sẽ cần một thời gian để cập nhật phần mở rộng. Nếu các mở rộng liệt kê ở đây không được tìm thấy, hãy chờ thêm một chút và chúng sẽ xuất hiện sớm.

Nếu bạn không có Firefox, hãy tải xuống và cài đặt nó từ Firefox.com. Sau khi cài đặt, trên ổ cứng hoặc nếu bạn thích trực tiếp với USB, bước tiếp theo của bạn là tải xuống và cài đặt một số tiện ích hoặc tiện ích bổ sung.

TIỆN ÍCH BỔ SUNG

Bạn sẽ tìm thấy khu vực tiện ích bằng cách nhấp vào nút Settings trên Firefox (S-W / O1) và chọn Add-ons. Từ đây, bạn có thể tìm kiếm các tiện ích để thêm và tìm một tab liệt kê tất cả các tiện ích đã cài đặt của bạn (tab này được gọi là Extensions). Từ đó bạn cũng có thể tìm thấy Options cho mỗi tiện ích.

Tìm và cài đặt những tiện ích sau:

- RefControl,
- NoScript,
- BetterPrivacy,
- HTTPS Everywhere, and
- Keyscrambler.

Refcontrol. Khi bạn truy cập một trang web, trang web sẽ thấy bạn đến từ đâu. Tức là, nếu bạn đang ở trên google, và sau đó vào Facebook, Facebook sẽ được thông báo rằng bạn đã đến trang của họ từ Google. Đây là một tham khảo, và được sử dụng để phân tích cách mọi người kết thúc trên các trang web. Cài đặt RefControl cho phép bạn dừng việc này bằng một vài cú nhấp chuột đơn giản. Sau khi cài đặt, hãy nhấp vào Option và chọn Forge hoặc Block ở cuối của cửa sổ có nói Default for sites not listed.

NoScript. Chương trình này sẽ tự động ngăn chặn việc chạy Javascript từ trình duyệt của bạn. Điều này rất quan trọng bởi vì nhiều loại virut được truyền qua vô số các tập lệnh bị nhiễm bệnh. Nó vô hiệu hóa đồ hoạ di động, tự động phát lại video và hơn thế nữa. Nó đặt một biểu tượng trong trình duyệt của bạn, và nếu bạn muốn cho phép một trang web mà bạn tin cậy để chạy

các tập lệnh và thường thì bạn cần cho phép nó có đầy đủ chức năng, bạn chỉ cần nhấp vào biểu tượng và cho phép. Nếu bạn đang ở trên trang web không tải hoặc hoạt động không bình thường, đó là vì một số tập lệnh bị chặn và trong trường hợp đó bạn cần phải cho phép. Không cần thay đổi thêm nữa cho NoScript.

BetterPrivacy. Bằng cách cài đặt tiện ích này, bạn sẽ có nhiều tuỳ chọn xóa dữ liệu tự động từ trình duyệt của bạn khi bạn đóng nó. Chỉ bằng cách cài đặt tiện ích này, bạn sẽ có tùy chọn để xóa LSO một cách đúng đắn, một loại mới để loại bỏ cookie. Sau khi cài đặt kích vào Options, sau đó chọn tab Options & Help. Chọn Delete Flash cookies on Firefox exit. Cũng chọn Also delete Flashplayer default cookie và On cookie deletion also delete empty cookie folders.

HTTPS Everywhere. Một số trang web mã hóa thông tin liên lạc giữa máy tính của bạn và trang web, chẳng hạn như ngân hàng, một số nhà cung cấp dịch vụ email, một số phương tiện truyền thông xã hội và những thứ khác. Nó thêm một lớp bảo mật. Mặc dù nhiều trang web đang cung cấp HTTPS, nó không phải là phổ quát và một số cho phép nó không làm điều đó một cách tự động. Tiện ích này tự động bật mã hóa HTTPS trên các trang web bạn truy cập. Sau khi tải về, bạn sẽ thấy biểu tượng trong thanh công cụ Firefox. Nhấp vào Enable HTTPS Everywhere và nó sẽ hoạt động tự động.

Không giống như các add-on ở trên, KeyScrambler mà ta nói dưới đây không thể được cài đặt thông qua các khu vực add-on. Thay vào đó, hãy vào download.com và tìm KeyScrambler. Chọn để tải xuống và cài đặt nó như một chương trình bình thường. Máy tính sẽ cần được khởi động lại trước khi chương trình bắt đầu hoạt động.

KeyScrambler là một chương trình nhỏ mã hóa các phím bấm của bạn khi nhập tên người dùng và mật khẩu trong trình duyệt của bạn. Một hacker có thể đặt một chương trình keylogger trên máy tính của bạn. Keylogger này ghi lại tất cả các tổ hợp phím của bạn, và kẻ tấn công có thể truy cập vào mọi thứ bạn nhập, bao gồm tên người dùng và mật khẩu. Bằng cách tự động mã hóa các phím bấm đăng nhập và mật khẩu, chương trình nhỏ này sẽ bảo vệ bạn khỏi cuộc tấn công này.

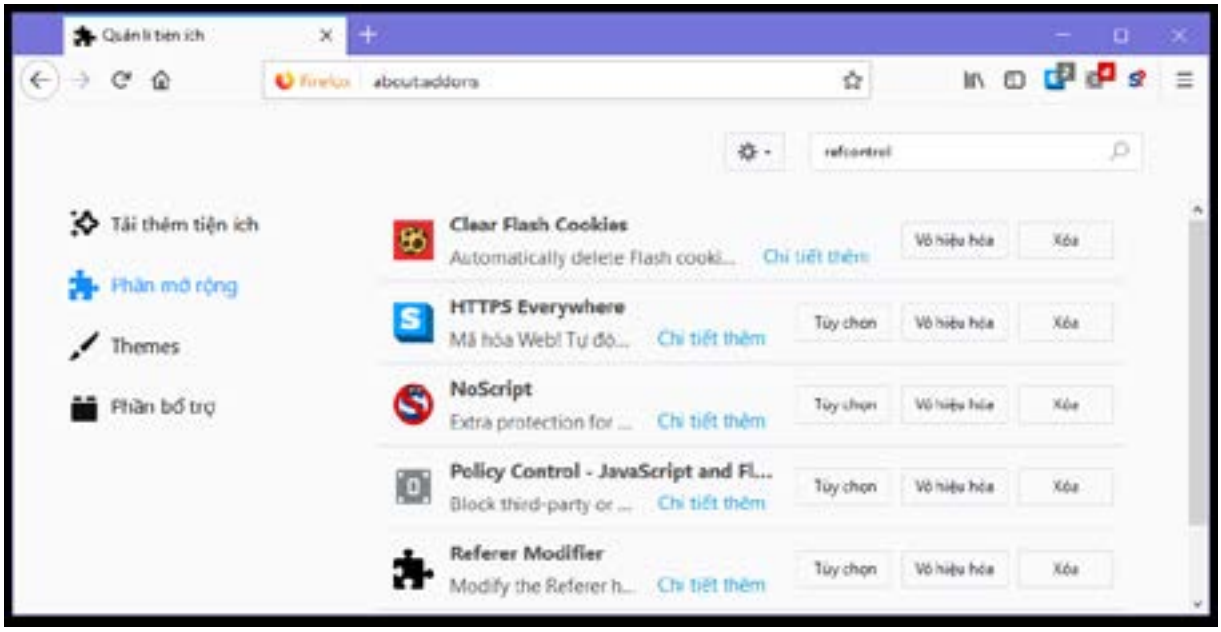
Sau khi cài đặt (S-W / O2), vui lòng dành chút thời gian vào cửa hàng tiện ích mở rộng của Firefox và tìm hiểu để hiểu rõ hơn về những gì hiện có và những tiện ích bổ sung nào tồn tại. Bạn có thể tìm thấy các tiện ích bổ sung hữu ích khác phù hợp với tính bảo mật hoặc hiệu suất và năng suất. Bạn cũng có thể có Best Security Add-ons for Firefox của Google cho Firefox hoặc tương tự, để xem liệu có tiện ích bổ sung khác cho bạn hay không.

Bây giờ, bạn đã đi được một nửa quãng đường bảo mật cho trình duyệt an toàn. Tiếp theo chúng ta cần phải thực hiện một số thay đổi nhanh chóng để cài đặt.

CÁC CÀI ĐẶT VÀ TÙY CHỌN

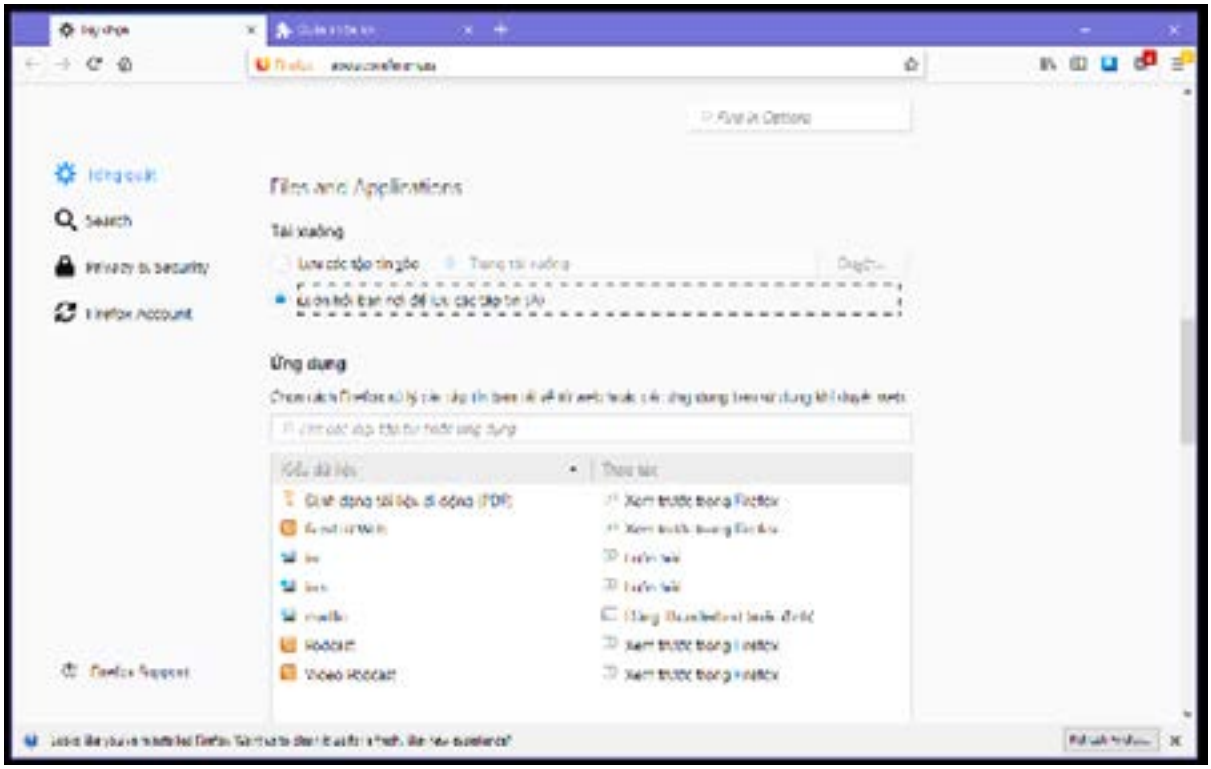
Lưu ý: Với các phiên bản cập nhật của Firefox, bố cục cho các cài đặt đôi khi sẽ thay đổi. Biết được điều gì cần tìm kiếm có nghĩa là sẽ vẫn dễ dàng tìm và điều chỉnh các cài đặt có liên quan, ngay cả khi bố cục có thể đã thay đổi.

Sau khi cài đặt Firefox và các add-on, đã đến lúc duyệt các cài đặt cho trình duyệt, để chắc chắn rằng nó đã được cấu hình một cách an toàn. Kích vào nút settings và sau đó Options (S-W / O1 ở trên). Đối với OSX, bạn cần mở Preferences (dưới biểu tượng Firefox ở đầu cửa sổ). Bên trong vùng Options, có một số tab. Trong mỗi tab được đề cập ở đây, một số thay đổi cần được thực hiện.



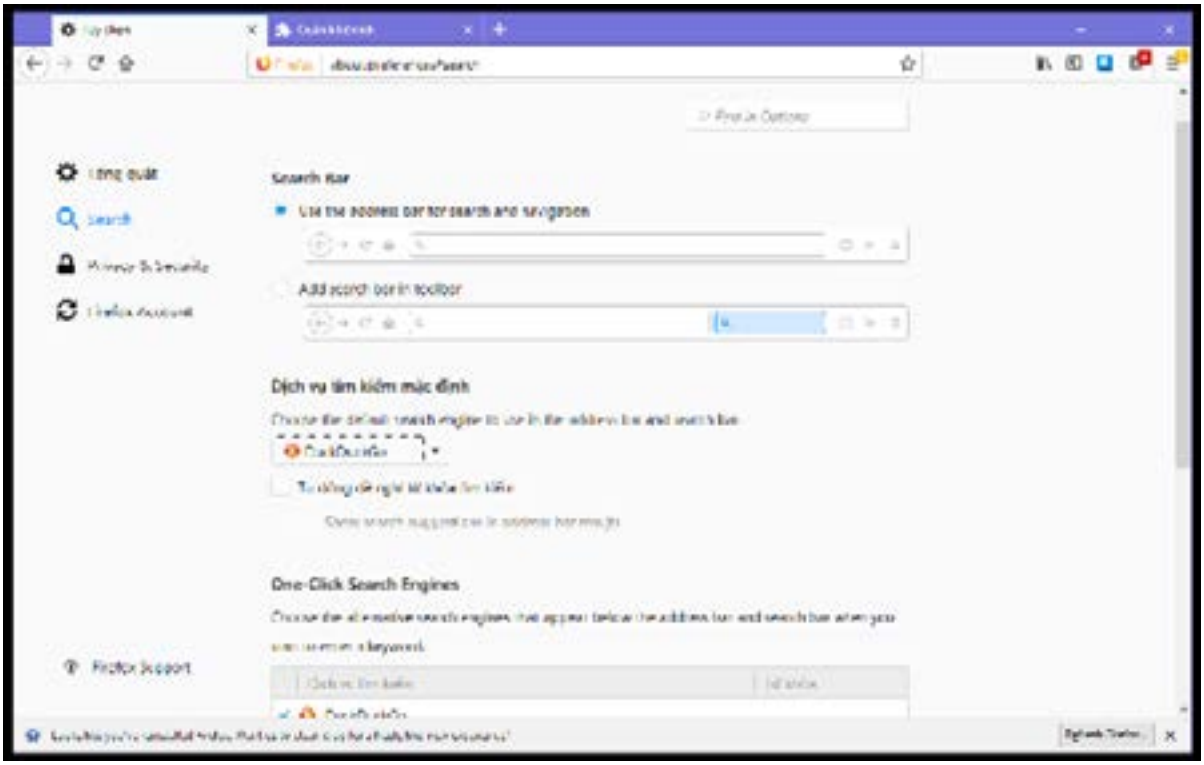
MỞ RỘNG

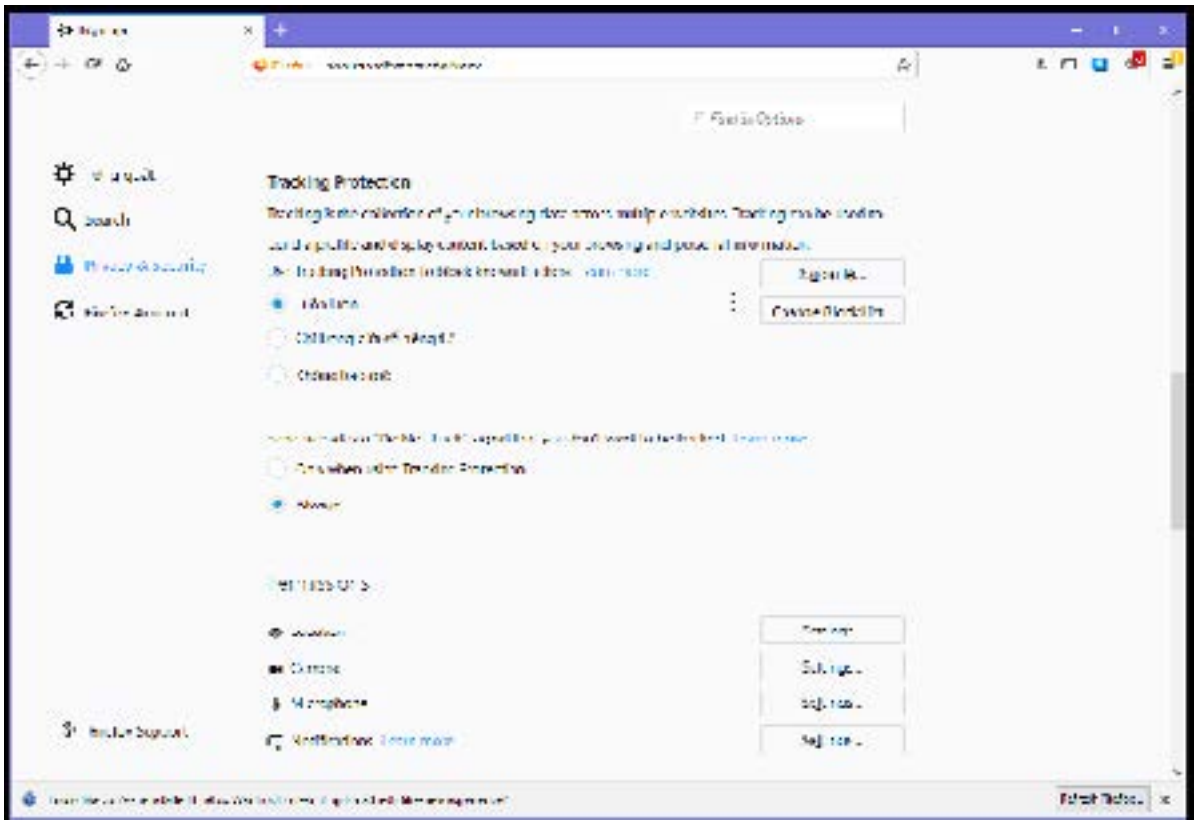
Bắt đầu trước bằng cách kiểm tra các tùy chọn cho các tiện ích khác nhau mà bạn đã cài đặt. Hầu hết đều được cấu hình sẵn, và không cần thay đổi, nhưng như mọi khi, điều quan trọng là bạn phải nhìn xung quanh để có một ý tưởng chung về các tùy chọn có sẵn.



GENERAL

Select Always ask me where to save files (WIN + OSX 13).



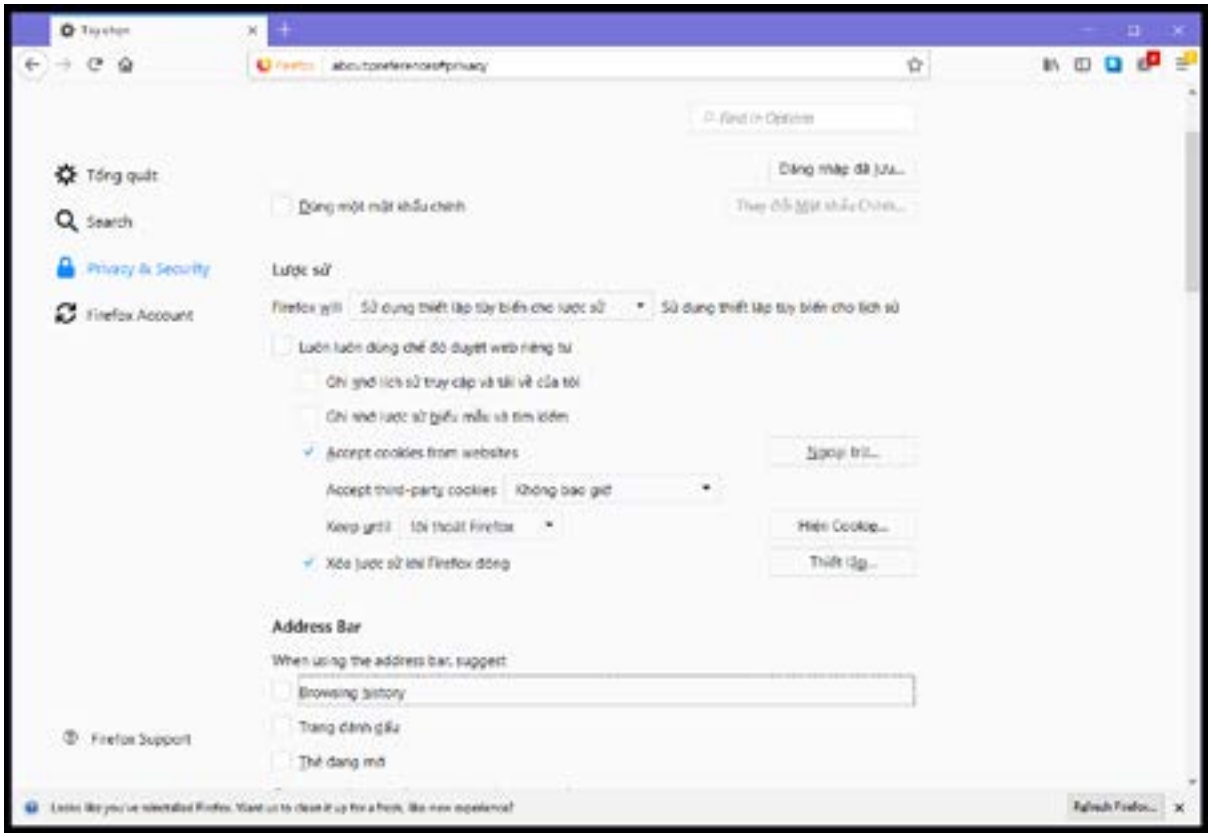


CHỌN

Always ask me where to save files (S-W/O2).

SEARCH

Đảm bảo rằng Provide search suggestions không được lựa chọn (S-W/O3).



PRIVACY

Kích hoạt Use Tracking Protection in Private Window. Dưới phần History, chọn Never Remember History. Dưới phần Location Bar, đảm bảo rằng không gì được lựa chọn (S-W/O4).

SECURITY

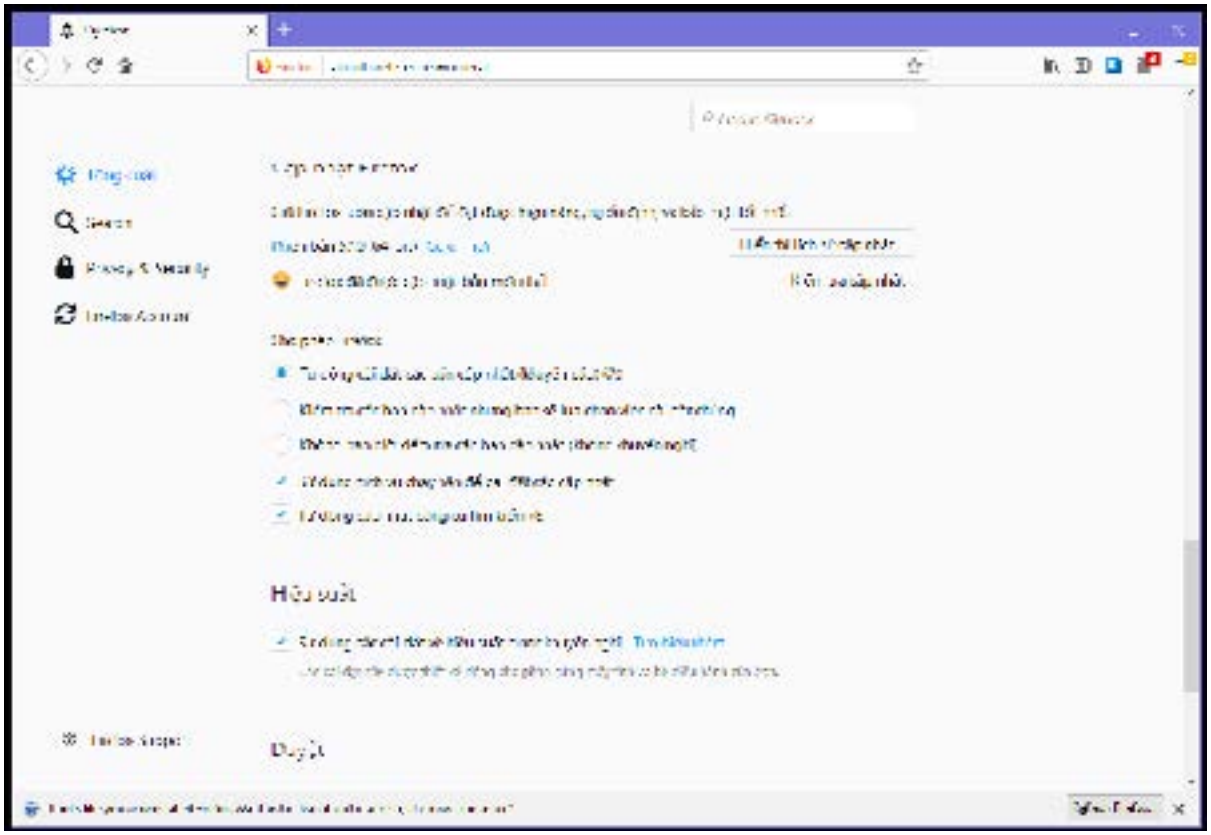
Dưới tab Security tab (S-W/O5), chọn cả bốn ô dưới phần General, và đảm bảo không tích hai ô của Logins (Remember logins for sites và Use a master password). Khi bạn ở đây, nhấn vào Saved Logins và nếu thấy bất kỳ điều gì được lưu trữ ở đây thì xóa đi.

SYNC

Không sử dụng Sync, và không liên kết Firefox với một tài khoản email hoặc điều gì đó tương tự. Không đăng nhập vào Firefox bằng tài khoản email của bạn.

ADVANCED

Trong phần Data choices, đảm bảo rằng cả ba hộp không được tích. Trong phần Network, chọn Override automatic cache management, và viết 50. Cuối cùng, trong tab Update chọn Automatically install updates. Đảm bảo bạn cũng đã chọn tự động cập nhật Search Engines (S-W/O6)



TECHNICAL SOLUTION: TOR

Bạn có thể cài đặt trình duyệt TOR (một chương trình / ứng dụng) trên máy tính của bạn hoặc trực tiếp vào USB. Nó đơn giản và hoạt động tự động khi bạn bắt đầu trình duyệt TOR. Với điều này, chỉ có trình duyệt cụ thể đó sử dụng TOR, không có gì khác trên máy tính của bạn. Nếu bạn muốn toàn bộ máy tính sử dụng TOR, bạn phải tải về và cài đặt chương trình thay thế. Nếu bạn làm như vậy, tất cả các kết nối sẽ được bao gồm bởi TOR, chẳng hạn như các trình duyệt khác, dữ liệu kết nối nền, Skype, v.v.

Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Stable Tor Browser

Language	Microsoft Windows (6.0.5)	Mac OS X (6.0.5)	Linux (6.0.5)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
العربية (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Deutsch (de)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Español (es-ES)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
فارسی (fa)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Français (fr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Italiano (it)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
日本語 (ja)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Korean (ko)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Nederlands (nl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Polish (pl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Português (pt-PT)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Русский (ru)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Türkçe (tr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Vietnamese (vi)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
简体字 (zh-CN)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

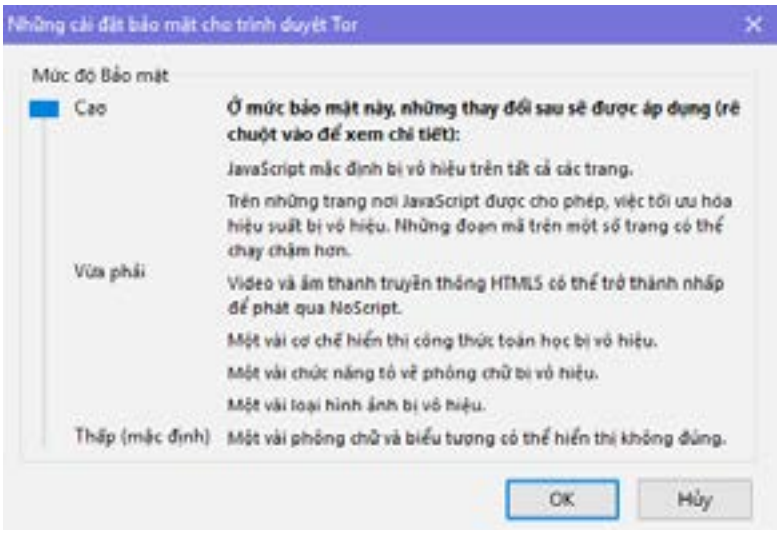
Đối với trình duyệt TOR, truy cập: https://www.torproject.org/projects/torbrowser.html.en và chọn trình duyệt bạn sẽ sử dụng, tùy thuộc vào hệ điều hành và ngôn ngữ của bạn. TOR cũng sản xuất phiên bản cho điện thoại di động.

Tải tệp tin về vị trí bạn muốn cài đặt, hoặc là USB hoặc ổ cứng đã được mã hóa ẩn. Nếu bạn không có ổ cứng hoặc bộ nhớ đã được mã hoá, hãy trở lại chương này sau khi đã thiết lập một chương theo Chương 5: Lưu trữ thông tin.

Hoặc cài đặt nó trên USB (xem bên dưới), hoặc cài đặt nó trên ổ cứng được mã hóa của bạn chứ không phải ổ cứng thông thường. Sau khi cài đặt, đảm bảo ngắt kết nối khỏi bất kỳ VPN đang chạy nào và bắt đầu thử nghiệm nếu nó hoạt động, bằng cách truy cập một trang web bị chặn.

Khi bạn bắt đầu chương trình, bạn có hai lựa chọn về cách kết nối. Hãy thử sử dụng Direct Connection trước, vì nó là cách đơn giản nhất. Bạn thực hiện lựa chọn này chỉ lần đầu tiên, sau đó nó sẽ nhớ sự lựa chọn và cài đặt của bạn, và sẽ bắt đầu giống như một trình duyệt bình thường.

Trình duyệt TOR được dựa trên Firefox và các tùy chọn tương tự như trong Firefox. Sau khi bắt đầu trình duyệt TOR lần đầu tiên, đi đến khu vực Options và thực hiện các lựa chọn tương tự như hướng dẫn cho Firefox trong trình mở rộng Firefox và Tiện ích mở rộng bên dưới.



Với TOR bạn cũng có một khu vực cài đặt khác. Dưới thanh địa chỉ là một biểu tượng củ hành xanh Green Onion Icon. Nhấp vào đó và chọn Privacy and Security Settings. Chọn tất cả các hộp. Cũng lưu ý thanh trượt Security level, nơi bạn có thể đặt mức bảo mật của mình. Chúng tôi khuyên bạn nên đặt nó ở mức High/Cao để bắt đầu, và nếu không mở được một số trang web thì bạn giảm mức độ bảo mật xuống cho đến khi nó có thể hoạt động như cần thiết

Bởi vì tầm quan trọng, bạn nên nhắc nhở bạn. Nếu bạn sử dụng TOR Browser, chỉ có lưu lượng truy cập của trình duyệt đó đi qua TOR chứ không phải truyền dữ liệu khác trên máy tính của bạn!

TOR TRÊN USB

TOR cũng có thể được cài đặt như là một chương trình USB với cùng một trình duyệt được cài sẵn. Với điều này, bạn chỉ cần kết nối USB với bất kỳ máy tính nào và bắt đầu trình duyệt đặc biệt, kết nối thông qua TOR. Bởi vì nó chạy trên USB, nó để lại ít dấu vết của việc sử dụng Internet của bạn trên máy tính bạn sử dụng. Xem xét mua một USB nhỏ, và cài đặt TOR trên USB này. Hãy chắc chắn rằng bạn không bao giờ sử dụng thẻ này cho bất cứ điều gì khác, chẳng hạn như lưu trữ các tập tin vv Quá trình cài đặt giống như trên, nhưng thay vào đó lưu các tập tin tải về vào USB của bạn và sau đó cài đặt nó trên USB. Trình duyệt giống nhau mặc dù được cài đặt trên USB và bạn cũng nên thực hiện những thay đổi tương tự với cài đặt trình duyệt như đã đề cập ở trên. Như trước, hãy đảm bảo nhập Setting areas của trình duyệt trước khi bạn bắt đầu sử dụng và thực hiện các lựa chọn có liên quan như đã đề cập trong trình duyệt Firefox.

THE DARK NET

Internet như bạn biết nó nhất giống như một tảng băng trôi, chỉ có 10% hoặc hơn là phần nhìn thấy được. Google và các công cụ tìm kiếm khác sử dụng indexing để cung cấp thông tin từ web cho bạn, và chỉ có phần được lập chỉ mục của internet là một phần rất nhỏ, có thể được tìm thấy bằng Google hoặc các công cụ tìm kiếm khác.

Phần còn lại thường được gọi là Deep Web. Không có điều gì đáng ngại về (hầu hết) mục đích này, tất cả các dữ liệu được giữ bởi các trường đại học, viện nghiên cứu, các tập đoàn, chính phủ vv, thường nằm trong mạng intranet, và dữ liệu này bạn không thể tìm thấy trừ khi bạn vào mạng intranet đó. Tương tự, bằng cách sử dụng cài đặt riêng tư, hầu hết thông tin trên phương tiện truyền thông xã hội của bạn, ví dụ như tài khoản Facebook, cũng là một phần của Deep Web vì không thể tìm và xem dữ liệu này bằng cách sử dụng công cụ tìm kiếm.

