KEVIN MITNICK

ROBERT VAMOSI

NGHỆ THUẬT

ẨN

The Art of Invisibility

Thu Giang dịch

DANH

BẢO MẬT CÁ NHÂN TRONG KỶ NGUYÊN DỮ LIỆU LỚN

alphabooks

NHÀ XUẤT BẢN CÔNG THƯƠNG

AN TOÀN THÔNG TIN TRONG KỶ NGUYÊN SỐ

Trong kỷ nguyên số, vấn đề bảo mật và an toàn trên không gian mạng ngày càng trở nên quan trọng, không chỉ đối với các doanh nghiệp, tổ chức, chính phủ, mà còn đối với từng cá nhân. Việt Nam có 58 triệu tài khoản Facebook (tính đến hết quý 1/2018); 127 triệu thẻ ngân hàng với 66,6 triệu tài khoản thanh toán cá nhân; cùng hàng tỷ các giao dịch mua bán, trao đổi trên mạng diễn ra mỗi ngày. Chính vì vậy, an ninh mạng trong kỷ nguyên số đang trở thành một chủ đề ngày càng nóng.

Chỉ rất gần đây, nhiều tài khoản Facebook cũng như email cá nhân đã bị hacker tấn công và chiếm đoạt. Thủ đoạn của hacker khá đơn giản khi tận dụng các sơ hở của người dùng cũng như các lỗi bảo mật của hệ thống, nhưng chúng đã gây ra những thiệt hại rất lớn cả về vật chất và tinh thần cho người dùng – rất nhiều thông tin cá nhân bị lộ và bị mất, và điều đó cũng đang xảy ra với rất nhiều tổ chức, công ty, cả tư nhân lẫn nhà nước.

Ngay đầu tháng 11/2018, một số nguồn tin lan truyền trên mạng cho rằng hệ thống công nghệ của Thế giới Di động bị hacker tấn công và thông tin của khách hàng bị tiết lộ. Các tài khoản thẻ ngân hàng cũng như email và số điện thoại cá nhân bị kẻ xấu công khai trên mạng dù cho nghi vấn lộ dữ liệu khách hàng vẫn đang tiếp tục được điều tra, xác minh.

Ngược về quá khứ, tháng 4/2018, website của ngân hàng Vietcombank bị tấn công. Sự cố xảy ra với trang con của website Vietcombank khi người dùng đăng ký email liên kết với tài khoản ngân hàng. Khi được chia sẻ qua Facebook, ảnh bìa của trang con này hiển thị dòng chữ “Đại học Quốc gia Hà Nội”. Hacker còn để lại hai câu thơ “Trăm năm Kiều vẫn là Kiều/ Sinh viên thi lại là điều tất nhiên”.

Năm 2016, hệ thống các sân bay lớn tại Việt Nam như Sân bay

Quốc tế Tân Sơn Nhất, Sân bay Quốc tế Nội Bài, Sân bay Quốc tế Đà Nẵng, Sân bay Phú Quốc đều bị hacker tấn công và để lại nhiều nội dung xúc phạm, xuyên tạc.

Cuối năm 2014, hệ thống các website của VCCorp cũng bị tấn công, làm tê liệt hoạt động truy cập vào toàn bộ hệ thống website báo chí đối tác của VCCorp và gây thiệt hại trực tiếp tới hoạt động của các trang này, đồng thời ảnh hưởng tới hàng triệu độc giả và người tiêu dùng sử dụng các dịch vụ trực tuyến của họ. Theo VCCorp, ước tính sơ bộ sau hai ngày bị tấn công, số tiền VCCorp bị thiệt hại vào khoảng 5 tỷ đồng, bao gồm tất cả các loại doanh thu như quảng cáo, thương mại điện tử…

Trên thực tế, không ít những vụ tấn công mạng đã xảy ra liên tiếp tại Việt Nam trong thời gian gần đây và để lại những hậu quả không hề nhỏ. Những vụ việc như thế này đang gióng lên một hồi chuông cảnh báo đối với các cá nhân cũng như doanh nghiệp trong thời đại số. Với xu thế phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0 trên toàn thế giới, trong đó có Việt Nam, sự bùng nổ của các thiết bị IoT sẽ mang lại nhiều nguy cơ tiềm ẩn về các cuộc tấn công trên không gian mạng hoặc bị kẻ xấu lợi dụng để tấn công vào các hạ tầng.

Chuyên gia an toàn thông tin, vấn đề bảo mật không có tính tuyệt đối. Ngay cả các cường quốc trong ngành công nghệ thông tin-bảo mật như Anh, Pháp, Đức, Mỹ, Trung Quốc… cũng đều bị hacker tấn công. Vậy các doanh nghiệp và người dùng Việt Nam phải làm gì để vừa có thể tận dụng được những lợi thế của nền công nghiệp IoT mà vẫn đảm bảo an toàn thông tin trên mạng?

Nhằm mang tới cho độc giả và các doanh nghiệp, tổ chức những kiến thức cơ bản về bảo mật dữ liệu, cảnh báo người đọc về vấn đề quyền riêng tư và nâng cao ý thức bảo mật thông tin, Apha Books trân trọng giới thiệu bộ sách “An toàn thông tin trong kỷ nguyên số” gồm 4 cuốn: The Cuckoo’s Egg (Gián điệp mạng), Ghost in the Wires (Bóng ma trên mạng), The Art of Invisibility (Nghệ thuật ẩn mình) và Hackers lược sử. Thông qua các câu chuyện ly kỳ hấp dẫn về những cuộc truy bắt hacker, những chiến công của các

hacker mũ trắng – những kẻ mê máy tính thông minh và lập dị, dám mạo hiểm, bẻ cong các quy tắc và đẩy thế giới vào một hướng đi hoàn toàn mới, độc giả sẽ có được cái nhìn toàn diện về hacker, về đạo đức nghề nghiệp cũng như tương lai của ngành công nghệ để có được cái nhìn rõ ràng hơn về an ninh mạng, chủ đề chưa bao giờ hết nóng hổi của các tín đồ mạng.

Bộ trưởng TT&TT Nguyễn Mạnh Hùng đã nhấn mạnh: "An toàn, an ninh mạng được coi là điều kiện để thúc đẩy chính phủ điện tử, chính phủ số và nền công nghiệp nội dung số. Vì vậy, Việt Nam phải trở thành cường quốc về an ninh mạng". Đồng hành với những vấn đề thời sự nhức nhối hiện nay, với bộ sách này, Apha Books và các đối tác – những nhà cung cấp các giải pháp bảo mật & an ninh mạng như CMC, Netnam, Securitybox, CyRadar... mong muốn đóng góp một phần tri thức cho xã hội, giúp nền kinh tế số Việt Nam phát triển lành mạnh, bền vững.

Trân trọng giới thiệu!

Tháng 11/2018

Công ty Cổ phần Sách Alpha

LỜI GIỚI THIỆU

Kevin Mitnick là một cái tên rất nổi tiếng trong ngành bảo mật thông tin thế giới. Không chỉ là diễn giả tại các hội thảo bảo mật lớn trên thế giới như DEFCON, diễn đàn thảo luận mở TED mà ông còn nổi tiếng vì quá khứ tù tội của mình. Năm 1988, Kevin bị tù 1 năm và năm 1995 bị phạt tù 48 tháng cùng 3 năm quản chế vì hàng loạt tội danh liên như: lừa đảo qua mạng, nghe lén các phương tiện thông tin liên lạc mà không được phép, truy cập trái phép vào hệ thống máy tính của chính phủ liên bang hay phá hoại tài sản máy tính. Tuy nhiên, điều đặc biệt là sau khi ra tù, Kevin đã thực sự trở thành chuyên gia hàng đầu, thực hiện những công việc tư vấn về bảo mật nhằm giúp tăng cường an toàn thông tin cho rất nhiều các tổ chức lớn tại Mỹ cũng như khắp thế giới.

Về cuốn sách này, đối với những độc giả có kiến thức trung bình về kỹ thuật máy tính thoáng qua có thể thấy khá phức tạp bởi những thuật ngữ chuyên ngành hay nhiều lúc nội dung cuốn sách sẽ nói sâu về các kỹ thuật áp dụng. Tuy nhiên, nếu lướt qua các thông tin đó, đọc hết cuốn sách thì các độc giả sẽ thấy đây không chỉ dừng lại là cuốn sách hướng dẫn về các thủ thuật, kỹ thuật dùng để bảo vệ quyền riêng tư của mình khi sống trong thời đại đang chuyển đổi số như hiện nay, mà Kevin còn mô tả cho các độc giả thấy hiện trạng giám sát mạng, hiện trạng bảo mật trên thế giới đang ra sao và thực tế diễn ra là như thế nào. Các ví dụ trong cuốn sách cũng rất sát với hiện trạng ngoài đời thực, nó không phải diễn ra chỉ ở Mỹ mà nó đang diễn ra ở mọi nơi trên thế giới.

Đối với những độc giả hiện đang làm trong ngành bảo mật hoặc đã có những nghiên cứu, kinh nghiệm trong lĩnh vực công nghệ thông tin, cuốn sách có thể cung cấp rất nhiều thủ thuật, cách thức hiệu quả để bảo vệ thông tin cá nhân của mình khi hoạt động trên mạng Internet và cả những ví dụ hết sức trực quan về những mối nguy hiểm hay các hình thức thu thập thông tin cá

nhân của nhiều tổ chức.

Vấn đề về quyền riêng tư cá nhân (privacy) thực tế là vấn đề rất nóng hổi ở các nước phát triển. Quy định bảo vệ dữ liệu chung Châu Âu (GDPR) vừa được EU thông qua năm 2016 là một minh chứng cho vấn đề này. Tại Việt Nam, quá trình chuyển đổi số vẫn đang diễn ra rất nhanh và bắt kịp xu hướng thế giới với các ứng dụng ngân hàng trực tuyến, thương mại điện tử, các hãng taxi công nghệ, tiền mã hóa, blockchain… Tuy nhiên, các vấn đề về bảo mật hệ thống hay quyền riêng tư cá nhân vẫn chưa phát triển với tốc độ tương đương. Điển hình là vẫn còn rất nhiều các tình trạng chia sẻ thông tin cá nhân (nhiều nhất số điện thoại cá nhân phục vụ mục đích quảng cáo, tele-sales) mà chủ sở hữu thông tin không hề hay biết hoặc cho phép.

Đó là câu chuyện của thế giới, trở về bối cảnh của Việt Nam thì từ 10 năm trước, Tập đoàn Công nghệ CMC đã tiên phong đầu tư vào lĩnh vực bảo mật, an toàn thông tin (ATTT) với sự ra đời của công ty CMC Infosec. Cho đến thời điểm này, các sản phẩm phòng chống mã độc, giải pháp trung tâm giám sát dịch vụ ATTT, dịch vụ rà soát, phòng chống và ứng cứu khi bị tấn công mạng của CMC Infosec đã chứng tỏ năng lực công nghệ của các chuyên gia bảo mật của Việt nam. Đầu tư cho lĩnh vực An ninh ATTT vừa là định hướng phát triển vừa là trách nhiệm đối với quốc gia của một đơn vị làm công nghệ như CMC.

Quay lại với cuốn sách của Kevin, tôi tin rằng nó sẽ có ích cho không chỉ những người đang làm công nghệ và tốt cho tất cả chúng ta, những người vẫn đang hàng ngày sống và làm việc trên môi trường số. Tôi cũng tin chắc rằng, sau khi đọc xong cuốn sách, độc giả sẽ có một cách nhìn khác về việc tự bảo vệ thông tin cá nhân của mình khi sử dụng các dịch vụ hay tham gia kết nối, chia sẻ trên môi trường Internet.

Tập đoàn Công nghệ CMC rất hân hạnh đồng hành cùng Alpha Books giới thiệu cuốn sách có ý nghĩa thời sự này tới quý độc giả.

Nguyễn Trung Chính

Chủ tịch HĐQT/TGĐ Tập đoàn Công nghệ CMC

LỜI TỰA TỪ MIKKO HYPPONEN

Vài tháng trước, tôi tình cờ gặp lại một người bạn cũ từ thời trung học. Chúng tôi đi uống cà phê để hàn huyên và chia sẻ với nhau về cuộc sống mỗi người. Bạn tôi đang phân phối và hỗ trợ các loại thiết bị y tế hiện đại, còn tôi thì cho hay suốt 25 năm nay tôi chỉ chuyên làm về quyền riêng tư và an ninh trên Internet. Nghe nhắc đến quyền riêng tư trên mạng, bạn tôi bật cười khúc khích. "Nghe cũng hay đấy," anh nói, "nhưng tôi không thực sự lo lắng về chuyện đó. Xét cho cùng, tôi không phải là tội phạm, cũng không làm điều gì xấu. Tôi không quan tâm chuyện người khác theo dõi những gì tôi làm trên mạng."

Tôi thấy buồn khi nghe người bạn cũ giải thích vì sao anh ấy lại không coi trọng sự riêng tư. Tôi buồn vì đã từng nghe những lí do này rồi, rất nhiều lần là đằng khác. Tôi nghe từ những người cho rằng họ không có gì phải giấu diếm. Tôi nghe từ những người cho rằng chỉ tội phạm mới cần tự bảo vệ mình. Tôi nghe từ những người cho rằng chỉ khủng bố mới sử dụng mã hóa. Tôi nghe từ những người đinh ninh rằng chúng ta không cần bảo vệ các quyền của mình. Nhưng thực sự thì chúng ta cần phải bảo vệ các quyền của mình. Và quyền riêng tư không chỉ ảnh hưởng đến các quyền của chúng ta, mà bản thân nó chính nó là một quyền của con người. Trên thực tế, quyền riêng tư đã được công nhận là một quyền cơ bản của con người trong Tuyên ngôn Quốc tế Nhân quyền của Liên Hợp Quốc năm 1948.

