BẢO MẬT KỸ THUẬT SỐ THỰC HÀNH

bảo mật ngoài công nghệ

Giới Thiệu:

BẢO MẬT KỸ THUẬT SỐ DỰA TRÊN HÀNH VI

practicaldigitalprotection.com

BẢO MẬT KỸ THUẬT SỐ DỰA TRÊN HÀNH VI

Tóm lược và giới thiệu về Bản mật kỹ thuật số thực hành

practical**digital**protection.com

a project by

safeguard DEFENDERS

DANH MỤC

GIỚI THIỆU

Chào mừng bạn đến với phiên bản rút gọn của Bảo mật kỹ thuật số thực hành, một tài liệu hướng dẫn thực tiễn, tự học về an ninh mạng cho những người hoạt động trong các môi trường thù địch. Tài liệu ngắn gọn này phác thảo các khía cạnh hành vi cơ bản của an ninh mạng, đồng thời giúp bạn phân tích tình hình, nhu cầu và ưu tiên của bạn. Để xem đầy đủ các khái niệm này và các giải pháp kỹ thuật cho các vấn đề được trình bày, hãy xem tài liệu hướng dẫn đầy đủ.

Một trong nhiều lý do cho cuốn cẩm nang này là cung cấp một nguồn đáp ứng các nhu cầu thực sự liên quan đến an ninh mạng cho các nhà báo, luật sư, các nhân viên NGO và người bảo vệ nhân quyền ở những nơi như Trung Quốc, Việt Nam, Myanma và nhiều nước khác. Mỗi phiên bản của cuốn cẩm nang đầy đủ được điều chỉnh cho quốc gia và ngôn ngữ đó, được phát triển cùng với một nhóm các bên hưởng lợi ở nước đó, cung cấp thông tin và giải pháp liên quan đến nhu cầu và mong muốn của họ.

“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, Việt Nam hay Ấn Độ 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.

HIỂU VỀ CÁC MỐI ĐE DỌA CỦA BẠN

Lời giới thiệu: 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 mangjg 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 MẬT 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.

CÁC QUY TẮC CƠ BẢN TRONG BẢO MẬT KỸ THUẬT SỐ

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 đểtuân 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 khókhăn 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 bỏchúng. 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 vệvà 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 làcũng 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 homật 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 tựnhư 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 đósẽ 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 bịbắt, 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 bổsung 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 kỹthuật 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 đãđược 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, vàsau khi điều đó xảy ra. Ngoài ra, bạn phải biết những gì bạn đồng nghiệp và bạn bè của bạn sẽlàm. Bạn cần một kế hoạch. Cách duy nhất để đạt được điều này là nói về điều đó trước vàthỏa 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 cókiểm 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 giữan toàn nhưng một đồng nghiệp không làm thì các nỗ lực của bạn có thể trở nên vô nghĩa vàkhiến 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 kếhoạch 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 VẤN ĐỀ VỚI ĐIỆN THOẠI THÔNG MINH

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.

Không giống với máy tính, bạn không thể bảo vệ nội dung của mình trong điện thoại 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 (GOING DARK)

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”

BẠN MUỐN BIẾT THÊM NỮA?

Bảo mật Kỹ thuật số thực hành còn có một số câu chuyện thực tế về việc lực lượng an ninh cố gắng sử dụng những công cụ trên, và liệu chúng có thành công hay không phụ thuộc vào mức độ bảo mật của người hoạt động.

BẠN MUỐN BIẾT THÊM?

Hướng dẫn sử dụng Bảo vệ Kỹ thuật số Thực hành có một số câu chuyện trong thực tế về cách cảnh sát hoặc nhân viên an ninh đã sử dụng nhiều công cụ và họ đã thành công hay thất bại tùy thuộc vào cách người hoạt động đã chuẩn bị để đối phó.

Practical Digital Protection