Bên trong Deep Web là một khu vực thường được gọi là Dark Net. Ngay cả khi đưa địa chỉ đến một trang web Dark Net trình duyệt của bạn sẽ không thể mở nó. Tất cả các trang web Dark Net sử dụng .onion và không có .com, .org, v.v ... trên Dark Web. Tất cả các địa chỉ được chọn ngẫu nhiên, và trông giống như "572abeh6g9gfd8gfd438gfd975.onion". The Dark Web hoạt động dưới Internet, hoàn toàn giấu tên. Điều này có nghĩa là một số người sử dụng nó cho các hoạt động bất hợp pháp, như nhiều trang về đấu thầu vũ khí, mua bán chất gây nghiện online, trao đổi ảnh khiêu dâm trẻ em và hơn thế nữa. Tuy nhiên, nó cũng có thể được sử dụng cho các lý do chính đáng, như mua sắm trực tuyến bằng cách sử dụng bitcoin hoặc các loại tiền tệ ảo, phòng chat nơi bạn có thể vẫn vô danh, và nhiều hơn nữa.

Cách duy nhất để truy cập Dark Web là kết nối TOR và mở trình duyệt TOR. Đây là cách duy nhất để đọc và truy cập các địa chỉ .onion. Nếu bạn muốn tìm hiểu thêm, khởi chạy TOR và trình duyệt của nó, và đi đến địa chỉ này:

http://zqktlwi4fecvo6ri.onion/

Đây là trang web giống như Wikipedia với thông tin và đường dẫn về Dark Net, và cũng có chứa tài liệu để bạn có thể biết được Dark Net là gì, nó hoạt động như thế nào và liệu nó có ích cho bạn hay không. Việc truy cập Dark Net là hoàn toàn hợp pháp, và chúng tôi khuyên bạn nên thử và tìm hiểu thêm. Tuy nhiên, các giải pháp truyền thông đã được trình bày trong cuốn cẩm nang này phải đủ để đảm bảo an toàn cho bạn, vì vậy chúng tôi sẽ không trình bày Dark Web một cách chi tiết hơn. Để khởi động TOR và sử dụng trình duyệt TOR, hãy xem chương trước đây đã trình bày về nó.

CHƯƠNG 5
LƯU TRỮ THÔNG TIN

Chương này sẽ giới thiệu cho bạn hai loại mã hóa khác nhau. Cách mã hóa thứ nhất, Mã hóa cơ bản, sử dụng mã hóa tự động được tích hợp sẵn trong máy tính của bạn, và bất kỳ USB nào bạn muốn, theo cách tương tự như cách điện thoại thông minh ngày nay đi kèm với mã hóa. Hình thức mã hóa thứ hai và quan trọng hơn là tạo một khu vực mật mã bí mật (mã hoá nâng cao) của ổ cứng hoặc USB, nơi bạn sẽ giữ tất cả các tài liệu của mình.

Mã hóa là một từ được sử dụng rất nhiều trong những ngày này, và bao gồm mọi thứ từ email và trò chuyện truyền thông, truy cập vào các trang web, để lưu trữ thông tin. Mã hóa có nghĩa là dữ liệu được bảo vệ để người ngoài không thể đọc nó. Chỉ có những người có khoá được sử dụng để mã hóa dữ liệu có thể đọc nó (được gọi là giải mã). Chương này chỉ đề cập đến mã hóa dữ liệu, cho việc sử dụng bộ nhớ của bạn, chẳng hạn như ổ đĩa cứng, USB ... và không đề cập đến email, kết nối internet, vv.

XÓA BỎ THÔNG TIN THỪA

Càng có nhiều dữ liệu lưu trữ trên các ổ cứng và thiết bị khác nhau, càng khó bảo vệ. Bước đầu tiên phải là chọn một nơi mà bạn sẽ lưu trữ dữ liệu công việc của mình và sau đó chỉ nơi đó. Thứ hai là xóa mọi thông tin mà bạn không cần nữa. Trừ khi bạn thực sự cần phải giữ dữ liệu, bạn nên xóa nó. Càng ít tài liệu cần bảo vệ thì việc bảo vệ càng dễ dàng hơn.

Bạn sẽ cần phải liên tục phân tích làm thế nào để hạn chế các mối đe dọa chống lại bạn. Bạn cũng cần phải phân tích làm thế nào bạn sẽ bị ảnh hưởng nếu bất kỳ lớp bảo vệ an ninh của bạn bị hỏng. Ví dụ: nếu lưu trữ được mã hóa của bạn cho các tệp công việc bị xâm nhập, thông tin bị lộ sẽ là những thông tin gì?

Thông tin bạn lưu giữ ít hơn, bạn càng ít lo lắng về thông tin. Điều này có nghĩa là bạn nên cố gắng chỉ duy trì những tài liệu mà bạn thực sự cần. Khi bạn viết một báo cáo dài, một số lượng đáng kể các nghiên cứu là cần thiết. Nếu bạn viết một đề nghị tài trợ, bạn có thể cần phải tạo ra rất nhiều thông tin cho điều đó. Nếu bạn sản xuất một báo cáo sử dụng nguồn tài trợ, bạn cũng

sẽ kết thúc với rất nhiều thông tin. Thông thường trong quá trình làm việc của chúng tôi, khi chúng tôi có sản phẩm hoàn chỉnh của chúng tôi, chúng tôi cũng có thể tạo ra rất nhiều tài liệu, dù là bản vẽ, bảng biểu và biểu đồ, các tài liệu văn bản riêng cho các khía cạnh khác nhau trước khi kết thúc các thông tin liên quan thành một tài liệu cuối cùng. Cho đến khi báo cáo cuối cùng được hoàn thành, bạn có thực sự cần phải giữ tất cả những tài liệu khác đã sử dụng trước đó? Chắc là không. Nếu vậy, hãy loại bỏ chúng và lưu và chỉ lưu trữ tài liệu cuối cùng. Chương 7: Xóa thông tin sẽ trình bày chi tiết về làm thế nào để xóa thông tin một cách an toàn.

NHỮNG GÌ ĐỂ SỬ DỤNG ĐỂ LƯU TRỮ

HDD, SSD, SD, USB là một số trong nhiều cách lưu trữ ở ngoài máy tính và chúng ta có nhiều cách lưu trữ khác nhau với những thiết bị đó. Loại lưu trữ bạn sử dụng sẽ ảnh hưởng trực tiếp đến mức độ bạn dễ dàng xóa thông tin khi bạn không cần nó nữa. Tại thời điểm này, bạn nên đọc phần HDD và SSD trong Chương 7: Xóa thông tin, trước khi quyết định bạn muốn sử dụng tài liệu lưu trữ công việc của mình như thế nào. Điều này sẽ xảy ra khi bạn thiết lập Mã hóa nâng cao của mình. Đầu tiên, bạn có thể đọc và đi qua phần về Mã hóa cơ bản dưới đây.

MÃ HÓA CƠ BẢN

Nếu bạn sử dụng iPhone hoặc điện thoại Android, bạn sẽ nhận thấy rằng điện thoại được bán với mã hóa đã được bật. Ngay cả khi không, điện thoại cho phép bạn mã hóa chúng một cách dễ dàng và tất cả những gì bạn cần làm là chọn một mã PIN hoặc mật khẩu (và không có dữ liệu hiện có nào bị xóa trong quá trình này).

Những ngày này, cả Win10 và OSX đều có cùng chức năng, cho phép bạn mã hóa ổ cứng máy tính của bạn một cách dễ dàng và chọn một mã PIN hoặc mật khẩu. Không giống như điện thoại, nó không được bật khi bạn mua máy tính, vì vậy bạn phải làm điều đó cho mình. Bật tính năng mã hóa này không định dạng lại hoặc xóa ổ cứng của bạn hoặc xóa bất cứ thứ gì từ máy tính của bạn. Sau khi kích hoạt mã hóa mọi thứ đã có trước đó sẽ vẫn ở đó, và bạn sẽ không nhận thấy bất kỳ thay đổi nào.

Mã hóa cơ bản này nên được mọi người sử dụng vì nó bảo vệ dữ liệu của bạn một cách rất dễ dàng. Sự khác biệt cho bạn với tư cách người dùng là rất nhỏ. Nếu mã hoá được kích hoạt, bạn cần phải nhập mã PIN hoặc mật khẩu trước khi máy tính hoặc điện thoại của bạn khởi động. Nếu bạn nhập không đúng nó không thể bắt đầu, bởi vì nó không thể truy cập vào ổ đĩa cứng, và do đó không thể bắt đầu hệ điều hành (OS). Bạn cũng có thể bật biểu mẫu mã hoá này trên ổ cứng, USB ... (trong trường hợp đó bạn sẽ được yêu cầu nhập mật khẩu hoặc mã PIN sau khi cắm vào máy tính.)

Vì hầu hết các điện thoại và máy tính yêu cầu mật khẩu hoặc mã PIN để mở, bạn có thể tự hỏi sự khác biệt là gì. Sự khác biệt là loại cũ nhập mật khẩu hoặc mã PIN bạn đã sử dụng là để mở khóa giao diện máy tính hoặc điện thoại (chuyển từ màn hình khóa sang giao diện hệ điều hành). Những mật khẩu này chỉ được yêu cầu sau khi hệ điều hành đã được nạp và đang chạy, và chỉ ngăn cản mọi người truy cập vào giao diện. Điều này có nghĩa là không có gì được mã hóa, và nếu ai đó muốn thông tin của bạn, họ chỉ có thể lấy ổ cứng hoặc bộ nhớ khác được sử dụng, và cắm nó vào một máy tính khác và đọc mọi thứ trên đó. Mã hóa thiết bị và ổ cứng sẽ ngăn chặn điều này.

Có mật khẩu để vô hiệu màn hình khóa và nhập giao diện giống như có cửa ra vào nhà bạn. Mã hóa giống như có khóa trên những cánh cửa. Một cánh cửa không khóa không hữu ích nếu ai đó muốn phá vỡ.

> Mã hóa cơ bản sẽ chỉ cho bạn cách bật tính năng này trên máy tính của bạn, tính năng này được gọi là BitLocker. Tuy nhiên, chỉ có Win10 PROFESSIONAL chứ không phải HOME, cung cấp điều này. Nếu bạn có phiên bản HOME, bạn không thể sử dụng và có thể bỏ qua INSERT/Chèn: Mã hóa Nâng cao.

MÃ HÓA NÂNG CAO VÀ NƠI LƯU CÁC TỆP CÔNG VIỆC CỦA BẠN

Sử dụng Mã hóa cơ bản cung cấp cho máy tính bảo mật cơ bản của bạn. Nếu được sử dụng, trong tương lai, bạn sẽ nhập mật khẩu hoặc mã PIN khi khởi động máy tính và đó là nó. Tiếp theo chúng ta thảo luận các bước phức tạp hơn một chút, đó là nơi tập tin công việc của bạn sẽ được lưu trữ. Ngay cả khi bạn không thể sử dụng Mã hóa cơ bản, mã hóa ẩn này sẽ giữ các tệp công việc của bạn an toàn và ẩn cho bất kỳ người ngoài. Chương trình chúng tôi sẽ sử dụng là Veracrypt hoặc Truecrypt, có chức năng tương tự cho dù bạn có Win10 hay OSX.

Chúng tôi sẽ tạo ra một không gian mã hóa an toàn, ẩn cho các tệp công việc của bạn. Như đã trình bày ở trên, chẳng hạn như khi thảo luận về Chính sách Hộp thư đến trống trơn, mối đe dọa chính không phải là ai đó sử dụng hacker tiên tiến để phá vỡ mã hóa của bạn, nhưng điều gì sẽ xảy ra khi cảnh sát hoặc bọn tội phạm buộc bạn phải cung cấp mật khẩu cho họ. Nếu bạn làm như vậy, và bạn rất có thể, tất cả sự bảo vệ của bạn sẽ bị mất. Giống như trình duyệt web và email bạn sử dụng, chìa khóa để bảo vệ là họ không biết rằng bạn có nó, bởi vì họ không thể yêu cầu những gì họ không biết rằng có tồn tại.

Có một cách dễ dàng và thông minh hơn xung quanh vấn đề này, và nó được gọi là mã hóa ẩn. Vấn đề là không ai thậm chí sẽ biết rằng nó tồn tại, và do đó không ai có thể buộc bạn đưa ra bất kỳ mật khẩu. Phần này, cùng với Chính sách Hộp thư trống và Chương 7: Xóa thông tin là những phần quan trọng nhất của toàn bộ hướng dẫn sử dụng này. Đó là sự kết hợp của những điều này sẽ bảo vệ bạn. Chúng tôi cũng sẽ dành thời gian để cho bạn biết rằng nó không phải là tiên tiến hoặc khó sử dụng. Chỉ cần dành một thời gian ngắn để thiết lập nó, nhưng một khi thực hiện, bạn sử dụng nó với một bấm vào một nút.

ĐIỀU GÌ TẠO RA SỰ AN TOÀN NÀY?

Khi một ổ đĩa cứng, hoặc một phần của một ổ cứng hoặc USB vv được mã hóa, máy tính không thể đọc được phần đó. Bạn cần phải giải mã nó trước khi bạn có thể đọc nó (bằng cách nhập mật khẩu). Bằng cách sử dụng phân tích kỹ thuật, cảnh sát, bọn tội phạm hoặc những người khác có thể kết luận rằng bạn đang sử dụng mã hóa (hoặc ổ cứng của bạn bị hỏng). Điều gì sẽ xảy ra là họ sẽ cố buộc bạn đưa ra mật khẩu của bạn. Không có cách nào xung quanh điều này.

Cách khắc phục vấn đề này là bạn không tạo ra một mật mã, nhưng hai không gian mật mã, trong cùng không gian. Không gian này sẽ có những gì được gọi là Outer Volume và Inner

Volume. Volume chỉ là một tên khác cho không gian mã hóa. Một mật khẩu sẽ được lập để mở Outer Volume, trong khi một mật khẩu an toàn hơn nhiều, sẽ để mở Inner Volume. Bạn đang sử dụng mã hóa ảo.

Bởi vì Inner Volume được chứa ở bên trong của Outer Volume, không có phân tích kỹ thuật nào có thể phát hiện thấy bạn có Inner Volume.

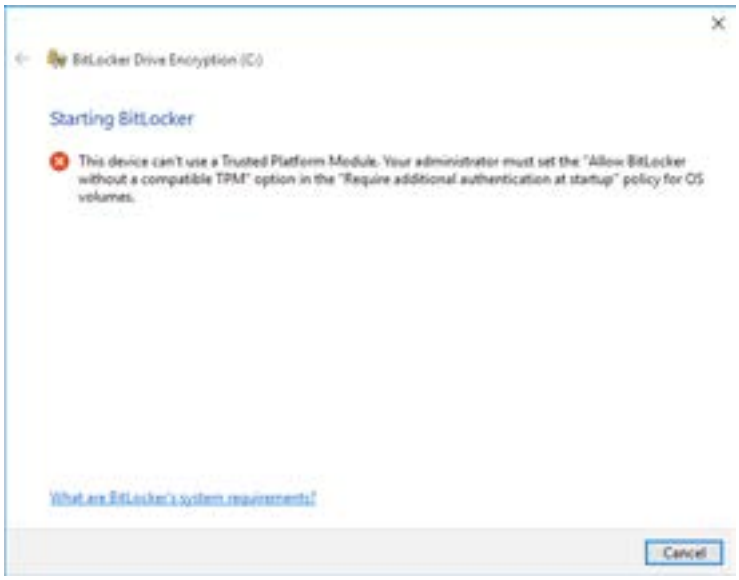
Để thực hiện mục đích, khi bạn chọn để gắn kết khu vực mã hóa của bạn, nếu bạn nhập một mật khẩu nó sẽ mở Outer Volume. Outer Volume sẽ hoạt động như một cái mồi, có nghĩa là nếu cảnh sát hoặc bọn tội phạm buộc bạn khai mật khẩu và hiển thị nội dung nó sẽ không hiển hiện bất cứ điều gì quá nhạy cảm nhưng phải đáp ứng cho họ rằng họ đã phát hiện ra tất cả các thông tin mật mã của bạn. Bạn sẽ đặt một số tài liệu làm việc và các dữ liệu cá nhân khác trong Outer Volume, do đó, nếu bao giờ bạn bị buộc phải mở nó, họ sẽ tin rằng họ đã tìm thấy những gì họ muốn. Tuy nhiên, bạn sẽ giữ nguyên tài liệu nhạy cảm hơn chứa bên trong, trong Inner Volume.

NHỮNG ĐIỂM QUAN TRỌNG

- Bạn đã bật Mã hóa cơ bản cho máy tính của mình?
- Bạn đã hoàn thành việc thiết lập một mã hóa ẩn và kiểm tra nó?
- Bạn có hiểu tại sao việc sử dụng mã hoá ẩn (bên trong và bên ngoài) và ý tưởng về sự không chấp nhận được có thể giúp bạn, khác hơn là chỉ bảo vệ dữ liệu của bạn khỏi bị tấn công?
- Nhớ rằng, càng ít dữ liệu cần phải bảo vệ thì việc bảo vệ càng dễ dàng hơn. Loại bỏ các tệp công việc không cần thiết mà bạn không cần phải giữ.

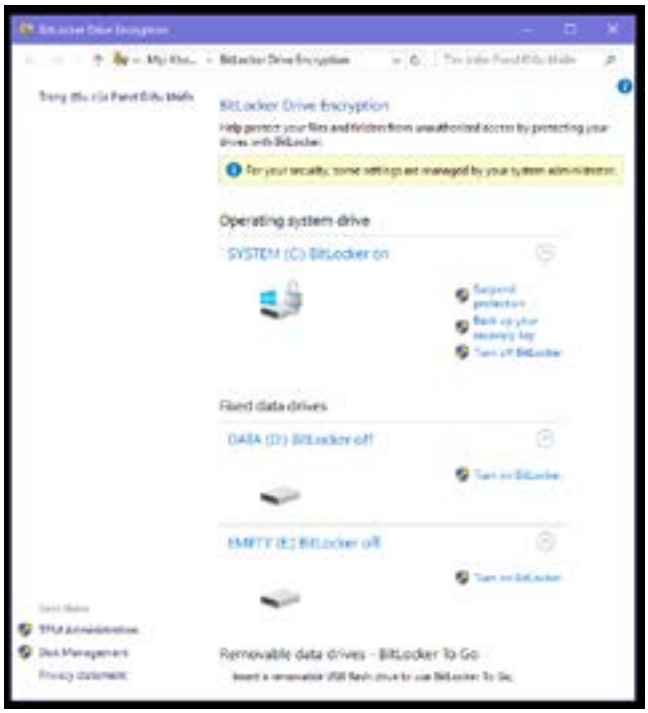
GIẢI PHÁP KỸ THUẬT: MÃ HÓA CƠ BẢN

Đối với Win10, chương trình được tích hợp để xử lý mã hóa được gọi là BitLocker (Search Term). Bạn bắt đầu chương trình bằng cách tìm kiếm nó trong khu vực tìm kiếm. Nó có thể mã hóa ổ cứng hệ điều hành của bạn, các ổ đĩa cứng khác, USB vv



Khi bạn mở BitLocker, bạn có thể thấy 20.

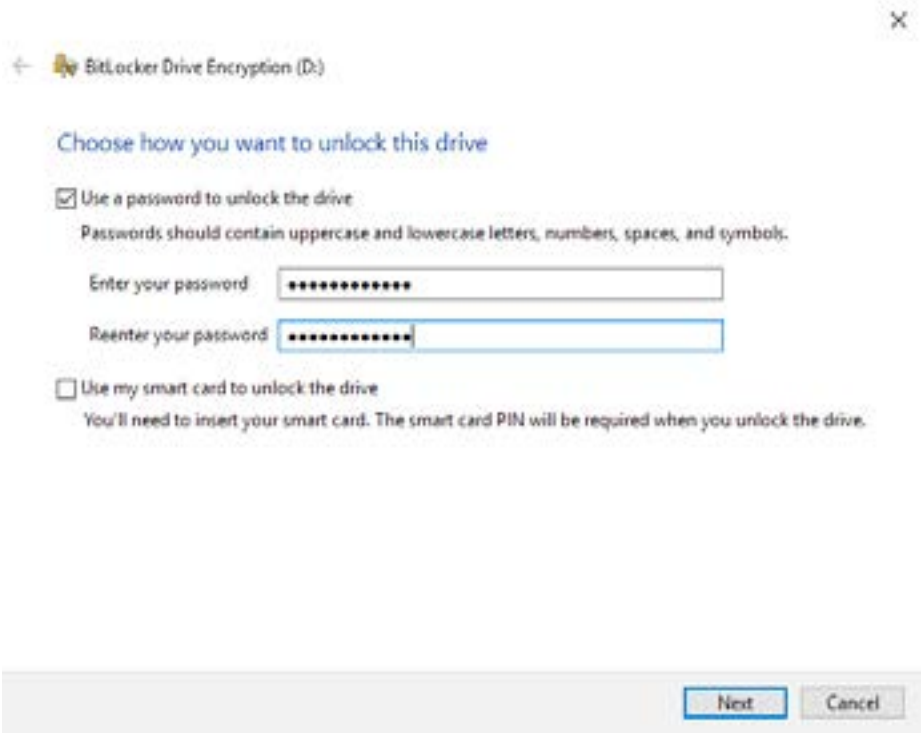
Nếu bạn làm vậy, điều này có nghĩa là bạn cần bật một thứ gọi là TPM. Bạn thực hiện việc này bằng cách làm theo các bước trên màn hình. Quá trình này sẽ yêu cầu bạn khởi động lại máy tính. Nếu bạn cần trợ giúp thêm về cách bật TPM, hãy sử dụng google và nó sẽ hiển thị rất nhiều trợ giúp về cách bật.

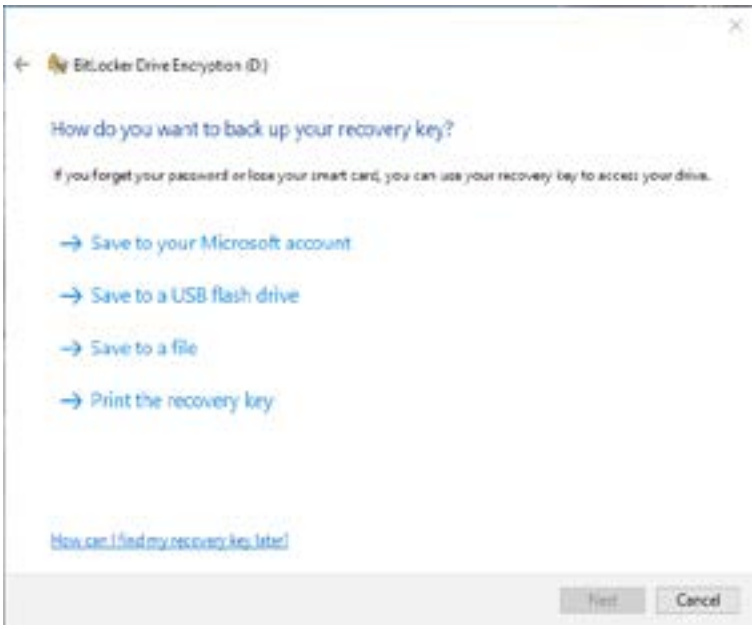


Khi bạn khởi động BitLocker, bạn có thể chọn ổ cứng hoặc phương tiện di động nào (USB, thẻ SD, ...) mà bạn muốn mã hóa từ menu chính BitLocker (21) hoặc bạn có thể kích chuột phải vào ổ đĩa trong Explorer và chọn Turn on BitLocker (22). Trước khi bắt đầu, đảm bảo bạn có một USB hoặc máy in gần đó mà bạn sẽ phải sử dụng một thời gian ngắn.

Bắt đầu quá trình cho bất kỳ ổ cứng hoặc USB bằng cách nhấp vào Turn on BitLocker. Bước đầu tiên là bạn sẽ được hỏi làm thế nào để mở khóa ổ đĩa mới được mã hóa, và bạn nên chọn Use a password (23) và sau đó nhấp Next Vì đây là mã hóa cơ bản, bạn có thể sử dụng mã PIN hoặc mật khẩu ngắn hơn.

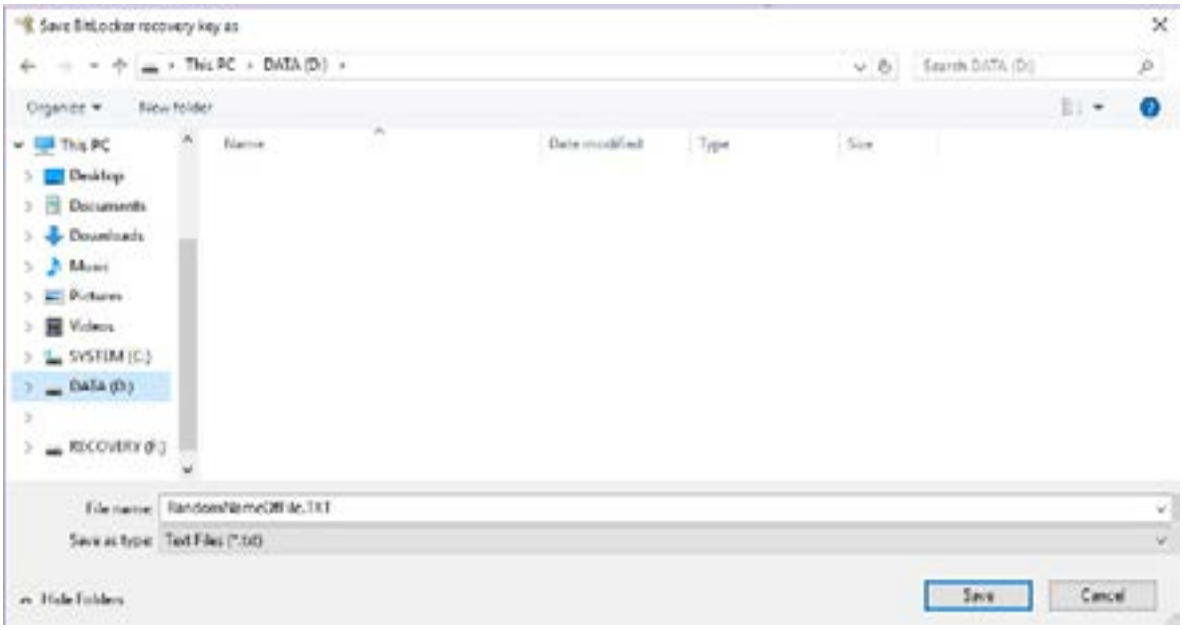
Tiếp theo, nó sẽ hỏi bạn nơi lưu khóa khôi phục. Khóa này, là một chuỗi ký tự, có thể được sử dụng để mở khóa ổ đĩa được mã hóa của bạn nếu bạn mất hoặc quên mật khẩu. Đây là một mối đe dọa an ninh lớn. Để chống lại vấn đề này, chọn Print the recovery key nếu bạn có một máy in. Nếu bạn không có máy in thì chọn Save to a file và lưu nó vào một USB (24, 25).
Bạn cũng có thể chọn để cho một bản sao được lưu trữ bởi Microsoft trong tài khoản Windows của bạn, nhưng nếu tài khoản Windows của bạn được truy cập trực tuyến, nó sẽ có nghĩa là bất cứ ai có quyền truy cập có thể giải mã ổ đĩa một cách dễ dàng mà không có mật khẩu của bạn, do đó, chỉ sử dụng nếu bạn cảm thấy bạn có thể bảo vệ tài khoản Windows của bạn.





Sau khi đã lưu Recovery file/tệp Phục hồi và nhấp vào Next, bạn sẽ được hỏi khối lượng ổ cứng hoặc USB để mã hóa và ở đây bạn luôn chọn Encrypt entire drive. Trên trang tiếp theo, bạn chọn chế độ mã hóa phù hợp nhất với bạn, thường là New encryption mode, nhưng tùy chọn thứ hai, Compatible mode, có thể cần thiết nếu đó là USB hoặc ổ cứng gắn ngoài mà bạn muốn có thể sử dụng trên các máy tính khác, những máy tính có thể không có hệ Windows mới nhất.

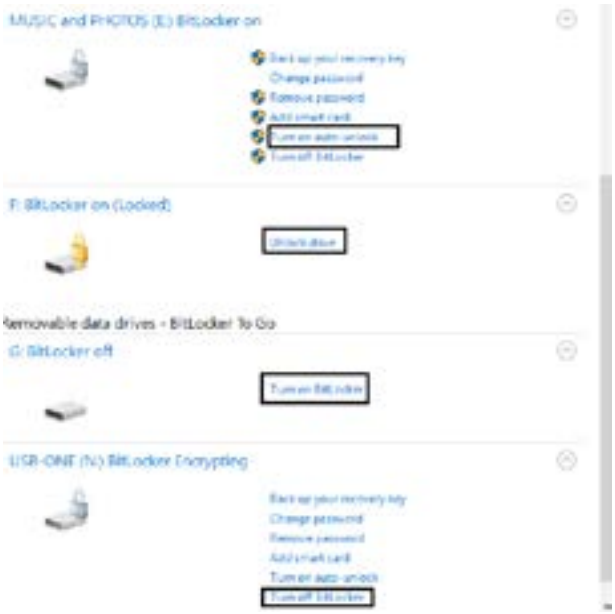
Bây giờ bạn đã sẵn sàng để mã hóa ổ đĩa, nhấp vào Start encr và để nó chạy dưới nền. Ổ đĩa cứng lớn thì nó sẽ chạy lâu hơn (26). Hãy để việc chạy chương trình tiếp tục cho đến khi hoàn thiện.



Cuối cùng, chúng ta cần phải thoát khỏi Recovery file. Nếu bạn in nó, phá hủy giấy để chuỗi ký tự không thể được đọc. Nếu bạn lưu vào USB, hãy xóa khóa. Sau khi xóa tập tin, nhấp chuột phải vào USB (trong cửa sổ Explorer) và chọn Format, và định dạng USB. Quá trình này sẽ loại bỏ tất cả dấu vết của khoá. Không sử dụng Quick Format vì sẽ không loại bỏ dữ liệu một cách an toàn. (27).

TINH CHỈNH VÀ SỬ DỤNG MÃ HÓA CƠ BẢN

Từ BitLocker, bạn có thể thấy rằng sau khi mã hóa được kích hoạt, bạn có một vài tùy chọn. Tất nhiên bạn có thể Turn of Bitlocker cho một ổ đĩa. Bạn cũng có thể quyết định xem thiết bị có nên Auto-unlock/Tự động mở khóa hay không. Tự động mở khóa có nghĩa là bạn sẽ được yêu cầu nhập mật khẩu hoặc mã PIN để mở khóa bất kỳ ổ cứng không phải là hệ điều hành, USB ... khi máy tính khởi động (hoặc nếu sử dụng USB hoặc ổ cứng gắn ngoài, khi đầu tiên được cắm vào). Nếu không bật, nó sẽ không mở khóa các ổ đĩa cho đến khi bạn nhấp vào chúng trong cửa sổ Explorer, tại thời điểm đó nó sẽ yêu cầu bạn cho mật khẩu hoặc mã PIN.



Tính năng mở khóa tự động hoặc không này không áp dụng cho ổ cứng với hệ điều hành. Đối với các ổ đĩa như vậy bạn luôn phải nhập mật khẩu hoặc mã PIN khi khởi động máy tính, nếu không nó không thể tải hệ điều hành. S-WXX cho thấy một số tùy chọn khác nhau.

Một khi bạn đã mở khóa một ổ đĩa, nó sẽ vẫn mở khóa cho đến khi bạn tắt máy tính của bạn.

Bây giờ bạn đã hoàn tất việc mã hoá cơ bản của máy tính.

Để thêm tính an toàn cho việc khởi động máy tính, bạn có thể đặt chế độ cho BitLocker yêu cầu mã PIN để khởi động máy tính. Để làm như vậy, mở chức năng tìm kiếm và viết gpedit (edit group policy). Trong cửa sổ popup xuất hiện, trong Computer Configuration, nhấn vào Administrative Templates, sau đó chọn Windows Components, và cuối cùng nhấn vào BitLocker Drive Encryption. Nhấp vào Operating System Drives. Tìm và nhấp đúp vào Require additional authentication at startup. (0X)

Một cửa sổ mới xuất hiện, và trong đó, chọn Enabled. Nhìn xuống dưới, dưới Configure TPM startup PIN, nhấp vào trình đơn thả xuống và chọn Require startup PIN with TPM. Nhấn Ok và đóng các cửa sổ. (0X)

Cuối cùng, nhấp chuột phải vào nút Windows, và chọn Windows PowerShell (Admin). Viết trong đó như sau:

manage-bde -protectors -add c: -TPMandPIN

Sau đó, nó sẽ yêu cầu bạn viết mã PIN của bạn. Làm như vậy, và nhấn Enter. Sau đó làm lại lần nữa. Nó sẽ cho bạn biết mã PIN đã được thiết lập. Cần 6 con số hoặc nhiều hơn. (0X)

Kể từ đó, khi bạn khởi động máy tính, bạn sẽ phải nhập mã PIN, hoặc máy tính sẽ không khởi động.