Nếu như ngay từ năm 1948, quyền riêng tư của chúng ta đã cần được bảo vệ, thì ngày nay chắc chắn nhu cầu đó càng ngày càng cấp thiết hơn. Suy cho cùng, chúng ta là thế hệ đầu tiên trong lịch sử nhân loại có thể bị theo dõi với mức độ chính xác như vậy. Chúng ta có thể bị theo dõi bằng kĩ thuật số trong suốt cuộc đời. Hầu như tất cả các nội dung liên lạc của chúng ta đều có thể bị nhìn thấy bằng cách này hay cách khác. Chúng ta thậm chí còn

liên tục mang những thiết bị theo dõi nhỏ trên người – chỉ có điều chúng ta không gọi chúng là thiết bị theo dõi, mà gọi là điện thoại thông minh.

Hoạt động theo dõi trực tuyến có thể cho thấy chúng ta mua sách gì và đọc bài báo nào – thậm chí là phần nào trong bài báo thu hút sự quan tâm của chúng ta nhất. Nó còn biết chúng ta đi đâu và đi với ai, chúng ta đang ốm, đang buồn, hay đang hưng phấn. Phần lớn các hoạt động theo dõi được thực hiện ngày nay đều nhằm biên soạn lại dữ liệu này để kiếm tiền. Bằng cách nào đó, các công ty cung cấp dịch vụ miễn phí đã biến sự "miễn phí" này thành hàng tỉ đô-la doanh thu – đây là một sự minh họa rõ nét, cho thấy giá trị của việc lập hồ sơ người dùng Internet ở quy mô lớn. Ngoài ra, cũng có loại giám sát xác định mục tiêu cụ thể hơn, do các cơ quan chính phủ thực hiện ở trong nước hoặc nước ngoài.

Giao tiếp kĩ thuật số đã giúp cho các chính phủ có thể thực hiện giám sát hàng loạt. Nhưng nó cũng giúp chúng ta tự bảo vệ mình tốt hơn thông qua những công cụ như mã hóa, bằng cách lưu trữ dữ liệu an toàn, và bằng cách tuân thủ những nguyên tắc cơ bản về an ninh vận hành (operations security – OPSEC). Tất cả những gì chúng ta cần bây giờ là một bản hướng dẫn cách thực hiện đúng điều đó.

Vâng, cuốn cẩm nang mà bạn cần đang ở ngay trong tay bạn đấy. Tôi rất vui vì Kevin đã dành thời gian để chia sẻ những kiến thức của mình về nghệ thuật ẩn mình. Suy cho cùng, ông ấy là bậc thầy trong lĩnh vực này rồi. Cuốn sách này là một nguồn tài nguyên tuyệt vời. Hãy đọc và áp dụng những kiến thức trong đây để bảo vệ bản thân bạn và các quyền của bạn.

Kể tiếp chuyện ở quán cà phê, sau cuộc hàn huyên, tôi và người bạn cũ chia tay nhau. Tôi cầu mong mọi điều tốt đẹp đến với anh ấy, nhưng đôi khi tôi vẫn nghĩ về những lời anh nói, "Tôi không quan tâm chuyện người khác theo dõi những gì tôi làm trên mạng." Có thể bạn không có gì phải giấu diếm. Nhưng bạn có rất nhiều thứ phải bảo vệ đấy.

Mikko Hypponen là nhà nghiên cứu trưởng của F-Secure[1]. Ông hiện là người duy nhất từng thuyết trình ở cả hai hội nghị DEF CON[2] và TED.

[1] F-Secure (tên cũ là Data Fellows): Một công ty của Phần Lan, chuyên về an ninh và quyền riêng tư trên mạng. Công ty này hiện đang hoạt động tại hơn 100 quốc gia.

[2] DEF CON (hay DEFCON, Defcon, và DC): Một trong những hội nghị lớn nhất thế giới về hacker, được tổ chức thường niên tại Las Vegas.

Lời giới thiệu: ĐẾN LÚC BIẾN MẤT RỒI

Gần hai năm sau ngày Edward Joseph Snowden, một nhân viên hợp đồng của Booz Allen Hamilton[3], lần đầu tiên công bố các tài liệu mật lấy được từ Cơ quan An ninh Quốc gia (NSA), diễn viên hài John Oliver của HBO đến Quảng trường Thời đại ở Thành phố New York để thực hiện một cuộc khảo sát ngẫu nhiên nhằm lấy tư liệu cho một chương trình về quyền riêng tư và giám sát. Các câu hỏi của anh rất rõ ràng. Edward Snowden là ai? Anh ta đã làm gì?

[3] Booz Allen Hamilton: Hãng tư vấn về công nghệ thông tin và quản lí, có trụ sở tại Virginia, Mỹ. (BTV)

Trong các trích đoạn phỏng vấn mà Oliver phát sóng sau đó, có vẻ như không ai biết câu trả lời. Có người nói họ nhớ tên Snowden, song cũng không thể nói chính xác anh ta đã làm gì (hay tại sao anh ta lại làm thế). Sau khi trở thành nhân viên hợp đồng cho NSA, Edward Snowden đã sao chép hàng nghìn tài liệu mật và tuyệt mật, sau đó đem trao cho các phóng viên để họ công bố rộng khắp. Lẽ ra Oliver có thể kết thúc chương trình phóng sự đó bằng một thông điệp buồn, rằng sau gần hai năm tích cực đưa tin của giới truyền thông, vẫn chưa có ai ở Mỹ thực sự quan tâm đến hoạt động gián điệp trong nước của chính phủ. Nhưng nam diễn viên này đã chọn một cách khác. Anh bay tới Nga, nơi Snowden hiện đang sống lưu vong, để thực hiện một cuộc phỏng vấn trực tiếp.

Câu hỏi đầu tiên mà Oliver đặt cho Snowden là: Anh mong muốn đạt được điều gì? Snowden trả lời rằng anh muốn cho thế giới thấy những gì NSA đang làm: thu thập dữ liệu về hầu hết tất cả mọi người. Khi Oliver cho anh xem các cuộc phỏng vấn thực hiện ở Quảng trường Thời đại, trong đó hết người này đến người khác trả lời rằng họ không biết Snowden là ai, anh nói, “Không thể cung cấp đầy đủ thông tin cho mọi người được.”

Tại sao chúng ta không được cung cấp nhiều thông tin hơn về các vấn đề liên quan đến quyền riêng tư mà Snowden và những người khác đã vạch ra? Tại sao dường như chúng ta không ai quan tâm đến việc bị cơ quan chính phủ nghe lén các cuộc điện thoại, email, thậm chí cả tin nhắn của mình? Có lẽ bởi vì nhìn chung, NSA không trực tiếp ảnh hưởng đến cuộc sống của hầu hết chúng ta – ít nhất là không theo một cách hữu hình, như một sự xâm nhập mà chúng ta có thể cảm nhận.

Nhưng như Oliver cũng đã phát hiện ra tại Quảng trường Thời đại ngày hôm đó, người Mỹ có quan tâm đến quyền riêng tư khi họ nhận thức rõ vấn đề. Ngoài các câu hỏi về Snowden, anh còn đặt các câu hỏi chung chung về quyền riêng tư. Ví dụ, khi anh hỏi họ nghĩ gì nếu chính phủ thực hiện một chương trình ghi lại các ảnh khỏa thân gửi qua Internet, quan điểm của người dân New York cũng rất tương đồng với nhau – chỉ có điều là lần này, tất cả đều phản đối chuyện đó. Một người thậm chí còn tiết lộ rằng gần đây có gửi đi một bức ảnh như vậy.

Tất cả những người được hỏi trong chương trình phỏng vấn ở Quảng trường Thời đại đều nhất trí rằng những người sinh sống ở nước Mỹ cần được tự do chia sẻ bất kì điều gì trên Internet một cách riêng tư – kể cả một bức ảnh chụp hình dương vật. Đó là lập luận cơ bản của Snowden.

Hóa ra chương trình giả tưởng nêu trên cũng không khác là mấy so với thực tế. Như Snowden đã giải thích cho Oliver trong cuộc phỏng vấn giữa hai người, do các công ty như Google đặt máy chủ ở khắp nơi trên thế giới, nên ngay cả một tin nhắn đơn giản (có thể bao gồm ảnh khoả thân) giữa hai vợ chồng sinh sống trong cùng một thành phố của Mỹ cũng có thể bị đẩy ra một máy chủ ở nước ngoài trước tiên. Vì dữ liệu đó đã rời khỏi lãnh thổ nước Mỹ, dù chỉ trong một nano giây, nên dựa vào Đạo luật Patriot4, NSA có thể thu thập và lưu trữ tin nhắn hoặc email đó (bao gồm cả hình ảnh khiếm nhã), bởi vì về mặt kĩ thuật, tại thời điểm dữ liệu đó được giữ lại, nó đã đi vào nước Mỹ từ một nguồn nước ngoài. Quan điểm của Snowden là: Những người dân Mỹ

bình thường đang bị cuốn vào một mẻ lưới hậu11/9, vốn ban đầu được thiết kế để ngăn chặn khủng bố nước ngoài nhưng giờ đây đã trở thành công cụ để theo dõi tất cả mọi người.

[4] Đạo luật Patriot (viết tắt của "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" – Đoàn kết và Tăng cường sức mạnh của nước Mỹ bằng cách Cung cấp Công cụ Phù hợp Cần thiết để Ngăn chặn Khủng bố): Đạo luật của Mỹ có hiệu lực từ ngày 26/10/2001, sau khi diễn ra cuộc khủng bố ngày 11/9/2001.

Có thể bạn sẽ nghĩ rằng, trước những tin tức liên tục về các vụ xâm phạm dữ liệu cùng các chiến dịch giám sát của chính phủ, chúng ta sẽ trở nên giận dữ hơn nhiều. Rằng trước tốc độ diễn ra của hiện tượng này – chỉ trong một vài năm – chúng ta sẽ vượt qua giai đoạn sốc và chuyển sang diễu hành biểu tình trên các đường phố. Nhưng trên thực tế, điều ngược lại mới đúng. Nhiều người trong số chúng ta, thậm chí nhiều độc giả của cuốn sách này, giờ đây đã đi đến chỗ chấp nhận rằng ít nhất là ở một mức độ nào đó, mọi việc chúng ta làm – gọi điện, nhắn tin, gửi email, tham gia mạng xã hội – đều có thể bị người khác trông thấy.

Và điều đó thật đáng thất vọng.

Có thể bạn không vi phạm pháp luật. Bạn sống một cuộc sống mà bạn tưởng là bình thường và lặng lẽ, và bạn cảm thấy giữa đám đông trên mạng ngày nay, không có ai chú ý đến mình. Nhưng hãy tin tôi đi: Ngay cả bạn cũng không vô hình đâu. Ít nhất là chưa.

Tôi thích ảo thuật, và một số người có thể nói rằng để xâm nhập được vào máy tính cần phải có sự khéo léo. Một trò ảo thuật phổ biến là khiến cho một vật trở thành vô hình. Tuy nhiên, bí mật ở đây là vật đó không thực sự biến mất hay trở thành vô hình mà vẫn luôn hiện hữu ở hậu cảnh – phía sau một bức màn, bên trên một ống tay áo, ở trong túi – bất kể chúng ta có nhìn thấy nó hay không.

Điều tương tự cũng đúng với những thông tin cá nhân của từng

người hiện đang được thu thập và lưu trữ, thường là ngoài sự nhận biết của chúng ta. Hầu hết chúng ta đều không biết chỗ tìm những thông tin này, và cũng không biết rằng người khác có thể dễ dàng xem được chúng. Và bởi vìchúng ta không nhìn thấy chúng, nên có thể đinh ninh rằng mình là vô hình trước người yêu cũ, cha mẹ, trường học, cấp trên, và thậm chí là cả chính phủ.

Vấn đề là nếu bạn biết chỗ tìm, thì tất cả những thông tin đó đều có sẵn và bất kì ai cũng có thể tiếp cận.

Trong các buổi thuyết trình, tôi thường bị người ta chất vấn về quan điểm trên. Trong một lần như vậy, tôi gặp một người chất vấn là một phóng viên rất đa nghi.

Khi ấy, chúng tôi ngồi trao đổi ở bàn riêng trong quầy bar khách sạn ở một thành phố lớn của Mỹ. Phóng viên này nói rằng cô chưa hề bị xâm phạm dữ liệu bao giờ. Theo cô, vì còn trẻ nên cô không có nhiều tài sản, do đó không có nhiều hồ sơ về cô. Cô cũng không bao giờ đưa thông tin cá nhân vào các bài báo hay trang mạng xã hội cá nhân – tất cả chỉ xoay quanh công việc mà thôi. Với cô, như vậy là vô hình. Tôi xin phép được tìm số An sinh Xã hội[5] và bất kì thông tin cá nhân nào khác của cô trên mạng. Cô miễn cưỡng đồng ý.

[5] Số An sinh Xã hội (áp dụng tại Mỹ): là dãy số riêng biệt gán cho từng cá nhân, dùng để theo dõi các lợi ích An sinh Xã hội và cho các mục đích nhận dạng cá nhân khác.

Trước sự chứng kiến của cô, tôi đăng nhập vào một website dành riêng cho các nhà điều tra tư nhân. Tôi đủ điều kiện truy cập nhờ tham gia điều tra các sự cố xâm phạm máy tính trên toàn cầu. Vì đã biết tên cô, nên tôi hỏi nơi cô ở. Nếu cô không chịu nói, tôi vẫn có thể tìm ra được thông tin này trên Internet, ở một website khác.

Sau vài phút, tôi biết số An sinh Xã hội của cô, thành phố nơi cô chào đời, và thậm chí cả tên thời con gái của mẹ cô. Tôi còn biết tất cả những nơi mà cô gọi là nhà và mọi số điện thoại mà cô từng sử dụng. Cô nhìn chằm chằm vào màn hình với vẻ ngạc nhiên

thấy rõ, và xác nhận rằng các thông tin này gần như là đúng hết.

Website mà tôi sử dụng ở trên chỉ giới hạn người dùng trong phạm vi các công ty hoặc cá nhân đã được xác thực. Họ thu một khoản phí hàng tháng khá thấp, cộng thêm chi phí bổ sung cho các hoạt động tra cứu thông tin, và thi thoảng họ lại tiến hành một đợt xác thực để kiểm tra xem mục đích tra cứu của người dùng có hợp pháp không.

Nhưng chỉ cần bỏ ra một khoản phí tra cứu nhỏ là bạn có thể tìm kiếm các thông tin tương tự về bất cứ ai. Và chuyện đó là hoàn toàn hợp pháp.

Bạn đã bao giờ điền vào một biểu mẫu trực tuyến, gửi thông tin tới một trường học hoặc một tổ chức đưa thông tin của họ lên mạng, hoặc đồng ý đăng tải lên Internet tin tức về một vụ việc pháp lý chưa? Nếu rồi, nghĩa là bạn đã tình nguyện cung cấp thông tin cá nhân cho một bên thứ ba và bên này có thể tùy nghi sử dụng thông tin đó. Rất có thể là một số – nếu không phải tất cả – dữ liệu đó bây giờ đã xuất hiện trên mạng và sẵn sàng phục vụ cho các công ty kiếm tiền từ việc thu thập từng mẩu thông tin cá nhân trên Internet. Tổ chức Privacy Rights Clearinghouse[6] cho biết có hơn 130 công ty chuyên thu thập thông tin cá nhân (bất kể chính xác hay không) về bạn.

[6] Privacy Rights Clearinghouse (PRC – Tổ chức Bảo vệ Quyền Riêng tư): Một tổ chức phi lợi nhuận ở Mỹ, chuyên cung cấp thông tin cho người tiêu dùng và bảo vệ quyền lợi của người tiêu dùng.

Và còn có cả những dữ liệu mà bạn không tình nguyện cung cấp trên mạng nhưng vẫn được các công ty và chính phủ thu thập – chúng ta gửi email, nhắn tin, và gọi điện cho ai; tìm kiếm thông tin gì trên mạng; mua sắm những gì (cả trên mạng và ở cửa hàng truyền thống); và đi những đâu (cả đi bộ lẫn đi xe). Khối lượng dữ liệu thu thập được về từng người trong số chúng ta đang tăng theo cấp số nhân mỗi ngày.

Có thể bạn cho rằng không cần phải lo lắng về điều này. Nhưng

hãy tin tôi đi: bạn cần phải lo lắng đấy. Tôi hy vọng rằng khi đọc hết cuốn sách này, bạn sẽ được trang bị đầy đủ thông tin và sẵn sàng bắt tay vào thực hiện hành động nào đó.

Chúng ta đang sống trong ảo tưởng về sự riêng tư, và có lẽ chúng ta đã sống như thế này suốt nhiều thập niên qua.

Có thể đôi lúc nào đó, chúng ta cũng thoáng nhíu mày khó chịu khi thấy chính phủ, công ty, cấp trên, thầy cô giáo, và bố mẹ mình lại tiếp cận được nhiều thông tin về đời sống riêng tư của mình đến thế. Song vì sự tiếp cận này được mở rộng dần dần, vì bấy lâu nay chúng ta cứ vô tư tiếp nhận từng sự thuận tiện nho nhỏ mà kỹ thuật số mang lại nhưng không kháng cự lại tác động của chúng đến quyền riêng tư của mình, nên giờ đây việc quay ngược thời gian càng lúc càng trở nên khó khăn hơn. Hơn nữa, có ai lại muốn vứt bỏ món đồ chơi ưa thích của mình chứ?

Mối nguy hại của việc sống trong trạng thái bị giám sát bằng kỹ thuật số không nằm ở việc dữ liệu bị thu thập (chúng ta gần như không thể làm được gì về điều đó) mà nằm ở việc người ta làm gì với dữ liệu sau khi thu thập được.

Hãy tưởng tượng những gì mà một công tố viên hăng hái có thể làm được với tập hồ sơ khổng lồ gồm các điểm dữ liệu thô về bạn, có thể là từ vài năm trước. Ngày nay, dữ liệu – đôi khi là cả những dữ liệu được thu thập ngoài ngữ cảnh – sẽ tồn tại vĩnh viễn. Ngay cả thẩm phán Stephen Breyer của Tòa án Tối cao Mỹ cũng đồng ý rằng, “Rất khó biết trước được khi nào thì phát ngôn của một người bỗng trở nên có liên quan đến cuộc điều tra nào đó của một vị công tố viên.” Nói cách khác, có thể bạn chẳng mảy may bận tâm đến bức ảnh chụp cảnh bạn say rượu mà một người nào đó đăng lên Facebook.

Có thể bạn cho rằng mình không có gì để giấu diếm, nhưng bạn dám chắc chưa? Trong một bài viết có lập luận chặt chẽ đăng trên tạp chí Wired, nhà nghiên cứu an ninh mạng nổi tiếng Moxie Marlinspike chỉ ra rằng ngay cả một chuyện đơn giản như sở hữu một con tôm hùm nhỏ cũng là tội phạm liên bang ở Mỹ. “Bất kể là

bạn mua nó tại cửa hàng, được người khác cho, nó đã chết hay còn sống, bạn tìm thấy nó sau khi nó chết vì các nguyên nhân tự nhiên, hoặc thậm chí bạn giết nó trong lúc tự vệ – bạn vẫn có thể vào tù vì một con tôm hùm." Vấn đề ở đây là có rất nhiều quy định nhỏ nhặt, chỉ mang tính danh nghĩa mà có khi bạn phạm phải nhưng không biết. Chỉ có điều, bây giờ đã có một đường mòn dữ liệu[7] để chứng minh điều đó chỉ sau vài cú click chuột, và bất cứ ai muốn cũng có thể tiếp cận được nó.

[7] Đường mòn dữ liệu (data trail): Là một chuỗi dữ liệu mà người dùng để lại khi sử dụng Internet, gửi tin nhắn, hay gọi điện thoại…

Quyền riêng tư rất phức tạp. Nó không phải là vấn đề áp dụng đồng đều cho tất cả mọi người. Mỗi chúng ta đều có những lý do khác nhau để phân biệt thông tin cá nhân nào có thể sẵn sàng chia sẻ tự do với người lạ, thông tin nào muốn giữ riêng cho mình. Có thể bạn không muốn vợ/chồng đọc được những nội dung cá nhân của mình. Có thể bạn không muốn công ty biết về đời sống riêng của mình. Hoặc cũng có thể bạn lo rằng mình đang bị một cơ quan chính phủ theo dõi.

Đó là những kịch bản rất khác nhau, nên không thể đưa ra lời khuyên nào cho phù hợp với tất cả được. Bởi vì chúng ta có những quan điểm phức tạp và đa dạng về sự riêng tư, nên tôi sẽ bàn về điều quan trọng nhất – chuyện gì đang diễn ra đối với hoạt động thu thập dữ liệu lén lút ngày nay – và để bạn tự quyết định xem điều gì là phù hợp với mình.

Mục đích của cuốn sách này là giúp bạn nắm được những phương thức khác nhau để duy trì sự riêng tư trong thế giới số, đồng thời đưa ra những giải pháp mà bạn có thể áp dụng hoặc không. Vì sự riêng tư là một lựa chọn cá nhân, nên mức độ ẩn danh cũng sẽ thay đổi theo từng quan điểm cá nhân.

Trong cuốn sách này, tôi sẽ chứng minh rằng từng người trong chúng ta đang bị theo dõi, ở nhà và bên ngoài – khi bạn ra phố, ngồi ở quán cà phê, hoặc lái xe xuống đường cao tốc. Máy tính,

điện thoại, ô tô, hệ thống báo động tại gia, thậm chí tủ lạnh của bạn cũng đều là những điểm tiếp cận tiềm năng vào cuộc sống riêng tư của bạn.

Tin vui là, ngoài việc làm bạn sợ, tôi cũng sẽ chỉ cho bạn những việc cần làm để khắc phục tình trạng thiếu vắng sự riêng tư vốn đã trở thành chuyện thường nhật.

Trong cuốn sách này, bạn sẽ học được cách:

- mã hóa và gửi email an toàn
- bảo vệ dữ liệu bằng việc quản lý tốt mật khẩu
- giấu địa chỉ IP thực khi truy cập vào các website
- che dấu vết để máy tính không bị theo dõi
- bảo vệ tính ẩn danh của bạn
- và nhiều hơn nữa.

Bây giờ, hãy sẵn sàng để làm chủ nghệ thuật ẩn mình.

Chương 1: MẬT KHẨU CỦA BẠN CÓ THỂ BỊ BẺ KHÓA!

Jennifer Lawrence đã có một cuối tuần trùng dịp Ngày lễ Lao động[8] mệt mỏi. Sáng hôm đó, năm 2014, nữ diễn viên từng giành giải Oscar này cùng với một số nhân vật nổi tiếng khác tỉnh dậy và phát hiện ra rằng những bức ảnh riêng tư nhất của họ – trong đó có nhiều bức khỏa thân – đã bị phát tán trên mạng Internet.

[8] Ngày lễ Lao động: Ngày lễ toàn quốc ở Mỹ, diễn ra vào ngày thứ Hai đầu tiên trong tháng Chín hằng năm.

Bây giờ, bạn hãy nhắm mắt hình dung về tất cả những bức ảnh hiện đang được lưu trữ trên máy tính, điện thoại, và email của mình. Dĩ nhiên, phần lớn đều là những hình ảnh vô hại. Bạn không thấy vấn đề gì khi để cả thế giới cùng xem những bức ảnh chụp cảnh hoàng hôn, những bức ảnh gia đình dễ thương, thậm chí cả những bức ảnh tự sướng hài hước. Nhưng liệu bạn có thấy thoải mái khi chia sẻ mọi bức ảnh của mình không? Bạn sẽ cảm thấy thế nào nếu đột nhiên tất cả chúng đều xuất hiện trên mạng? Có thể không phải ảnh cá nhân nào cũng mang tính nhạy cảm, nhưng dẫu sao, đó cũng vẫn là tư liệu về những khoảnh khắc riêng tư. Chúng ta phải là người có quyền quyết định xem có nên chia sẻ chúng hay không, khi nào, và bằng cách nào, nhưng với dịch vụ đám mây, sự lựa chọn đó có thể không phải lúc nào cũng thuộc về chúng ta.

Câu chuyện về Jennifer Lawrence thống trị khắp các mặt báo trong ngày hôm đó. Đây là một phần trong sự kiện The Fappening[9], một đợt rò rỉ lớn những bức ảnh khỏa thân và bán khỏa thân của Rihanna, Kate Upton, Kaley Cuoco, Adrianne Curry cùng gần 300 người nổi tiếng khác, hầu hết đều là phụ nữ – các bức ảnh lưu trữ trong điện thoại di động của họ đã bị truy cập từ xa rồi bị đem chia sẻ trên mạng. Dĩ nhiên, một số người rất thích thú khi được xem những bức ảnh này; tuy nhiên, với nhiều

người khác, sự cố này là một lời nhắc nhở đáng lo ngại rằng điều tương tự cũng có thể xảy ra với chính họ.

[9] The Fappening (từ ghép giữa từ fap (thủ dâm) và tên bộ phim thuộc thể loại tâm lý kinh dị, The Happening): Tên do giới truyền thông và người dùng Internet đặt cho sự kiện gần 500 bức ảnh riêng tư nhạy cảm của nhiều người nổi tiếng bị phát tán trên mạng, xảy ra vào ngày 31/8/2014.

Những hình ảnh riêng tư của Jennifer Lawrence và những người khác đã bị tiếp cận như thế nào?

Do tất cả những người nổi tiếng đều sử dụng iPhone, nên theo suy đoán ban đầu, đây có lẽ là một cuộc xâm phạm dữ liệu lớn nhắm vào iCloud, một dịch vụ lưu trữ đám mây của Apple dành cho người dùng iPhone. Khi thiết bị vật lý hết bộ nhớ, khách hàng có thể lưu các dữ liệu hình ảnh, file, nhạc, và trò chơi trên máy chủ ở Apple, thường là với một khoản phí nhỏ hàng tháng. Google cũng cung cấp dịch vụ tương tự cho Android.

Apple, vốn hầu như không bao giờ bình luận trên các phương tiện truyền thông về vấn đề an ninh, phủ nhận mọi sai sót từ phía họ. Công ty này đưa ra một tuyên bố gọi vụ việc trên là "cuộc tấn công nhắm vào tên người dùng, mật khẩu, và câu hỏi bảo mật," đồng thời bổ sung thêm rằng, "Trong các trường hợp mà chúng tôi đã điều tra, không có trường hợp nào xảy ra do hành vi xâm phạm vào các hệ thống của Apple, bao gồm iCloud hay ứng dụng Tìm iPhone."