GIẢI PHÁP KỸ THUẬT: MÃ HÓA NÂNG CAO

Để tạo mã hóa ẩn này, bạn cần tải về và cài đặt một chương trình có tên VeraCryptorTrueCrypt. Cả hai link sau đều cho kết quả như nhau

Veracrypt: https://veracrypt.codeplex.com/wikipage?title=Downloads

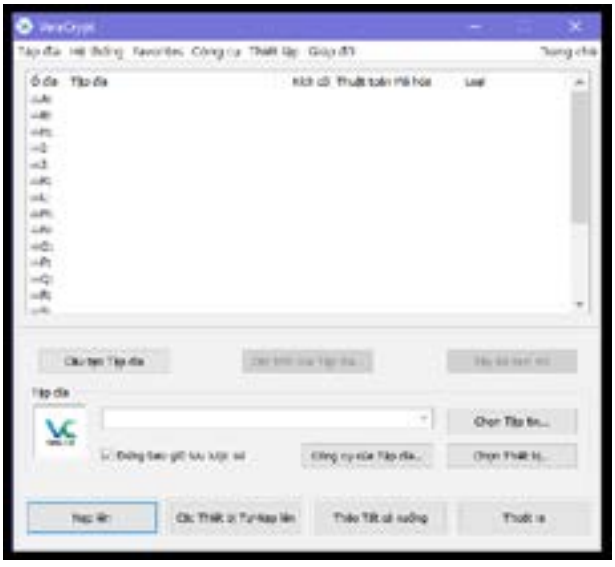
Truecrypt (7.1a): https://www.truecrypt71a.com/downloads/

Bạn có thể cài đặt Veracrypt trên máy tính của bạn, hoặc trong USB. Cách thứ hai an toàn hơn, nhưng yêu cầu bạn phải cắm USB vào máy tính khi bạn sử dụng nó. Bất kể khi nào, hãy tải tệp tin thẳng đến vị trí mà bạn sẽ để chứ không phải để trên màn hình của bạn.

Không giống như Mã hóa cơ bản, khi bạn muốn sử dụng mã hóa ẩn, như khi bạn cần tải tệp mới hoặc đang làm việc trên các tài liệu của mình, bạn chỉ cần bắt đầu Veracrypt và tải mã hoá ẩn, sẽ xuất hiện trong Explorer hoặc Finder của bạn cửa sổ giống như bất kỳ ổ cứng hoặc USB khác. Sau khi hoàn thành công việc, bạn chỉ cần dỡ bỏ nó. Các thuật ngữ dùng để nạp bộ nhớ được mật mã là mount. Để dỡ / khóa, nó được gọi là dismount/tháo dỡ. Không gian mã hoá được tạo ra thường được gọi là volume. Chúng tôi sẽ sử dụng các thuật ngữ này cho phần còn lại của chương để bạn làm quen với chúng. Một khi bạn gắn kết không gian mã hóa nó sẽ xuất hiện như một ổ đĩa cứng, ví dụ E: Tên, và một khi bạn tháo dỡ, nó sẽ biến mất.

CÀI ĐẶT

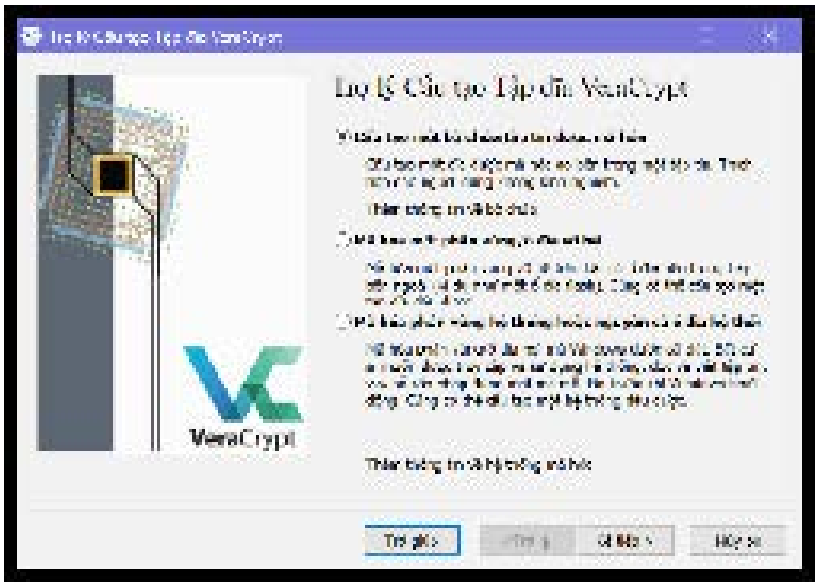
Bước đầu tiên là quyết định mã hóa sẽ ở đâu. Bạn có muốn sử dụng USB không? Bạn có muốn sử dụng một ổ cứng đầy đủ, một phân vùng của một ổ đĩa cứng, hoặc có thể chỉ là một phần nhỏ của một ổ cứng? Chúng tôi sẽ giới thiệu cách tạo một hệ thống cho cả USB và toàn bộ ổ đĩa cứng hoặc phân vùng và cho một phần nhỏ của ổ cứng. (Lưu ý: Chúng tôi sẽ không sử dụng tùy chọn để mã hóa ổ đĩa hệ điều hành).



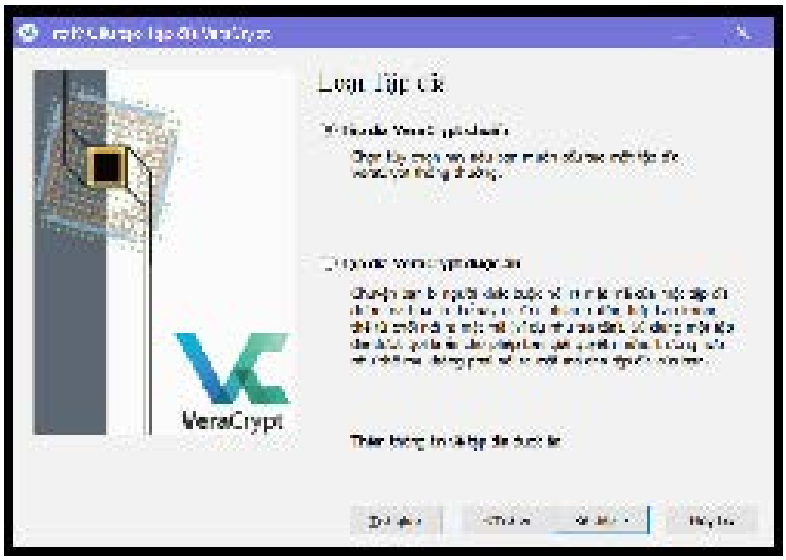
Trên cơ sở từng bước, đây là những gì bạn làm. Sau khi cài đặt chương trình trên máy tính hoặc USB, hãy bắt đầu chương trình.

Trong cửa sổ đầu tiên bạn nhìn thấy, đây cũng là cửa sổ chính (S-W / OXX) để sử dụng bình thường (gắn kết và tháo dỡ), hãy nhấp vào Create Volume.

Sau khi kích Create Volume, bạn sẽ có hai lựa chọn (S-W / OXX) (một lựa chọn thứ ba cho phân vùng hệ thống được hiển thị trong Win10, nhưng không liên quan đến chúng ta). Một lựa chọn, và một cách dễ nhất để sử dụng, là Encrypt a non-system partition/drive. Điều này mã hóa toàn bộ phân vùng hoặc ổ cứng (không cho ổ cứng với một hệ điều hành trên đó). Nó cũng áp dụng cho ổ cứng ngoài và USB.



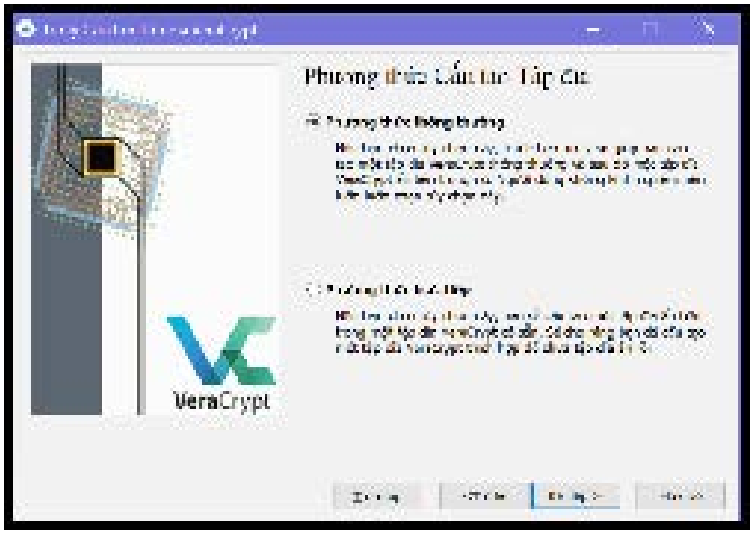
Tùy chọn khác là Create an encrypted file container, tức là tạo một thùng chứa tập tin được mã hóa, nơi bạn tự quyết định phần được mã hóa sẽ chiếm bao nhiêu phần của một ổ cứng, USB vv. Nếu bạn muốn sử dụng tùy chọn này, bạn cần tạo folder ở đâu đó, trên USB hoặc trên ổ cứng của bạn. Tạo một folder bất kỳ loại nào, nhưng không phải là folder văn bản hoặc tệp tin văn bản, ví dụ tệp cơ sở dữ liệu hoặc bản trình bày powerpoint hoặc cái gì đó. Tập tin này sau đó sẽ giữ không gian mã hóa. Nếu bạn xóa tập tin này, bạn xóa tất cả mọi thứ! Hãy ghi nhớ tệp bạn tạo và cất giữ nơi nào và đảm bảo bạn không vô tình xóa nó.



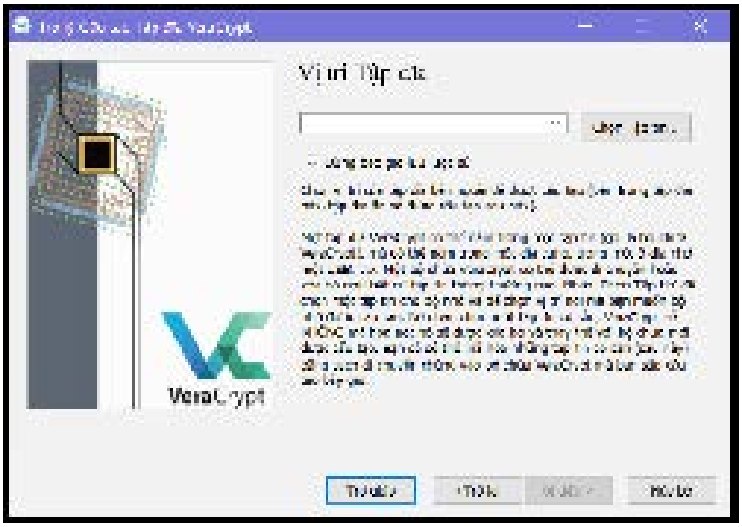
Sau khi chọn một trong hai tùy chọn và nhấn tiếp, bạn sẽ được hỏi nếu bạn muốn tạo Standard Veracrypt volume hoặc a Hidden Veracrypt volume(S-W/OXX). Chọn Hidden và nhấn Next. Sau đó bạn sẽ được yêu cầu chọn Normal mode hoặc Direct mode. Chọn Normal mode (chọn chế độ Direct mode nếu bạn đã mã hóa một không gian trước đó) (S-W/OXX).

Sau đó, phụ thuộc vào việc bạn chọn Create an encrypted file container hoặc Encrypt a non-system partition/drive.

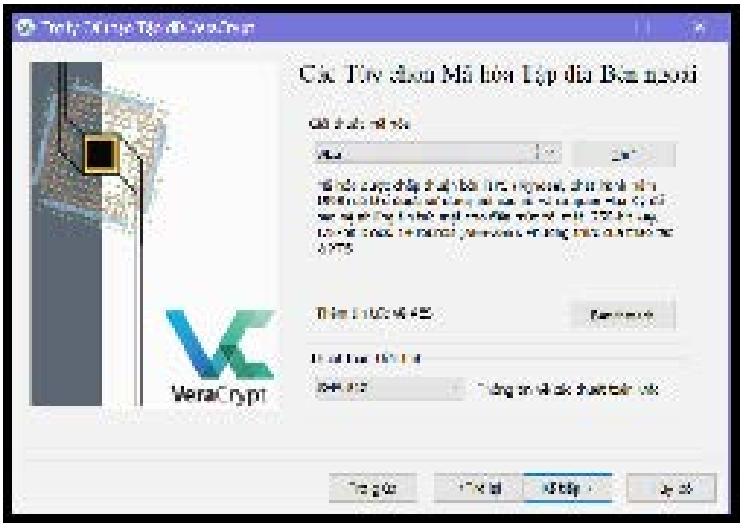
Quay trở lại Veracrypt và nhấn Select File từ màn hình (S-W/OXX), và tìm đến tệp tin folder mà bạn đã tạo ra và chọn nó. Nó sẽ cảnh báo bạn rằng mọi thông tin trong tệp tin này sẽ bị xóa.



Chọn Yes.

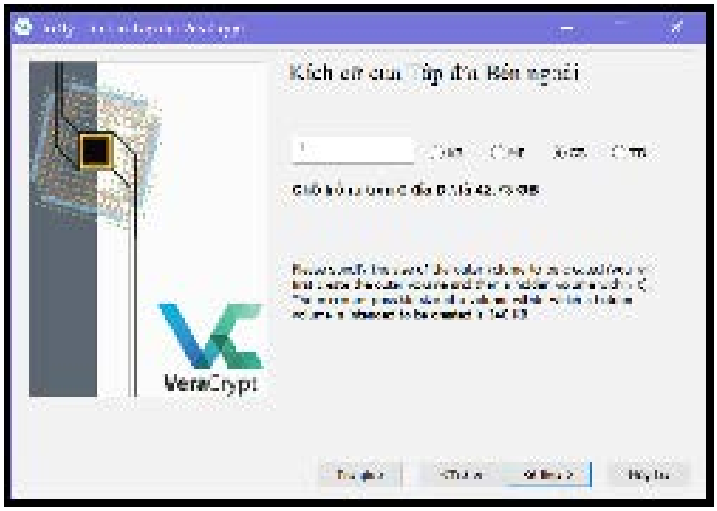


Nếu bạn chọn Encrypt a non-system partition/drive, bạn cũng nhấn Select File và từ cửa sổ chọn USB, ổ cứng hoặc ổ cứng gắn ngoài mà bạn muốn mã hóa. Mã hóa nó sẽ xóa tất cả dữ liệu trên đó, vì vậy hãy chắc chắn rằng bạn đã lưu giữ bất kỳ tập tin nào bạn muốn giữ lại ở chỗ khác.



Sau khi thực hiện lựa chọn này, phần còn lại của quá trình mã hóa là như nhau cho cả hai phương pháp.

Chương trình đầu tiên sẽ tạo ra Outer volume. Bạn không phải thực hiện bất kỳ thay đổi nào trong bước tiếp theo (Encryption options)

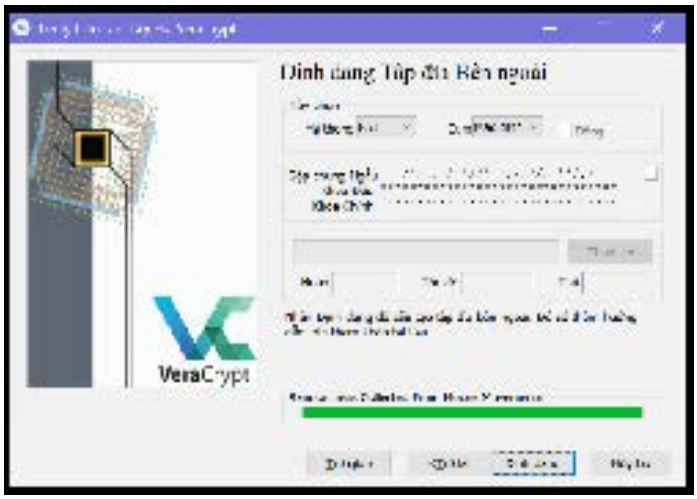


Sau khi kích vào Next nó sẽ hỏi bạn về kích thước cần mã hóa. Nếu bạn chọn Encrypt a non-system partition/drive thì bạn không thể thay đổi điều này và toàn bộ không gian sẽ được mã hóa. Nếu bạn chọn Create a file container bạn sẽ được hỏi kích thước sẽ được mã hóa là bao nhiêu. Trừ khi bạn có nhiều tài liệu phim ảnh, 10GB là đủ. (S-W/OXX). Hãy thực hiện lựa chọn và kích Next.

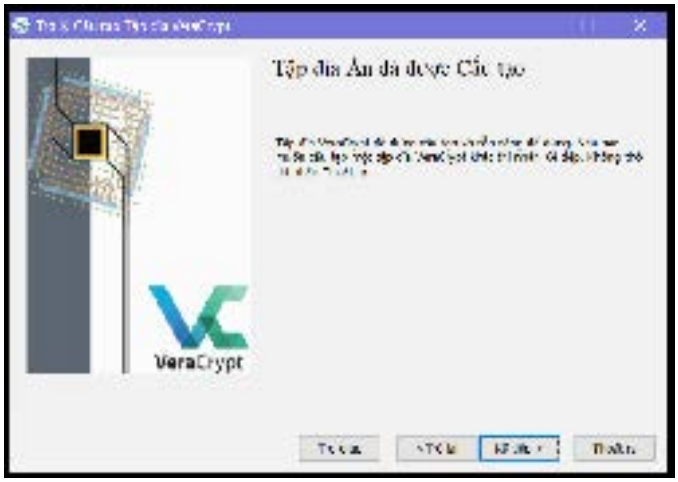
Cửa sổ tiếp theo là để tạo mật khẩu cho Outer volume (S-W/OXX). Đây là mật khẩu cho lớp vỏ bên ngoài và không cần phải phức tạp quá. Hãy chọn cái gì đó mà bạn dễ nhớ.

Sau khi nhấp Next, quá trình chuẩn bị mã hóa sẽ bắt đầu. Điều này sẽ không mất nhiều thời gian, nhưng phụ thuộc vào kích thước. Trong khi đang thực hiện, hãy di chuyển con chuột xung quanh càng nhiều càng tốt (S-W / OXX). Sự can thiệp này sẽ tăng cường sự mã hóa. Khi nó dừng lại và đã sẵn sàng, nhấp vào nút Format.

Sau khi hoàn thiện, màn hình sẽ xuất hiện như sau, và bạn nhấn vào Next(S-W/OXX).



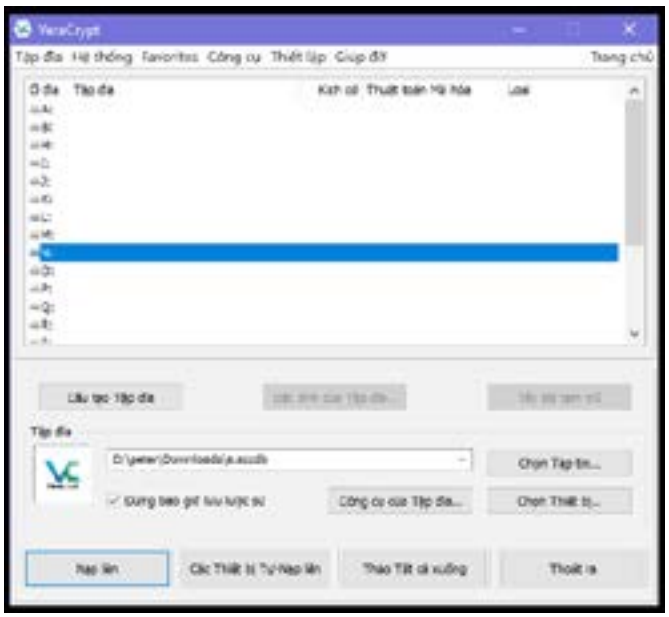
Sau đó quá trình tạo ra Inner volume bắt đầu. Nhấp vào Next. Điều này sẽ bắt đầu toàn bộ quá trình, nhưng là đối với Inner volume bên trong. Điều duy nhất để thay đổi là kích thước cần được thiết lập để nhỏ hơn Outer volume (chúng tôi đề xuất khoảng một nửa), và cần một mật khẩu rất mạnh mà bạn phải nhớ vì nếu quên bạn sẽ mất quyền truy cập mãi mãi. Tất cả các bước khác đều giống nhau và khi hoàn tất, cửa sổ như bên dưới sẽ được hiển thị và bạn nhấp vào Exit (S-W / OXX).



Bạn đã hoàn thiện cài đặt, cho cả Outer và Inner volume.

SỬ DỤNG VERACRYPT

Mọi thứ đã được thiết lập và bạn sẽ không phải lo lắng về điều này nữa. Để sử dụng Veracrypt chỉ cần bắt đầu chương trình (S-W / OXX). Để mount thiết bị của bạn, có hai cách. Nhấp chuột đầu tiên vào bất kỳ ký tự ổ đĩa. Sau khi mount, khối lượng mã hóa của bạn sẽ hiển thị trong cửa sổ Explorer hoặc Finder dưới dạng ổ cứng với ký tự này. Chọn E: hoặc F: hoặc bất cứ điều gì bạn thích.



Nếu bạn tạo ra toàn bộ một ổ cứng hoặc USB, chỉ cần nhấp vào Select Device, và từ cửa sổ bật lên chọn ổ cứng hoặc USB. Trong hộp mật khẩu hiển thị, nhập mật khẩu. Mật khẩu đơn giản sẽ tự động mở ra Outer volume. Mật khẩu nâng cao hơn sẽ mở ra Inner volume. Nếu có bị ép hoặc buộc phải cung cấp không gian mã hóa của bạn, bạn chỉ cung cấp mật khẩu cho Outer volume

Nếu bạn chọn To create a file container, nhấn vào Select File và tìm tệp bạn đã tạo để mã hóa. Một lần nữa, nếu bạn nhập mật khẩu đơn giản nó sẽ tự động mở Outer volume. Mật khẩu nâng cao hơn sẽ mở ra Inner volume.

Ngoài ra còn có nút Auto-mount Devices. Nhấp vào nút này sẽ tự động xác định bất cứ thứ gì có thể được gắn kết và yêu cầu bạn nhập mật khẩu. Phần còn lại hoạt động cùng một mật khẩu đơn giản cho Outer volume và mật khẩu mạnh cho Inner volume. Thật không may chức năng Auto-mount không phải lúc nào cũng hoạt động và có thể mất một chút thời gian để tải, nhưng nếu có, đó là cách đơn giản nhất để mở ra phần mã hóa của bạn.

Sau khi mở phần mã hóa, bạn có thể đóng chương trình và làm việc như bạn đã quen.

Khi bạn hoàn thành công việc của mình, hoặc không còn cần phải truy cập vào các tệp công việc của bạn, hoặc bạn sắp rời khỏi máy tính, hãy bắt đầu chương trình và chọn Dismount all. Thao tác này sẽ đóng ổ đĩa được mã hóa (và nó sẽ không còn hiển thị trong cửa sổ Explorer hoặc Finder nữa).

Trong tương lai, bạn chỉ cần thao tác mount và dismount.

NHỮNG BƯỚC CUỐI CÙNG

Khả năng từ chối truy cập vào mã hoá ẩn thực (Inner volume) là chìa khóa để bảo vệ chính bạn. Tuy nhiên, để làm việc, nó phải là đáng tin cậy. Có thể tin ở đây có nghĩa là thông tin trong Outer volume- mồi, phải là thứ mà bạn rõ ràng là không muốn chia sẻ. Một khi bạn buộc phải mở Outer volume, khi cảnh sát, bọn tội phạm hoặc bất cứ ai đó, thấy vật liệu trong đó, họ phải tin rằng đây là những gì bạn đang bảo vệ. Nếu trống rỗng, hoặc chỉ chứa âm nhạc, thì rõ ràng họ sẽ hiểu được đây không phải là điều họ đang tìm kiếm và tiếp tục gây áp lực cho bạn.

Vì vậy, sau khi thiết lập, mất một thời gian để đảm bảo đặt trong Outer volume rất nhiều tập tin nhạy cảm, nhưng không phải là rất nhạy cảm. Bạn phải đặt thông tin có vẻ nhạy cảm ở đây. Ví dụ: bạn có thể lưu trữ một số tài liệu ngân hàng, các tệp phương tiện vi phạm bản quyền hoặc tệp PDF của một cuốn sách đen. Bạn cũng cần đặt một số tệp công việc ở đây, ví dụ như các báo cáo, tài liệu bạn đã viết, hoặc các tệp liên quan đến công việc mà bạn đã tải xuống. Bạn sẽ đặt các bản sao của các tập tin này ở đây, nhưng sẽ không cần phải sử dụng chúng. Mỗi một lần trong một thời gian bạn nên thêm một số tài liệu mới vào Outer volume do đó nó xuất hiện như nó vẫn còn sử dụng.

Nếu một tình huống phát sinh với mối quan tâm về an ninh cao hơn, hãy sao chép một vài tệp công việc vào Outer volume ngoài. Tuy nhiên, các tài liệu thực sự nhạy cảm không nên đặt ở đây. Đây chỉ là một cái mồi. Mồi là để ném cho cảnh sát hoặc bọn tội phạm để chúng không đi tìm thông tin nhạy cảm thực sự của bạn.

Lý do bạn cần cập nhật Outer volume đôi khi là tất cả các tệp và thư mục đều có dấu thời gian khi tệp được di chuyển, thay đổi, chỉnh sửa lần cuối. Nếu họ truy cập vào Outer volume của bạn và thấy rằng không có tài liệu nào được thay đổi trong hai năm, họ có thể nhận ra rằng bạn không sử dụng nó, và tiếp tục gây sức ép để biết thêm thông tin.

Cách dễ nhất để tạo ra hệ thống này là di chuyển tất cả các tệp công việc của bạn đến Inner volume. Sau đó, bạn có thể sử dụng một số thông tin không quá nhạy cảm và đưa vào Outer volume. Một lần nữa, chọn các tệp tin của bạn, nhưng không nhạy cảm và không chứa tên, chi tiết hoặc gây hại cho người khác, v.v ...

Bởi vì Outer volume này phải đáng tin cậy, chúng tôi cũng khuyên bạn nên đặt bất cứ thứ gì thường được coi là nhạy cảm hoặc cá nhân. Các ví dụ bổ sung bao gồm:

Nhiều người lưu trữ một danh sách mật khẩu cho những thứ không nhạy cảm, như thông tin đăng nhập vào các trang web mua sắm trực tuyến, phương tiện truyền thông xã hội chỉ để sử dụng cá nhân vv Nếu có, hãy đặt nó ở đây.

- Có lẽ từ quá khứ của bạn, bạn đã viết rất nhiều thư cá nhân hoặc tài liệu, về các vấn đề sâu sắc và cá nhân. Nếu vậy, đặt nó ở đây.
- Có lẽ bạn đã chia sẻ thông tin cá nhân, ảnh và thư với người yêu. Nếu vậy, đặt nó ở đây.

Nói tóm lại, Outer volume này sẽ rất an toàn theo ý nghĩa bình thường và chỉ bị đe doạ nếu cảnh sát hoặc bọn tội phạm buộc bạn phải mở nó. Nếu mọi thứ trở nên nghiêm trọng đến mức chúng buộc bạn đưa ra các mật khẩu như thế này, hãy chuẩn bị để xem và đọc các vấn đề cá nhân như

vậy và nhận ra rằng cho phép điều này sẽ giúp bạn lâu hơn bằng cách làm cho họ tin rằng bạn thật sự không lưu thông tin bí mật nào.

Để có thể tin được, đừng sử dụnh mật khẩu cho Outer volume một cách đơn giản. Bạn vẫn nên cưỡng lại nếu bị tra hỏi, nếu không kẻ thù có thể trở nên nghi ngờ. Nếu họ tin bạn, thông tin nhạy cảm thực sự của bạn sẽ được an toàn. Và có, không ai muốn cảnh sát, một tên tội phạm hoặc một kẻ bắt cóc nhìn thấy những bức ảnh bạn chụp từ chính mình và gửi cho người yêu, nhưng so với hình phạt tù, sự lựa chọn nên đơn giản. Trên thực tế, nếu bạn không có loại thông tin cá nhân nào đề cập ở trên, khuyên bạn nên tạo ra nó ngay bây giờ và đặt ở đó, giả mạo nó nếu cần. Thiết lập này có thể có nghĩa là sự khác biệt giữa tự do và giam cầm.

KHÔNG DÙNG Ổ ẢO RẤT NGUY HIỂM

Một nhà hoạt động nhân quyền và nhà báo mới bị bắt cóc và đánh đập, và bị tịch thu điện thoại cùng máy tính. Do bị đánh đập và đe doạ nên người này phải cung cấp mật khẩu máy tính cho an ninh để họ lấy hết tài liệu có trong đó.

Trước đó, người này đã thu thập một số thông tin về nhiều nhà hoạt động khác. Tuy nhiên, do chủ quan nên người này không lưu thong tin vào ổ ẩn nên cảnh sát truy cập được vào tất cả tài liệu có trong máy tính.

Một thời gian trước khi bị bắt, người này nhận được một số hướng dẫn về bảo mật, bao gồm cách lưu trữ tài liệu trong ổ ảo cũng như cách xoá tài liệu một cách an toàn, tuy nhiên, do chủ quan và lười biếng nên không chịu đọc tài liệu để áp dụng.

Đây là một bài học cho những người hoạt động khác ở Việt Nam.

LƯU TRỮ THÔNG TIN

Một nhà hoạt động nhân quyền và bất đồng chính kiến đã bị bắt đầu năm 2017 và sau đó bị kết án gần 10 năm.

Khi bị bắt, công an đã tịch thu được laptop của cô và có lẽ có thu được một số tài liệu trong đó vì cô cũng chưa biết cách lưu trữ thông tin vào ổ ảo.

Cô có một cách bảo mật rất đặc biệt: đặt một chậu nước gần bàn làm việc và dự định ném laptop vào chậu nước nếu thấy nguy hiểm. Tuy nhiên, hôm bị bắt, vì một lý do nào đó mà cô không kịp ném laptop vào chậu nước.

Cô có sử dụng nhiều trang mạng xã hội như blog, youtube và Facebook nhưng cô để một người khác quản lý mật khẩu nên cho dù bị bắt, những tài khoản của cô vẫn được giữ bí mật đối với cảnh sát.

Bài học: đặt mật khẩu mạnh cho những tài khoản cá nhân và có thể, cho một người tin cẩn khác biết và quản lý cùng. Khi mình có vấn đề, thì người kia có thể thay đổi mật khẩu cho những tài khoản đó để tránh bị công an khai thác và truy cập.

Ổ ẢO VÀ KHÔI PHỤC FILE

Một luật sư nhân quyền có kinh nghiệm đã nhận được một tin nhắn từ Telegram từ một đồng nghiệp tin cậy rằng cảnh sát đã hỏi về cô và cô có thể bị giam giữ hoặc ít nhất bị thẩm vấn.

Cô luật sư này đã bảo vệ cho nhiều trường hợp và làm việc với nhiều luật sư nhân quyền trong nhiều năm. Cô tương đối giỏi về an ninh mạng vì luôn ý thức được rằng cảnh sát có thể bắt giữ cô hoặc thu máy tính và sử dụng thông tin trong đó để kết tội cô hoặc những người cùng hoạt động. Do vậy, cô ít khi sử dụng mạng xã hội. Cô thậm chí còn biết mã hoá ẩn và sử dụng trước đó một năm để giấu tài liệu.

Tuy không phải là nhà báo có nhiệm vụ bảo vệ nguồn tin bí mật nhưng cô có nhiều thông tin về cả khách hàng của chính mình và thông tin nhạy cảm liên quan đến công việc của người khác. Nếu những thông tin này rơi vào tay cảnh sát có thể bị sử dụng để chống lại cô và người khác. Đảm bảo tài liệu chắc chắn đã không rơi vào tay của cảnh sát là một vấn đề quan trọng đối với cô, và cho sự an toàn của đồng nghiệp và khách hàng.

Cô đã có đủ thông minh để nhận ra rằng mã hóa thông thường sẽ được giúp đỡ rất ít. Nếu cảnh sát biết phải hỏi gì, cô ấy nghi ngờ rằng cô ấy sẽ có thể kháng cự lâu dài, vì là một luật sư, cô hiểu rằng tra tấn và ngược đãi rất phổ biến ở nước mình dù bị cấm bởi luật pháp.

Với ý thức đó, cô học cách mã hoá ẩn cho dù ban đầu mất khá nhiều thời gian để tìm hiểu.

Cảnh sát bắt giữ cô và thẩm vấn hơn một tháng, tịch thu máy tính, điện thoại, và USBs.

Sau vài ngày bị giam giữ, cô ấy đã rất ngạc nhiên khi cảnh sát bắt đầu bắt đầu mỗi ngày mới bằng cách trưng ra những tài liệu của cô trong máy tính. Cô biết những tài liệu này đã được lưu giữ trong không gian mã hóa trên ổ cứng của cô mà cảnh sát hoàn toàn không có quyền truy cập. Cô cũng chưa bị cảnh sát thẩm vấn về ổ ảo này và mật khẩu còn là bí mật với cảnh sát vì cảnh sát chưa biết sự tồn tại của ổ ảo.

Trước khi bị giam, cô đã trao đổi các biện pháp bảo mật với các đồng nghiệp.

Cô suy nghĩ hằng đêm về việc tại sao cảnh sát lại có những thông tin như thế.

Cô nhận thấy tài liệu mà cảnh sát đưa ra rất ngẫu nhiêu, và chỉ ít trong số đó là nhạy cảm. Nhiều trong số tài liệu đó chỉ là một phần của những tài liệu lớn hơn.

Thật may mắn là cảnh sát không thể tiếp cận được với những thông tin đặc biệt nhạy cảm.

Sau khi được trả tự do nhưng cảnh sát có thể bắt lại bất cứ lúc nào, cô đã tìm hiểu và nhận ra rằng những thông tin mà cảnh sát trưng ra chính là lấy từ máy tính bằng cách khôi phục những file mà cô đã xoá nhưng không xoá triệt để.

Nếu không áp dụng các biện pháp đặc biệt thì tài liệu bị xoá vẫn còn tồn tại trên máy và có thể được khôi phục bằng một chương trình đơn giản

CHƯƠNG 6
CHIA SẺ THÔNG TIN

Giao tiếp an toàn qua email là một vấn đề quan trọng đối với nhiều người và chương này sẽ chỉ ra cách sử dụng email an toàn và cách sử dụng nó theo cách bảo vệ bạn, nếu có một mối đe dọa nghiêm trọng phát sinh

Chương này sẽ giải quyết chủ yếu bằng email, vì nó có thể là phương tiện truyền thông chủ yếu trong công việc của bạn. Trò chuyện, tin nhắn SMS và truyền thông di động sẽ được đề cập trong Chương 11: Các ứng dụng an toàn, ngoại trừ một số ghi chú về việc sử dụng các chương trình chat trên máy tính. Chương này sẽ thảo luận về mã hóa email, trình bày một số tùy chọn để sử dụng các trang webmail có mã hoá tự động.

Mã hóa rất hữu ích nhưng nó có thể trở nên quá phức tạp đối với hầu hết các tình huống. Vì lý do này chương này không bao gồm thông tin về mã hóa PGP. Không mã hóa nào có thể giúp bạn một khi bạn đã bị bắt giữ và bị buộc phải khai mật khẩu.

Nếu bạn muốn an toàn, phần quan trọng nhất là sử dụng trình duyệt công việc đúng cách để họ không thể biết bạn sử dụng dịch vụ email nào và sử dụng Chính sách Hộp thư đến trống không, vì vậy nếu họ tìm thấy email của bạn và lấy được mật khẩu của bạn thì không có gì để tìm.

MÃ HÓA SO VỚI "MÃ HOÁ HAI ĐẦU"

Cần phải hiểu và phân biệt hai khái niệm này.

Mã hóa 'bình thường' có nghĩa là dịch vụ bạn đang sử dụng, ví dụ như Gmail, mã hóa dữ liệu của bạn, trong trường hợp này, là email. Điều này có nghĩa là bạn cần phải gửi email đến các máy chủ của Google, sau đó mã hóa nó, và gửi chuyển tiếp tới người nhận. Có hai vấn đề ở

đây. Thứ nhất, ISP của bạn có thể đọc dữ liệu khi bạn gửi nó tới Google (trừ khi bạn sử dụng VPN hoặc TOR). Hai, điều này có nghĩa là nhà cung cấp dịch vụ (Google), mã hóa nó cho bạn. Điều này cũng có nghĩa là họ có thể giải mã. Bạn có thể tin cậy Google, nhưng bạn có thể tin tưởng vào một công ty địa phương ở Việt Nam, có thể dễ dàng bị buộc phải giải mã dữ liệu của bạn nếu cảnh sát yêu cầu?

Dịch vụ cung cấp mã hoá hai đầu có nghĩa là dữ liệu được mã hóa trên thiết bị của bạn, ví dụ điện thoại hoặc máy tính của bạn. Dữ liệu này sau đó sẽ gửi đến người nhận, người sẽ giải mã bằng điện thoại hoặc máy tính của họ. Điều này có nghĩa là ISP của bạn không thể theo dõi bạn, và nhà cung cấp dịch vụ không thể biết dữ liệu có chứa gì (như tin nhắn trò chuyện, email ...). Sử dụng mã hóa hai đầu rất quan trọng và luôn luôn được sử dụng nếu có như là một lựa chọn. Trong trường hợp này, ngay cả khi một công ty muốn theo dõi bạn, hoặc chính phủ buộc họ cung cấp thông tin, họ cũng không thể, bởi vì họ không mã hóa, và do đó không thể giải mã nó.

SỬ DỤNG EMAIL AN TOÀN

Để tiện lợi và an toàn thì bạn nên sử dụng một dịch vụ của một webemail an toàn và dễ sử dụng. Thứ hai, đó là sử dụng một webmail cung cấp mã hóa hai đầu, và cuối cùng, webmail đó không có máy chủ ở Việt Nam.

Bạn nên tránh sử dụng ứng dụng trên máy tính (hoặc điện thoại) để truy cập các email này, chỉ truy cập qua trình duyệt công việc của bạn. Bạn cũng nên tránh sử dụng ứng dụng thư trên máy tính của mình.

Khi bạn thiết lập một webmail an toàn theo lựa chọn của bạn, hãy đảm bảo không sử dụng tên hoặc biệt hiệu của bạn dưới tên của địa chỉ email. Việc sử dụng tên của bạn trong tài khoản email chỉ làm cho người ngoài dễ dàng xác định tài khoản email nào thuộc về bạn.

Ngoài việc sử dụng một trong các dịch vụ email an toàn mà chúng tôi trình bày dưới đây, chúng tôi khuyên bạn nên thiết lập một email Gmail. Nó cung cấp bảo mật tương đối mạnh, đặc biệt nếu bạn bật xác minh 2 bước và giữ Chính sách hộp thư đến trống trơn và có thể được sử dụng rất dễ dàng và hiệu quả cho phần lớn công việc của bạn mà không phải là rất nhạy cảm. Tuy nhiên, bạn sẽ cần một email an toàn hơn cho công việc nhạy cảm hơn qua email của bạn, và tốt hơn là một trong những tính năng bảo mật bổ sung.

Có một số webmail bảo mật với mã hóa hai đầu. Có lẽ tốt nhất, với các tính năng bảo mật bổ sung, là ProtonMail.com. Ngoài ra có Tutanota.com và Hushmail.com. Hiện tại không có giao diện tiếng Việt nào. Tuy nhiên, chúng dễ sử dụng, với giao diện sạch sẽ và dễ dàng, và bạn có thể nhanh chóng học cách sử dụng chúng ngay cả khi bạn không đọc tiếng Anh.

Hầu hết các nhà cung cấp dịch vụ email và hệ thống mã hóa đều không mã hóa dòng chủ đề. Hãy nhớ điều này, vì hầu hết các email được mật mã sẽ vẫn hiển thị tiêu đề / chủ đề mà bạn đã viết. Tốt nhất nên chọn một chủ đề bí ẩn mà sẽ không thu hút sự chú ý.

Nhược điểm của các webmail bảo mật đã đề cập ở trên là chúng chỉ cung cấp sự độ bảo mật tối đa khi giao tiếp giữa các tài khoản nội bộ. Điều đó có nghĩa là nếu bạn sử dụng email

ProtonMail, người bạn gửi email cũng nên sử dụng ProtonMail. Như vậy, trước khi thiết lập một email an toàn mới, bạn nên trao đổi với những người bạn thường xuyên email, bạn bè, đồng nghiệp, đối tác ... Bằng cách này, bạn có thể quyết định sử dụng cùng một dịch vụ.

Ngoài ra còn có cách để gửi các email bảo mật từ webmail an toàn này tới email thông thường, nơi bạn chỉ cần điền vào một mật khẩu mà người nhận cần phải biết để đọc chúng. Hơn nữa, ProtonMail được đề xuất, bao gồm cả email tự hủy, được thiết lập để hẹn giờ, để bạn có thể gửi email cho những người khác hoặc những người mà bạn không chắc chắn nếu họ an toàn, và email sẽ tự động phá hoại cả từ email của bạn và email của họ - và công việc này thậm chí không phải là ProtonMail.

Tóm lại, việc thiết lập và học cách sử dụng một trong những email an toàn này rất quan trọng.

Chúng tôi khuyên bạn nên không cài đặt bất kỳ Ứng dụng Điện thoại nào cho những email này, đặc biệt không dành cho bất kỳ ứng dụng nào không có bảo vệ mật khẩu. Có một ứng dụng cài đặt trên điện thoại của bạn có nghĩa là bất cứ ai truy cập vào điện thoại của bạn biết bạn sử dụng dịch vụ email nào. Nếu bản thân ứng dụng không phải có mã PIN hoặc mật khẩu bảo vệ, người khác cũng có thể truy cập vào hộp thư đến của bạn. Tất cả chúng ta đều rất dũng cảm, nhưng khi bị cảnh sát, các nhân viên an ninh hoặc bọn tội phạm yêu cầu, bạn khó có thể từ chối cung cấp mật khẩu này. Sự nguy hiểm của các ứng dụng được thảo luận thêm trong phần III (Bảo mật Điện thoại) của hướng dẫn này.

Sau khi bạn thiết lập một trong những email này, hãy nhập khu vực cài đặt và tự làm quen với các tùy chọn, nhưng không cần thay đổi vì chúng được thiết lập cho bảo mật ở mức cao lúc bắt đầu. Giải pháp kỹ thuật: Sử dụng ProtonMail và gửi email "bình thường" sẽ hiển thị cho bạn giao diện của ProtonMail, và cách gửi tin nhắn tự động phá hủy và email an toàn cho các email "bình thường" khác.

Hơn nữa, việc chèn "Gửi thông tin an toàn" trên các trang XX-XX sẽ rất hữu ích đối với nhiều độc giả, và cũng dựa trên ProtonMail như một giải pháp.

IMAP VÀ EMAIL CLIENTS

Chúng tôi khuyên bạn nên không sử dụng bất kỳ ứng dụng thư nào, chẳng hạn như Outlook, Mail hoặc Thunderbird cho email an toàn của bạn. Không có tùy chọn đáng tin cậy để khóa quyền truy cập vào các chương trình này bằng mã PIN hoặc mật khẩu (chúng có lỗi và không an toàn), những email bảo mật liệt kê ở trên không hỗ trợ sử dụng các ứng dụng email. Nó đi kèm thêm một rủi ro bảo mật không cần thiết và việc thực hiện Chính sách Hộp thư đến trống trơn không giúp ích cho việc bảo mật. Việc cài đặt email trong một chương trình trên điện thoại hoặc máy tính của bạn cũng có nghĩa là bất cứ ai đã biết bạn sử dụng email nào và có thể ép buộc bạn cung cấp mật khẩu. Chúng ta đã nói về việc sử dụng một ứng dụng thư trên máy tính hoặc điện thoại của bạn, cụ thể là cách giấu các tài liệu và đảm bảo rằng người khác không thể hiểu được bạn sử dụng những gì.

BỐN HÀNH VI CHÍNH

CHÍNH SÁCH HỘP THƯ ĐẾN TRỐNG (XÓA HẾT THƯ SAU KHI ĐÃ ĐỌC XONG)

Như đã nêu ra nhiều lần, mối đe dọa chủ yếu đối với email của bạn sẽ không xuất phát từ cuộc tấn công nâng cao nhưng là từ người nào đó buộc bạn phải cung cấp mật khẩu cho họ. Nếu được thực hiện, rất có thể là cảnh sát sẽ truy cập vào email của bạn. Do vậy, thực hiện Chính sách Hộp thư đến trống quan trọng nhất cho sự an toàn của bạn.

> "Chính sách Hòm thư trống là một trong những công cụ quan trọng nhất để giữ cho bạn an toàn"

Giả sử rằng email của bạn sẽ bị truy cập bởi kẻ khác nhưng nếu bạn đã thực hiện Chính sách Hộp thư đến trống thì họ không có gì để đọc cả. Tóm lại, giữ hộp thư đến của bạn (và các thư mục khác) trống. Trong 99% thời gian, điều này không gây ra bất kỳ vấn đề nào vì hầu hết các email không cần được lưu trữ lâu dài. Không thể nhấn mạnh đủ mức độ quan trọng của chính sách này. Tương tự như vậy, đảm bảo rằng đồng nghiệp hoặc bạn bè của bạn cũng làm như vậy.

KHÔNG SỬ DỤNG CHỨC NĂNG REPLY/TRẢ LỜI

Thay vì trả lời vào thư gửi đến, bạn nên trả lời bằng một thư mới không có nội dung thư đến. Đây là sự mở rộng của Chính sách hộp thư đến trống.

Nếu thực sự email của bạn bị truy cập bởi người lạ, người bắt giữ bạn có thể đợi cho đến khi bạn nhận được email mới và đọc tất cả các thông tin liên lạc trước đó và có thể khai thác thông tin có thể được dung để buộc tội. Điều này là do cách chúng ta thường xuyên xử lý email. Khi chúng ta giao tiếp, chúng ta thường nhấp vào "Reply/Trả lời" vào một email hiện có, thay vì viết một email mới. Với điều này, giao tiếp trước đó được đưa vào email trả lời. Thường thì việc sử dụng trả lời này có thể kéo dài trong một thời gian dài và do đó, một email mới ngắn có thể bao gồm một danh sách dài các email trước đó. Điều này có nghĩa là nếu email của bạn bị xâm nhập, người có trách nhiệm chỉ có thể đợi ai đó gửi email cho bạn bằng cách sử dụng chức năng trả lời và xem thông tin trước đó của bạn.

Như vậy, khi bạn trả lời email cho đồng nghiệp hoặc bạn bè, hãy tránh sử dụng chức năng Reply/Trả lời, hoặc nếu bạn làm như vậy, hãy chắc chắn xóa văn bản gốc. Nói với bạn bè của bạn, dạy họ những điều tương tự. Điều này đảm bảo rằng sau khi bị tạm giam, khi cảnh sát đang truy cập vào email của bạn, bất kỳ email mới nào đến sẽ chứa càng ít thông tin trở lại càng tốt.

TRUY CẬP VÀO ỨNG DỤNG

Mặc dù Win10 bây giờ cho phép cài đặt ứng dụng, giống như trên điện thoại, chúng tôi khuyên bạn không nên sử dụng các ứng dụng như vậy. Để bắt đầu, hầu hết không có mật khẩu gốc (được cài sẵn) hoặc bảo vệ mã PIN, nghĩa là bất kỳ ai truy cập vào máy tính của bạn đều có thể mở giao diện ứng dụng hạn chế và đọc tin nhắn, thực hiện cuộc trò chuyện, lịch, email, hoặc gửi , giả vờ làm bạn. Việc cài đặt ứng dụng cũng cho thấy rõ bạn đang sử dụng những dịch vụ nào và bạn sẽ mất khả năng tự bảo vệ mình nếu bạn bị giam giữ.

LƯU TRỮ ĐÁM MÂY

Lưu trữ trên đám mây thường dùng để chỉ lưu trữ thông tin trực tuyến. Một số dịch vụ đám mây rất chặt chẽ để sao lưu các tài liệu, trong khi một số lưu trữ và cập nhật cài đặt và chương trình máy tính. Những người khác hoạt động như một nền tảng hợp tác, cho phép bạn chia sẻ tài liệu của bạn với người khác và đồng thời chỉnh sửa các tài liệu đó. Nói chung, mọi thứ được lưu trữ trực tuyến ít an toàn hơn. Vì lý do này, không bao giờ sử dụng các dịch vụ như OneDrive dành cho Windows, iCloud for Mac hoặc Google Drive cho bất kỳ mục đích công việc nhạy cảm nào.

	Dung lượng cần	Mã hoá hai đầu	Dung lượng được mã hoá	Mã PIN	Xác minh hai bước
Google Drive	15GB	Không	Có, nhưng không mạnh	Không	Có
iCloud	5GB	Không	Có, nhưng không mạnh	Không	Có
One Drive	5GB	Không	Không	Có	Có
Dropbox	2GB	Không	Có	Có	Có
SpideroakONE	2GB	Có	Có	Có	Không
Tresorit	5GB	Có	Có	Có	Có

Điều đó nói rằng, các dịch vụ đám mây không phải là xấu và có thể được sử dụng an toàn nếu bạn biết bạn đang làm gì.

Bạn chắc chắn có dịch vụ lưu trữ trên đám mây, ngay cả khi bạn không biết đến chúng. Ví dụ: nếu bạn có Gmail, bạn cũng có Google Drive. Nếu bạn có một máy tính Mac, bạn có iCloud, và nếu trên hệ thống Windows hoặc bạn sử dụng Hotmail, bạn có OneDrive. Nhiều dịch vụ đám mây được cài đặt sẵn bằng điện thoại và máy tính của bạn.

Trọng tâm của bạn, nếu bạn cần dịch vụ đám mây, là nên sử dụng dịch vụ cung cấp bản sao lưu các tệp bạn chọn cụ thể. Các chương trình này sẽ chạy dưới nền trên máy tính và điện thoại của bạn và bất kỳ khi nào bạn thay đổi tài liệu của mình, lưu trữ trên đám mây sẽ được cập nhật. Do đó, bạn có thể sao lưu dự phòng trong trường hợp bạn bị mất máy tính hoặc điện thoại, hoặc bị tịch thu. Nhưng nó cũng có nghĩa là lưu trữ trên đám mây của bạn là một cách khác để ai đó có thể truy cập vào thông tin của bạn và do đó cần được bảo vệ.

Thứ nhất, bạn nên kiểm tra điện thoại và máy tính của mình và xem các dịch vụ nào đã được bật

và những ứng dụng nào được cài đặt. Đối với những phần mà bạn không sử dụng thì bạn nên vô hiệu hóa. Điện thoại đặc biệt được cấu hình sẵn để lưu cài đặt cá nhân của bạn cũng như ảnh, video và tài liệu tự động. Điều này có thể rất nguy hiểm, đặc biệt là vì hầu hết các dịch vụ này có thể được truy cập trên điện thoại mà không cần phải nhập tên người dùng hoặc mật khẩu thông qua ứng dụng tương ứng của chúng. Xóa/gỡ cài đặt mọi dịch vụ đám mây bạn sẽ không sử dụng.

Thứ hai, phù hợp với những gì đã được che đậy về việc giấu thông tin của bạn, bạn không nên dựa vào các ứng dụng để truy cập vào bộ lưu trữ đám mây của bạn. Ứng dụng rất dễ sử dụng, nhưng đặt ra những rủi ro thực sự. Bất cứ ai lấy điện thoại hoặc máy tính của bạn sẽ dễ dàng nhìn thấy dịch vụ bạn đang sử dụng, và họ có thể buộc bạn phải cung cấp mật khẩu và/hoặc tên người dùng. Có rất ít ích lợi trong việc sử dụng mã hoá ẩn để lưu trữ dữ liệu công việc của bạn nếu bạn không thực hiện các bước để bảo vệ thông tin tương tự được lấy ra từ lưu trữ đám mây trực tuyến của bạn. Chỉ truy cập các dịch vụ đám mây của bạn trong trình duyệt công việc, thông qua VPN của bạn. Chúng tôi khuyên bạn nên sử dụng SpiderOAK hoặc Tresorit, nhưng có nhiều tùy chọn khác, và nếu bạn yêu cầu sử dụng một công ty lưu trữ trên đám mây, bạn sẽ phải tìm kiếm google để tìm các tùy chọn thích hợp cho bạn.

Một số dịch vụ đám mây sẽ chạy một quy trình ở chế độ nền để tự động tải các tài liệu mới và những thay đổi được thực hiện trong khi làm việc. Điều này không được khuyến khích. Đối với những dịch vụ đám mây khác, bạn phải tự nhập dịch vụ đám mây và tải lên các tài liệu bạn muốn lưu trực tuyến. Chúng tôi khuyên bạn nên thực hiện điều này, vì nó cho phép bảo vệ và che giấu sự lựa chọn dịch vụ của bạn từ bất kỳ ai truy cập vào điện thoại hoặc máy tính của bạn. Với tình hình hiện tại, không bao giờ sử dụng dịch vụ lưu trữ đám mây được cung cấp bởi một công ty Việt Nam.

KHÔNG SỬ DỤNG CHỨC NĂNG TỰ ĐỘNG ĐĂNG NHẬP VÀ NGUY CƠ ĐĂNG NHẬP CHÉO QUA NHIỀU DỊCH VỤ

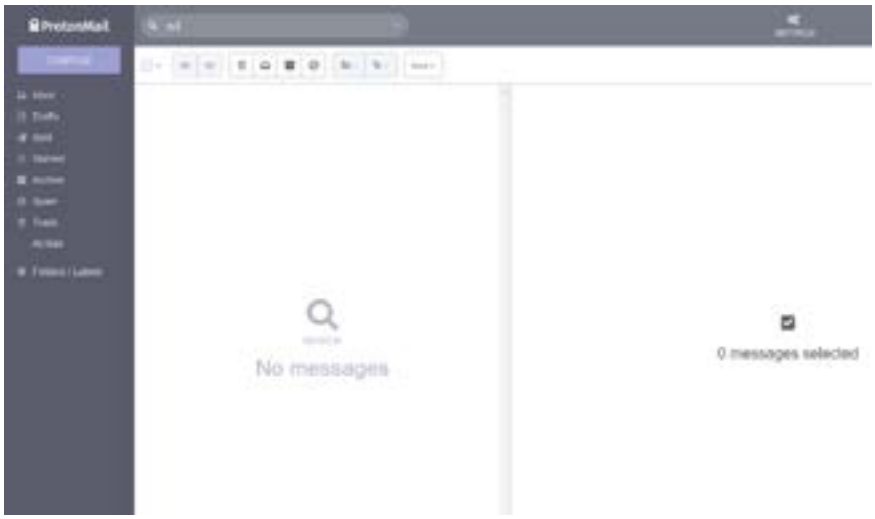
Đăng nhập tự động có thể là một mối đe dọa thực sự, đặc biệt là kể từ khi truy cập vào một tài khoản có thể cho phép người khác truy cập vào các tài khoản khác của cùng một nhà cung cấp. Ví dụ: nếu bạn đăng nhập vào gmail của mình trong trình duyệt, bạn có thể tự động sử dụng các dịch vụ khác của Google mà không phải đăng nhập, như Google Drive (lưu trữ trên đám mây), Youtube, vv. Tương tự với nhóm dịch vụ cung cấp bởi Apple, Windows và nhiều công ty khác.

Cách tốt nhất để tránh điều này là chỉ sử dụng một dịch vụ từ bất kỳ công ty nào. Nếu bạn sử dụng Gmail, không sử dụng Google Drive cho lưu trữ đám mây, v.v. Điều này sẽ chặn nguy cơ tự động đăng nhập và đồng bộ hóa tài khoản. Đối với trình duyệt công việc của bạn, không bao giờ 'đăng nhập' bằng bất kỳ tài khoản nào, mà nhiều người thường áp dụng trên Chrome và Firefox. Việc truy cập nhanh vào các tài khoản khác nhau mang lại tiện ích cho người dùng nhưng cũng sẽ giúp cảnh sát hoặc bọn tội phạm truy cập nhanh như thế.

Các dịch vụ cũng giống như tự động đồng bộ vào những ngày này. Nếu bạn sử dụng Google Chrome trên Điện thoại của mình và bạn đăng nhập vào trình duyệt Google Chrome trên máy PC hoặc MAC, thì tự động đồng bộ hóa sẽ cho phép đồng bộ hóa hai trình duyệt khác nhau từ hai thiết bị khác nhau. Dấu trang được lưu trong Chrome trên PC hoặc MAC sẽ hiển thị trên Chrome trên điện thoại của bạn, cùng với lịch sử duyệt web, mật khẩu đã lưu và hơn thế nữa. Đây là một vấn đề lớn. Không đăng nhập vào trình duyệt công việc của bạn.

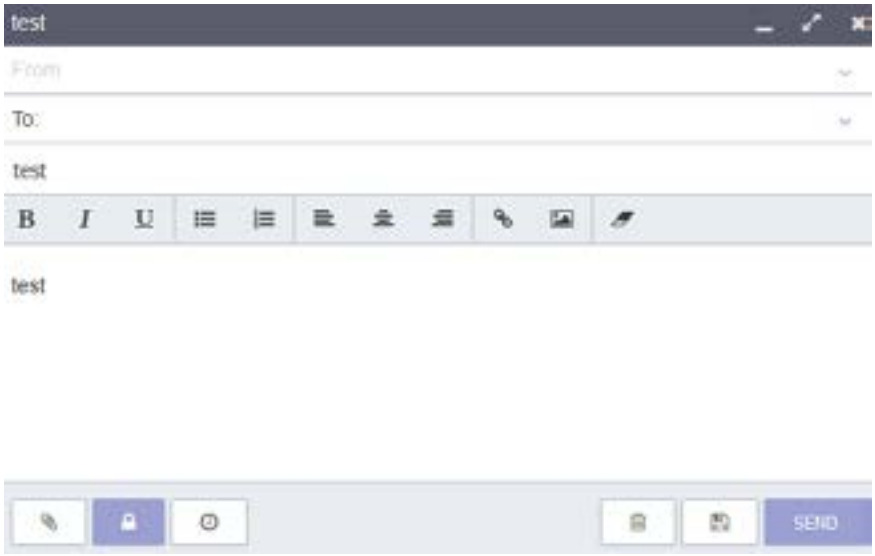
GIẢI PHÁP KỸ THUẬT: SỬ DỤNG PROTONMAIL VÀ GỬI ĐẾN EMAIL "BÌNH THƯỜNG"

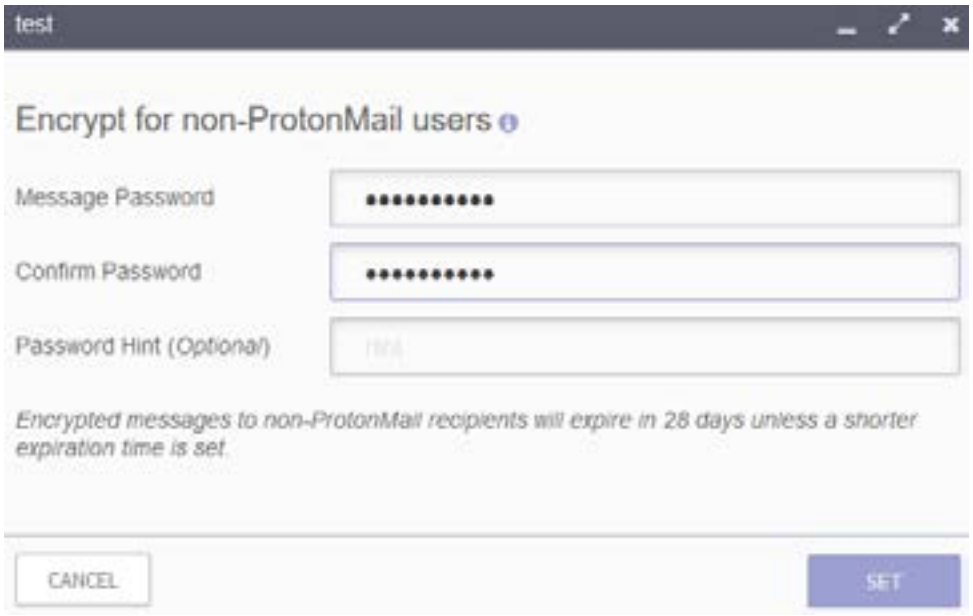
Sử dụng các webmail bảo mật này là đơn giản và không cần phải giải thích nhiều. Tuy nhiên, do các hạn chế về ngôn ngữ, các ảnh chụp màn hình bên dưới cho giao diện chính sẽ được giải thích. Để học cách sử dụng, đăng nhập vào email và làm quen, và bạn sẽ dễ dàng có thể sử dụng ProtonMail mà không gặp khó khăn nào. Nếu bạn chọn Tutanota hoặc Hushmail, cả hai đều hoạt động tương tự.

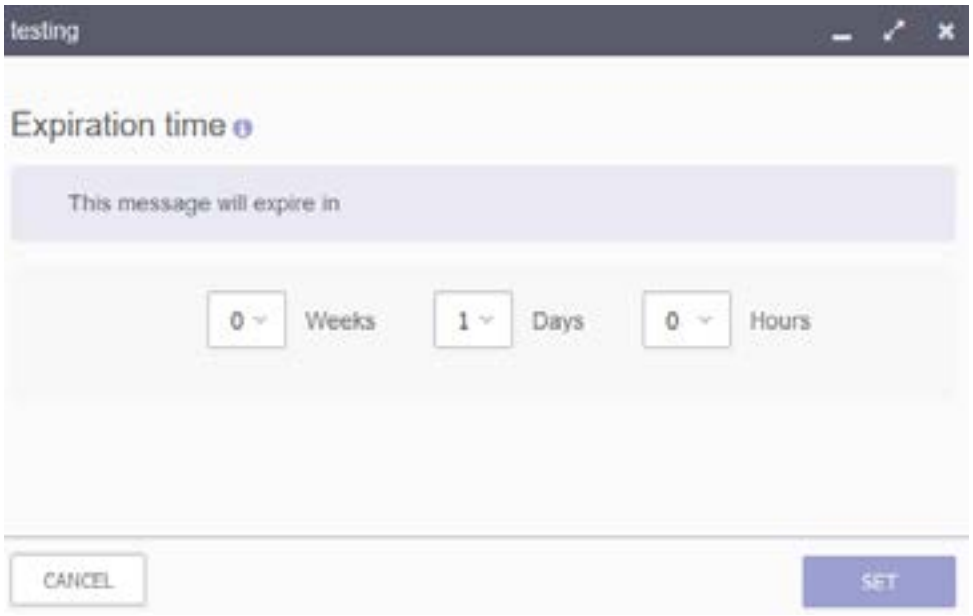


Nếu bạn muốn sử dụng ProtonMail (S-W / OXX) để gửi một tin nhắn đến một email bình thường, ví dụ như Gmail, bạn phải chọn và viết mật khẩu. Khi bạn gửi email, người nhận sẽ không nhận được email, thay vào đó họ nhận được một liên kết (trong hộp thư email của mình). Khi họ nhấp vào liên kết này, họ sẽ được yêu cầu nhập mật khẩu bạn đặt để có thể đọc nó (và trả lời email).

Do đó, sau khi bạn gửi email cho ai đó, bạn cần sử dụng một ứng dụng trò chuyện bảo mật để cung cấp cho họ mật khẩu hoặc bạn có thể đã đồng ý về một mật khẩu chuẩn trước. Chúng tôi khuyên bạn nên gửi mật khẩu qua tín hiệu hoặc điện tín có chức năng tự hủy, có thể tham khảo thêm ở Chương 11: Các ứng dụng an toàn để sử dụng trong Phần III (Bảo mật Điện thoại).







Khi bạn thực hiện việc này, hoặc thậm chí bạn chỉ gửi email cho một ProtonMail khác, bạn cũng có thể đặt một bộ đếm thời gian tự hủy, do đó email sẽ tự động bị hủy và nó sẽ bị phá hủy cả cho người gửi và người nhận, cũng rất mạnh. Các ảnh chụp màn hình và văn bản dưới đây sẽ chỉ ra cách sử dụng các chức năng này.

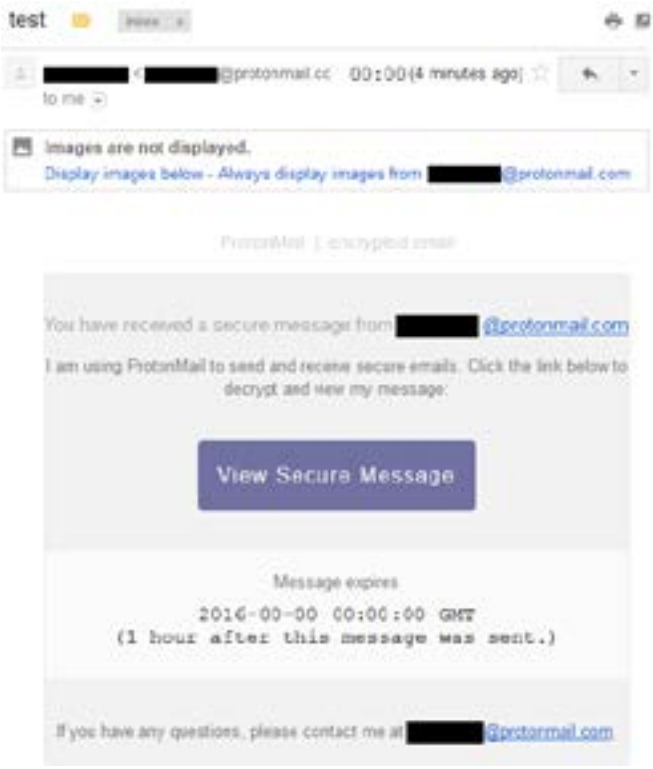
Mở Compose để gửi một email mới. Ở góc dưới cùng bên trái có ba nút, cho tệp đính kèm, để mã hóa / tạo mật khẩu và cho bộ đếm thời gian tự động hủy. Nhấp vào giữa để tạo mã hóa/tạo mật khẩu.

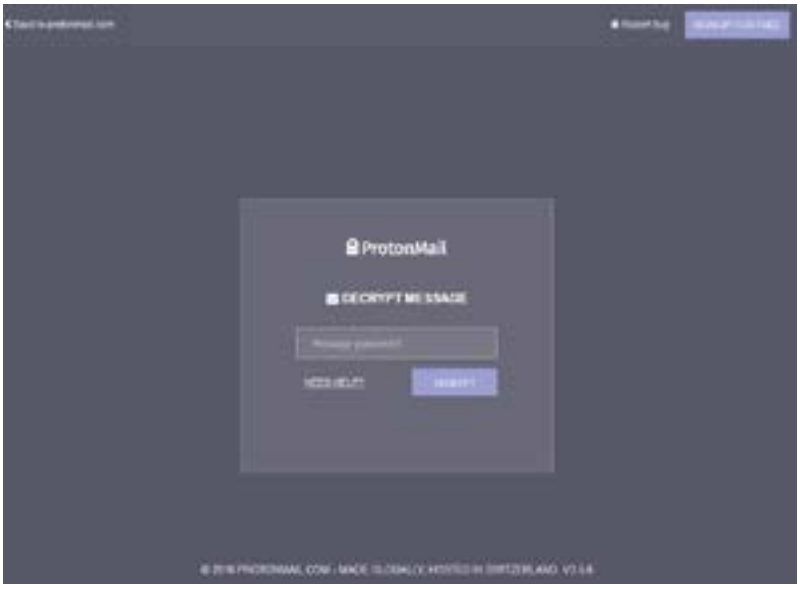
Tạo mật khẩu và kích vào Set(S-W/OXX) và bạn sẽ quay trở lại màn hình đầu tiên. Tiếp theo, bạn kích vào nút thứ ba để đặt thời gian tự hủy.