Những bức ảnh trên xuất hiện trước tiên ở một diễn đàn hacker chuyên đăng tải ảnh bị đánh cắp. Diễn đàn này có nhiều cuộc thảo luận sôi nổi về các công cụ điều tra số[10] dùng để đánh cắp những bức ảnh đó. Các nhà nghiên cứu, điều tra viên, và cơ quan thực thi pháp luật sử dụng những công cụ này để truy cập dữ liệu từ các thiết bị hoặc đám mây, thường là để điều tra một vụ phạm tội. Và tất nhiên, chúng cũng còn nhiều công dụng khác.

[10] Điều tra số (digital forensics): Một nhánh của khoa học pháp y,

bao gồm việc khôi phục và điều tra các tài liệu được tìm thấy trong các thiết bị kỹ thuật số, thường là có liên quan đến tội phạm máy tính.

Một trong những công cụ được thảo luận công khai trên diễn đàn này, Elcomsoft Phone Password Breaker[11], gọi tắt là EPPB, được thiết kế để giúp các cơ quan thực thi pháp luật cũng như các cơ quan chính phủ có thể truy cập vào các tài khoản iCloud và được rao bán công khai. Đây chỉ là một trong nhiều công cụ có sẵn, nhưng có vẻ nó là phổ biến nhất trên diễn đàn này. EPPB yêu cầu trước tiên người dùng phải có thông tin về tên đăng nhập và mật khẩu iCloud của mục tiêu cần tấn công. Tuy nhiên, đối với những người sử dụng diễn đàn này, việc lấy tên đăng nhập và mật khẩu iCloud không phải là chuyện khó. Tình cờ, vào dịp cuối tuần nghỉ lễ đó trong năm 2014, một người đã đăng lên kho lưu trữ mã nguồn trực tuyến phổ biến Github một công cụ gọi là iBrute, một cơ chế bẻ khóa mật khẩu được thiết kế để lấy thông tin đăng nhập iCloud của bất kỳ ai.

[11] Elcomsoft Phone Password Breaker: Công cụ trả phí dùng để tìm lại các dữ liệu cần thiết, như dò lại mật khẩu iCloud khi bị quên thông qua bản dự phòng trên iTunes.

Sử dụng kết hợp iBrute và EPPB, kẻ xấu có thể mạo danh nạn nhân và tải xuống bản sao lưu đầy đủ dữ liệu iPhone của nạn nhân đó trên đám mây và đưa vào một thiết bị khác. Tính năng rất hữu ích với người dùng khi họ nâng cấp điện thoại. Và nó cũng có giá trị đối với kẻ tấn công, bởi hắn có thể thấy mọi hoạt động bạn từng thực hiện trên thiết bị di động của mình. Điều này mang lại nhiều thông tin hơn so với việc chỉ đăng nhập vào tài khoản iCloud của nạn nhân.

Jonathan Zdziarski, cố vấn điều tra số kiêm nhà nghiên cứu an ninh, chia sẻ với tạp chí Wiredrằng kết quả kiểm tra các bức ảnh bị rò rỉ do ông thực hiện khớp với việc sử dụng iBrute và EPPB. Khi chiếm được quyền truy cập vào một bản sao lưu dữ liệu iPhone được khôi phục, kẻ tấn công sẽ lấy được rất nhiều thông

tin cá nhân có thể sử dụng để tống tiền sau này.

Tháng 10 năm 2016, Ryan Collins, một người 36 tuổi sống ở Lancaster, Pennsylvania, bị kết án 18 tháng tù vì tội "truy cập trái phép vào một máy tính được bảo vệ để lấy thông tin" liên quan đến vụ tấn công trên. Hắn bị buộc tội truy cập trái phép vào hơn 100 tài khoản email của Apple và Google.

Để bảo vệ tài khoản iCloud và các tài khoản trực tuyến khác của mình, bạn phải đặt mật khẩu mạnh. Điều đó là hiển nhiên. Tuy nhiên, theo kinh nghiệm của bản thân với tư cách là một chuyên gia kiểm định an ninh – tức người được thuê để tấn công vào các mạng máy tính nhằm tìm kiếm các lỗ hổng – tôi thấy rằng nhiều người, kể cả lãnh đạo các tập đoàn lớn, rất lười đặt mật khẩu. Một ví dụ là Michael Lynton, Giám đốc Điều hành của hãng Sony Entertainment. Ông này dùng cụm ký tự "sonyml3" làm mật khẩu tài khoản tên miền của mình. Không có gì ngạc nhiên khi email của ông bị tấn công và phát tán trên Internet vì kẻ tấn công nắm được quyền truy cập vào gần như mọi cơ sở dữ liệu trong công ty với vai trò quản trị viên.

Ngoài mật khẩu liên quan đến công việc, còn có mật khẩu bảo vệ các tài khoản riêng tư. Việc chọn một mật khẩu khó đoán không ngăn được các công cụ tấn công như oclHashcat (một công cụ phá mật khẩu lợi dụng các đơn vị xử lý đồ họa – hay GPU – để thực hiện tấn công tốc độ cao), nhưng nó sẽ làm cho quá trình này diễn ra chậm lại, đủ để kẻ tấn công nản chí mà chuyển sang một mục tiêu dễ ăn hơn.

Có thể đưa ra một dự đoán hợp lý rằng trong vụ tấn công Ashley Madison vào tháng 7 năm 2015[12], các mật khẩu bị tiết lộ chắc chắn cũng được dùng ở những nơi khác nữa, như tài khoản ngân hàng và thậm chí tài khoản của máy tính ở nơi làm việc. Trong danh sách 11 triệu mật khẩu của Ashley Madison bị phát tán trên mạng, phổ biến nhất là "123456," "12345," "password", "DEFAULT," "123456789," "qwerty", "12345678", "abc123," và "1234567." Nếu cũng đang sử dụng những mật khẩu như trên, thì rất có thể bạn sẽ trở thành nạn nhân của các vụ xâm phạm dữ

liệu, vì hầu hết các bộ công cụ bẻ mật khẩu có sẵn trên mạng đều có các cụm từ thông dụng này. Bạn có thể truy cập website www.haveibeenpwned.com để kiểm tra xem tài khoản của mình đã từng bị xâm phạm bao giờ chưa.

[12] Ashley Madison: Một dịch vụ hẹn hò và mạng xã hội trực tuyến ở Canada, nhắm đến đối tượng là những người đã lập gia đình hoặc đã có bạn trai/bạn gái. Tháng 7/2015, một nhóm hacker đánh cắp dữ liệu người dùng của công ty này và phát tán lên mạng.

Trong thế kỷ 21, chúng ta có thể làm tốt hơn. Thực ra là tốt hơn rất nhiều, với nhiều cách sắp xếp ký tự chữ và số dài hơn, phức tạp hơn nhiều. Nghe có vẻ khó, nhưng tôi sẽ hướng dẫn bạn cả cách tự động và thủ công để thực hiện điều đó .

Cách dễ nhất là đừng tự tạo mật khẩu mà hãy tự động hóa quy trình này. Hiện đã có một số phần mềm quản lý mật khẩu có thể lưu trữ mật khẩu trong kho chứa có khóa và cho phép bạn truy cập bằng một cú nhấp chuột khi cần, đồng thời còn tạo ra được những mật khẩu mới, rất mạnh và độc đáo.

Tuy nhiên, phương pháp này có hai vấn đề cần lưu ý. Một là, các phần mềm quản lý mật khẩu sử dụng một mật khẩu chính để truy cập. Nếu có kẻ khiến máy tính của bạn lây nhiễm một phần mềm độc hại và đánh cắp cơ sở dữ liệu mật khẩu và mật khẩu chính lưu trong đó bằng chương trình keylog[13], thì trò chơi kết thúc. Khi đó, kẻ này sẽ có quyền truy cập vào tất cả các mật khẩu của bạn. Trong các dự án kiểm định an ninh, thi thoảng tôi thay thế phần mềm quản lý mật khẩu bằng một phiên bản sửa đổi để lấy mật khẩu chính (trong trường hợp đó là phần mềm mã nguồn mở). Điều này được thực hiện sau khi tôi giành được quyền truy cập vào mạng lưới của khách hàng bằng vai trò quản trị. Sau đó, tôi sẽ tấn công tất cả các mật khẩu đặc quyền. Nói cách khác, tôi sẽ sử dụng các phần mềm quản lý mật khẩu làm cửa sau để lấy chìa khóa xâm nhập.

[13] Keylog: Chỉ việc sử dụng phần mềm để ghi lại mọi thao tác

trên bàn phím của người dùng máy tính, đặc biệt là để tiếp cận trái phép mật khẩu và các thông tin bí mật khác.

Vấn đề thứ hai khá rõ ràng: Nếu để mất mật khẩu chính, bạn sẽ mất tất cả các mật khẩu còn lại. Nhưng không sao, bởi bạn luôn có thể cài đặt lại mật khẩu cho từng tài khoản, nhưng đó sẽ là một rắc rối lớn nếu bạn có nhiều tài khoản khác nhau.

Tuy có những sai sót này, nhưng những mẹo sau đây cũng đủ giúp bạn giữ an toàn cho mật khẩu của mình.

Đầu tiên, các cụm mật khẩu[14], chứ không đơn thuần chỉ là mật khẩu, phải dài – ít nhất 20-25 ký tự. Lý tưởng nhất, hãy sử dụng các ký tự ngẫu nhiên, như ek5iogh#skf&skd. Thật không may, con người thường khó học thuộc được các chuỗi ngẫu nhiên. Vì vậy, hãy sử dụng phần mềm quản lý mật khẩu, như thế còn tốt hơn nhiều so với việc tự chọn mật khẩu. Tôi thích các phần mềm quản lý mật khẩu mã nguồn mở như Password Safe và KeePass, vốn chỉ lưu trữ dữ liệu cục bộ trên máy tính của bạn.

[14] Cụm mật khẩu (passphrase): Một chuỗi ký tự dùng để kiểm soát quyền truy cập một hệ thống, chương trình, hay dữ liệu trên máy tính. Cụm từ mật khẩu cũng tương tự như mật khẩu (password) xét về cách sử dụng, nhưng nhìn chung là dài hơn để tăng cường an ninh.

Một nguyên tắc quan trọng khác là không bao giờ sử dụng cùng một mật khẩu cho hai tài khoản khác nhau. Điều này rất khó thực hiện vì ngày nay, chúng ta dùng mật khẩu cho hầu như tất cả mọi thứ. Do đó, hãy để phần mềm quản lý mật khẩu tạo và lưu giữ các mật khẩu mạnh, riêng biệt cho bạn.

Nhưng ngay cả khi bạn đã có mật khẩu mạnh, kẻ xấu vẫn có thể sử dụng công nghệ để đánh bại bạn. Có những chương trình đoán mật khẩu như John the Ripper, một chương trình mã nguồn mở miễn phí mà bất kỳ ai cũng có thể tải xuống và hoạt động trong các tham số cấu hình do người dùng thiết lập. Ví dụ, người dùng có thể chỉ định số lượng ký tự cần thử, có sử dụng các ký hiệu đặc biệt hay không, có bao gồm các bộ ký tự ngoại ngữ hay không,...

John the Ripper và các phần mềm tấn công mật khẩu khác có thể hoán vị các ký tự trong mật khẩu bằng cách sử dụng các bộ quy tắc cực kỳ hiệu quả trong việc đánh cắp mật khẩu. Điều này đơn giản có nghĩa là chúng sẽ thử mọi tổ hợp có thể có của các số, chữ cái, và ký hiệu trong các tham số cho đến khi bẻ được mật khẩu. May mắn nằm ở chỗ, hầu hết chúng ta đều không có ý định phòng vệ trước chính quyền, vốn có thời gian và nguồn lực dư dả đến vô hạn định. Có chăng, chúng ta chỉ muốn phòng vệ trước vợ/chồng, người thân, hay một người mà chúng ta thực lòng căm ghét (nhưng khi gặp phải một mật khẩu dài 25 ký tự, người đó sẽ không có đủ cả thời gian lẫn nguồn lực để ngồi phá giải).

Giả sử bạn muốn tạo mật khẩu theo cách cũ, và đã chọn được một số mật khẩu rất mạnh. Hãy đoán thử xem chuyện gì sẽ xảy ra? Nhớ là đừng có viết thẳng băng trên mặt giấy rằng, “Ngân hàng Bank of America: 4the1sttimein4ever*.” Như thế khác nào vẽ đường cho hươu chạy. Trong trường hợp này, hãy dùng một dạng ký tự mã hóa thay cho tên ngân hàng của bạn (giả dụ thế), chẳng hạn “Lọ bánh quy” (vì trước đây có người đã giấu tiền trong các lọ bánh quy) và theo sau đó là “4the1st.” Hãy lưu ý, tôi không ghi cụm từ mật khẩu hoàn thiện. Không cần phải làm thế. Bạn đã biết phần còn lại của cụm từ là gì rồi. Nhưng người khác có thể không biết.

Người nào tìm thấy bản danh sách các mật khẩu không đầy đủ này đều sẽ thấy rối trí – ít nhất là lúc đầu. Xin kể ra đây một câu chuyện thú vị: Một lần, tôi tới nhà một người bạn – anh này là một nhân viên nổi tiếng của Microsoft – và trong bữa tối, chúng tôi trao đổi vấn đề an ninh mật khẩu với vợ con của anh. Giữa chừng câu chuyện, vợ của bạn tôi đứng dậy và đi về phía tủ lạnh. Chị đã viết tất cả các mật khẩu của mình vào một mảnh giấy và dùng nam châm gắn nó vào cửa tủ lạnh. Bạn tôi chỉ còn biết lắc đầu, tôi thì cười toe toét. Viết mật khẩu ra giấy có thể không phải là một giải pháp hoàn hảo, và không sử dụng mật khẩu mạnh cũng vậy.