Đặt thời gian tự hủy (thời gian mà email còn có thể đọc) và nhấn vào Set để quay trở lại màn hình ban đầu (S-W/OXX). Bạn chọn Weeks/Tuần, Days/ngày, Hours/giờ theo trình tự từ trái sang phải.Sau khi gửi email, người nhận sẽ nhận được một email có chứa một liên kết (S-W / OXX).

Họ bấm vào liên kết đó và được đưa đến trang web để nhập mật khẩu (S-W / OXX). Nếu họ nhập mật khẩu, họ sẽ có thể đọc được tin nhắn (S-W / OXX). Lưu ý: Nếu thay vào đó bạn đã gửi đến một ProtonMail khác, nó sẽ xuất hiện trong hộp thư của họ giống như một thư thường (nhưng bộ đếm thời gian tự hủy sẽ hoạt động giống nhau).

Tại thời điểm này họ có thể nhấp vào Trả lời, và gửi trả lời cho bạn, sử dụng cùng một mật khẩu (S-W / OXX).





GỬI THÔNG TIN CHO NGƯỜI ĐANG ĐỐI MẶT NGUY HIỂM

Có nhiều cách để bạn gửi thông tin, cho dù là câu hỏi, thông tin hoặc hướng dẫn, tới một người đang đối mặt nguy hiểm trong khi hạn chế nguy cơ tiềm ẩn. Người này có thể có nguy cơ bị giam giữ, bắt cóc hoặc bị bắt giữ ngoài ý muốn của họ. Người này có thể bị đánh cắp dữ liệu, hoặc đơn giản là không áp dụng các biện pháp bảo mật để bảo vệ các thông tin nhạy cảm. Không phải tất cả mọi người sẽ theo bạn hướng dẫn làm thế nào để xử lý thông tin một cách an toàn, và do vậy, bạn cần áp dụng các biện pháp để hạn chế rủi ro cho bạn và những người khác.

Không có những biện pháp để một người sử dụng bình thường để cung cấp thông tin và dữ liệu đến một máy tính của người khác mà không mất quyền kiểm soát vì một chương trình khác, chẳng hạn xóa dữ liệu sau khi đọc xong, bị nhiễm virus hoặc bị chặn.

Thứ nhất, bạn nên luôn luôn gửi càng nhiều thông tin. Không bao giờ sử dụng tập tin đính kèm trừ khi cần thiết. Nếu bạn thực sự cần gửi tệp đính kèm, đảm bảo giới hạn thông tin trong tệp đính kèm và xóa dữ liệu nhạy cảm trước khi gửi.

GỬI EMAIL SẼ TỰ ĐỘNG HỦY

Thứ nhất, ưu điểm chính của ProtonMail so với các email khác là chức năng tự động hủy email. (Telegram, Signal) được trình bày trong phần Bảo mật Điện thoại của hướng dẫn này. Bây giờ bạn có thể viết một email cho ai đó, và đặt chế độ hẹn giờ. Bộ đếm thời gian này bắt đầu tính khi bạn gửi email. Điều này rất quan trọng. Bộ đếm thời gian bắt đầu khi bạn gửi email, không phải khi người nhận nhấp chuột đọc. Bây giờ bạn có thể đặt một bộ đếm thời gian giới hạn, ví dụ 1 giờ, hoặc 1 ngày, v.v., sau đó thông báo sẽ bị hủy. Thông báo bị hủy cả trong email của bạn (người gửi) cũng như cho người nhận. Đảm bảo gửi một tin nhắn bảo mật đến người nhận để họ biết kiểm tra email nhanh chóng, xem bên dưới.

Một ưu điểm quan trọng khác của ProtonMailis là bạn có thể sử dụng nó để gửi an toàn đến các tài khoản không Protonmail trong khi vẫn cho phép chức năng tự động hủy. Thông báo Protonmail, như thể hiện trong Chương 5: Chia sẻ thông tin, nhưng thông điệp Protonmail sẽ không được gửi đến Protonmail. Trong thực tế, thông điệp đã được tự động tiêu huỷ. Bất kỳ tài liệu đính kèm được gửi bằng email cũng sẽ bị hủy. Tuy nhiên, bất kỳ tệp đính kèm nào đã được tải xuống sẽ không bị xóa. Một lần nữa, tránh gửi kèm theo càng ít càng tốt.

Để sử dụng hệ thống này, bạn cần phải liên lạc với người trên điện thoại. Đây là điều cần thiết cho tất cả chúng ta. Nếu họ không đọc nó trong thời gian đã hẹn thì họ sẽ bỏ lỡ nó. Như vậy, ProtonMail nên được sử dụng cùng với một chương trình chat an toàn. Nếu bạn gửi ProtonMail đến một email không phải ProtonMail, bạn cần phải chọn một mật khẩu mà người nhận cần biết. Xem Chương 5: Chia sẻ thông tin để được nhắc nhở về cách thực hiện việc này. Chat với bạn bè hoặc bạn bè để gửi tin nhắn cho họ.

Sử dụng chức năng tự huỷ có nghĩa là bạn sẽ không phải lo lắng nếu người nhận không áp dụng các biện pháp bảo mật. Nếu bạn có bất kỳ câu hỏi nào, vui lòng liên hệ với chúng tôi. Không ai có thể bị đưa vào hoàn cảnh rủi ro do sự vô ý của người khác trong vấn đề bảo mật.

Gửi tài liệu đính kèm khi cần thiết

Như phần Metadata sau này trình bày, bất kỳ tài liệu nào bạn gửi có chứa nhiều thông tin hơn mọi người nghĩ. Thông tin trong tài liệu của bạn còn là siêu dữ liệu. Siêu dữ liệu chứa thông tin như văn bản được tạo ra khi nao, máy tính hoặc điện thoại nào được sử dụng để tạo ra nó, tên của người đó nếu điện thoại hoặc máy tính của họ được cá nhân hóa, thuê GPS ở đâu, Ngay cả tên của cá nhân trong hình ảnh dựa vào việc nhận dạng khuôn mặt tự động trên điện thoại của bạn và các thông tin tương tự khác. Để hiểu được siêu dữ liệu tốt hơn và cách xóa nó, xem phần Đặc biệt về Siêu dữ liệu trong Phần II.

Nếu bạn cần phải gửi tệp tin cho người khác thì:

- Không bao gồm hình ảnh, biểu đồ excel, bảng hoặc các thông tin đồ họa khác;
- Không để siêu dữ liệu trong tài liệu
- Gửi dưới dạng tệp PDF, không phải Word, Excel hoặc tương tự; và
- Đặt mật khẩu để bảo vệ tệp PDF.

Khi bạn chuyển từ Word hoặc Excel sang PDF, bạn sẽ có tùy chọn để bảo vệ tệp. Chúng tôi khuyên bạn nên sử dụng chương trình này làm tùy chọn. Một tệp tin được bảo vệ bằng mật khẩu, cũng giống như một hộp thư trống, sẽ bảo đảm cho người nhận khỏi bị tấn công, vì bất kỳ truy cập nào sẽ có giảm thiểu hậu quả. Đối với hầu hết các tài liệu, bạn sẽ không cần giữ chúng mãi mãi. Ngay sau khi bạn sử dụng thông tin ở tệp đính kèm, bạn nên xóa chúng theo chỉ dẫn giới thiệu ở Chương 7: Xóa dữ liệu.

Cuối cùng, như một lời nhắc quan trọng, cố gắng luôn giữ và tuân theo chính sách Hộp thư trống và thảo luận khái niệm này với bất kỳ ai mà bạn liên lạc. Chính sách này là công cụ tuyệt vời nhất của bạn để đảm bảo an toàn.

DỮ LIỆU META, XUẤT BẢN PHẨM VÀ MS OFFICE

Dữ liệu Meta là thông tin về một thứ gì đó ngoài nội dung. Đối với email, ví dụ: email đã được gửi, kích thước, địa chỉ (địa chỉ IP) đã sử dụng, thư nội dung chủ đề và ai đã gửi nó và ai đã nhận nó. Đối với tài liệu MS Word hoặc các tệp PDF, nó sẽ là thông tin về bản thân tài liệu, tác giả (tên của người dùng máy tính), thời gian thay đổi và hơn thế nữa. Tương tự với các công cụ xuất bản và thiết kế, như MS Publisher, InDesign vv

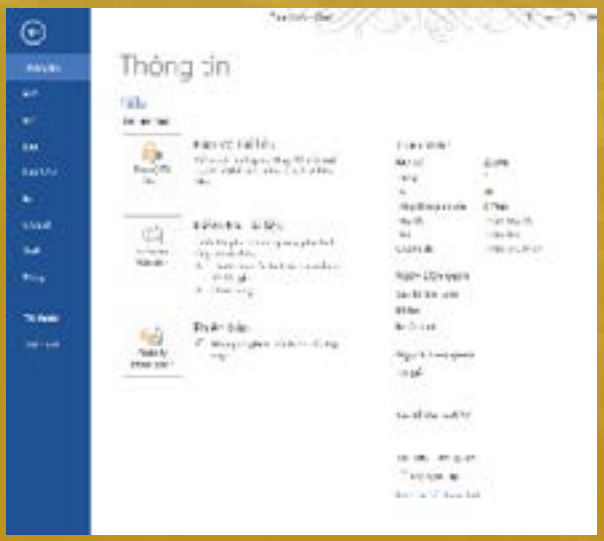
Những ngày này, ảnh bạn chụp bằng điện thoại hoặc video cũng sẽ chứa dữ liệu meta như vậy. Nếu bạn cho phép địa điểm, nó sẽ biểu hiện bức ảnh/video được chụp khi nào, ở đâu với độ chính xác cao dựa vào GPS. Thậm chí nhiều hơn, các ứng dụng ảnh bây giờ rất tinh vi để có thể nhận ra những người trong ảnh và gắn thẻ họ theo tên dựa vào sổ địa chỉ và ảnh chụp trước đó. Với điều này trong tâm trí, bạn nhận ra có bao nhiêu dữ liệu có thể được bao gồm trong một tập tin PDF bạn xuất bản, hoặc một hình ảnh bạn gửi một ai đó.

Bạn hãy lưu ý là dữ liệu Meta để lại nhiều dấu vết mà có thể bạn không muốn.

CÁC TÀI LIỆU TẠO RA BỞI OFFICE VÀ PDF

MS Office bao gồm Word, Publisher, Excell … kèm với một công cụ tích hợp để loại bỏ dữ liệu meta như vậy từ tài liệu. Điều này cũng có nghĩa là nó đã bị xóa trước khi được lưu dưới dạng PDF… Nó hoạt động giống nhau trên Win10 và OSX, và bạn có thể xác định vị trí chức năng một cách dễ dàng, cụ thể là nhấp vào File, sẽ đưa bạn đến tab cho Info như dưới đây.

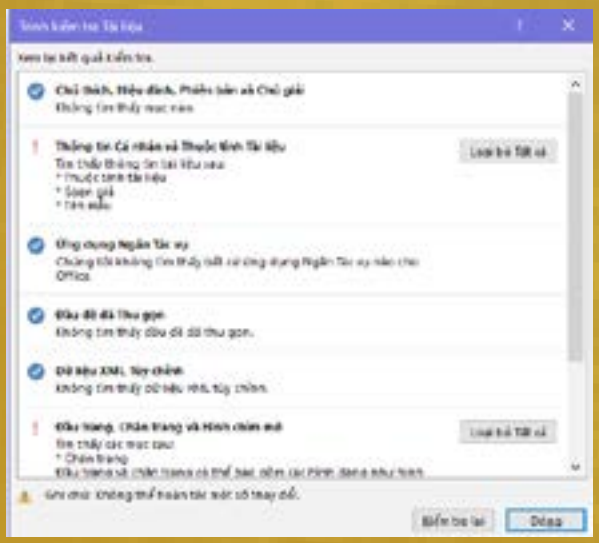
Nhấp vào nút Inspect Document trong S-W / OXX và từ trình đơn thả xuống, hãy nhấp vào Inspect Document. Một cửa sổ popup sẽ xuất hiện (S-W / OXX).

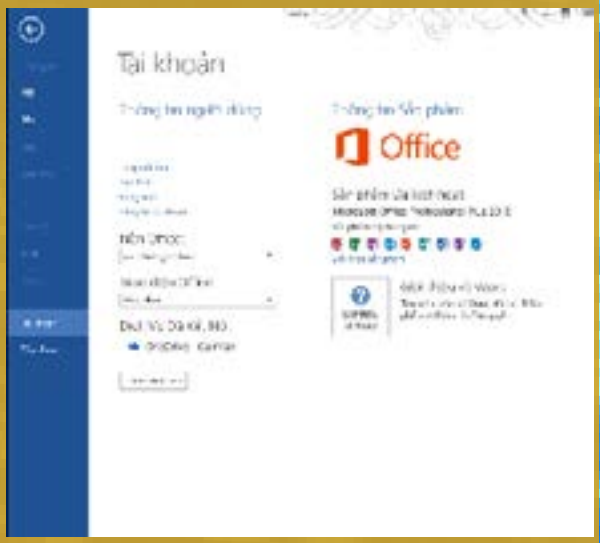


Sau khi nhấn vào Inspect, cửa sổ sẽ chỉ cho bạn thông tin được tìm thấy trong mỗi mục (S-W/OXX), và nếu thông tin nào được tìm thấy, sẽ có nút Remove All ở bên trái. Nhấn vào tất cả những nút này và nhấn vào Close. Tất cả các dữ liệu meta sẽ bị xía và bạn có thể ghi lại file như bạn muốn, hoặc chuyển nó thành dạng PDF.

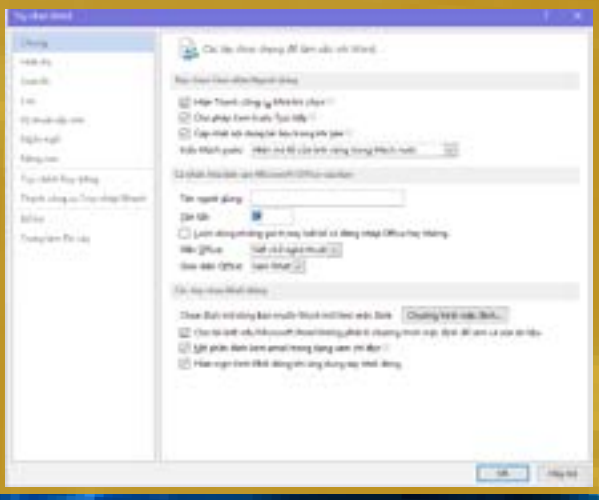
THIẾT LẬP MS OFFICE

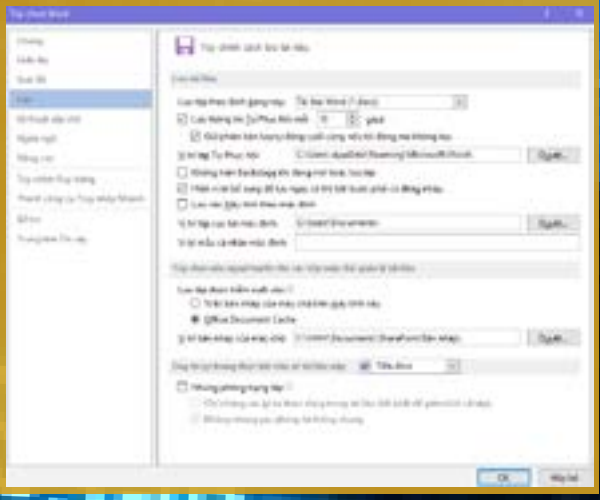
Tại thời điểm này, cần kiểm tra một số cài đặt về bộ Office của bạn. Mở tệp Word hoặc Excel và nhấp vào tab File ở góc trên cùng bên trái. Trên trình đơn bên, bạn sẽ tìm thấy hai tab ở cuối Account và Options. Nếu bạn nhấp vào tab Account (S-W / OXX), bạn sẽ nhìn thấy Sign into Office. Điều này cho phép bạn đồng bộ sử dụng và thiết lập của Word và các chương trình khác trong Office. Nếu bạn muốn bỏ dữ liệu meta của bạn khỏi các tệp công việc của bạn, đừng đăng nhập.



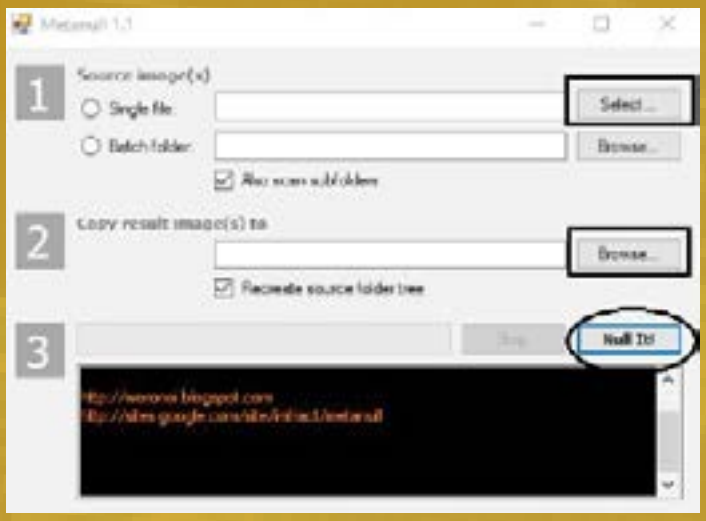


Nếu bạn nhấn vào Options, một cửa sổ popup sẽ xuất hiện. Có hai tab quan tâm. Đầu tiên là General.. Nhìn ở giữa (S-W / OXX) và bạn thấy các mục User Name và Initials. Chúng xuất hiện trong tài liệu của bạn, vì vậy hãy đảm bảo rằng tên của bạn không được viết ở đây. Bạn có thể thay đổi nó và nhấp vào ok.

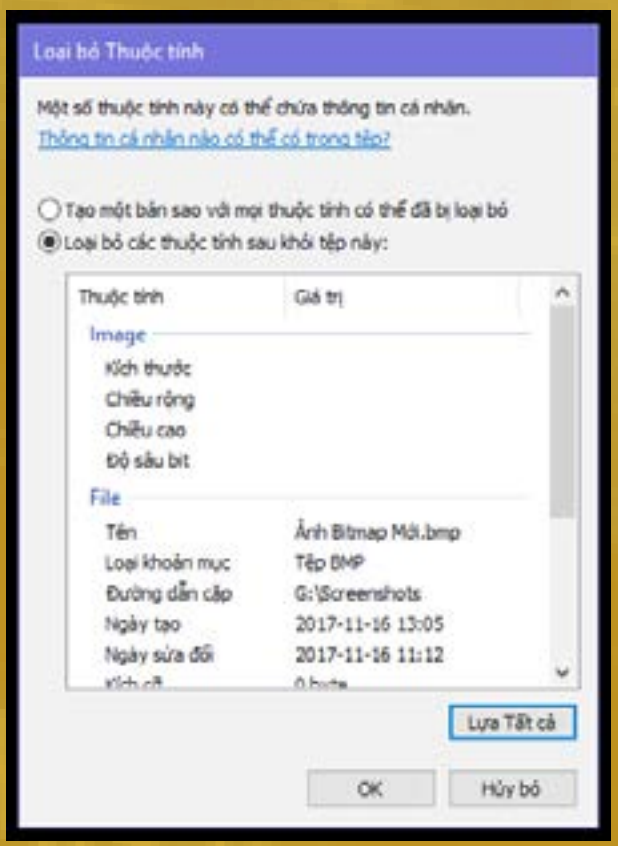




Các tab khác rất quan trọng là Save. Có hai mục bạn cần chú ý, thể hiện trong S-W / OXX là Auto Recover file location và Default local file location.



Trong suốt quá trình sử dụng Word hoặc các chương trình Office khác, các tài liệu bạn làm việc sẽ được lưu tự động trong những khoảng thời gian nhất định. Đây là chức năng giúp bạn không làm mất tất cả công việc của mình. Tuy nhiên, nếu bạn không thay đổi nó, văn bản chỉ bị xóa khi bạn ghi văn bản đó và đóng Word hoặc các chương trình Office khác. Như chúng ta đã biết trong phần xóa tài liệu, văn bản không thực sự bị xóa đúng cách, và rất không an toàn. Vì vậy, để bảo vệ chống lại mối đe dọa nhỏ nhưng nguy hiểm này, hãy đảm bảo rằng bạn đã ghi văn bản vào ổ ẩn hoặc USB và chọn ghi nhớ tự động.



ẢNH

Đối với bất kỳ ảnh nào bạn có và sử dụng trên máy tính của bạn, có một số chương trình nhỏ và hiệu quả có thể xóa dữ liệu meta bằng một cú nhấp chuột. Bạn cũng có thể làm điều đó bằng tay trong Win10 hoặc OSX. Nếu bạn có ý định đăng ảnh online từ máy tính của bạn, hoặc sử dụng trong văn bản nào đó, chúng tôi khuyên bạn cần loại bỏ dữ liệu meta trước.

> "Đối với tất cả các tệp tin, và cho cả WIN10 và OSX, bạn có thể sử dụng hệ điều hành OS để loại bỏ dữ liệu meta."

Đối với Win10, chúng tôi khuyên dùng MetaNull, có thể tải xuống tại địa chỉ http://download.cnet.com/Metanull/3000-20432_4-75732772.html. Bạn chỉ cần bắt đầu chương trình, chọn ảnh bạn/tập tin muốn xóa dữ liệu meta và chọn nơi đặt phiên bản mới (S-WXX).

Nếu bạn không muốn sử dụng chương trình này cho việc xóa dữ liệu meta, Properties sau đó nhấp vào Details. Ở cuối cửa sổ bật lên, bạn sẽ thấy Xóa Remove Properties and Personal Information. Nếu bạn nhấp vào nút Select All và sau đó OK, nó sẽ xóa dữ liệu này (S-WXX).

CHAPTER 7
XÓA THÔNG TIN

Phần này sẽ hướng dẫn bạn làm thế nào để xóa các tập tin và thông tin một cách hiệu quả, và sẽ cho bạn thấy rằng tất cả mọi thứ bạn nghĩ rằng bạn biết về xóa thông tin có thể là sai.

Trước khi bạn đọc phần này, bạn sẽ cần một thông tin quan trọng, đó là ổ cứng HDD (Ổ cứng) hoặc SSD (Solid Disk Drive). Nếu sử dụng Win10, chỉ cần mở chức năng tìm kiếm và tìm Disk Defragmenter (SearchTerm). Khởi động chương trình, và ngay lập tức sẽ hiển thị loại ổ cứng, phân vùng, USBs, ... được kết nối với máy tính. Đối với OSX, bạn tìm hiểu bằng cách nhấp vào >About this Mac>System Report>Hardware>Serial-ATA (xem "Medium type").

Phần lớn phần này dựa trên việc bạn sử dụng ổ cứng truyền thống, vốn vẫn là loại ổ cứng thông dụng nhất. Nếu bạn có một máy tính xách tay mới hơn, cao cấp, hoặc gần đây đã mua ổ cứng gắn ngoài, nó có thể là một ổ SSD. Nếu bạn có một ổ SSD, phần lớn những gì được viết ở đây không áp dụng. Đối với SSD, một phần đặc biệt được nhắc tới trong phần tiếp theo, tuy nhiên bạn nên đọc chương này như bình thường, đặc biệt vì nó vẫn áp dụng cho các ổ đĩa cứng khác, thanh USB, vv

"Hành vi an toàn, mật khẩu mạnh và mã hóa sẽ không bảo vệ bạn khỏi chương trình khôi phục tập tin nếu bạn không áp dụng cách xóa an toàn."

Bạn nghĩ gì? Khi bạn nhấp vào Delete/Xóa trên một tệp, hoặc 'Empty recycle bin', không có gì là thực sự bị xóa. Tài liệu mà bạn nghĩ bạn đã xóa ngày hôm qua, hoặc 2 năm trước đây, vẫn còn trên máy tính của bạn để được đọc bởi bất cứ ai muốn. Đối với những người cần bảo vệ thông tin hoặc nguồn, điều này tạo thành một vấn đề rất lớn. Tệp có thể biến mất từ cửa sổ Explorer hoặc Finder, nhưng vẫn ở đó, cho bất cứ ai đọc. Truy cập các tệp 'đã xoá' như vậy là một yêu

thích của nhiều băng nhóm tội phạm cũng như cảnh sát và các nhân viên an ninh, và rất dễ thực hiện.

Xoá tài liệu là một điểm mù đối với nhiều người. Tức là, ngay cả những người được đào tạo về an ninh mạng thường không quan tâm đến việc xóa an toàn. Để hiểu những rủi ro gây ra do xóa bỏ không an toàn, chúng ta cần phải hiểu làm thế nào ổ đĩa hoạt động. Điều này áp dụng cho tất cả các dạng lưu trữ kỹ thuật số, chẳng hạn như USB, SSD và ổ cứng máy tính.

LƯU TRỮ DỮ LIỆU

Định dạng lưu trữ khác nhau hoạt động khác nhau. Điều này làm cho việc xóa an toàn trở nên khó khăn hơn. Vì lý do này, cũng như nhiều lý do khác đã được đưa ra, bạn cần phải hạn chế mình với những gì máy tính, điện thoại, ổ đĩa cứng và USB bạn làm việc với. Bạn càng cần phải giải quyết càng nhiều càng khó khăn.

Tất cả các lưu trữ kỹ thuật số (ổ đĩa cứng, USB, vv) bao gồm, ở mức cơ bản nhất, của hai loại dữ liệu; không gian trống hoặc dữ liệu có sẵn và dữ liệu đã sử dụng. Dữ liệu đã sử dụng của bạn là dĩ nhiên không gian được thực hiện bởi các tệp, video của bạn, v.v ... Không gian trống hoặc không gian sẵn có bao gồm không gian bạn đã để lại. Tuy nhiên, không gian trống không phải là không gian chính xác. Đây là khoảng trống trên máy tính của bạn hiện không chiếm dụng dữ liệu đã sử dụng và có thể lưu dữ liệu mới khi bạn làm việc.

Khi bạn xóa một cái gì đó, hoặc dọn thùng rác, dữ liệu đó không thực sự bị xóa. Nó vẫn ở đó, trong cùng một vị trí trên ổ cứng nơi nó đã được trước đó. Việc xóa chỉ là bạn đã nói với máy tính rằng bạn không còn cần dữ liệu đó. Khi một phần dữ liệu đã được đánh dấu là không cần thiết, nó được coi là miễn phí (có sẵn) không gian, nơi các tệp tin mới có thể được lưu trong tương lai. Là người dùng, bạn không thể thấy dữ liệu trước đó nhưng nó đã không biến mất. Hãy suy nghĩ về nó như là ẩn cho đến khi nó được lưu trong máy tính. Nhưng với phần mềm khôi phục đơn giản, được gọi là File Recovery, nó rất dễ dàng tìm thấy.

Dữ liệu "đã xoá" vẫn có thể được đọc. Thậm chí tệ hơn, nó không đòi hỏi kỹ năng công nghệ để đọc nó. Tất cả bạn phải làm là tải về một chương trình miễn phí, và với một nút bấm, tất cả các tập tin đó sẽ được hiển thị. Những chương trình này là những công cụ thường được sử dụng bởi an ninh và những kẻ phạm tội.

Cũng cần lưu ý rằng dữ liệu "đã xoá" không được lưu trữ theo trình tự thời gian. Khi bạn lưu dữ liệu mới, nó không nhất thiết phải tiết kiệm trên không gian trống cũ hơn hoặc mới hơn gần đây hơn. Nó là ngẫu nhiên. Điều này có nghĩa là bạn không nên có bất kỳ kỳ vọng nào về dữ liệu có thể đã được lưu lại và dữ liệu có thể tồn tại. Đây là lý do tại sao cần xóa tất cả dữ liệu một cách an toàn.

Đối với dữ liệu cũ "đã xoá" thực sự bị xóa, phải ghi đè bằng dữ liệu mới. Chỉ sau khi không gian giữ dữ liệu cũ đã bị ghi đè bằng dữ liệu mới thì thông tin cũ mới thực sự bị xóa. Để làm cho vấn đề tồi tệ hơn, giống như với một tài liệu từ, bạn có thể "hoàn tác" một hành động. Có thể bạn đã xóa một đoạn văn do nhầm lẫn và bạn chọn lùi lại để khôi phục nó. Loại chức năng hoàn tác này cũng có thể được thực hiện, và một người bên ngoài có thể truy cập ít nhất một số các tập tin đã

xóa của bạn ngay cả khi nó đã được ghi đè lên. Tóm lại, đối với bảo mật, dữ liệu cũ phải được ghi đè nhiều lần, để đảm bảo không ai có thể truy cập nó.

May mắn thay, có những chương trình sẽ giải quyết vấn đề này cho bạn. Chương trình này được gọi là CCleaner, dễ sử dụng, và nó được trình bày trong Giải pháp Kỹ thuật: CCleaner dưới đây.

Ổ ĐĨA SSD

Hầu hết các ổ đĩa cứng đều là HDD (Hard Drives) và hiện nay, nhiều máy tính vẫn sử dụng HDD. Theo thời gian, các chương trình và kỹ thuật đã được phát triển để xóa an toàn dữ liệu của các thiết bị như vậy, ví dụ như sử dụng CCleaner. Tuy nhiên, một loại ổ đĩa cứng mới đang trở nên phổ biến hơn, được gọi là SSD (Solid State Drive). Chúng có kích thước nhỏ hơn nhưng nhanh hơn và có hiệu suất cao hơn. Do đó, chúng vẫn được bán kèm theo các máy tính cao cấp và thậm chí nếu bạn có một máy tính mới, bạn cũng có thể có một ổ cứng như thế.

Phần Tốt. Các ổ SSD trong máy tính xách tay của bạn sẽ tự động đi kèm với một tính năng mới đặc biệt, cho phép. Đây được gọi là TRIM. Nó hoạt động để xóa các tài liệu bạn chọn để xóa một cách an toàn hơn nhiều so với một HDD truyền thống, làm cho việc khôi phục dữ liệu của tội phạm hoặc cảnh sát trở nên khó khăn.

Phần xấu Vấn đề, về bản chất, là chức năng của CCleaner (và các chương trình tương tự khác) ghi đè dữ liệu "đã xóa" không hoạt động hoặc ít nhất là không hoạt động tốt. Trên thực tế, trên CCleaner cho OSX, chức năng này đã được gỡ bỏ hoàn toàn. Ngay cả khi bạn có nó, nó sẽ không được rất hữu ích, và cũng sẽ làm tổn thương ổ cứng SSD, làm nó hỏng rất nhanh chóng. Bởi vì các chức năng CCleaner thông thường không hoạt động, nó sẽ không cho bạn biết chắc rằng thông tin thực sự đã biến mất, bởi vì bạn không biết khi lệnh TRIM được chạy để xóa nó.

TRIM được tự động kích hoạt trên các máy tính OSX. Trong Win10 nó cũng thường được kích hoạt. Nếu bạn cần chắc chắn, hãy nhấp vào khu vực tìm kiếm, hãy viết "Command Prompt" và nhấp chuột phải vào nó và chọn "Run as administrator". Trong cửa sổ mới được hiển thị, hãy sao chép mã này trong: "fsutil behavior query DisableDeleteNotify" và nhấp Enter (không bao gồm ""). Phản hồi sẽ là "NTFS disabledeletenotify = 0". Các 0 cho thấy nó đã được bật, 1 cho thấy nó không. Nếu nó đọc "1", sau đó sao chép trong lệnh này: "fsutil behavior set disabledeletenotify NTFS 0" và nhấn Enter. Bây giờ nó sẽ được thiết lập để cho phép TRIM.

DI CHUYỂN TỆP

Điều quan trọng là phải nhận ra di chuyển một tập tin thực sự có nghĩa là thế nào. Khi bạn di chuyển tệp, bạn chỉ cần tạo một bản sao của tệp đó tại vị trí mới, trong khi tệp ở vị trí cũ là "đã bị xóa" như trong cuộc thảo luận ở trên. Điều đó có nghĩa là nếu bạn, như nhiều người khác làm, là tạo một tài liệu từ mới trên màn hình của bạn (được lưu trữ trên ổ cứng hệ điều hành) và sau đó di chuyển nó vào không gian mã hóa của bạn, tệp cũ sẽ chỉ được đánh dấu là không gian trống và dễ dàng được truy cập bởi người khác bằng cách sử dụng một chương trình phục hồi tập tin đơn giản. Tương tự với bất kỳ tệp nào bạn tải xuống qua trình duyệt đến vị trí tải mặc định (hầu như luôn luôn trên ổ cứng máy tính của bạn) và sau đó di chuyển đến không gian mã hóa của bạn.

Một lý do quan trọng là giữ các tệp từ đầu đến cuối ở vị trí an toàn là do đảm bảo sẽ không có dấu vết nào được tìm thấy bởi người khác. Bất kỳ tệp nào được lưu trữ, dù là ngắn gọn, ví dụ ổ C: của bạn, sẽ có sẵn thông qua khôi phục tệp trên ổ cứng đó. Nếu mặt khác, bạn lưu trữ một tập tin trực tiếp trên USB và giữ nó ở đó, một khi đã bị xóa, nó sẽ chỉ có sẵn ở USB đó. Bạn có thể dễ dàng xóa nó khỏi vị trí đó bằng cách sử dụng CCleaner.

Đây là một lý do khác khiến điện thoại của bạn không bao giờ được sử dụng để lưu trữ, thậm chí tạm thời, một tệp làm việc. Không bao giờ tải tệp tin từ email của bạn, ví dụ, vào điện thoại của bạn, ngay cả khi nó chỉ đọc nó một cách nhanh chóng trước khi 'xóa' nó.

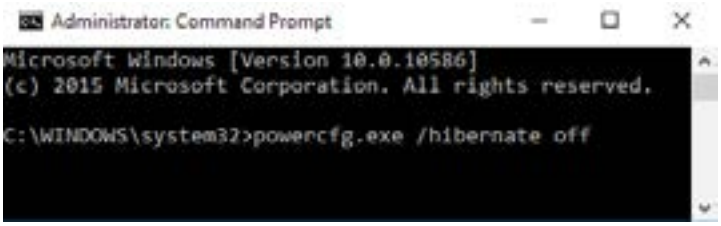
BỘ NHỚ ẢO

Cuối cùng, lưu ý bên dưới, trong Chương 2: Chuẩn bị máy tính của bạn, bạn đã thực hiện thay đổi trong Local Security Policy (Win10), để tự động xóa "tệp trang" khi tắt. Trong OSX, sự thay đổi này được thực hiện trong phần Security dưới Use Secure Virtual Memory. Lý do bạn đã được hướng dẫn để làm như vậy là một máy tính sẽ làm việc bằng cách sử dụng bộ nhớ, mà giữ thông tin về những gì bạn đang làm việc. Khi bạn tắt, bộ nhớ này, được gọi là RAM, sẽ bị xóa. Tuy nhiên, máy tính cũng sử dụng một phần của ổ cứng để hỗ trợ việc này, và khu vực này sẽ thu thập thông tin về những gì bạn đang làm. Bộ nhớ "giả mạo" này được gọi là nhiều thứ, như bộ nhớ ảo, tệp hoán đổi hoặc tệp trang. Bởi vì sự thay đổi mà bạn đã thực hiện, bạn đã cài đặt máy tính để xóa đúng cách này mỗi lần bạn tắt máy tính. Nếu không, ổ cứng có thể chứa thông tin về những gì bạn đã làm trước đây, cho những người có kỹ năng kỹ thuật để đọc sau khi dùng máy tính của bạn. Vấn đề này đã được giải quyết.

NGỦ ĐÔNG

Hibernation là một chức năng trong Win10 cho phép máy tính của bạn nhanh chóng khôi phục hoạt động từ nơi bạn đã dừng lại sau khi máy tính đã tắt. Nhiều người sử dụng chức năng này bởi vì người dùng có thể tiếp tục công việc trên máy tính một cách nhanh chóng. Lý do hoạt động là hệ điều hành sẽ lấy tất cả thông tin của bạn và lưu nó vào ổ cứng. Khi bạn khởi động máy tính của mình, nó sẽ tải lại tất cả thông tin đó. Điều này có nghĩa là nếu máy tính của bạn được sử dụng và bắt đầu, nó sẽ hiển thị mọi thứ bạn làm mới nhất, nhật ký trên trình duyệt của bạn và nhiều thông tin hơn. Thông tin này được lưu trữ mà không cần mã hóa. Điều này rất nguy hiểm.

Để vô hiệu Hibernation ở Win 10, nhấn vào vùng tìm kiếm và viết "Command Prompty" và kích chuột phải, chọn Run as administrator. Trong cửa sổ mới, đánh "powercfg.exe /hibernate off" và nhấn Enter (SWXX). Cài đặt ngủ và sử dụng năng lượng có thể được tìm thấy bằng việc tìm "powercfg.exe /hibernate off."



NHỮNG ĐIỂM QUAN TRỌNG

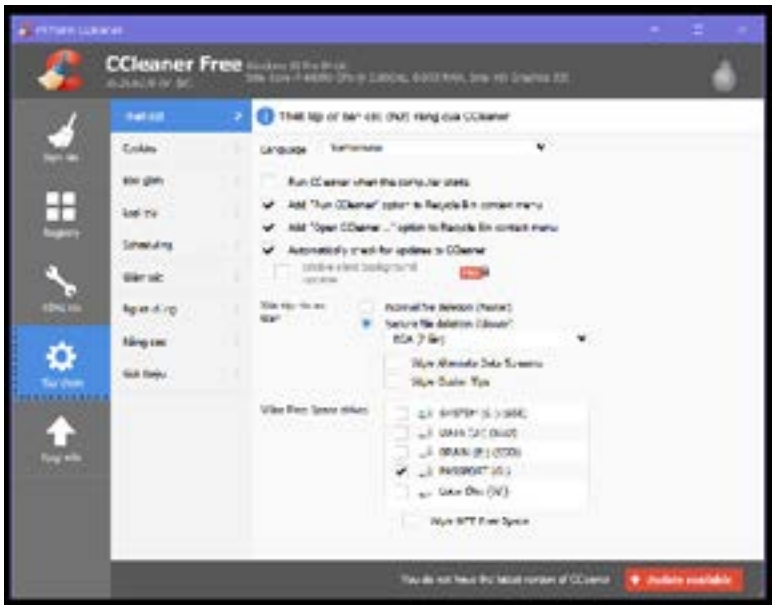
- Khi bạn tạo một tài liệu hoặc tệp mới, hãy làm như vậy trong không gian được mã hóa hoặc nơi nào mà bạn định lưu trữ
- Không tạo tài liệu mới trên máy tính để bàn.
- Cẩn thận về di chuyển các tập tin vì việc này để lại dấu vết.
- Không được truy cập các tập tin hoặc lưu trữ các tập tin làm việc trên điện thoại hoặc bàn phím.
- Không sử dụng chức năng ngủ đông. Khi bạn rời khỏi máy tính trong một khoảng thời gian dài hoặc nếu đi ngủ, hãy tắt máy tính.

GIẢI PHÁP KỸ THUẬT: CCLEANER

CCleaner là một chương trình nhỏ sẽ cho phép chúng ta giải quyết nhiều vấn đề. Chương trình này sẽ xóa một cách an toàn tất cả các loại dữ liệu thu thập được về những gì bạn đang làm, như các tập tin cookie, các tập tin tạm, thông tin trong Microsoft Word trên các tài liệu bạn đang làm việc vv ... mà còn đảm bảo an toàn cho không gian máy tính của chúng ta và " xóa "các tập tin.

> Lưu ý: Chức năng "Erase Free Space" sẽ không hữu ích, hoặc trong một số trường hợp, kể cả có sẵn, nếu bạn có một ổ cứng SSD. Tuy nhiên, tất cả các chức năng khác, để loại bỏ các dấu vết và các bản ghi, đọc thì bạn nên cài đặt và sử dụng chương trình này.

Đối với cả Win10 và OSX bạn có thể tải xuống chương trình trên download.com. Sau khi tải về, cài đặt chương trình. Bắt đầu chương trình bằng cách nhấp vào biểu tượng đặt trên thư mục máy tính để bàn hoặc ứng dụng. Trong Win10, bạn cũng có thể click chuột phải vào Recycle Bin và chọn Open CCleaner.



Mở chương trình bạn sẽ tìm thấy một số tab ở bên trái. Các phiên bản Win10 có nhiều tab, trong khi phiên bản OSX chỉ có ba, nhưng chúng có chứa một số cài đặt và các tùy chọn tương tự.

Chương trình bắt đầu trên tab Cleaner. Trong cửa sổ bên phải bạn sẽ thấy hai tab, một cho hệ điều hành (Windows hoặc Mac OSX), và một cho các ứng dụng. Trong tab Windows hoặc Mac OSX, chọn tất cả các hộp. Đây là tất cả các loại thông tin khác nhau sẽ được gỡ bỏ một cách an toàn khi bạn chạy chương trình. Trong Win10, ở dưới cùng của danh sách là Wipe Free Space (không chọn cái này nếu bạn có một ổ cứng SSD).

Trong tab Ứng dụng, bạn sẽ tìm thấy nhiều tuỳ chọn hơn cho những gì để xóa an toàn. Các mục bạn tìm thấy phụ thuộc vào những gì được cài đặt trên máy tính của bạn. Ở đây bạn nên chọn tất cả các hộp với một ngoại lệ. Nếu bạn đã quyết định sử dụng trình duyệt sử dụng cá nhân và không muốn xóa tất cả thông tin, đừng chọn hộp cho trình duyệt đó hoặc chọn hộp để chọn (ví dụ bạn có thể xóa lịch sử duyệt web, nhưng không xóa thông tin đăng nhập). Xem S-WXX làm ví dụ.

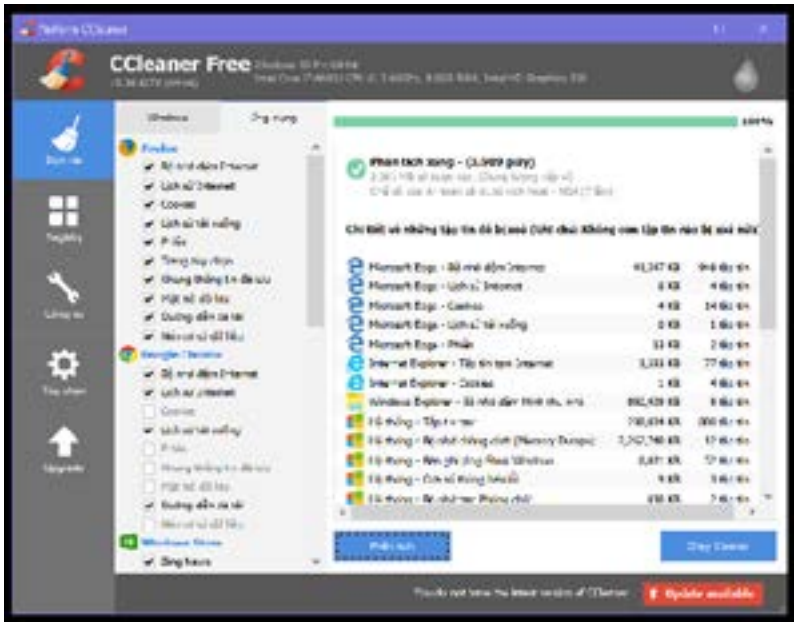
Sau đó, nhấp vào tab Options dưới đây. Đầu tiên nó sẽ hiển thị Settings subsection như được hiển thị bên dưới. Trên OSX, bạn chỉ cần chọn Secure file deletion và từ trình đơn thả xuống chọn Advanced Overwrite (3 lần) hoặc Complex Overwrite (7 pass) (S-OXX). Số lần vượt qua sẽ càng an toàn khi xóa dữ liệu, nhưng nó sẽ mất nhiều thời gian để hoàn thành lệnh.

Trên Win10, theo S-WXX bạn thực hiện lựa chọn tương tự, nhưng cũng có thể thực hiện các lựa chọn khác. Nhấp vào hộp Automatically check for updates, sau đó nhìn vào phía dưới cùng và chọn (các) ổ đĩa cứng (nếu bạn có nhiều) tới Wipe Free Space. Bất kỳ USB nào trong máy tính của bạn cũng sẽ hiển thị trong danh sách này, nếu bạn muốn xóa tài liệu trong đó.

> Lưu ý: Nếu bộ nhớ đã được mã hóa của bạn được mở/gắn khi bắt đầu CCleaner, nó cũng sẽ được hiển thị trong danh sách này. Không cần phải đưa nó vào. Ở hầu hết thời gian, bạn chỉ cần chọn ổ cứng thông thường (C :).

Trên Win10 bạn cũng có một khu vực khác trong Options được gọi là Advanced. Nhấp vào đó, và nhấp vào Hide warning messages. Bạn cũng có thể chọn Shutdown sau khi làm sạch, nếu bạn làm vậy, máy tính sẽ tự động tắt sau khi chương trình đã làm sạch xong.

Cuối cùng, bạn có một tab Drive Wiper trong Tools. Điều này cho phép bạn chỉ lau không gian trống mà không sử dụng chức năng Run Cleaner- hãy nhớ trước đó chúng ta thảo luận rằng không gian trống thực sự là các tập tin cũ bạn đã xóa. Chỉ cần đảm bảo rằng (S-WXX) bạn chọn Free Space Only như thể hiện trong ảnh chụp màn hình, nếu không nó sẽ xóa dữ liệu hiện có của bạn.



Bây giờ bạn đã hoàn thành thiết lập và có thể chạy thử nghiệm. Trở lại tab Cleaner và nhấn Analyze. Sau khi phân tích nhanh, nó sẽ hiển thị những gì sẽ bị xóa. Để xóa các tập tin đã chọn, hãy nhấp vào Run Cleaner. Nếu bạn đã bao gồm Wipe Free Space (Win10) và Erase Free Space (OSX), sẽ mất một thời gian dài. Nếu bạn chỉ muốn xóa dấu vết khỏi hệ điều hành, hoạt động của trình duyệt vv, hãy chắc chắn rằng bạn không chọn Wipe Free Space (S-WXX và S-OXX), sau đó trở lại và nhấp vào Analyze. Nếu bạn chưa đóng tài liệu, chương trình hoặc trình duyệt cần xóa, chương trình sẽ yêu cầu bạn đóng chúng, nếu không thì chương trình không thể làm sạch.

SỬ DỤNG CCLEANER

Bạn có thể chạy CCleaner theo hai cách, có hoặc không có Wipe Free Space-Clear Free Space. Nếu có Wipe Free Space chương trình mất nhiều thời gian hơn (trừ khi bạn có một ổ cứng rất nhỏ). Nếu bạn chỉ muốn dọn dẹp dấu vết dữ liệu của mình thì chạy chương trình mà không chọn Wipe Free Space. Hãy làm thường xuyên điều này. Trên thực tế, khi bạn đã hoàn thành công việc hàng ngày, bạn nên chạy nó trước khi tắt máy tính.

Nếu sự đe dọa gia tăng, bạn cũng nên dành thời gian để chạy Wipe Free Space thường xuyên hơn. Bạn thực hiện việc này bằng cách đưa nó vào khi chạy Run Cleaner, hoặc bạn có thể sử dụng công cụ Wipe Free Space đặc biệt được trình bày trong S-WXX và S-OXX.

SỬ DỤNG CCLEANER ĐỂ ĐÓNG WIN10

Tiếc thay tùy chọn này không có trong OSX. Trong khi kiểm tra tab Advanced của Options (S-WXX), bạn đã nhìn thấy một hộp Shutdown after cleanin. Nếu bạn chọn mục này, máy tính của bạn sẽ tắt tự động sau khi hoàn thành CCleaner.

Nếu bạn đang sử dụng Win10, rất khuyên bạn nên kiểm tra việc này. Sau đó, bạn chỉ cần tắt máy tính bằng CCleaner thay vì nút hoặc chức năng Shutdown bình thường.

•

NHỮNG ĐIỂM QUAN TRỌNG

- Việc gì xảy ra nếu bạn nhấn vào Delete/Xoá hoặc Empty/ làm trống?
- Làm thế nào để xoá mọi dấu vết về lịch sử làm việc trên mạng trong máy tính của bạn?
- Tại sao việc xoá dữ liệu thường xuyên trên máy tính lại quan trọng?
- Nếu bạn sử dụng máy tính Win10, bạn sẽ tắt máy tính thế nào trong tương lai?
- Chuyện gì xảy ra khi bạn chuyển một tập tin?

SIÊU DỮ LIỆU METADATA VÀ JOHN MCAFEE

Đó là câu chuyện về một chuyên gia máy tính nổi tiếng thế giới vào năm 2012 khiến mọi người suy nghĩ về mối nguy hiểm của siêu dữ liệu (Metadata). Tuy nhiên, hầu hết mọi người vẫn chưa biết Metadata là gì và làm thế nào nó lại là một nguy cơ. Công dân Hoa Kỳ John McAfee là một trong những người sáng tạo ra chương trình McAfee Antivirus, một trong những chương trình chống virus thành công nhất từng được tạo ra.

Trong năm 2012 khi đang sống ở Belize, anh ấy đã có liên quan đến một giết người hàng xóm. Anh ta đã trở về Hoa Kỳ và đã được miễn truy cứu trách nhiệm hình sự. Tuy nhiên, mặc dù vô tội, ông vẫn hoang tưởng về cảnh sát và đi sống một nơi bí mật

Tuy nhiên, nơi anh sống cuối cùng đã được tiết lộ sau cuộc phỏng vấn anh ta bởi một nhà báo VICE. Nhà báo này đã chụp vài bức ảnh trong cuộc phỏng vấn, sau đó đăng tải cùng với bài viết. Nhà báo đã không nhận ra loại thông tin mà một bức ảnh có thể tiết lộ.

Một khi bài viết đã được đăng trên mạng, mọi người dễ dàng tải bức ảnh xuống và quét nó để lấy metadata. Bất cứ ai có các kỹ năng máy tính cơ bản cũng có thể nhanh chóng nhìn thấy thời điểm bức ảnh được chụp, thiết bị dùng để chụp cùng với vị trí GPS nơi ảnh đã được chụp.

Không lâu sau khi bài viết được công bố, cảnh sát Belizean bắt giữ McAfee. Ông đã phải chịu cảnh giảm giữ tù đày ở một trung tâm trước khi được thả ra và bị trục xuất.

Câu chuyện này là bài học quan trọng cho các nhà bảo vệ nhân quyền khi bị truy đuổi.

PHẦN III BẢO MẬT ĐIỆN THOẠI

PHẦN III CỦA CUỐN CẨM NANG NÀY BAO GỒM BỐN CHƯƠNG, TẤT CẢ ĐỀU LIÊN QUAN ĐẾN ĐIỆN THOẠI CỦA BẠN.

CHƯƠNG 8

Hiểu biết về Bảo mật Điện thoại, sẽ cung cấp một số thông tin chung về cách điện thoại hoạt động và những vấn đề bảo mật chính là gì.

CHƯƠNG 9

Sử dụng điện thoại, sẽ trình bày một số hướng dẫn về cách bạn nên sử dụng điện thoại một cách an toàn và một số vấn đề khác liên quan đến hành vi của bạn khi sử dụng điện thoại

CHƯƠNG 10

Cài đặt Điện thoại, giống như Chương 2 dành cho máy tính của bạn, một chương buồn tẻ với các cài đặt cơ bản trên điện thoại của bạn và cách bạn có thể thay đổi các cài đặt đó để tăng tính bảo mật.

CHƯƠNG 11

Các ứng dụng bảo mật, giới thiệu các ứng dụng có liên quan, có thể cho phép bạn tiếp tục sử dụng điện thoại hiệu quả, nhưng với tính bảo mật cao hơn.

CHƯƠNG 8
HIỂU BIẾT VỀ BẢO MẬT ĐIỆN THOẠI

Trong chương này chúng tôi sẽ giới thiệu cách điện thoại thông minh của bạn có thể được sử dụng để theo dõi bạn, những mối đe dọa chính là gì và chỉ ra cách các ứng dụng đã cài đặt làm tăng nguy cơ mất an toàn về bảo mật.

Trước hết, mặc dù ngày nay điện thoại giống như máy tính nhỏ, chúng bị hạn chế về điện và do đó bạn có thể làm được gì để giải quyết các mối đe dọa an ninh. Tóm lại, điện thoại của bạn sẽ không bao giờ được an toàn. Điều này rất quan trọng cần nhớ. Nếu nghi ngờ, hoặc trong tình huống có mối lo ngại về bảo mật, đừng bao giờ dựa vào điện thoại của bạn. Tắt nó đi, khi có thể tháo pin ra và để ở nơi an toàn. Khi pin còn ở trong điện thoại, bạn có thể bị theo dõi. Nếu bạn cần mang điện thoại, hãy xem ở Chương 11: Sử dụng Điện thoại.

“Nói tóm lại, điện thoại của bạn sẽ không bao giờ được an toàn.“

Bạn có thể kiểm tra cho mình cách điện thoại của bạn có thể gây ra vấn đề cho bạn. Tháo thẻ SIM ra khỏi điện thoại của bạn. Đi dạo. Nếu bạn kiểm tra chức năng vị trí, bạn sẽ thấy nó vẫn hoạt động ngay cả khi không có thẻ SIM. Nếu bạn có thể theo dõi các hoạt động của bạn trên Google Maps hoặc các chương trình khác có nghĩa là cảnh sát hoặc bất cứ ai khác muốn theo dõi hoạt động của bạn. Điều này là bởi vì nếu không đặt “chế độ máy bay,”, điện thoại của bạn sẽ tiếp tục sử dụng sóng vô tuyến. Đây là cách điện thoại kết nối với mạng điện thoại để gọi điện thoại, SMS và theo dõi. Đây cũng là lý do khiến ngay cả khi không có thẻ SIM, tất cả điện thoại vẫn có thể gọi cho dịch vụ khẩn cấp. Điều này có nghĩa là cảnh sát có thể theo dõi bạn bất cứ khi nào họ muốn.

Điều này mang lại cho chúng ta vấn đề về vị trí. Chức năng theo dõi vị trí chủ yếu hoạt động như sau: Mỗi lần trong một khoảng thời gian điện thoại của bạn, ngay cả khi bạn không thực hiện

cuộc gọi hoặc gửi văn bản, sẽ gửi ra một tín hiệu vô tuyến, sẽ được thu thập bởi tháp điện thoại di động gần nhất. Điện thoại của bạn giữ liên lạc liên tục như thế này để khi có ai đó gọi cho bạn hoặc văn bản bạn, điện thoại của bạn đã sẵn sàng nhận nó. Ở các thành phố lớn có rất nhiều tháp di động này, và bằng cách xem điện thoại của bạn kết nối với họ như thế nào, họ có thể xác định vị trí của điện thoại của bạn rất hẹp, đôi khi đến căn phòng nào trong căn nhà bạn đang ở (triangulation bằng cách sử dụng một số khác tháp di động). Những điện thoại ngày nay có chức năng GPS, và cũng có thể sử dụng kết nối Internet không dây của bạn để giúp đỡ việc này. Điều này có nghĩa là lần duy nhất điện thoại của bạn được theo dõi an toàn là khi ở chế độ máy bay hoặc bị chặn không cho truy cập vào các tín hiệu khác nhau này. Cuối cùng, ngày nay nhiều ứng dụng trên điện thoại của bạn cũng yêu cầu vị trí của bạn, chẳng hạn như WeChat. Điều này mở ra nhiều lựa chọn hơn cho cảnh sát để xác định vị trí điện thoại của bạn. Theo dõi vị trí không phải là vấn đề duy nhất bạn cần phải cân nhắc.

Nếu bạn quan tâm đến cuộc trò chuyện của mình với các đồng nghiệp, khách hàng hoặc nguồn tin đang bị nghe lén thì điện thoại lại gây ra vấn đề. Về mặt kỹ thuật, sử dụng điện thoại thông minh để nghe lén cuộc trò chuyện của bạn được gọi là "lỗi lưu thông", nhưng theo cách thức bình thường, chúng ta chỉ có thể gọi nó là nghe trộm.

Để nghe lén cuộc trò chuyện, trước tiên, cảnh sát phải xác định điện thoại của bạn. Điều này rất dễ dàng vì Việt Nam yêu cầu đăng ký thẻ SIM thực. Trong khi các thẻ SIM trên thị trường chợ đen chưa đăng ký có thể làm chậm quá trình này, thì chúng không phải là bảo đảm, vì cảnh sát chỉ đơn giản có thể xác định được điện thoại đang gửi tín hiệu từ địa điểm đã biết của bạn, chẳng hạn như nhà riêng hoặc văn phòng của bạn. Sau khi điện thoại của bạn đã được xác định, họ có thể truy cập vào điện thoại của bạn và bật micrô để ghi và truyền bất cứ thứ gì trong phạm vi microphone. Thao tác này được thực hiện dưới dạng dịch vụ nền và chạy mà không có thông báo, vì vậy bạn sẽ không biết. Cũng giống như vậy, máy ảnh trên điện thoại của bạn có thể được bật mà bạn không biết và sử dụng để ghi lại bạn, khách hàng và môi trường xung quanh. Hãy nhớ rằng, nguy cơ các micrô và máy ảnh truy cập từ xa cũng được áp dụng cho máy tính của bạn.

> "Máy ảnh và micrô trên điện thoại của bạn có thể được bật mà bạn không biết".

Điện thoại thông minh ngày nay gây ra nhiều vấn đề. Cách điện thoại di động trước đây được thiết kế đã làm cho việc đối phó với các mối đe dọa này trở nên dễ dàng hơn bằng cách tháo pin hoàn toàn khỏi điện thoại. Nhưng ngày nay, có thể tắt điện thoại nhưng thường không thể tháo pin. Hoặc nếu pin có thể được gỡ bỏ, hầu hết các điện thoại đi kèm với một tích hợp pin nhỏ hơn. Việc này được thực hiện để ngay cả khi bạn tắt điện thoại vào ban đêm, báo thức sẽ vẫn phát ra vào buổi sáng hoặc nếu bạn tắt điện thoại trong một thời gian, cài đặt lịch và múi giờ của bạn sẽ chính xác khi bạn khởi động lại. Ngay cả khi điện thoại của bạn bị tắt và bạn đã tháo pin, cảnh sát của một số quốc gia đã tìm cách nghe lén, bởi vì pin nhỏ này cho phép xâm nhập như trên. Vì vậy, chỉ đơn giản là tắt điện thoại sẽ không bao giờ cung cấp bảo mật thích hợp, và tháo pin điện thoại đã trở thành chuyện của quá khứ.

. "... chỉ tắt điện thoại của bạn sẽ không bao giờ có được bảo mật thích hợp".

Nếu bạn là một nguy cơ nghiêm trọng đối với cảnh sát, có nhiều cách khác nhau để họ có thể truy cập vào điện thoại của bạn, đọc tài liệu của bạn, chụp màn hình và hơn thế nữa. Ngày nay bạn không cần phải là một hacker chuyên nghiệp để đạt được những điều này.

Do các mối đe dọa như vậy, điện thoại của bạn nên được coi như là một thiết bị truyền thông chứ không phải là một máy tính làm việc nhỏ. Không bao giờ tải hoặc lưu các tệp, tài liệu hoặc ảnh nhạy cảm vào điện thoại của bạn. Xóa hoàn toàn các tập tin từ điện thoại có thể là thực sự khó khăn, và nếu bạn nhớ từ chương về xóa tài liệu, chỉ xóa một tập tin không thực sự loại bỏ nó. Do đó, không sử dụng điện thoại của bạn để lưu trữ, thậm chí tạm thời, bất kỳ tài liệu làm việc nào.

IMSI catchers là một công cụ yêu thích mới của cảnh sát ở nhiều quốc gia và là một công cụ nhỏ, dễ sử dụng và tiết kiệm chi phí để giám sát bằng điện thoại, thường được sử dụng trong biểu tình hay sự kiện có nhiều người tham gia. Một IMSI catcher đóng vai trò như là một tháp điện thoại di động (trạm cơ sở), và tất cả các điện thoại gần đó kết nối với nó, nghĩ đó là một tháp di động. Những IMSI catcher hiện nay nhỏ đến nỗi chúng không chỉ có thể bỏ vào va li, mà còn được bán dưới dạng thiết bị cá nhân. Tiêu chuẩn mã hoá điện thoại của bạn luôn được thiết lập bởi tháp di động chứ không phải điện thoại, do đó IMSI catcher hướng dẫn điện thoại của bạn không sử dụng mã hóa hoặc mã hóa rất cơ bản. Cảnh sát có thể xác định tất cả các điện thoại ở bất kỳ khu vực nào, ghi lại tất cả các tín hiệu và dữ liệu, và trực tiếp đọc nó. IMSI catcher tự đặt mình giữa điện thoại của bạn và tháp di động. Đây thường được gọi là tấn công "người đàn ông ở giữa", và cũng được sử dụng cho lưu lượng truy cập trên máy tính và internet, mặc dù nó hoạt động theo cơ chế khác.

Cuối cùng, một lần nữa để nhắc bạn rằng, bên cạnh những rủi ro này, được đặt ra theo cách hoạt động của điện thoại, các ứng dụng bạn cho phép trên điện thoại sẽ cho phép truy cập giống nhau nhưng thông qua Apps thay vào đó, thậm chí còn dễ dàng hơn. Hãy cẩn thận với những gì bạn cài đặt và nhận ra rằng ở Việt Nam sẽ rất nguy hiểm vì cảnh sát có quyền truy cập trực tiếp vào các công ty và máy chủ của họ, và các công ty này không cung cấp cho bạn sự bảo vệ hợp pháp trước khi đưa ra bất cứ điều gì cho cảnh sát.

ĐIỆN THOẠI CỦA BẠN CÓ BỊ NGHE TRỘM KHÔNG?

Trước đây, việc phát hiện điện thoại bị nghe trộm khá dễ dàng. Những âm thanh được lặp lại là điều thường thấy ở điện thoại cố định khi bị nghe trộm, hoặc nhiễu loạn bất thường và tiếng vang được nghe trên điện thoại di động của bạn. Ngày nay, việc nghe trộm được thực hiện thông qua các ứng dụng ẩn, và tương tự như việc hacker máy tính hơn là cách nghe trộm điện thoại cổ điển khai thác. Tuy nhiên, việc nghe trộm điện thoại tiếp tục được sử dụng rộng rãi.

Như vậy, có một số điều cần xem xét.

Nói chung, nếu đường dây điện thoại của bạn đang bịc theo dõi, nó sẽ có tiếng ồn, bởi vì liên kết được chia sẻ với người nghe khác. Nếu bạn lớn lên trong một hộ gia đình với nhiều điện thoại đến một đường điện thoại cố định, bạn sẽ biết rằng nếu ai đó nghe trộm điện thoại trong khi bạn nhận thấy một cách rõ ràng.

Để có thể sử dụng tính năng này, bạn cần phải chú ý đến tiếng ồn thông thường mà bạn nghe thấy khi bạn gọi một người cụ thể. Nếu bạn nhận thấy sự thay đổi của loại tiếng ồn, đó là một mối bận tâm.

Tuy nhiên, gọi những người khác nhau ở những vị trí khác nhau sẽ có tiếng ồn khác nhau, vì vậy bạn phải so sánh với người cụ thể và cuộc đàm thoại nhất định, và xem nếu bạn nhận thấy sự thay đổi.

Âm thanh điển hình là:

- Lặp lại các âm thanh nhấp chuột
- tiếng ồn nhiễu tĩnh
- tiếng ồn ào cao

Để kiểm tra việc này, đảm bảo bạn không ở gần các thiết bị điện tử khác (TV, router, máy tính vv) là những vật có thể gây ra tiếng ồn.

Điện thoại của bạn có thể đã bị xâm nhập thông qua một số ứng dụng nếu bạn nhận thấy:

- tin nhắn SMS ngẫu nhiên chứa văn bản hay số … (một lỗi trong giám sát phần mềm dùng để kiểm soát điện thoại của bạn
- nhanh cạn kiệt pin
- quảng cáo popup
- hoạt động chậm, xấu hoặc không đều
- Dung lượng sử dụng tăng đột biến
- quá nóng

NHỮNG ĐIỂM QUAN TRỌNG

- Nhận thức được loại mối đe dọa đang tồn tại đối với điện thoại
- Giới hạn số lượng ứng dụng bạn cài đặt
- Xem xét cài đặt điện thoại của bạn và kiểm tra các ứng dụng được cài đặt trước, loại bỏ tất cả những thứ bạn không cần
- Nếu nghi ngờ hoặc cảm thấy có nguy cơ điện thoại bị xâm nhập, không sử dụng điện thoại của bạn, không mang theo với bạn, đừng để nó bật
- Không sử dụng điện thoại làm việc thay cho máy tính, nó chỉ là một thiết bị truyền thông
- Tránh các ứng dụng và dịch vụ của các công ty Trung Quốc
- Google (hoặc thậm chí tốt hơn, DuckGoGo) là bạn của bạn - bất cứ điều gì trong cài đặt điện thoại của bạn hoặc bất kỳ ứng dụng cài sẵn nào mà bạn không hiểu thì có thể kiểm tra bằng Google.

CHƯƠNG 9
SỬ DỤNG ĐIỆN THOẠI

Chương này sẽ chỉ cho bạn cách sử dụng điện thoại một cách an toàn, quan trọng hơn nhiều so với các giải pháp kỹ thuật có thể có.

ĐIỆN THOẠI CỦA BẠN KHÔNG

Không giống với máy tính, bạn không thể bảo vệ nội dung của mình theo bất kỳ cách hiệu quả nào. Ngay cả khi bạn giữ nó được mã hóa (và hầu hết các điện thoại được mã hóa tự động những ngày này), bạn không thể sử dụng bất kỳ phương pháp tiên tiến hơn cho nó. Có vài lớp bảo mật từ mã PIN bạn nhập để truy cập vào điện thoại của bạn đến tất cả các phần khác nhau của điện thoại. Để giữ những gì bên trong an toàn trong trường hợp bạn bị mất điện thoại không phải là một vấn đề lớn, nhưng thật khó giữ nó an toàn từ cảnh sát hay tội phạm nếu bạn đã bị bắt và buộc phải cung cấp mã PIN. Trong trường hợp sau, nội dung bên trong điện thoại của bạn sẽ không thể bảo vệ được.

Bởi vì thiếu lớp bảo vệ, và việc sử dụng chung các ứng dụng để truy cập các dịch vụ thay vì sử dụng một trình duyệt (và việc thiếu khả năng xóa dấu vết của trình duyệt của điện thoại), nếu bạn đang bị buộc phải đưa ra số PIN của bạn, họ sẽ không chỉ nhận được quyền truy cập vào điện thoại mà vào bất kỳ dịch vụ ứng dụng nào có trên điện thoại, hoặc những gì truy cập qua trình duyệt gần đây. Thông qua đó, bất cứ ai cũng có thể bắt buộc bạn để dễ dàng truy cập vào các dịch vụ nếu không được bảo vệ tốt. Vì vậy, họ có thể sử dụng điện thoại của bạn để khai thác tài liệu nếu không được bảo mật an toàn. Không cho phép họ sử dụng điện thoại của bạn để phá vỡ các biện pháp bảo mật của bạn cũng như không sử dụng điện thoại làm máy tính thứ hai.