Một số website – chẳng hạn website ngân hàng – sẽ khóa người

dùng sau một vài lần thử mật khẩu không thành công, thường là ba lần. Tuy nhiên, nhiều nơi vẫn chưa thực hiện điều này. Nhưng ngay cả khi một website áp dụng cơ chế khóa người dùng sau ba lần thử không thành công, thì những kẻ xấu sử dụng John the Ripper hoặc oclHashcat cũng không bẻ mật khẩu theo cách đó. (Nhân tiện, oclHashcat phân tán quá trình tấn công qua nhiều GPU và mạnh hơn nhiều so với John the Ripper.) Ngoài ra, hacker cũng không mò mẫm thử từng mật khẩu khả dĩ trên một website trực tiếp.

Giả sử kẻ xấu đã lấy cắp được dữ liệu, và trong phần dữ liệu kết xuất có cả tên người dùng cũng như mật khẩu. Nhưng các mật khẩu thu được từ cuộc xâm phạm này chỉ là những thứ vô nghĩa.

Mà như vậy thì kẻ tấn công đâu có được lợi ích gì?

Hễ khi nào bạn gõ một mật khẩu, dù là để mở khóa máy tính xách tay hay một dịch vụ trực tuyến – mật khẩu đó sẽ được đưa qua một thuật toán một chiều gọi là hàm băm. Nó khác với quá trình mã hóa. Mã hóa là hai chiều: bạn có thể mã hóa và giải mã, với điều kiện bạn có chìa khóa trong tay. Hàm băm là một dạng dấu vân tay đại diện cho một chuỗi ký tự cụ thể. Về lý thuyết, các thuật toán một chiều là bất khả đảo – hoặc ít nhất là không dễ dàng.

Nội dung được lưu trữ trong cơ sở dữ liệu mật khẩu trên máy tính cá nhân truyền thống, thiết bị di động, hoặc tài khoản đám mây của bạn không phải là MaryHadALittleLamb123$, mà là giá trị băm của nó, tức là một chuỗi các số và chữ cái, đóng vai trò là dấu hiệu đại diện cho mật khẩu của bạn.

Bộ nhớ được bảo vệ trên máy tính lưu trữ giá trị băm của mật khẩu, chứ không phải là bản thân mật khẩu, và các giá trị này có thể bị đánh cắp trong một cuộc tấn công vào các hệ thống mục tiêu hoặc bị rò rỉ trong các vụ xâm phạm dữ liệu. Sau khi đã lấy được các giá trị băm mật khẩu này, hacker có thể sử dụng nhiều công cụ có sẵn công khai, như John the Ripper hoặc oclHashcat, để phá vỡ chúng nhằm tìm ra mật khẩu thực thông qua kỹ thuật

vét cạn[15] hoặc thử từng từ trong một danh sách các từ, chẳng hạn từ điển. Các tùy chọn trong John the Ripper và oclHashcat cho phép kẻ tấn công sửa đổi các từ được thử trước nhiều bộ quy tắc, ví dụ bộ quy tắc leetspeak – một hệ thống dùng để thay thế các chữ cái bằng số, như trong "k3v1n m17n1ck." Quy tắc này sẽ thay đổi tất cả các mật khẩu thành nhiều kiểu hoán vị leetspeak khác nhau. Các phương pháp bẻ khóa mật khẩu này hiệu quả hơn nhiều so với phương pháp tấn công vét cạn đơn giản. Thông thường, những mật khẩu đơn giản và phổ biến nhất sẽ bị phá trước, sau đó mới dần chuyển sang các mật khẩu phức tạp hơn. Thời gian cần thiết cho quá trình này phụ thuộc vào một số yếu tố. Sử dụng công cụ bẻ khóa kết hợp với tên người dùng và giá trị băm mật khẩu đánh cắp được, hacker có thể truy cập vào một hoặc nhiều tài khoản của bạn bằng cách thử mật khẩu đó trên nhiều website kết nối với địa chỉ email hoặc các dữ liệu định danh khác của bạn.

[15] Tấn công vét cạn (brute force): Kiểu tấn công được dùng cho tất cả các loại mã hóa, hoạt động bằng cách thử tất cả các chuỗi mật khẩu có thể để tìm ra mật khẩu. Vì thế, thời gian thực hiện phương pháp này rất lâu, tùy theo độ dài của mật khẩu. Thông thường, kỹ thuật này chỉ được dùng khi các phương pháp khác đều không có hiệu quả.

Nhìn chung, mật khẩu càng nhiều ký tự thì các chương trình đoán mật khẩu như John the Ripper sẽ càng mất nhiều thời gian để quét tất cả các biến khả dĩ. Vì các bộ vi xử lý máy tính ngày nay càng lúc càng chạy nhanh hơn, nên thời gian cần thiết để tính toán toàn bộ số mật khẩu có sáu, thậm chí tám, ký tự cũng ngày một rút ngắn đi. Đó là lý do tại sao tôi khuyên bạn nên sử dụng mật khẩu từ 25 ký tự trở lên.

Sau khi bạn đã tạo được những mật khẩu mạnh, đừng bao giờ tiết lộ chúng. Chuyện này nghe có vẻ hiển nhiên đến mức không cần phải nhắc, nhưng các cuộc khảo sát ở London và nhiều thành phố lớn khác cho thấy, người ta sẵn sàng trao đổi mật khẩu của mình để lấy những thứ vặt vãnh như một cây bút hoặc một miếng sô-

cô-la.

Một người bạn của tôi có lần cho bạn gái biết mật khẩu Netflix của mình. Quyết định này ngay vào thời điểm đó là điều dễ hiểu, vì anh muốn để cô tự chọn phim cho cả hai cùng xem. Nhưng trong phần phim được đề xuất trên Netflix là những bộ phim được giới thiệu với lý do "vì bạn đã từng xem…," bao gồm cả những bộ phim mà anh đã xem với các cô bạn gái trước kia.

Tất nhiên, ai chẳng có người yêu cũ. Có khi chính bạn còn nghi ngờ nếu hẹn hò với một người chưa từng có ai. Nhưng không cô bạn gái nào muốn nhìn thấy bằng chứng về những cô gái đã đến trước mình cả.

Nếu đã bảo vệ các dịch vụ trực tuyến của mình bằng mật khẩu, thì bạn cũng nên bảo vệ các thiết bị cá nhân bằng mật khẩu. Hầu hết chúng ta đều có máy tính xách tay, và nhiều người vẫn có máy tính để bàn. Có thể bây giờ bạn đang ở nhà một mình, nhưng còn những vị khách mà bạn mời tới ăn tối lát nữa đến thì sao? Tại sao lại phải chấp nhận rủi ro rằng một người trong số họ có thể truy cập các file, ảnh, và trò chơi của bạn khi ngồi vào máy? Sau đây là một câu chuyện cảnh giác khác về Netflix: Vào thời Netflix chủ yếu vẫn gửi DVD, một cặp vợ chồng đã bị chơi khăm một vố như thế này. Trong một bữa tiệc tại gia, họ để mở tài khoản Netflix trên trình duyệt máy tính của mình. Sau đó, họ phát hiện ra rằng nhiều loại phim khiêu dâm đã được thêm vào danh sách đăng ký – nhưng họ chỉ phát hiện ra điều này sau khi nhận được những bộ phim đó qua thư.

Việc tự bảo vệ mình bằng mật khẩu tại văn phòng thậm chí còn quan trọng hơn. Hãy nghĩ về những lần bạn đang ngồi ở bàn làm việc thì bị gọi đi họp đột xuất. Ai đó có thể đi ngang qua chỗ bạn và thấy được bảng tính ngân sách cho quý tiếp theo. Hay tất cả các email có trong hộp thư đến của bạn. Hay tệ hơn, nếu không đặt chế độ bảo vệ bằng mật khẩu khi màn hình ở chế độ chờ và hẹn máy tự động kích hoạt chế độ này khi màn hình không hoạt động một vài giây, thì bất cứ khi nào bạn rời khỏi bàn làm việc trong một thời gian dài – ví dụ ra ngoài ăn trưa hoặc tham dự một

cuộc họp kéo dài – một người nào đó có thể ngồi vào chỗ bạn, viết một email và gửi đi với tư cách là bạn. Hoặc thậm chí thay đổi ngân sách quý tiếp theo trên bảng tính.

Có nhiều phương pháp mới sáng tạo giúp ngăn chặn những tình huống này, như phần mềm khóa màn hình sử dụng Bluetooth để xác minh xem bạn có ở gần máy tính hay không. Nói cách khác, nếu bạn vào nhà vệ sinh và điện thoại di động của bạn ra khỏi phạm vi Bluetooth của máy tính, thì màn hình sẽ bị khóa ngay lập tức. Ngoài ra, còn có các phiên bản sử dụng thiết bị Bluetooth như dây đeo cổ tay hoặc đồng hồ thông minh nhưng có cơ chế hoạt động tương tự.

Tạo mật khẩu để bảo vệ các tài khoản và dịch vụ trực tuyến là một chuyện, nhưng điều đó cũng không giúp ích gì nếu có người lấy được thiết bị của bạn, nhất là khi bạn đang để các tài khoản trực tuyến ở trạng thái đăng nhập. Vì vậy, nếu bạn quyết định chỉ bảo vệ bằng mật khẩu đối với một loại thiết bị nhất định, hãy bảo vệ các thiết bị di động, vì chúng dễ bị mất hoặc đánh cắp nhất. Tuy nhiên, tổ chức Consumer Reports cho hay 34% người Mỹ không bảo vệ các thiết bị di động của mình bằng bất kỳ biện pháp nào, như khóa màn hình bằng mã PIN đơn giản gồm 4 chữ số.

Năm 2014, một sĩ quan cảnh sát ở thành phố Martinez, California đã thú nhận hành vi ăn cắp các bức ảnh khỏa thân trên điện thoại di động của một người bị nghi là lái xe trong lúc say rượu – đây là sự vi phạm Tu chính án thứ tư trong Tuyên ngôn Nhân quyền của Hiến pháp. Cụ thể, Tu chính án thứ tư cấm các hành vi tìm kiếm và thu giữ không hợp lý khi không có lệnh của thẩm phán và không có lý do rõ ràng – chẳng hạn, các nhân viên thực thi pháp luật phải nêu rõ tại sao họ muốn lấy điện thoại của bạn.

Nếu bạn vẫn chưa bảo vệ thiết bị di động của mình bằng mật khẩu, hãy đặt sách xuống và làm ngay nhé. Tôi nói nghiêm túc đấy.

Có ba cách khóa điện thoại phổ biến – áp dụng với cả Android, iOS, hay bất kỳ loại nào khác. Thông dụng nhất là passcode – một

dãy số được sắp xếp theo thứ tự nhất định mà bạn nhập vào để mở khóa điện thoại. Nhưng đừng chấp nhận lượng chữ số mà điện thoại đề xuất. Hãy vào mục cài đặt và tự đặt cấu hình mật khẩu để passcode được mạnh hơn – nếu thích, bạn có thể đặt bảy số (chẳng hạn, lấy một số điện thoại cũ đã lâu không dùng.) Đừng dùng passcode dưới bốn số.

Một số thiết bị di động cho phép bạn chọn passcode bằng chữ. Một lần nữa, hãy chọn ít nhất bảy ký tự. Các thiết bị di động hiện đại hiển thị cả khóa bằng chữ và số trên cùng một màn hình, giúp việc chuyển đổi qua lại giữa chúng trở nên dễ dàng hơn.

Một cách khóa khác là bằng hình ảnh. Từ năm 2008, điện thoại Android đã được trang bị các mẫu khóa gọi là ALP (Android Lock Pattern – ALP). Chín dấu chấm xuất hiện trên màn hình, và bạn kết nối chúng theo bất kỳ thứ tự nào tùy ý; chuỗi kết nối đó sẽ trở thành passcode của bạn. Có thể bạn cho rằng giải pháp này thật tài tình, và chỉ riêng số lượng các cách kết hợp khả dĩ ở đây cũng đã đủ để khiến chuỗi mà bạn chọn trở nên không thể phá vỡ nổi. Nhưng tại hội thảo PasswordsCon16 năm 2015, theo thông tin từ các nhà nghiên cứu, trong một cuộc khảo sát, những người tham gia cho biết họ chỉ sử dụng một số rất ít trong số 140.704 mẫu có trong ALP – quả đúng là bản chất khó bỏ của con người. Và những mẫu dễ đoán đó là gì vậy? Thường là chữ cái đầu tiên của tên người dùng. Nghiên cứu này cũng phát hiện ra rằng mọi người có xu hướng sử dụng các chấm ở giữa và ít sử dụng các dấu chấm ở bốn góc xa. Lần tới khi bạn đặt ALP, hãy để ý đến điều này nhé.

[16] Hội nghị PasswordsCon: Hội nghị chuyên về mật khẩu, mã PIN, và xác thực số, ra mắt lần đầu tại Bergen, Na-uy năm 2010 và được tổ chức thường niên.