> “Không giống với máy tính, bạn không thể bảo vệ nội dung (trên điện thoại của bạn) hiệu quả theo bất kỳ cách nào.”

Tất cả điều này có nghĩa là điện thoại của bạn không phải là máy tính để làm việc. Không bao giờ nên lưu trữ bất kỳ tài liệu công việc nào, sử dụng thiết bị chuyển tệp, cũng không nên cho phép truy cập từ điện thoại của bạn vào bất kỳ dịch vụ công việc nào mà bạn sử dụng trên máy tính của bạn.

ĐIỆN THOẠI CỦA BẠN CÓ THỂ LÀ GÌ

Mặc dù tất cả những gì đã được nói ở trên, và trong chương trước, điện thoại của bạn có thể là một công cụ truyền thông rất hiệu quả và an toàn. Điều quan trọng là chỉ sử dụng nó cho mục đích này, và không cho phép nó được sử dụng vào bất cứ điều gì khác. Một bước cần thực hiện để đạt được điều này là sử dụng các ứng dụng bảo mật để truyền thông như vậy, cho phép tự động hủy các tin nhắn của bạn để ngăn những người bên ngoài có thể theo dõi nội dung cuộc trò chuyện trước đó nếu họ có điện thoại của bạn. Các chương trình chat được mã hóa cuối cùng kết hợp với việc tự động hủy các bản ghi cuộc trò chuyện của bạn là một công cụ mạnh mẽ và hiệu quả cho truyền thông.

ĐI TỐI

Đi tối, có nghĩa là ngắt điện thoại của bạn khỏi bất kỳ loại truyền nào, là cách duy nhất để đảm bảo điện thoại của bạn không được sử dụng chống lại bạn. Nếu bạn đang thảo luận và muốn chắc chắn rằng cuộc trò chuyện của bạn không được ghi lại, đó là giải pháp duy nhất. Tương tự như vậy nếu bạn không muốn máy quay ghi lại bạn, hoặc vị trí chính xác nơi bạn được biết, bạn phải đi tối. Bạn có thể làm điều này bằng nhiều cách, và cách đơn giản nhất là bật Chế độ trên máy bay (Flight mode). Bằng cách đó, bạn sẽ ngừng truyền mạng di động (lưu lượng điện thoại đến tháp điện thoại di động), truyền internet không dây, cũng như Bluetooth. Cho dù nó sẽ tắt nhận tín hiệu GPS thay đổi theo điện thoại. Tuy nhiên, điện thoại thông minh chỉ nhận được dữ liệu GPS, nó không (cũng không thể) gửi nó. Điều đó có nghĩa là miễn là các dạng truyền khác đã bị tắt, bạn vẫn an toàn.

Một điểm yếu của phương pháp ở trên là nếu một ứng dụng chuyển dữ liệu mà bạn không biết mà bạn có thể thực hiện nếu điện thoại của bạn được nhắm mục tiêu. Một điểm khác là vị trí GPS của bạn vẫn sẽ được ghi lại nếu bạn đã bật GPS và dữ liệu vị trí có thể được gửi bằng ứng dụng sau khi bạn không còn ở Chế độ trên máy bay nữa.

Một cách khác để Đi tối, một cách rất dễ dàng, là sử dụng thiếc nhôm. Nhiều người làm việc với các vấn đề nhạy cảm và nguy hiểm thường đóng gói một vài tờ thiếc nhôm trong túi của họ. Bằng cách gói điện thoại của bạn trong hai lớp thiếc (bao gồm tất cả các phần của điện thoại), bạn sẽ chặn tất cả các truyền. Đó là phương pháp tốt nhất của bạn để đi tối. Ngày nay, các cửa hàng trực tuyến cũng bán các túi điện thoại nhỏ đặc biệt, được lót bằng vật liệu bằng thiếc ở bên trong, sẽ đạt được điều tương tự mà không nghi ngờ gì. Chúng tôi khuyên bạn nên kiểm tra nó. Bao bọc trong điện thoại của bạn trong hai lớp và cố gắng gọi nó. Gửi tin nhắn hoặc email và xem nó có nhận được tin nhắn hay không (tạo ra âm thanh có liên quan). Nếu có, thì bạn cần một lớp khác, nhưng nó rất không chắc. Tuy nhiên, nếu bạn muốn sử dụng phương pháp này, thậm chí chỉ là sao lưu, hãy thử nó trước để bạn biết kết quả cho điện thoại của mình.

> “Bằng cách gói điện thoại của bạn trong hai lớp giấy thiếc (bao gồm tất cả các phần của điện thoại), bạn sẽ chặn tất cả các truyền”

TỰ ĐỘNG ĐỒNG BỘ VÀ SAO LƯU

Một mối đe dọa bảo mật lớn với điện thoại là nó đi kèm với đăng nhập tự động vào nhiều dịch vụ. Các ứng dụng này thường chỉ có một giao diện hạn chế so với dịch vụ đầy đủ có sẵn trong một trình duyệt. Tuy nhiên, truy cập thường không có mật khẩu hoặc mã PIN được bảo vệ. Việc truy cập vào điện thoại của bạn có nghĩa là truy cập vào tất cả các dịch vụ được cài đặt. Đừng đánh giá thấp mối đe dọa này. Không bao giờ cài đặt các dịch vụ liên quan đến các ứng dụng mà bạn thường truy cập thông qua trình duyệt công việc của bạn trên máy tính của bạn, mặc dù nó có thể gây cám dỗ như thế nào. Tương tự như vậy, không sử dụng bất kỳ dịch vụ lưu trữ đám mây nào hoặc dịch vụ trực tuyến khác trên cả máy tính và điện thoại cho công việc của bạn. Sử dụng tài khoản và dịch vụ riêng. Ví dụ: nếu bạn muốn lưu trữ trên đám mây, hãy sử dụng Google Drive trên máy tính làm việc của bạn và sử dụng DropBox hoặc OneDrive hoặc một thứ khác cho điện thoại của bạn. Tách bạch giữa máy tính công việc và điện thoại của bạn, và các dịch vụ có trên điện thoại.

Vì vậy, chìa khóa an toàn là để hạn chế cách bạn sử dụng điện thoại và xem điện thoại của bạn chỉ như một thiết bị truyền thông và không sử dụng cho các mục đích công việc khác với giao tiếp. Đừng nghiên cứu trực tuyến bằng điện thoại của bạn, không tải tài liệu hoặc có các tệp công việc trên đó.

BA BƯỚC BAN ĐẦU ĐỂ ĐẢM BẢO ĐIỆN THOẠI CỦA BẠN

> "Giữ sự riêng biệt giữa máy tính công việc và điện thoại của bạn, và các dịch vụ có trên điện thoại."

Chế độ bay cũng sẽ bật NFC (trên Android đôi khi được gọi là Beam), đó là một hệ thống truyền dẫn ngắn - về cơ bản bạn có thể đặt hai điện thoại bên cạnh nhau và chúng có thể giao tiếp và chuyển dữ liệu.

CÀI ĐẶT LẠI MÁY

Trừ khi bạn có hiểu biết đầy đủ về điện thoại của mình và cảm thấy an toàn trong trạng thái bảo mật điện thoại hiện tại, bạn cần bắt đầu bảo vệ nó bằng cách thực hiện khôi phục cài đặt gốc. Điều này sẽ làm bạn mất bất cứ thứ gì trên điện thoại của mình, vì vậy hãy sao lưu bất kỳ ảnh hoặc các tệp khác mà bạn có thể có và muốn giữ lại (Android - XX).

MÃ HÓA

Điện thoại của bạn có thể đã được bật mã hóa. Nếu bạn có điện thoai Android, rất có thể là nó chưa. Điện thoại, và bất kỳ thẻ SD nào trong đó, có thể được mã hóa rất dễ dàng. Sau khi thiết lập lại nhà máy, những điều đầu tiên bạn làm là bật mã hóa nếu không bật, và chọn một mã PIN hoặc mật khẩu thích hợp. Bao gồm thẻ SD (nếu có) khi bạn làm việc này.

Đối với điện thoại của bạn, bạn chỉ cần vào Bảo mật trong Cài đặt và nhấp vào Encrypt device/ Thiết bị mã hóa (Android - XX), và nó sẽ yêu cầu nhập mã PIN hoặc mật khẩu và bắt đầu quá trình. Không có dữ liệu sẽ bị xóa. Bạn cũng có thể chọn Encrypt external SD card/Mã hóa thẻ nhớ ngoài và nếu điện thoại của bạn sử dụng thẻ nhớ SD, bạn nên thực hiện việc này sau khi đã mã hóa thiết bị của mình.

XOÁ/XÓA CÀI ĐẶT

Xem các ứng dụng và dịch vụ được cài đặt trên điện thoại của bạn sau khi khôi phục cài đặt gốc và mã hóa đã được thực hiện và gỡ cài đặt hoặc vô hiệu hóa bất kỳ ứng dụng và dịch vụ nào mà bạn sẽ không sử dụng. Nhiều điện thoại đi kèm với ứng dụng thậm chí sau khi thiết lập lại nhà máy. Xóa tất cả chúng, giúp an toàn cho bạn nhưng cũng làm cho điện thoại của bạn nhanh hơn và để pin kéo dài hơn.

ĐIỆN THOẠI CÓ THỂ PHÁ HUỶ TẤT CẢ

Người đứng trong câu chuyện này không phải là luật sư hay nhà báo, sống ở một thị trấn nhỏ trong một tỉnh nghèo ở một quốc gia ở Đông Nam Á. Ông còn chưa tốt nghiệp trung học. Tuy nhiên, ông có nhiều kinh nghiệm sống.

Trong hơn 10 năm, ông đã làm việc không mệt mỏi để hỗ trợ nhiều nạn nhân của chính sách đàn áp của chính phủ.

Mặc dù không sống ở thành phố lớn, ông có thể sử dụng email, máy tính để học hỏi và nghiên cứu các luật của quốc gia và sử dụng để hỗ trợ những nạn nhân của chính phủ.

Thông thường, khi một nông dân khác có nguy cơ bị cướp đất, anh ta sẽ cầu cứu nhiều nông dân khác đến hỗ trợ. Tuy nhiên, nhiều trong số những người được gọi hỗ trợ đã không bao giờ đến, số khác bị cảnh sát chặn trước khi ra khỏi nhà và nhiều người đã bị tạm giữ hoặc bị đưa đi mất tích.

Từ những vụ việc trên, ông hiểu rằng tin nhắn của họ đã bị đọc trộm. Thông minh hơn so với được đào tạo, ông bắt đầu học cách giao tiếp an toàn và chia sẻ ý tưởng của mình với nhiều người khác.

Mặc dù ông đã bị cảnh sát quản thúc tại nhà và nhiều lần bị bắt giữ lên đồn công an để thẩm vấn và bị khám nhà và thu giữ máy tính và điện thoại, nhưng cảnh sát không có bằng chứng chống lại ông do ông đã thực hiện chính sách "hộp thư trống" cũng như đặt chế độ tự xoá cho những chương trình chat.

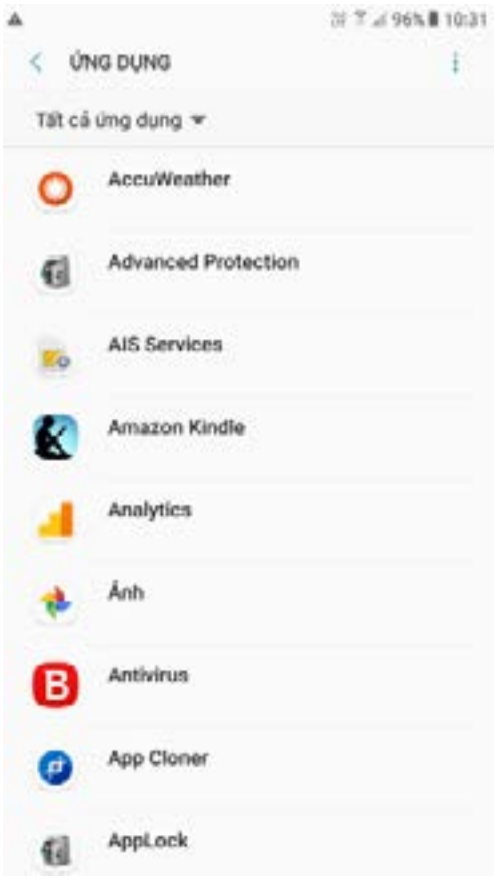
Ông đã sử dụng VPN để đăng nhập Internet do vậy việc liên lạc với người cần được hỗ trợ không bị rò rỉ.

Do thiếu bằng chứng kết tội ông hỗ trợ nạn nhân của chính quyền, ông chỉ bị giam giữ 15 ngày. Cảnh sát cảnh báo nếu ông tiếp tục công việc, ông có thể bị bắt và khởi tố.

CHƯƠNG 10
CÀI ĐẶT ĐIỆN THOẠI

Chương này, như Chương 2: Chuẩn bị máy tính của bạn, sẽ cung cấp thông tin về cài đặt để bạn có thể kiểm soát điện thoại của mình. Như với máy tính, tìm hiểu các cài đặt này, và làm thay đổi cho phù hợp, là một bước quan trọng và luôn là bước đầu tiên để bảo đảm an toàn trong giao tiếp bằng điện thoại. Không có ứng dụng hoặc chương trình nào có thể bảo mật điện thoại của bạn trừ khi ác cài đặt cơ bản đã được điều chỉnh đầu tiên.

Chúng ta đã sẵn sàng để đi đến khu vực cài đặt của điện thoại và thực hiện các thay đổi cần thiết để mang lại cho bạn sự bảo mật cơ bản. Vì điện thoại Android thay đổi về ngoại hình và bố cục của các menu và khu vực cài đặt, nhưng gần như luôn luôn sử dụng cùng một cụm từ và biểu thức, chúng tôi sẽ cung cấp các thuật ngữ hoặc biểu thức và để bạn tìm thấy nó bên trong khu vực cài đặt của điện thoại thay vì hiển thị màn hình của từng bước. Nó cũng sẽ cho phép bạn làm quen với khu vực cài đặt của điện thoại nếu bạn chưa quen.



Do thay đổi giữa các phiên bản khác nhau của hệ điều hành trên điện thoại và các nhà sản xuất điện thoại Android khác nhau, một số điện thoại có thể sử dụng thuật ngữ khác hoặc thay đổi cách tìm cài đặt. Nếu hướng dẫn dưới đây không hoạt động cho điện thoại của bạn, hãy sử dụng DuckGoGo hoặc Google để tìm cách thực hiện các thay đổi này trên điện thoại của bạn.

CÀI ĐẶT VÀ QUYỀN TRUY CẬP CÁC ỨNG DỤNG

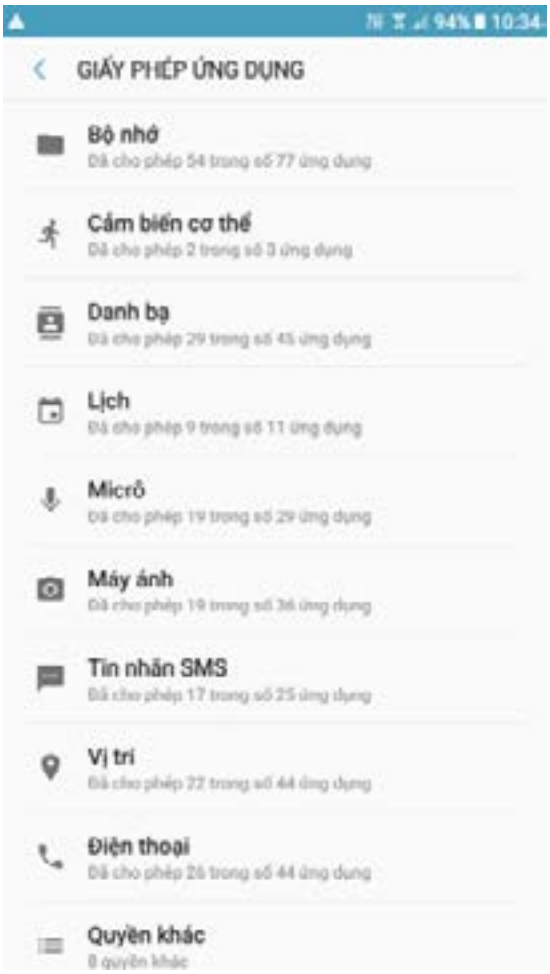
Đối với điện thoại Android, chúng ta sẽ đến khu vực Setting/Cài đặt. Trên Android, nếu bạn có một khu vực Cài đặt Google, chúng tôi cũng cần phải đi đến đó.

Cách đơn giản nhất để kiểm soát điện thoại của bạn và giới hạn những gì các ứng dụng có thể làm là truy cập vào Application Manager và nhấp vào mỗi ứng dụng và chọn quyền mà ứng dụng có thể, ví dụ: quyền truy cập vào lịch, máy ảnh, vị trí, vv (Android - XX và XX).

Trên nhiều điện thoại (nhưng không phải tất cả) cũng sẽ có một khu vực cài đặt khác, nơi bạn có thể kiểm tra từng dịch vụ (Android - XX và XX), ví dụ Vị trí, Microphone, v.v ... và xem Ứng dụng nào có quyền cho dịch vụ cụ thể đó. Bạn tìm thấy các cài đặt này bằng cách:

SAMSUNG: Settings > Applications > Application manager
ANDROID: Settings > Apps > Select which APP
SAMSUNG: Settings > Privacy and Safety > App Permissions
ANDROID: Settings > Apps > Permissions > Select Permission category

Thật không may các ứng dụng thường yêu cầu truy cập tối đa ngay cả khi nó không cần thiết, và ngay cả khi một ứng dụng thậm chí không thể sử dụng sự cho phép đó. Do đó, điều quan trọng là dành một chút thời gian và đi qua một trong hai khu vực đã đề cập ở trên, và kiểm tra các quyền cho mọi thứ. Đây là cách tốt nhất để kiểm soát chính xác những gì các ứng dụng có thể làm trên điện thoại của bạn.



Điều này cũng có nghĩa là bạn có hai lựa chọn. Bạn có thể tắt hoàn toàn một dịch vụ, ví dụ như Localtion/Vị trí, hoặc bạn có thể cho phép nó, nhưng quản lý vi mô những gì các ứng dụng được phép sử dụng. Sẽ là tốt nếu bạn tắt hoàn toàn một dịch vụ, nhưng đó có thể không phải luôn luôn phù hợp và hiệu quả cho bạn. Nếu bạn để lại dịch vụ, hãy đảm bảo xem lại (như ở trên) ứng dụng nào được phép sử dụng và thực hiện thường xuyên sau khi cài đặt bất kỳ ứng dụng mới nào.

Vị trí, Camera và Micro là ba dịch vụ chính cần lưu ý. Các loại cho phép khác bạn có thể kiểm soát bao gồm đọc/gửi SMS, truy cập kho lưu trữ, lịch, danh sách liên lạc, đọc/gửi email ... Hãy đảm bảo bạn có toàn quyền kiểm soát ứng dụng nào có thể sử dụng vị trí, máy ảnh và micrô của bạn. Chúng tôi khuyên bạn nên tắt hoàn toàn vị trí.

Bạn nên tắt kết nối khác mà bạn không sử dụng. Bên cạnh Wi-Fi, điện thoại của bạn cũng cung cấp Bluetooth, NFC và trong một số trường hợp Android Beam. Hãy tắt tất cả những thứ này trừ khi bạn đang sử dụng chúng. Đây là những lựa chọn kết nối không dây tầm xa và không cần phải giữ chúng hoạt động trừ khi bạn thường xuyên sử dụng chúng.

SAMSUNG: Settings > Bluetooth + NFC and Payment + More connection settings > set Nearby device scanning off

ANDROID: Settings > Bluetooth + Wireless & Networks > More…

Những gì có thể được cài đặt? Trong phần bảo mật và quyền riêng tư, bạn sẽ tìm thấy cài đặt cho phép hoặc không cho phép Unknown Sources/Nguồn không xác định. Bạn không nên cho phép điều này. Điều này sẽ chặn cho phép cài đặt bất kỳ chương trình hoặc ứng dụng nào không được chính thức xác minh bởi cửa hàng điện thoại. Nếu bạn cần cài đặt một cái gì đó đặc biệt bạn chỉ cần tắt nó trong khi cài đặt chương trình nói trên, sau đó bật lại. Đối với Điện thoại iOS bạn không cần phải lo lắng về điều này, vì chỉ có Apple Store Apps có thể được cài đặt theo chuẩn.

SAMSUNG: Settings > Lock screen and security

ANDROID: Settings > Security

THÔNG BÁO, KHÓA MÀN HÌNH, TỰ ĐỘNG KHÓA VÀ TỰ ĐỘNG HỦY

Nếu bạn muốn không cho những người khác truy cập tin nhắn và các hình thức truyền thông khác trên điện thoại, khóa bảo vệ màn hình của bạn là chìa khóa. Hầu hết các điện thoại đều được cài sẵn để hiển thị thông báo đầy đủ trên màn hình khóa của bạn, nghĩa là bạn có thể đọc các tin nhắn, email, v.v. mới trên màn hình khóa mà không phải mở điện thoại. Điều này cần được thay đổi. Một lần nữa, như ở trên, bạn có thể đặt để ẩn tất cả các thông báo, hoặc bạn có thể chọn để cho phép chúng, và sau đó kiểm tra danh sách trong cài đặt đó và cho phép / từ chối cho từng ứng dụng riêng lẻ. Bạn không nên để ứng dụng sử dụng cho công việc được phép hiển thị thông báo trên màn hình khóa của bạn.

SAMSUNG: Settings > Lock screen and security > Notifications on Lock Screen

ANDROID: Settings > Sound & Notifications > When Device is Locked (select Hide sensitive notification content

Bạn cũng có thể kiểm soát những ứng dụng nào có thể hoặc sẽ cung cấp cho bạn thông báo trong điện thoại (không phải trên màn hình khóa). Có thể có ứng dụng mà bạn không muốn bất kỳ thông báo nào cả và chỉ kiểm tra bằng tay.

SAMSUNG: Settings> Notifications

ANDROID: Settings> Sound and Notification

ANDROID: Settings > Sound & Notification > App Notifications

ANDROID: Apps > Permissions OR Apps > Click Gear Icon > Select App Permissions

Trong khi bạn đang xử lý khóa màn hình, hãy đảm bảo bật Lock Automatically/Khóa tự động và đặt thời gian ngắn, như 5, 10 hoặc 15 giây. Đồng thời bật Khóa ngay bằng phím nguồn nếu có thể (màn hình khóa tiếp tục bật khi bạn nhấn phím nguồn). Cuối cùng, bật Auto factory reset/Tự động khôi phục cài đặt gốc. Cài đặt cuối cùng này có nghĩa là nếu ai đó nhập mã PIN sai vào điện thoại của bạn 10 hoặc 15 lần liên tiếp, điện thoại của bạn sẽ tự động được cài đặt lại/xóa.

SAMSUNG: Settings> Lock screen and security > Secure Lock settings

ANDROID: Settings> Security

Bạn đã chọn mã PIN hoặc mật khẩu khi bật Mã hoá, nhưng nếu vì lý do nào đó không bật Khóa màn hình, hãy đảm bảo bật. Ngoài ra, nếu điện thoại hoặc bàn phím của bạn cho phép nhận dạng vân tay (chạm), giọng nói, nhận dạng khuôn mặt hoặc nhận dạng võng mạc (mắt) như một cách để mở khóa điện thoại hoặc bàn phím của bạn, hãy tắt nó đi.

CẬP NHẬT TỰ ĐỘNG

Giống như máy tính của bạn, điện thoại của bạn chỉ an toàn như cập nhật mới nhất. Đảm bảo bật tính năng cập nhật tự động cho điện thoại của bạn.

SAMSUNG: Settings > About Device

ANDROID: Settings > About Phone

ĐỒNG BỘ HÓA VÀ LƯU TRỮ ĐÁM MÂY

Xác định bất kỳ dịch vụ đám mây được xây dựng nào, sẽ hiển thị trong khu vực cài đặt của bạn và thực hiện những thay đổi cần thiết. Hãy chắc chắn rằng bất kỳ dịch vụ đám mây như vậy hoặc là tắt, hoặc nó không bao gồm bất cứ điều gì liên quan đến công việc của bạn. Nếu bạn muốn sử dụng sao lưu hoặc lưu trữ dựa trên Cloud, hãy tham khảo Chương 6: Chia sẻ thông tin, và quyết định cách sử dụng nó tốt nhất và những dịch vụ nào cần sử dụng.

Một vài ghi chú cuối cùng về cài đặt điện thoại.

Đối với điện thoại Android và iOS Không tham gia quảng cáo (Android).

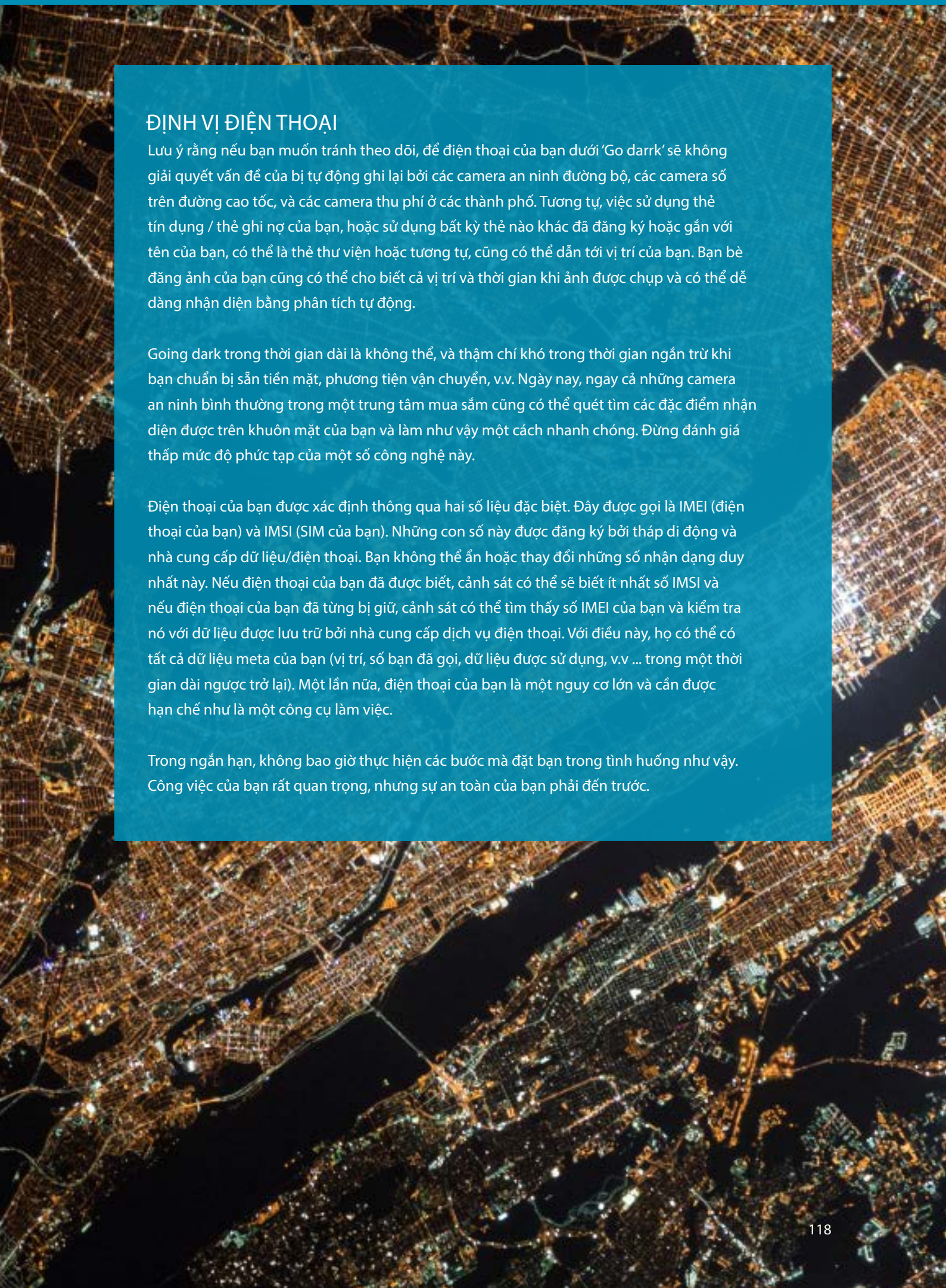
ANDROID: Google Settings > Ads

Để an toàn, bạn có thể muốn tắt chức năng lệnh bằng giọng nói (OK Google, Cortana, Siri vv), hoặc ít nhất là đảm bảo rằng nó không thể được sử dụng khi Lock Screen được bật.

Cuối cùng, nếu bạn sử dụng điện thoại Android có cài đặt Google trên đó, hãy duyệt qua khu vực và đảm bảo bạn biết cài đặt, ứng dụng và thiết bị nào được kết nối với tài khoản của bạn và tắt Smart Lock for Passwords và thực hiện các thay đổi khác như bạn thấy phù hợp.

NHỮNG ĐIỂM QUAN TRỌNG

- Đảm bảo rằng không thể đọc được các tin nhắn mới, email vv ... khi màn hình khóa.
- Đảm bảo bạn có toàn quyền kiểm soát và hiểu về các ứng dụng và các chức năng có thể sử dụng vị trí của bạn.
- Kiểm tra lại những ứng dụng mà bạn có, và thay đổi cho phù hợp.
- Đảm bảo máy ảnh của bạn không bao giờ được phép có thông tin về vị trí của bạn.



ĐỊNH VỊ ĐIỆN THOẠI

Lưu ý rằng nếu bạn muốn tránh theo dõi, để điện thoại của bạn dưới 'Go darrk' sẽ không giải quyết vấn đề của bị tự động ghi lại bởi các camera an ninh đường bộ, các camera số trên đường cao tốc, và các camera thu phí ở các thành phố. Tương tự, việc sử dụng thẻ tín dụng / thẻ ghi nợ của bạn, hoặc sử dụng bất kỳ thẻ nào khác đã đăng ký hoặc gắn với tên của bạn, có thể là thẻ thư viện hoặc tương tự, cũng có thể dẫn tới vị trí của bạn. Bạn bè đăng ảnh của bạn cũng có thể cho biết cả vị trí và thời gian khi ảnh được chụp và có thể dễ dàng nhận diện bằng phân tích tự động.

Going dark trong thời gian dài là không thể, và thậm chí khó trong thời gian ngắn trừ khi bạn chuẩn bị sẵn tiền mặt, phương tiện vận chuyển, v.v. Ngày nay, ngay cả những camera an ninh bình thường trong một trung tâm mua sắm cũng có thể quét tìm các đặc điểm nhận diện được trên khuôn mặt của bạn và làm như vậy một cách nhanh chóng. Đừng đánh giá thấp mức độ phức tạp của một số công nghệ này.

Điện thoại của bạn được xác định thông qua hai số liệu đặc biệt. Đây được gọi là IMEI (điện thoại của bạn) và IMSI (SIM của bạn). Những con số này được đăng ký bởi tháp di động và nhà cung cấp dữ liệu/điện thoại. Bạn không thể ẩn hoặc thay đổi những số nhận dạng duy nhất này. Nếu điện thoại của bạn đã được biết, cảnh sát có thể sẽ biết ít nhất số IMSI và nếu điện thoại của bạn đã từng bị giữ, cảnh sát có thể tìm thấy số IMEI của bạn và kiểm tra nó với dữ liệu được lưu trữ bởi nhà cung cấp dịch vụ điện thoại. Với điều này, họ có thể có tất cả dữ liệu meta của bạn (vị trí, số bạn đã gọi, dữ liệu được sử dụng, v.v ... trong một thời gian dài ngược trở lại). Một lần nữa, điện thoại của bạn là một nguy cơ lớn và cần được hạn chế như là một công cụ làm việc.

Trong ngắn hạn, không bao giờ thực hiện các bước mà đặt bạn trong tình huống như vậy. Công việc của bạn rất quan trọng, nhưng sự an toàn của bạn phải đến trước.

CHƯƠNG 11

CÁC ỨNG DỤNG BẢO MẬT TRÊN ĐIỆN THOẠI

Trong chương này, chúng tôi sẽ trình bày một chuỗi các ứng dụng và chương trình bạn cần làm để giao tiếp một cách an toàn và tốt hơn. Chúng tôi sẽ thay thế chương trình quản lý SMS đã xây dựng bằng một chương trình tương tự nhưng với mã hoá hai đầu, chúng tôi sẽ chỉ ra cách sử dụng TOR một cách dễ dàng để lướt web một cách an toàn và không có giới hạn, và trình bày các chương trình trò chuyện mà không chỉ mã hóa nhưng tự động hủy các bản ghi trò chuyện của bạn.

Khi bạn cài đặt ứng dụng lần đầu tiên, đảm bảo đi đến khu vực cài đặt của nó và tự làm quen với phần cài đặt của ứng dụng. Một số ưng dụng an toàn, như Signal và Telegram, đi kèm với bảo vệ bằng mã PIN hoặc mật khẩu. Điều này có nghĩa là ứng dụng cho phép bạn thiết lập một mã PIN riêng để truy cập ứng dụng đó. Đối với Signal và Telegram, đây là điều bắt buộc. Nhiều ứng dụng không có mật khẩu riêng. Bằng cách sử dụng mã PIN riêng cho ứng dụng, bạn có thể đảm bảo rằng ngay cả khi điện thoại thông minh của bạn bị rơi vào tay người khác, thì một số ứng dụng vẫn an toàn.