Cuối cùng là khóa sinh trắc học. Apple, Samsung, và các nhà sản xuất lớn khác hiện cho phép khách hàng sử dụng ứng dụng quét vân tay để mở khóa điện thoại. Nhưng xin lưu ý, những ứng dụng này cũng không phải là không thể phá vỡ. Sau khi Touch ID ra mắt, các nhà nghiên cứu – có lẽ đang kỳ vọng rằng Apple sẽ có

nhiều cải thiện so với các ứng dụng quét vân tay đang có mặt trên thị trường – ngạc nhiên khi thấy rằng vẫn có thể áp dụng một số phương pháp tấn công ứng dụng quét vân tay cũ trên iPhone, chẳng hạn như dùng phấn rôm trẻ em và băng dính trong để lấy dấu vân tay.

Các điện thoại khác sử dụng camera tích hợp để nhận diện khuôn mặt của chủ sở hữu. Nhưng cách làm này cũng có thể bị phá giải bằng cách đặt một bức ảnh có độ phân giải cao của chủ sở hữu trước màn hình camera.

Nhìn chung, bản thân các phương pháp sinh trắc học cũng dễ bị tấn công. Lý tưởng nhất, nên sử dụng sinh trắc học làm một yếu tố xác thực. Vuốt ngón tay hoặc cười trước camera, sau đó nhập mã PIN hoặc passcode. Điều đó sẽ giữ an toàn cho thiết bị di động của bạn.

Điều gì sẽ xảy ra nếu bạn tạo được một mật khẩu mạnh nhưng không viết ra để ghi nhớ? Đặt lại mật khẩu sẽ là một tính năng hữu ích khi bạn không thể truy cập vào một tài khoản không sử dụng thường xuyên. Nhưng đó cũng có thể là một miếng mồi dễ ăn cho những kẻ tấn công. Sử dụng manh mối mà chúng ta rải khắp Internet, như thông tin hồ sơ cá nhân trên mạng xã hội, hacker có thể truy cập vào email cũng như các dịch vụ khác của chúng ta chỉ bằng cách đặt lại mật khẩu.

Trong một cuộc tấn công đã được báo chí đưa tin, hacker lấy bốn chữ số cuối cùng trong số thẻ tín dụng của mục tiêu, sau đó dùng chúng làm bằng chứng nhận dạng khi gọi điện cho một nhà cung cấp dịch vụ và yêu cầu thay đổi địa chỉ email. Bằng cách đó, kẻ tấn công có thể tự ý đặt lại mật khẩu mà chủ sở hữu hợp pháp không biết.

Quay trở lại năm 2008, David Kernell, một sinh viên tại Đại học Tennessee, đã thử tìm cách truy cập tài khoản email Yahoo cá nhân của ứng cử viên phó tổng thống Mỹ khi đó là Sarah Palin. Kernell có thể sử dụng cách đoán mật khẩu, nhưng quyền truy cập tài khoản sẽ bị khóa sau vài lần thử không thành công. Thay

vào đó, sinh viên này sử dụng chức năng đặt lại mật khẩu mà theo nhận định sau này của anh là "dễ dàng."

Tôi chắc rằng chúng ta ai cũng từng nhận được email lạ từ bạn bè và đồng nghiệp, trong đó chứa đường dẫn liên kết tới các website khiêu dâm ở nước ngoài, và về sau mới biết được rằng tài khoản email của họ đã bị chiếm đoạt. Email bị chiếm đoạt thường là do mật khẩu bảo vệ tài khoản không mạnh. Hoặc có người đã biết được mật khẩu – thông qua một cuộc xâm phạm dữ liệu – hoặc kẻ tấn công sử dụng chức năng đặt lại mật khẩu.

Khi thiết lập tài khoản lần đầu tiên, chẳng hạn tài khoản email hay tài khoản ngân hàng, có thể bạn sẽ được hỏi những thông tin gọi là câu hỏi bảo mật, thường là ba câu. Hầu hết sẽ có trình đơn (menu) liệt kê các câu hỏi gợi ý để bạn chọn. Các câu hỏi này thường rất rõ ràng.

Bạn sinh ra ở đâu? Bạn học cấp ba ở đâu? Hay đại học? Và tên thời con gái của mẹ bạn – câu này đã được dùng làm câu hỏi bảo mật từ ít nhất là năm 1882. Như tôi sẽ trình bày dưới đây, các công ty có thể và trên thực tế có thực hiện việc quét Internet để thu thập thông tin cá nhân, khiến việc trả lời những câu hỏi bảo mật cơ bản này trở nên hết sức đơn giản. Một người có thể dành ra vài phút trên Internet là đã có thể trả lời tất cả các câu hỏi bảo mật của một cá nhân.

Mãi đến gần đây, các câu hỏi bảo mật này mới được cải thiện phần nào. Ví dụ, "Anh rể của bạn sinh ra ở bang nào?" là một câu hỏi tương đối rõ ràng, song việc trả lời chính xác những câu hỏi "tốt" này cũng có những rủi ro riêng (tôi sẽ nói kỹ hơn ở ngay sau đây). Nhưng nhiều câu được gọi là câu hỏi bảo mật vẫn còn quá dễ dàng, chẳng hạn như, "Quê của bố bạn ở đâu?"

Nhìn chung, khi đặt câu hỏi bảo mật, hãy tránh sử dụng các gợi ý rõ ràng có sẵn trong trình đơn. Ngay cả khi website chỉ bao gồm các câu hỏi bảo mật cơ bản, hãy sáng tạo. Không ai bắt bạn phải trả lời đúng câu hỏi cả. Bạn có thể tha hồ phát huy sự láu lỉnh của mình. Ví dụ, với câu hỏi, "Màu sắc ưa thích của bạn là gì?" bạn có

thể trả lời là kẹo trái cây. Ai mà đoán được chứ. Nội dung mà bạn đưa ra làm câu trả lời sẽ trở thành câu trả lời "chính xác" cho câu hỏi bảo mật đó.

Khi cung cấp các câu trả lời sáng tạo, hãy nhớ ghi lại cả câu hỏi và câu trả lời rồi cất chúng ở một nơi an toàn (hoặc lưu trong phần mềm quản lý mật khẩu). Sau này, biết đâu có lúc bạn lại cần đến dịch vụ hỗ trợ kỹ thuật, và họ hỏi bạn những câu hỏi bảo mật. Hãy ghi vào một cuốn sổ tay hoặc một tờ giấy rồi cất trong ví (hoặc học thuộc lòng và sử dụng nhất quán một bộ câu trả lời) để giúp bạn nhớ rằng, ví dụ, với câu "Bạn sinh ra ở đâu?" thì câu trả lời là "Trong bệnh viện." Sự mập mờ đơn giản này phần nào có thể ngăn chặn trường hợp một ai đó tìm hiểu về bạn trên Internet và thử một câu trả lời hợp lý hơn, chẳng hạn, "Columbus, Ohio."

Việc trả lời trung thực các câu hỏi bảo mật còn mang lại những rủi ro khác về sự riêng tư: Bạn cung cấp nhiều thông tin cá nhân hơn so với những gì đã có trên mạng. Ví dụ, câu trả lời trung thực cho câu hỏi "Anh rể của bạn sinh ra ở bang nào?" có thể sẽ bị website mà bạn cung cấp câu trả lời này bán lại cho một bên thứ ba, và có thể được dùng kết hợp với các thông tin khác hay để điền thông tin còn thiếu. Ví dụ, từ câu trả lời về người anh rể, một người có thể suy luận ra rằng bạn đã hoặc đang có gia đình, và rằng vợ/chồng (hoặc vợ/chồng cũ) của bạn có anh em trai, hoặc kết hôn với một người đàn ông sinh ra ở tiểu bang mà bạn cung cấp. Đó là một lượng lớn thông tin bổ sung rút ra từ một câu trả lời đơn giản. Ngược lại, nếu bạn không có anh rể, cứ mạnh dạn trả lời câu hỏi này một cách sáng tạo, ví dụ viết "Puerto Rico." Điều đó sẽ khiến cho những kẻ muốn tìm hiểu về bạn phải bối rối. Càng cung cấp nhiều thông tin đánh lạc hướng, bạn càng trở nên vô hình trên mạng.

Khi trả lời những câu hỏi tương đối không phổ biến này, hãy cân nhắc đến giá trị của website đối với bạn. Ví dụ, bạn có thể tin tưởng cung cấp cho ngân hàng của mình các thông tin cá nhân bổ sung này, nhưng với dịch vụ phát video trực tuyến thì không. Đồng thời, hãy tìm hiểu về chính sách bảo mật của website đó,

lưu ý đến những đoạn nói hoặc ngụ ý nói rằng họ có thể bán thông tin họ thu thập được cho các bên thứ ba.

Để đặt lại mật khẩu cho tài khoản email Yahoo của Sarah Palin, cần phải cung cấp thông tin về ngày sinh, mã bưu chính, và câu trả lời cho câu hỏi bảo mật "Bạn gặp chồng mình ở đâu?" Có thể dễ dàng tìm thấy ngày sinh và mã bưu chính của Palin trên mạng (vào thời điểm đó, bà đang là Thống đốc bang Alaska). Câu hỏi bảo mật đòi hỏi nhiều công sức hơn một chút, nhưng Kernell cũng có thể tìm ra được. Trong các cuộc phỏng vấn, Palin đã nhiều lần nói rằng chồng bà chính là người yêu từ thời trung học. Và hóa ra đó cũng là câu trả lời chính xác cho câu hỏi bảo mật của bà: "Trường trung học."

Bằng cách đoán câu trả lời cho câu hỏi bảo mật của Palin, Kernell đã đặt lại mật khẩu email Yahoo của bà, nhờ vậy anh ta có thể đọc tất cả các email cá nhân trong đó. Ảnh chụp màn hình hộp thư đến của Palin được đăng lên một website dành cho hacker. Bản thân Palin cũng bị khóa khỏi email cho đến khi bà đặt lại mật khẩu.

Hành vi của Kernell là bất hợp pháp vì vi phạm Đạo luật Gian lận và Lạm dụng Máy tính. Cụ thể, anh ta bị kết án vì hai tội: cản trở pháp luật bằng cách phá hủy hồ sơ (trọng tội), và giành quyền truy cập trái phép vào máy tính (tội nhẹ). Năm 2010, anh ta bị kết án một năm và một ngày tù, cộng với ba năm quản thúc.

Nếu tài khoản email của bạn bị chiếm đoạt, như trường hợp của Palin, trước tiên bạn phải thay đổi mật khẩu bằng cách sử dụng tùy chọn đặt lại mật khẩu (vâng, giải pháp dễ đoán, đúng không?). Hãy đặt mật khẩu mới mạnh hơn như tôi đã hướng dẫn ở trên. Thứ hai, hãy kiểm tra mục Thư đã gửi để xem những nội dung nào đã được gửi đi bằng tên của bạn. Có thể bạn sẽ phát hiện ra rằng một thư rác đã được gửi tới nhiều bên, thậm chí là gửi cho toàn bộ danh sách liên hệ của bạn. Bây giờ thì bạn đã biết lý do tại sao bao nhiêu năm qua, bạn bè của bạn cứ gửi thư rác cho bạn rồi chứ? Có người đã tấn công tài khoản email của họ đấy.

Ngoài ra, hãy kiểm tra xem liệu có ai đã tự thêm họ vào tài khoản của bạn hay không. Ở phần trước, chúng ta đã nói về việc chuyển tiếp thư liên quan đến nhiều tài khoản email. Kẻ tấn công giành được quyền truy cập vào dịch vụ email của bạn cũng có thể cài đặt chế độ chuyển tiếp tất cả email của bạn tới tài khoản của hắn. Bạn vẫn sẽ nhận email như bình thường, nhưng kẻ tấn công cũng sẽ đọc được chúng. Nếu có kẻ đã tự thêm hắn vào tài khoản của bạn, hãy xóa địa chỉ email chuyển tiếp này ngay lập tức.

Mật khẩu và mã PIN là một phần của giải pháp bảo mật, nhưng chúng ta vừa thấy rằng hai yếu tố này là có thể đoán được. Ngoài việc đặt mật khẩu phức tạp, còn có một cách tốt hơn nữa là xác thực hai yếu tố. Trước vụ việc ảnh khỏa thân của Jennifer Lawrence và những người nổi tiếng khác bị phát tán trên Internet, Apple đã thiết lập cơ chế xác thực hai yếu tố, hay còn gọi là 2FA (two-factor authentication), cho các dịch vụ iCloud của mình.

2FA là gì?

Trong quá trình xác thực người dùng, các website hoặc ứng dụng sẽ xét đến ít nhất hai trong số ba yếu tố, thông thường là: một thứ mà bạn có, một thứ mà bạn biết, và một thứ là bạn. Một thứ mà bạn có có thể là thẻ tín dụng/thẻ ghi nợ gắn chip hay có dải từ tính. Một thứ mà bạn biết thường là mã PIN hoặc câu trả lời cho câu hỏi bảo mật. Và một thứ là bạn bao gồm các thông số sinh trắc học như vân tay, nhận dạng khuôn mặt, nhận dạng giọng nói… Càng có nhiều thông tin này, bạn càng có thể chắc chắn rằng người dùng chính là người mà họ đã tự nhận.

Nghe có vẻ đây là công nghệ mới, nhưng không phải. Trong hơn 40 năm qua, hầu hết chúng ta đều đã thực hiện 2FA mà không nhận ra điều đó.

Khi sử dụng máy ATM, tức là bạn đang thực hiện 2FA đấy. Làm sao lại có thể như vậy? Bạn có một chiếc thẻ do ngân hàng phát hành (thứ mà bạn có) và một mã PIN (thứ mà bạn biết). Khi kết hợp chúng lại với nhau, máy ATM không người điều khiển trên

đường phố sẽ biết rằng bạn đang muốn truy cập vào tài khoản ghi trên thẻ. Một số quốc gia áp dụng thêm các phương tiện xác thực khác tại các máy ATM, chẳng hạn như nhận diện khuôn mặt và in lòng bàn tay. Đây gọi là xác thực đa yếu tố (multifactor authentication – MIF).