IN NHẮN SMS VÀ CUỘC GỌI

Cài đặt Signal Private Messenger, ứng dụng sẽ thay thế cả tin nhắn SMS và chương trình gọi điện thoại của bạn. Khi gửi tin nhắn SMS (Settings >SMS and MMS> select SMS Enabled) hoặc thực hiện cuộc gọi đến bất cứ ai sử dụng Signal, bạn sẽ tự động sử dụng mã hóa hai đầu đầu và tin nhắn SMS và cuộc gọi điện thoại của bạn được bảo vệ khỏi bị nghe trộm.

Signal đi kèm với PIN hoặc bảo vệ mật khẩu. Bật và sử dụng mã PIN cụ thể để truy cập Signal (Settings > Privacy). Đối với tin nhắn, khi trên Wi-Fi sẽ hoạt động giống như tin nhắn trò chuyện bình thường (không được gửi dưới dạng SMS, và do đó tiết kiệm tiền) (Settings > SMS and MMS > enable WiFi Calling i). Cuối cùng, nhập lại cài đặt và Chats and Media và cho phép Delete old messages và thiết lập thời gian (ví dụ, nó sẽ tự động xóa bất cứ điều gì nhiều hơn 5 tin nhắn mới nhất).

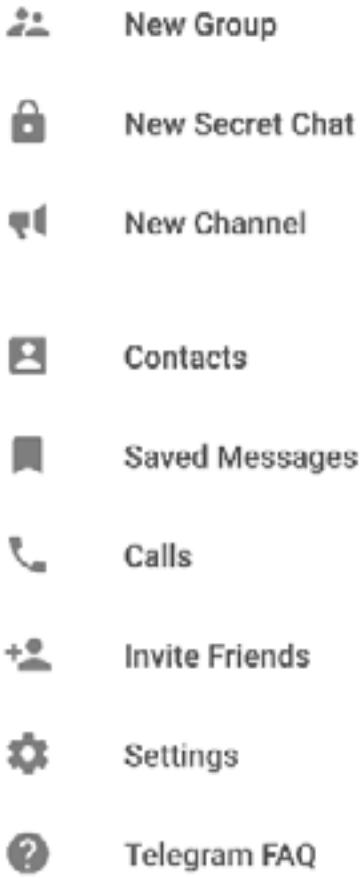
Khi bạn bắt đầu cuộc trò chuyện, hãy nhấp vào góc trên bên phải và bạn sẽ thấy một tùy chọn cho các thông báo Delete/Xóa. Nhấp vào đây và chọn hẹn giờ. Điều này có nghĩa là mọi tin nhắn được gửi và nhận sẽ bị xóa sau một khoảng thời gian đã đặt (sau khi đã được đọc).

Để sử dụng mã hóa hai đầu cho tin nhắn trò chuyện SMS và cuộc gọi điện thoại, bạn và người

nhận phải cài đặt Signal Private Messenger. Như vậy, đảm bảo bạn cài đặt nó, và để cho đồng nghiệp, bạn bè và bạn bè của bạn làm như vậy. Ngay cả khi ISMI catcher được sử dụng để loại bỏ mã hóa tín hiệu điện thoại bình thường của bạn, bạn sẽ vẫn an toàn, vì chương trình sử dụng mã hóa hai đầu.

TRÒ CHUYỆN

Như là một sự bổ sung cho Signal Private Messenger, chúng tôi khuyên bạn nên cài đặt Telegram. Telegram có thể hoạt động giống như một chương trình trò chuyện bình thường (với mã hóa thông thường), nhưng cũng có một chức năng gọi là Secret Chat/Trò chuyện bí mật. Nếu sử dụng trò chuyện bí mật, tin nhắn của bạn được mã hóa hai đầu và bạn có thể đặt một bộ đếm thời gian tự động hủy cho tất cả các tin nhắn được gửi và nhận.



Đối với chương trình nhắn tin mã hoá hai đầu mà cho phép tự xoá tin nhắn (bạn có thể đặt thời gian xoá), hãy chọn "Chat bí mật mới"/"New Secret Chat". (67).

Như đã đề cập trước đây, việc tự động hủy các bản ghi trò chuyện là chìa khóa cho sự an toàn của bạn, hơn là mã hóa tiên tiến vì nó không để lại bằng chứng nào cho thấy dấu vết và thông tin mà người khác có thể ăn cắp hoặc sử dụng chống lại bạn. Giống như Signal Private Messenger, Telegram có mã PIN / mật khẩu được xây dựng sẵn hoặc có sẵn. Chọn mã PIN duy nhất để mở Telegram.

SURFING, TOR VÀ VPNS

Cách đơn giản nhất trên Android để lướt web an toàn là sử dụng Orbot hoặc Orfot của dự án Guardian. Orbot là TOR cho Android và là ứng dụng bắt đầu TOR trên thiết bị của bạn. Bạn có thể, trong khu vực cài đặt, chọn ứng dụng cần được chuyển qua TOR (nghĩa là bạn phải kết nối ứng dụngthông qua kết nối TOR) và bạn có thể chọn tất cả nếu muốn. Sau đó, bạn có thể bắt đầu bất kỳ trình duyệt và lướt qua kết nối TOR của bạn.

OrFox là một ứng dụng khác, một trình duyệt được xây dựng đặc biệt để được sử dụng với Orbot / TOR. Nếu bạn bắt đầu OrFox, trình duyệt đó sẽ tự động kết nối thông qua TOR, và bạn không phải làm gì khác. Tuy nhiên, trong trường hợp này, chỉ có trình duyệt OrFox được thiết lập để sử dụng TOR, tất cả các kết nối khác như bình thường. Nếu bạn sử dụng OrFox, trước khi bạn bắt đầu lướt web, hãy đi tới khu vực cài đặt và chọn Security/Bảo mật, sau đó nhấp Clear private data on exit và chọn tất cả các dạng dữ liệu. Thao tác này sẽ quét các dấu vết về trình duyệt của bạn khi bạn đóng ứng dụng.

Nếu bạn sử dụng các trình duyệt khác để lướt web, khuyên bạn đừng bao giờ sử dụng các trình duyệt tích hợp sẵn. Luôn gỡ cài đặt những phần đó, hoặc nếu không thể, hãy vô hiệu hóa chúng, sau đó tải về một trình duyệt có uy tín như Opera, Chrome hoặc Firefox. Giống như máy tính của bạn, đảm bảo nhập khu vực cài đặt và tắt tự động lưu mật khẩu, tự động điền vào các biểu mẫu, vv. Bật Do Not Track/Không theo dõi và chắc chắn nhấp vào Clear browsing data /Xoá dữ liệu duyệt web sau khi kết thúc sử dụng trình duyệt của bạn.

Một lần nữa, không sử dụng điện thoại hoặc trình duyệt trên điện thoại của bạn để truy cập vào các tài liệu làm việc của bạn, chẳng hạn như email, lưu trữ trên đám mây ... Không bao giờ, truy cập qua điện thoại của bạn. Không thể xóa dữ liệu đúng cách trên điện thoại.

SIÊU DỮ LIỆU/METADATA

Như đã đề cập trong chương trước về siêu dữ liệu, bộ sưu tập này còn tệ hại hơn trên điện thoại vì ảnh chụp có thể bao gồm vị trí và tự động đặt tên cho những người xuất hiện trong ảnh từ danh sách liên hệ của bạn. Do đó, cho dù bạn sử dụng Android hay iOS, bạn cần cân nhắc việc này khi chụp ảnh từ máy ảnh của mình để sử dụng trên bất kỳ phương tiện truyền thông xã hội nào, chuyển sang máy tính để sử dụng trong tài liệu, xuất bản vv hoặc cho bất kỳ mục đích sử dụng nào khác . Trong các chương trình siêu dữ liệu ứng dụng điện thoại thường sử dụng thuật ngữ Exif or Exifdata (Exchangeable image file format).

Nếu bạn đưa ảnh vào máy tính của mình, bạn có thể xóa siêu dữ liệu bằng cách sử dụng máy tính của bạn và các phương pháp chúng tôi đã hướng dẫn. Nếu bạn muốn trực tiếp đăng tải nội dung nào đó từ điện thoại của mình, bạn sẽ phải cài đặt một chương trình xóa siêu dữ liệu.

Đối với Android, chúng tôi khuyên bạn nên sử dụng Exif Eraser hoặc Metadata remover. Cả hai đều dễ sử dụng nhưng cũng có nhiều tùy chọn khác. Cài đặt một chương trình và kiểm tra nó, để đảm bảo bạn hiểu nó hoạt động như thế nào. Nếu không chắc chắn, hãy thử một chương trình khác cho đến khi bạn cảm thấy thoải mái. Hầu như tất cả các chương trình đều có hướng dẫn về cách sử dụng chúng trực tuyến.

MỘT SỐ ỨNG DỤNG KHÁC

Dự án Guardian đã đề cập ở trên cũng tạo ra một số loại ứng dụng bảo mật khác.

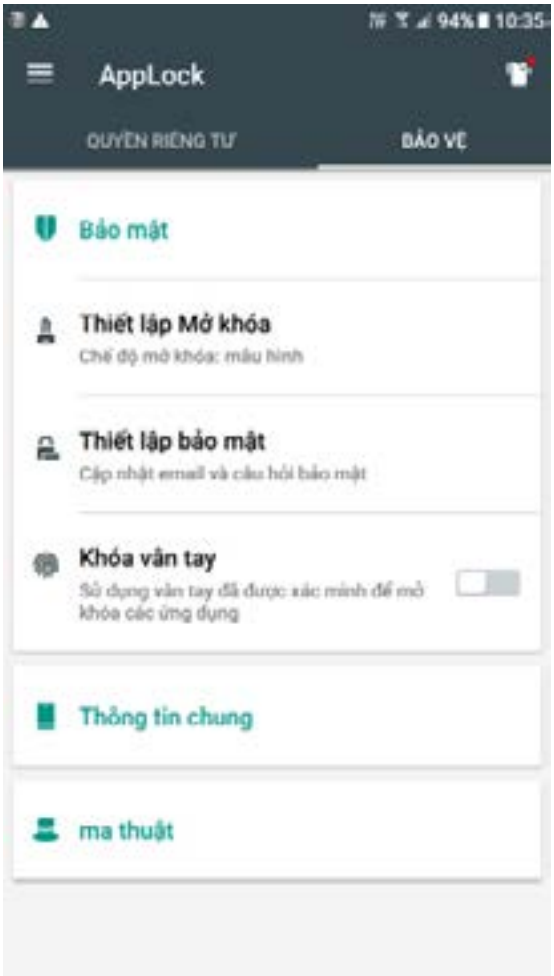
Trong số đó có ChatSecure, một chương trình để quản lý / sử dụng trò chuyện trên cả Android và iOS của bạn. Sử dụng Chatsecure cho phép bạn sử dụng GoogleTalk / Trò chuyện với mã hóa mạnh mẽ và có thể được đặt để bắt đầu tự động với TOR. Điều đó có nghĩa là bất kỳ giao tiếp nào trong tài khoản đó chỉ được thông qua kết nối TOR. Bạn cũng có thể mã PIN hoặc mật khẩu bảo vệ chương trình, cũng như thiết lập tự động xóa các tin nhắn.

Một ứng dụng phổ biến khác từ Dự án Guardian là ObscuraCam. Đây là ứng dụng Máy ảnh xác định khuôn mặt trong ảnh bạn chụp và làm mờ khuôn mặt, vì vậy mọi người không thể nhận dạng được. Nó cũng có thể được sử dụng trên các bức ảnh hiện có để làm mờ khuôn mặt của những bức ảnh đó. Họ cũng có các ứng dụng khác, do đó hãy truy cập vào trang web của họ và xem qua.

Nếu bạn muốn có ý tưởng tốt hơn về tháp điện thoại di động (trạm cơ sở, hoặc BTS) mà điện thoại của bạn đang sử dụng và được cảnh báo nếu nghi ngờ bạn đang được chuyển hướng đến IMSI catcher, bạn có thể sử dụng AIMSICD. Chương trình này chỉ có bằng tiếng Anh. Bạn có thể tải chương trình từ: https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/releases

Khi tải về bạn sẽ được hướng dẫn sử dụng, và sau đó bạn phải chọn để cài đặt nó cho mình. Bạn sẽ cần phải đi đến Settings và thay đổi thành Allow Unknown Sources. Sau khi cài đặt hoàn tất, quay lại Setting và thay đổi lại thành Not Allow Unknown Sources. Chương trình cung cấp thông tin về những gì BTS điện thoại của bạn được kết nối từ đó, và sẽ cảnh báo bạn nếu nó nghi ngờ điện thoại của bạn để kết nối với một IMSI catcher. Ngoài ra còn có một chức năng bản đồ sẽ hiển thị những tháp di động xung quanh bạn.

AppLock là ứng dụng chỉ có phiên bản tiếng Anh. Nếu ngôn ngữ cho phép, sử dụng AppLock vì nó đã được thử nghiệm và xác minh là an toàn. AppLock là một ứng dụng cho phép bạn tạo một mã PIN và chọn bất kỳ ứng dụng nào bạn muốn sử dụng nó. Với điều này, bạn có thể tạo mã PIN bảo vệ bất kỳ ứng dụng hoặc chức năng nào bạn muốn, ngay cả khi ứng dụng đó không có hỗ trợ mã PIN gốc. Bản thân chương trình bị ẩn đi, vì vậy những người khác không thể dễ dàng biết được bạn đang sử dụng nó. Nó chỉ cho phép một mã PIN (hoặc mẫu), vì vậy tất cả các ứng dụng bạn chọn sẽ sử dụng mã PIN để truy cập.



Sau khi cài đặt AppLock, nó sẽ yêu cầu bạn cài đặt một chương trình hỗ trợ (có nhiều tùy chọn hơn cho AppLock) gọi là Advanced System Protection. Với cài đặt này, bạn sẽ tạo một mật khẩu cho AppLock, và nó cũng sẽ ẩn chương trình, và làm cho nó không thể cho những người không có mật khẩu để gỡ bỏ nó.

Sau khi cài đặt, điều hướng xung quanh để xem những gì bạn có thể sử dụng App cho. Ứng dụng có hai tab, Security, nơi bạn có thể chọn chức năng và ứng dụng nào bạn muốn bảo vệ và Protection, nơi bạn có thể thay đổi cài đặt, như nếu bạn muốn Mã PIN hoặc Mẫu, nếu bạn muốn ẩn AppLock để không thể dễ dàng tìm thấy (cái mà bạn muốn). Nếu bạn chọn ẩn ứng dụng, trong tương lai để bắt đầu ứng dụng, bạn cần mở bàn phím số (giống như khi thực hiện cuộc gọi điện thoại), và viết trong số 1234 và bấm vào cuộc gọi. Thao tác này sẽ khởi chạy ứng dụng. Nếu Advanced Protection không được cài đặt tự động, nhấn để kích hoạt tính năng Advanced Protection dưới nút Protect.

KẾT HỢP VỚI SỬ DỤNG MÁY TÍNH

Như đã được đề cập nhiều lần, điều quan trọng là phải tách riêng việc sử dụng máy tính và điện thoại của bạn. Chúng tôi thường khuyên bạn không sử dụng bất kỳ ứng dụng trên điện thoại nào trên máy tính của bạn. Ví dụ: Telegram có máy tính App for Windows, nơi bạn có thể sử dụng chương trình trò chuyện trực tiếp từ máy tính của mình. Tuy nhiên, phiên bản dựa trên máy tính không cho phép trò chuyện bí mật, và không thể được bảo vệ bằng mật khẩu. Tương tự, các ứng dụng khác cũng có thể có các chương trình cho máy tính của bạn, nhưng chúng tôi khuyên bạn nên không sử dụng nó. Ngoài ra còn có các chương trình máy tính để đọc, gửi và quản lý lưu lượng SMS của bạn những ngày này, nhưng một lần nữa, hãy tránh.

Một ngoại lệ là Signal Private Messenger, có thể chạy trên cả Win10 và OSX và vẫn có khả năng tự xóa tin nhắn Disappearing messages, và cũng có thể làm như vậy cho các cuộc trò chuyện nhóm. Tuy nhiên, bạn cần sử dụng điện thoại của mình để bắt đầu cuộc trò chuyện hoặc trò chuyện nhóm với Disappearing messages vì nó không thể khởi động từ chương trình máy tính, nhưng một khi đã bắt đầu có thể sử dụng và kiểm soát từ máy tính.

CHUYỆN GI XẢY RA NẾU?

Nếu bạn, mặc dù biết cách bảo vệ điện thoại thật khó khăn, bạn cần sử dụng nó để nghiên cứu trình duyệt, truy cập trình duyệt đến email hoặc tài khoản, hoặc sử dụng điện thoại để lưu trữ một tệp tin hoặc dữ liệu, hãy thực hiện các biện pháp phòng ngừa sau. Bất kỳ việc sử dụng trình duyệt nào cũng có nghĩa là bạn phải nhập khu vực cài đặt cho trình duyệt và đảm bảo rằng không có mật khẩu nào được lưu, không sử dụng chức năng tự động điền và sau khi sử dụng trình duyệt đã kết thúc, bạn chọn 'rõ ràng tất cả dữ liệu cá nhân 'từ trình duyệt.

Nếu bạn đã từng lưu trữ bất kỳ tệp hoặc dữ liệu trên điện thoại của mình, hãy cài đặt chương trình xóa không gian trống và chạy chương trình sau khi xóa / xóa tệp hoặc dữ liệu. Điều này sẽ không hoạt động tốt như trên máy tính nhưng sẽ giúp đảm bảo rằng không thể phục hồi tệp dễ dàng để tìm tệp. Chúng tôi khuyến cáo sử dụng Secure Eraser. Nhiều ứng dụng tương tự khác cũng tồn tại. Nếu điện thoại của bạn có thẻ SD, hãy đảm bảo chạy 'xóa không gian trống' trên thẻ SD cũng như trên ổ cứng nội bộ của điện thoại.

NHỮNG ĐIỂM QUAN TRỌNG

- Trước khi đăng tải ảnh hoặc bất cứ thứ gì khác từ điện thoại của bạn, đảm bảo bạn biết rằng chúng có chứa siêu dữ liệu (metadata)
- Đảm bảo chương trình trò chuyện an toàn của bạn được cài đặt để tự động xóa các cuộc trò chuyện của bạn và nếu không có chức năng ẩn tự động xóa, hãy chắc chắn xóa nội dung sau khi kết thúc
- cuộc trò chuyện.
- Sử dụng Signal như một chương trình trò chuyện mặc định và sử dụng nó trong gửi tin nhắn SMS và đàm thoại.

MỘT NGÀY TRONG CUỘC ĐỜI

Với mỗi ngày làm việc bình thường, một cách an toàn để bảo vệ bạn chống lại các cuộc tấn công trong tương lai, hãy xem xét quy trình làm việc được trình bày dưới đây.

Khi đến nơi làm việc, bạn khởi động máy tính của mình, đã được tắt hoàn toàn đêm qua mà không để chế độ ngủ. Bạn bắt đầu một ngày bằng cách bật VPN và truy cập các nguồn tài liệu bình thường, kiểm tra và trả lời email, v.v. Điều này, và bất kỳ nghiên cứu khác được thực hiện bằng cách sử dụng công việc chuyên dụng của bạn với cài đặt bảo mật được áp dụng.

Sử dụng công cụ tìm kiếm của Google mà không cần đăng nhập vào Gmail hoặc bất kỳ tài khoản Google nào khác trong cùng một trình duyệt.

Bạn cũng có thể tải về các tập tin về USB stick, nhưng cũng có thể về một phân vùng trên ổ cứng của bạn hoặc một thùng chứa tập tin. Chỉ sau khi đã gắn ổ đĩa mã hoá của bạn, bạn bắt đầu tải xuống bất kỳ tệp nào hoặc tạo tệp mới. Mọi thứ được tải xuống hoặc tạo trực tiếp trên ổ đĩa này chứ không phải trên màn hình máy tính hoặc ở thư mục tải về tạm thời.

Ngay sau khi bạn rời khỏi máy tính, bạn đóng ổ cứng được mã hóa và khóa máy tính. Nếu bạn đi lâu thì nên tắt máy tính.

Nếu bạn không có VPN, thì bạn cần phải cài đặt VPN. Sau khi truy cập trình duyệt TOR bạn sử dụng dịch vụ này. Khi bạn đã thực hiện công việc đòi hỏi thêm tính bảo mật và ẩn danh, bạn tắt TOR và khởi chạy lại VPN của mình, vì TOR chậm và chỉ để truy cập email hoặc trình duyệt khi bảo mật quan trọng hơn tốc độ.

Trong ngày, bất kỳ tệp PDF hoặc bất kỳ tài liệu trình bày khác được tạo, hoặc bất kỳ tài liệu văn bản nào bạn cần chia sẻ, hoặc yêu cầu xóa bất kỳ siêu dữ liệu nào để đảm bảo thông tin bạn thực sự chia sẻ. Trong hầu hết các trường hợp, bạn chỉ cần xóa siêu dữ liệu.

Hãy sử dụng điện thoại mà không dùng máy tính để thực hiện các dịch vụ chat như Signal hay Telegram và hai chương trình này đều phải sử dụng chat bí mật (Secret chat) để không lưu trữ lịch sử giao tiếp.

Nếu bạn đã tạo ra rất nhiều tài liệu trong khi làm việc trong ngày, đặc biệt là các tài liệu nhỏ, bạn có thể quyết định xem chúng có còn quan trọng hay đã được đưa vào các tài liệu lớn hơn và không cần nữa. Nếu bạn quyết định giữ chúng cẩn thận, bạn hãy hợp nhất chúng lại thành ít tài liệu hơn hoặc lưu lại chúng dù bạn muốn chúng trong phân vùng được mật mã của bạn. Bạn không bao giờ để tài liệu trên máy tính để bàn hoặc các thư mục có thể truy cập vào cuối ngày làm việc.

Vào cuối ngày, bạn thực hiện một số bước cơ bản. Các thư mục Hộp thư đến (Inbox), Đã gửi (Sent) và Thùng rác (Thrash), để người truy cập trái phép vào email của bạn không thể lấy được tài liệu gì. Hãy đảm bảo ghi lại những tài liệu còn dang dở và xóa mọi dữ liệu khác khi bạn chạy CCleaner. Hãy xóa thủ công những phần chat ở điện thoại nếu không đặt chế độ xóa tự động. Và cuối cùng, đóng trình duyệt cũng như đóng phần ổ cứng mã hõa, chạy CCleaner để xóa hết dấu vết từ các hoạt động trong ngày.

Trước khi ra về, hãy đảm bảo máy tính đã được khóa và phần ổ cứng mã hóa phải được đóng lại.

NHỮNG ĐIỂM QUAN TRỌNG

- Không sử dụng trình duyệt cá nhân của bạn để làm việc
- Không tiến hành công việc mà không có VPN (hoặc TOR)
- Không tải hoặc lưu trữ các tập tin trên điện thoại của bạn
- Không lưu hoặc tạo tài liệu bên ngoài ổ cứng đã mã hóa của bạn
- Hàng ngày chạy CCleaner, đặc biệt là sau một ngày làm việc

PHẦN IV
CHUẨN BỊ NẾU ĐỐI DIỆN NGUY CƠ BỊ BẮT

CHƯƠNG 12
CHUẨN BỊ NẾU ĐỐI DIỆN NGUY CƠ BỊ BẮT

Nếu bạn đang đọc những dòng nay, điều đó có nghĩa là bạn đang hoặc sẽ đối mặt với nguy hiểm mà không nên bỏ qua. Hãy đọc từng phần dưới đây, mỗi phần không mất quá 15 phút, và làm theo những đề xuất. Những điều này có thể đóng vai trò quan trọng để giữ bạn được an toàn trong tương lai.

Dựa trên danh sách những điều đưa ra, bạn có thể tạo ra một tài liệu có chứa những thông tin như vậy, và thêm bất cứ điều gì mà bạn muốn.

Trước khi bạn bắt đầu viết, bạn cần phân tích tình trạng của bạn, và dạng hỗ trợ nào bạn muốn khi bạn rơi vào nguy hiểm. Bạn hãy xem ba điểm dưới đây.

BƯỚC 1: NHỮNG MỐI NGUY HIỂM CỦA BẠN LÀ GÌ? VÀ NHỮNG TÌNH HUỐNG NÀO CÓ THỂ XẢY RA?

Hãy liệt kê ra những mối nguy hiểm mà bạn có thể phải đối mặt, và mục đích của những mối đe doạ này. Ví dụ, nếu bạn là nhà báo, thì mục tiêu của một vụ bắt giữ ngắn hạn là nhằm không cho đăng tải bài viết, hoặc thu giữ những tài liệu để tìm ra nguồn cung cấp, hoặc nghiêm trọng hơn là bắt giữ với cáo buộc nhằm buộc bạn phải dừng công việc hoàn toàn.

Với những mối đe doạ khác nhau cần có sự chuẩn bị để đối phó khác nhau. Những công việc gì, hoặc những người nào cùng làm việc có thể gia tăng mối đe doạ? Bạn có viết về tham nhũng ở địa phương hay thay mặt nạn nhân của tra tấn trong một phiên toà thù địch? Một khi bạn đã viết ra đuọc những hành động mà là nguyên nhân của sự trả thủ, bạn có thể xác định được sự trả thù đến từ đâu. Bạn có biết người có thể là tác giả của những vụ tấn công như quan chức chính phủ, an ninh, cảnh sát quốc gia? Bạn có biết những điều như phương pháp và cáo buộc có thể được dùng để chống lại bạn ? Hãy trả lời những câu hỏi này, đầy đủ nhất có thể, và bạn có thể nâng cao khả năng nhận được trợ giúp trong thời gian ngắn hơn.

BƯỚC 2: LOẠI HỖ TRỢ NÀO BẠN MUỐN?

Dựa trên những dạng hành động liệt kê bên trên, loại hỗ trợ nào mà bạn muốn nhận? Bạn có nghĩ rằng sự chú ý của truyền thông quốc tế sẽ hữu dụng trong một hoàn cảnh cụ thể ? và nếu có, thì cần được sử dụng theo cách nào? Ví dụ, nếu bị bắt, bạn có muốn được truyền thông quan tâm ngay trong tuần đầu tiên khi sự việc xảy ra, hay là bạn chỉ muốn sự chú ý của truyền thông địa phương hay là bạn muốn có sự can thiệp ngoại giao hoặc của Liên Hợp quốc một cách thầm lặng và không muốn truyền thông đưa tin.

Bạn hãy nhớ rằng mỗi cách tiếp cận khác nhau sẽ có kết quả khác nhau phụ thuộc vào tình huống cụ thể và bạn có thể muốn nói với đồng sự thân tín về lựa chọn của bạn, và họ có thể là người sẽ nói thay bạn. Loại hình trợ giúp mà bạn muốn có là gì?

Bạn có người thân nào trong gia đình mà dựa vào hỗ trợ tài chính của bạn và cần hỗ trợ tài chính trong thời gian bạn bị bắt hoặc bị đưa đi mất tích? Loại hình trợ giúp nào? Tài chính, y tế, học phí, tiền thuê nhà….?

Nếu bị bắt, và trong trường hợp xấu, thì loại hình hỗ trợ pháp lý nào bạn muốn? Bạn có yêu cầu cụ thể nào về pháp lý không? Bạn đã có luật sư người hứa sẽ trợ giúp bạn khi bạn cần? Nếu có, thì liên lạc với người đó như thế nào? Người này có quyền bào chữa không?

Nếu điều này bạn có thể quyết định, thì bạn nên ghi lại người đại điện pháp lý cho bạn, nói rõ ràng rằng trong mọi trường hợp bạn không muốn thay thế họ bằng luật sư do nhà nước chỉ định, và chuyển văn bản này cho đồng sự hoặc bạn tin tưởng của mình.

BƯỚC 3: TÌM MỘT NGƯỜI ĐÁNG TIN CẬY MÀ KHÔNG BỊ NGUY HIỂM

Người này sẽ được cung cấp những thông tin bên trên và sẽ có trách nhiệm chia sẻ những thông tin đó cho những người có trách nhiệm khác nếu điều xấu xảy ra với bạn. Mọi thông tin được cung cấp cho người này và hướng dẫn người này hành động với những thông tin đó khi bạn gặp nguy hiểm.

Bạn cũng chỉ định một thành viên trong gia đình đại diện hợp pháp cho bạn trong việc tìm luật sư nếu cần. Hãy suy nghĩ kỹ, và hãy biết rằng nhiều thành viên trong gia đình thường không có kinh nghiệm xử lý trong những tình huống như vậy. Bạn cũng nên nhớ rằng cảnh sát có thể sách nhiễu hoặc bắt giữ thành viên trong gia đình hay trừng phạt họ, do vậy bạn phải thảo luận về những mối nguy hiểm và những yêu cầu đối với thành viên trong gia đình để họ hiểu và đồng ý. Hãy lựa chọn một thành viên trong gia đình hiểu về công việc của bạn, và nói với người này rằng bạn đã lựa chọn cô ta/anh ta và nếu cần, người này cần phải tìm luật sư cho bạn một cách không lưỡng lự. Hãy cho gia đình biết về người mà bạn tin tưởng và chia sẻ thông tin, để họ có thể lien lacj với nhau và chia sẻ thông tin trong việc hỗ trợ bạn.

Dưới đây là danh sách (Checklist) những vấn đề và những điểm có thể được coi như là chỉ dẫn cho những loại thông tin gì cần đưa vào

DANH SÁCH

- CV
- Bản viết kể về bạn và những công việc của bạn, cố gắng đưa những việc mà có thể là nguyên nhân của việc bạn bị nguy hiểm. Điều này đặc biệt quan trọng nếu những biện pháp của nhà nước và cảnh sát áp dụng chống lại bạn chỉ vì những hoạt động nhân quyền và xã hội của bạn. Điều này đặc biệt quan trọng trong việc bào chữa cho bạn và không nên bị bỏ qua.
- Thông tin liên lạc về luật sư người đã đồng ý cung cấp hỗ trợ pháp lý cho bạn.
- Thông tin liên lạc về người tin cẩn của bạn, người giữ các thông tin cần thiết của bạn nhằm phục vụ cho việc bào chữa.
- Thông tin liên lạc của thành viên gia đình hoặc bạn tin cẩn.
- Thông tin liên lạc về những nhà báo hoặc nhà ngoại giao mà bạn muốn nhận hỗ trợ.
- Bản viết về những đồng sự hoặc người cùng làm việc, với thông tin liên lạc.
- Chụp một bức ảnh của mình mà có thể được cung cấp cho báo chí hoặc người hỗ trợ bạn.
- Điều này giúp bạn kiểm soát được hình ảnh của mình.

TÀI LIỆU CHUẨN BỊ TRƯỚC

Tài liệu chuẩn bị trước (bởi chính bạn) sẽ được công bố trong trường hợp bạn bị bắt giữ hoặc gặp vấn đề khác. Bạn nên ghi chú rõ tài liệu này được công bố thế nào. Bạn có thể làm một video clip ngắn, rất có ích.

Nội dung của tài liệu chuẩn bị trước này phụ thuộc vào bạn và căn cứ vào công việc của bạn cũng như dạng đe doạ mà bạn đối mặt.

Trong những ngày này, bị ép cung trở nên phổ biến. Gui Minhai, một công dân Thuỵ Điển, bị bắt cóc ở Thái Lan và bị đưa về Trung QUốc. Trong bản ép cung, anh ta bị ép từ chối không nhận trợ giúp ngoại giao từ Thuỵ Điển, và bị buộc nói rằng anh muốn từ bỏ quốc tịch Thuỵ Điển. Hãy tưởng tượng rằng nếu anh ta đã chuẩn bị một tài liệu nói rằng nếu anh ta xuất hiện ở Trung Quốc thì là do anh ta bị bắt cóc (bởi vì anh không có visa vào Trung Quốc), hoặc nếu trước khi bị bắt anh ta đã làm một video trong đó anh giải thích rằng anh sẽ không bao giờ từ bỏ quốc tịch Thuỵ Điển hoặc từ chối hỗ trợ ngoại giao, thì sẽ là một bằng chứng thuyết phục chống lại luận điệu của nhà nước như lời ép cung. Những sự chuẩn bị như vậy đã có thể lôi kéo sự chú ý cho trường hợp của anh này và tăng khả năng được hỗ trợ.

Nhiều người hoạt động nhân quyền bị bắt giam và từ chối gặp gỡ với gia đình hoặc luật sư còn cảnh sát thì khẳng định rằng họ không muốn được bảo vệ bởi luật sư của mình mà sử dụng luật sư chỉ định bởi nhà nước. Hãy tưởng tượng nếu những người này đã làm video chuẩn bị trước nói rõ rằng họ không bao giờ từ chối quyền được tự lựa chọn luật sư, và không bao giờ sử dụng hỗ trợ bởi luật sư chỉ định bởi nhà nước.

Nếu cảnh sát sử dụng một khía cạnh nào đó trong công việc của bạn để chống lại bạn, hãy tưởng tượng nếu bạn có một video chuẩn bị trước giải thích về công việc của bạn và nói rõ việc này hoàn toàn hợp pháp. Bạn có thể bổ sung những đàn áp trước đó.

Nếu bạn nghĩ rằng cảnh sát có thể cáo buộc bạn về những hành động bất hợp pháp trong công việc phi chính phủ, hoặc cáo buộc bạn gian lận tài chính,, thì một bản báo cáo tài chính và kiểm toán gửi cho người tin cẩn, sẽ có thể chống lại những vu cáo trên.

CHÚ Ý: Nếu có những thay đổi thông tin nào đó, bạn nên cập nhật và gửi lại thông tin đã cập nhật cho người mà bạn tin tưởng.