Có thể áp dụng các phương pháp tương tự trên môi trường trực tuyến. Nhiều tổ chức tài chính và chăm sóc sức khỏe, cũng như các tài khoản email thương mại và tài khoản mạng xã hội cho phép bạn chọn 2FA. Trong trường hợp này, thứ mà bạn biết là mật khẩu của bạn, và thứ mà bạn có là điện thoại di động. Việc sử dụng điện thoại để truy cập vào các website này được coi là "ngoài dải" vì điện thoại không kết nối với máy tính mà bạn đang sử dụng. Nhưng nếu bạn sử dụng tính năng 2FA, kẻ tấn công sẽ không thể truy cập các tài khoản được bảo vệ bằng 2FA nếu không có thiết bị di động của bạn trong tay.

Lấy Gmail làm ví dụ. Để kích hoạt tính năng 2FA, bạn cần nhập số điện thoại di động của mình vào website Gmail. Sau đó, để xác minh danh tính, Google sẽ gửi đến điện thoại của bạn một tin nhắn chứa mã gồm sáu chữ số. Tiếp theo, bạn xác minh rằng máy tính này và số điện thoại kia là có kết nối với nhau bằng cách nhập mã đó vào website Gmail.

Về sau, khi có người muốn thay đổi mật khẩu trên tài khoản của bạn từ một máy tính hoặc thiết bị mới, Google sẽ gửi tin nhắn đến điện thoại của bạn. Sau khi mã xác minh chính xác được nhập vào website thì các thay đổi đối với tài khoản của bạn mới được thực hiện.

Tuy nhiên, ở đây có một vấn đề. Theo các nhà nghiên cứu tại Symantec, khi gửi tin nhắn để xác nhận danh tính, nếu bạn không để ý, một người nào đó tình cờ biết được số điện thoại di động của bạn sẽ có thể thực hiện tấn công social engineering[17] và đánh cắp mã đặt lại mật khẩu được bảo vệ bằng 2FA.

[17] Social Engineering (tấn công phi kỹ thuật): Trong lĩnh vực an

ninh thông tin, tấn công social engineering chỉ việc thao túng người khác bằng tâm lý học để khiến họ thực hiện các hành động hoặc tiết lộ các thông tin bí mật.

Giả sử tôi muốn chiếm tài khoản email nhưng không biết mật khẩu của bạn. Tôi biết số điện thoại di động của bạn vì thông tin về bạn rất dễ tìm thấy trên Google. Tôi có thể vào trang cài đặt lại cho dịch vụ email của bạn và yêu cầu đặt lại mật khẩu. Do bạn đã bật tính năng xác thực hai yếu tố, nên dịch vụ này sẽ gửi tới điện thoại của bạn một tin nhắn chứa mã xác thực. Tới đây thì mọi chuyện vẫn ổn đúng không? Chờ đã.

Vụ tấn công điện thoại của nhà hoạt động chính trị DeRay Mckesson gần đây cho thấy kẻ xấu có thể đánh lừa nhà cung cấp dịch vụ di động để thực hiện đổi SIM như thế nào. Nói cách khác, kẻ tấn công có thể giành quyền kiểm soát dịch vụ di động của bạn và nhận các tin nhắn gửi tới bạn – chẳng hạn như tin nhắn chứa mã xác thực từ Google gửi đến để đặt lại tài khoản Gmail đã được bảo vệ bằng 2FA. Điều này dễ thực hiện hơn là lừa một người đọc to tin nhắn chứa mật khẩu mới của họ – nhưng cách này vẫn khả thi, và đòi hỏi kỹ thuật tấn công social engineering.

Do không đọc được mã xác minh mà nhà cung cấp dịch vụ email gửi đến điện thoại của bạn, nên tôi sẽ phải giả vờ là một người khác để lấy được nó từ tay bạn. Chỉ vài giây trước khi bạn nhận được tin nhắn thực sự từ nhà cung cấp email, chẳng hạn Google, tôi có thể gửi tin nhắn cho bạn với nội dung: “Google vừa phát hiện có hoạt động bất thường trên tài khoản của bạn. Vui lòng gửi lại mã đã được gửi tới thiết bị di động của bạn để ngăn chặn hoạt động trái phép”.

Bạn sẽ thấy rằng quả nhiên, bạn vừa mới nhận được một tin nhắn từ Google trong đó có chứa một mã xác minh hợp lệ, và nếu mất cảnh giác, bạn có thể vô tư gửi nó cho tôi. Khi đó, tôi sẽ có dưới 60 giây để nhập mã này và truy cập vào trang đặt lại mật khẩu rồi chiếm tài khoản email của bạn. Hoặc bất kỳ tài khoản nào khác.

Vì mã xác thực cung cấp trong tin nhắn không được mã hóa và có

thể chiếm đoạt theo cách tôi vừa mô tả, nên để thực hiện 2FA an toàn hơn, hãy tải xuống ứng dụng Google Authenticator từ Google Play hoặc cửa hàng ứng dụng iTunes nếu là iPhone. Ứng dụng này sẽ tạo một mã truy cập duy nhất gồm 6 chữ số trên chính nó mỗi lần bạn muốn truy cập một website yêu cầu 2FA – vì vậy không cần phải gửi tin nhắn nào cả. Mã do ứng dụng tạo ra này được đồng bộ hóa với cơ chế xác thực để cấp quyền truy cập của website. Tuy nhiên, Google Authenticator lưu trữ hạt giống mật khẩu một lần của bạn trong Keychain[18] của Apple với phần cài đặt cho "Chỉ riêng thiết bị này." Điều đó có nghĩa là nếu bạn sao lưu dữ liệu iPhone và khôi phục chúng sang một thiết bị khác (vì bạn nâng cấp hoặc thay thế một điện thoại bị mất), các mã Google Authenticator sẽ không được di chuyển, và việc đặt lại các mã đó là cả một rắc rối lớn. Hãy in ra giấy các mã khẩn cấp để đề phòng trường hợp bạn phải thay đổi thiết bị. Các ứng dụng khác như 1Password cho phép bạn sao lưu và khôi phục các hạt giống mật khẩu một lần để tránh cho bạn rắc rối này.

[18] Từ iOS 7.0.3 và OS X 10.9, Apple có một tính năng mới là iCloud Keychain (chùm chìa khóa iCloud). Nó có nhiệm vụ đồng bộ hóa các thông tin về tên đăng nhập, mật khẩu website, thông tin thẻ tín dụng và một số thông tin khác giữa các thiết bị iOS với máy tính Mac, nhờ đó người dùng sẽ không phải tốn thời gian nhập liệu thủ công.

Sau khi đã đăng ký một thiết bị, nếu vẫn tiếp tục đăng nhập vào website trên từ thiết bị đó, bạn sẽ phải tích chọn ô tin tưởng vào thiết bị này trong 30 ngày (nếu có), nếu không bạn vẫn sẽ bị hỏi mã truy cập mới. Tuy nhiên, nếu bạn sử dụng một thiết bị khác – giả sử bạn mượn máy tính của vợ/chồng mình – thì khi đó bạn sẽ được yêu cầu xác thực bổ sung. Không cần phải nói, nếu bạn sử dụng 2FA, hãy luôn mang theo điện thoại di động bên mình.

Với tất cả những biện pháp phòng xa này, có thể bạn sẽ thắc mắc không biết tôi có lời khuyên gì dành cho những người thực hiện các giao dịch tài chính trực tuyến.

Với chi phí khoảng 100 đô-la/năm, bạn có thể sử dụng dịch vụ bảo vệ tường lửa và chống virus cho ba máy tính. Vấn đề nằm ở chỗ, khi lướt web, bạn có thể tải vào trình duyệt của mình một biểu ngữ quảng cáo chứa phần mềm độc hại. Hoặc có thể bạn mở một email chứa phần mềm độc hại. Nếu máy tính của bạn thường xuyên tiếp xúc với Internet, thì bằng cách này hay cách khác, kiểu gì nó cũng sẽ bị nhiễm độc, và sản phẩm chống virus của bạn có thể không ngăn chặn được tất cả.

Vì vậy, tôi khuyên bạn nên bỏ ra khoảng 200 đô-la để mua Chromebook[19]. Tôi thích iPad, nhưng chúng đắt quá. Chromebook gần giống với một chiếc máy tính bảng dễ sử dụng như iPad, nhưng có giá rẻ hơn nhiều.

[19] Chromebook: Một loại máy tính xách tay hoặc máy tính bảng sử dụng hệ điều hành là Chrome OS dựa trên Linux. Thiết bị này chủ yếu được dùng để thực hiện các tác vụ trên trình duyệt Google Chrome, trong đó phần lớn các ứng dụng và dữ liệu được lưu trên đám mây thay vì lưu trong máy. Các thiết bị Chromebook ra mắt từ cuối năm 2017 cũng có thể chạy các ứng dụng Android.

Quan điểm của tôi là, bạn cần phải có một thiết bị phụ để dùng riêng cho các hoạt động liên quan đến tài chính, có thể là cả các hoạt động liên quan đến y tế nữa. Để cài đặt bất kỳ ứng dụng nào, trước tiên bạn phải đăng ký bằng tài khoản Gmail – điều này sẽ giúp bạn hạn chế mở trình duyệt để lướt Internet.

Sau đó, bạn hãy kích hoạt 2FA trên website để nó nhận ra Chromebook. Sau khi thực hiện xong các hoạt động liên quan đến ngân hàng hoặc y tế, hãy cất Chromebook đi một chỗ để chờ tới lần sử dụng tiếp theo, khi bạn cần phải cân đối sổ sách hay thu xếp một cuộc hẹn với bác sĩ.

Cách này có vẻ phiền hà. Đúng là như vậy. Bạn sẽ không còn được hưởng cái tiện lợi của việc có thể giao dịch với ngân hàng vào bất kỳ lúc nào. Nhưng kết quả mà nó mang lại là giảm thiểu khả năng kẻ xấu sục sạo các thông tin về ngân hàng và tín dụng của bạn.

Nếu bạn chỉ cài đặt và sử dụng hai hoặc ba ứng dụng cho Chromebook, và nếu bạn đánh dấu website ngân hàng hoặc website y tế mà không truy cập vào các website khác, thì khả năng thiết bị của bạn bị nhiễm Trojan hoặc các phần mềm độc hại khác là rất thấp.

Như vậy, chúng ta vừa thống nhất với nhau rằng cần phải tạo các mật khẩu mạnh và không được chia sẻ chúng, và rằng cần phải kích hoạt 2FA bất cứ khi nào có thể. Trong các chương tiếp theo, chúng ta sẽ cùng xem các hoạt động tương tác phổ biến hằng ngày có thể để lại dấu vân tay số ở mọi nơi như thế nào, và bạn có thể làm gì để bảo vệ sự riêng tư của mình.

Chương 2: CÒN AI KHÁC ĐANG ĐỌC EMAIL CỦA BẠN?

Nếu bạn giống tôi, thì một trong những việc đầu tiên bạn làm vào buổi sáng là kiểm tra email. Và, nếu bạn giống tôi, thì hẳn bạn cũng thắc mắc không biết còn ai khác đọc được email của mình nữa không. Đó không phải là một sự lo lắng thiếu cơ sở đâu. Nếu bạn sử dụng dịch vụ email trên nền web[20] như Gmail hoặc Outlook 365, thì câu trả lời đã rõ ràng và rất đáng sợ đấy.

[20] Email trên nền web (hay webmail): Hệ thống email trong đó người dùng có thể truy cập email qua trình duyệt trên bất kỳ máy tính hay thiết bị nào có kết nối Internet.

Dù bạn xóa email ngay sau khi đọc, việc đó cũng không nhất thiết có nghĩa là nội dung email đã bị xóa hẳn. Vẫn còn một bản sao của nó ở đâu đó. Webmail hoạt động dựa trên công nghệ đám mây, do đó, để bạn có thể truy cập email từ bất cứ thiết bị nào, ở bất cứ đâu, vào bất cứ lúc nào, chắc chắn phải có vô số bản sao dự phòng. Ví dụ, nếu bạn sử dụng Gmail, từng email được gửi và nhận qua tài khoản Gmail của bạn đều được lưu trữ bản sao trong nhiều máy chủ khác nhau của Google trên toàn thế giới. Điều này cũng đúng nếu bạn sử dụng các hệ thống email của Yahoo, Apple, AT&T, Comcast, Microsoft, hoặc thậm chí là của tổ chức nơi bạn làm việc. Công ty chủ quản có thể kiểm tra bất cứ email nào mà bạn gửi đi vào bất cứ lúc nào. Trên lý thuyết, việc này là để lọc các phần mềm độc hại, nhưng thực tế là các bên thứ ba có thể và thực sự đang truy cập email của chúng ta vì nhiều lý do khác, với dụng ý xấu và mang tính tư lợi hơn.

Về nguyên tắc, hầu hết chúng ta sẽ không đời nào cho phép bất cứ ai khác đọc được thư của mình, ngoại trừ người mà chúng ta gửi thư đến. Đã có các quy định pháp lý nhằm bảo vệ thư từ được gửi qua Dịch vụ Bưu chính ở Mỹ và các quy định nhằm bảo vệ những nội dung được lưu trữ như email. Tuy nhiên, trong thực tế, chúng ta thường biết và có lẽ đã chấp nhận rằng tồn tại một sự

thỏa hiệp nhất định nào đó liên quan đến sự thuận tiện trong giao tiếp mà email mang lại. Chúng ta biết rằng Yahoo (cùng với rất nhiều công ty khác) cung cấp dịch vụ webmail miễn phí, và chúng ta biết rằng phần lớn nguồn thu nhập của Yahoo là đến từ quảng cáo. Nhưng có lẽ chúng ta chưa biết hai chuyện trên liên hệ với nhau thế nào, và điều đó có thể ảnh hưởng ra sao đến sự riêng tư của mình.

Một ngày nọ, Stuart Diamond, một cư dân sống ở Bắc California, đã nhận ra điều đó. Anh để ý thấy rằng các quảng cáo mà anh nhìn thấy ở góc trên bên phải của email Yahoo không hiện ra ngẫu nhiên mà được dựa theo nội dung các email ra vào hòm thư của anh. Ví dụ, nếu trong một email tôi nhắc đến chuyến đi diễn thuyết sắp tới ở Dubai, thì những quảng cáo xuất hiện trong tài khoản email của tôi có thể sẽ liên quan đến các hãng hàng không, khách sạn, và những việc cần làm khi ở các Tiểu vương quốc Ả-rập Thống nhất.

Hành vi này thường được nêu ra một cách cẩn thận trong các điều khoản dịch vụ mà hầu hết chúng ta đều nhấn nút đồng ý nhưng có lẽ chưa một lần đọc qua. Không ai muốn xem những quảng cáo không liên quan gì tới sở thích cá nhân của mình, phải vậy không nào? Và miễn là email di chuyển giữa các chủ tài khoản Yahoo, thì việc công ty đó có thể quét nội dung email để tìm quảng cáo phù hợp cho chúng ta, và biết đâu chặn được phần mềm độc hại hay thư rác, cũng là điều hợp lý kia mà.

Tuy nhiên, Diamond, cùng với David Sutton, cũng đến từ Bắc California, bắt đầu nhận ra rằng nội dung các email được gửi và nhận qua các địa chỉ bên ngoài Yahoo cũng ảnh hưởng đến nội dung quảng cáo dành cho họ. Điều đó cho thấy công ty này đã chặn và đọc tất cả các email của họ, chứ không chỉ riêng những email ra vào qua các máy chủ Yahoo.

Dựa trên những gì quan sát được, năm 2012, hai người đã gửi đơn kiện tập thể thay mặt cho 275 triệu chủ tài khoản của Yahoo, trong đó nêu lên những mối lo ngại xung quanh hoạt động tương đương với hành vi nghe trộm bất hợp pháp của công ty này.

Sự kiện này có giúp chấm dứt hoạt động quét email không? Không hề.

Trong các vụ kiện tập thể, thường có một khoảng thời gian để cả hai bên liên quan tìm hiểu và phản hồi thông tin cho nhau. Trong trường hợp trên, giai đoạn ban đầu này kéo dài gần ba năm. Tháng Sáu năm 2015, một thẩm phán ở San Jose, California, ra phán quyết rằng Diamond và Sutton có đủ cơ sở để tiếp tục theo đuổi vụ kiện, và rằng theo Đạo luật Lưu trữ Thông tin Liên lạc, những người đã gửi hoặc nhận email qua Yahoo từ ngày 2 tháng Mười năm 2011, thời điểm Diamond và Sutton lần đầu đệ đơn khiếu kiện, có thể tham gia vào vụ kiện này. Ngoài ra, các chủ tài khoản email không thuộc hệ thống Yahoo sống tại California cũng có thể đệ đơn kiện chiểu theo Đạo luật Xâm phạm Quyền riêng tư của bang này. Cho tới nay, vụ việc này vẫn đang chờ xử lý.

Trong quá trình biện hộ trước một vụ kiện khác vào đầu năm 2014 cũng liên quan đến hoạt động quét email, Google đã vô tình công bố thông tin về quy trình quét email của họ trong một phiên điều trần trước tòa, sau đó vội vàng tìm cách chỉnh sửa hoặc gỡ bỏ thông tin trên nhưng không thành công. Vụ kiện này liên quan đến nghi vấn Google đã quét hoặc đọc chính xác những gì. Theo các nguyên đơn, trong đó có một số hãng truyền thông lớn, bao gồm cả các chủ sở hữu của tạp chíUSA Today, Google nhận ra rằng nếu chỉ quét nội dung của hộp thư đến, họ sẽ bỏ qua rất nhiều nội dung có thể là hữu ích khác. Vụ kiện này cho rằng Google đã chuyển từ chỉ quét email được lưu trữ và nằm trên máy chủ Google sang quét tất cả các email vẫn đang trong quá trình di chuyển, bất kể email đó được gửi đi từ iPhone hay máy tính xách tay, khi người dùng còn ngồi trong quán cà phê.

Đôi khi các công ty thậm chí còn tìm cách quét lén email vì mục đích riêng. Một ví dụ nổi tiếng là Microsoft. Hãng này đã vấp phải phản ứng dữ dội khi tiết lộ rằng họ đã quét hộp thư đến của một người dùng Hotmail bị nghi ngờ sao chép trái phép một phần mềm của Microsoft. Sau vụ việc này, Microsoft tuyên bố trong

tương lai họ sẽ để cho các cơ quan thực thi pháp luật xử lý những cuộc điều tra tương tự.

Nhưng hành vi này không chỉ giới hạn ở phạm vi email cá nhân. Nếu bạn gửi email qua mạng công ty, thì bộ phận IT[21] trong công ty cũng có thể quét và lưu trữ nội dung liên lạc của bạn. Đội IT có quyền quyết định cho phép các email đi qua máy chủ và mạng của công ty hay báo cho cơ quan thực thi pháp luật. Điều này bao gồm các email chứa bí mật thương mại hoặc các tài liệu có vấn đề, chẳng hạn như chứa nội dung khiêu dâm. Họ cũng thực hiện quét email để tìm phần mềm độc hại. Nếu đội IT thực hiện quét và lưu trữ email của bạn, họ cần phải nêu rõ chính sách của mình mỗi khi bạn đăng nhập – nhưng hầu hết các công ty đều không làm điều đó.

[21] IT (information technology): Công nghệ thông tin.

Tuy hầu hết chúng ta đều có thể chấp nhận được việc email của mình bị quét để tìm kiếm phần mềm độc hại, và có lẽ một số người cũng có thể nhắm mắt bỏ qua việc quét email vì mục đích quảng cáo, nhưng việc các bên thứ ba đọc email của chúng ta rồi đưa ra hành động dựa theo đó là hết sức đáng lo ngại. (Tất nhiên, ngoại trừ vấn đề liên quan đến các nội dung ấu dâm).

Vì vậy, hễ khi nào bạn viết email, dù nội dung không mấy quan trọng, và kể cả khi bạn đã xóa nó khỏi hộp thư đến, hãy nhớ rằng rất có thể một bản sao của những câu chữ và hình ảnh trong đó sẽ bị quét và tồn tại trong một thời gian dài. (Một số công ty có thể có chính sách lưu trữ ngắn, nhưng đa phần đều giữ email trong một thời gian dài).

Như vậy, bạn đã biết chính phủ và các công ty đều đọc email của mình, và việc tối thiểu mà bạn có thể làm là khiến cho việc đó trở nên khó khăn hơn rất nhiều.

Hầu hết các dịch vụ email trên nền web đều sử dụng mã hóa trong lúc email trên đường lưu chuyển. Tuy nhiên, khi chuyển email qua lại giữa các chương trình chuyển thư (Mail Transfer Agent – MTA), một số dịch vụ có thể không sử dụng mã hóa,

khiến email của bạn bị sơ hở. Ví dụ, trong môi trường làm việc, người lãnh đạo có thể truy cập được vào hệ thống email của công ty. Để ẩn mình, bạn phải mã hóa được các email – nghĩa là khóa chúng lại sao cho chỉ những người nhận mới có thể mở khóa để đọc. Mã hóa là gì? Đó là một mật mã.

Lấy ví dụ rất đơn giản là mật mã Caesar. Phương pháp này thay thế mỗi chữ cái bằng một chữ cái khác cách nó một khoảng cách nhất định trong bảng chữ cái. Chẳng hạn, nếu khoảng cách ấn định là 2, thì khi sử dụng phương pháp Caesar, a sẽ trở thành c, c sẽ trở thành e, z sẽ trở thành b, và cứ thế đến hết. Với cơ chế mã hóa bù trừ 2 đơn vị, “Kevin Mitnick” sẽ trở thành “Mgxkp Okvpkem.”

Tất nhiên, hầu hết các hệ thống mã hóa được sử dụng ngày nay đều mạnh hơn nhiều so với mật mã Caesar cơ bản. Do vậy, việc phá mã sẽ khó khăn hơn rất nhiều. Nhưng mọi dạng mã hóa đều cần đến chìa khóa, đóng vai trò là mật khẩu để khóa và mở thông điệp mã hóa. Mã hóa đối xứng có nghĩa là cùng một chìa khóa được dùng để khóa và mở thông điệp mã hóa. Tuy nhiên, khó có thể chia sẻ các khóa đối xứng, khi hai bên không biết nhau hoặc cách xa nhau về mặt địa lý, vì cả hai đều ở trên Internet.

Trên thực tế, việc mã hóa email chủ yếu sử dụng kỹ thuật mã hóa bất đối xứng. Điều đó có nghĩa là tôi tạo ra hai khóa: một khóa bí mật được lưu trong thiết bị của tôi và tôi không bao giờ chia sẻ nó với ai, và một khóa công khai mà tôi có thể đăng tải tự do trên Internet. Hai khóa khác nhau nhưng lại có mối liên hệ với nhau về mặt toán học.

Ví dụ: Bob muốn gửi cho Alice một email an toàn. Anh lên mạng tìm kiếm khóa công khai của Alice hoặc trực tiếp hỏi cô, và khi gửi email cho Alice, anh mã hóa nó bằng khóa của cô. Email này sẽ vẫn ở trạng thái mã hóa cho đến khi Alice – và chỉ riêng Alice – sử dụng cụm mật khẩu để mở khóa bí mật của mình và mở email được mã hóa.

Vậy việc mã hóa nội dung email được thực hiện như thế nào?

Phương pháp mã hóa email phổ biến nhất là PGP (Pretty Good Privacy). Phần mềm này không miễn phí mà là một sản phẩm của công ty Symantec. Nhưng người tạo ra nó, Phil Zimmermann, còn phát triển phiên bản nguồn mở miễn phí của nó là OpenPGP. Và lựa chọn thứ ba, GPG (GNU Privacy Guard), do Werner Koch tạo ra, cũng là phần mềm miễn phí. Tin vui là cả ba đều tương thích với nhau, tức là bất kể bạn sử dụng phiên bản PGP nào, các chức năng cơ bản đều giống nhau.

Khi quyết định tiết lộ những dữ liệu nhạy cảm lấy được từ NSA, Edward Snowden cần sự hỗ trợ của những người cùng tư tưởng với mình ở khắp nơi trên thế giới. Nghịch lý nằm ở chỗ, anh phải thoát khỏi mạng lưới trong khi vẫn duy trì hoạt động trên Internet, tức là phải trở nên vô hình.

Dù không có bí mật quốc gia nào để chia sẻ, nhưng bạn cũng nên lưu ý giữ gìn sự riêng tư cho các email của mình. Kinh nghiệm của Snowden và những người khác cho thấy đây là việc không dễ làm, nhưng có thể làm được, nếu chúng ta thận trọng một chút.

Snowden liên lạc với người khác bằng tài khoản cá nhân thông qua một công ty có tên là Lavabit. Nhưng email không sử dụng giao thức point-to-point[22] trực tiếp, tức là một email có thể đi qua một số máy chủ trên thế giới trước khi đến hộp thư đến của người nhận. Snowden biết rằng trong cuộc hành trình này, những người chặn được đường đi của email có thể đọc được nội dung mà anh viết trong đó.

[22] Point-to-Point Protocol (PPP – Giao thức điểm-nối-điểm): Một giao thức liên kết dữ liệu được dùng để thiết lập kết nối trực tiếp giữa hai nút mạng.

Vì vậy, anh phải áp dụng một chiến thuật tinh vi để thiết lập một phương tiện giao tiếp thực sự an toàn, ẩn danh, và được mã hóa hoàn toàn với Laura Poitras, nhà làm phim và cũng là người ủng hộ cho quyền riêng tư (gần đây bà mới hoàn thành một bộ phim tài liệu kể về cuộc sống của những người tố giác). Snowden muốn tạo một cuộc trao đổi mã hóa với Poitras, nhưng chỉ ít người biết

khóa công khai của bà. Đến khóa công khai Poitras cũng không thực sự để công khai cho lắm.

Để tìm chìa khóa công khai của Poitras, Snowden phải tiếp cận với một bên thứ ba, Micah Lee thuộc Tổ chức Biên giới Điện tử (Electronic Frontier Foundation), một tổ chức ủng hộ quyền riêng tư trực tuyến. Khóa công khai của Lee đã có sẵn trên mạng, và theo một bài viết trên tạp chí trực tuyến Intercept, anh có khóa công khai của Poitras, nhưng trước tiên anh cần kiểm tra xem liệu bà có cho phép anh chia sẻ nó hay không. Poitras đồng ý.

Tại thời điểm này, cả Lee và Poitras đều không biết ai muốn biết khóa công khai của Poitras; họ chỉ biết rằng có người đang tìm nó. Snowden sử dụng một tài khoản khác để liên lạc, chứ không dùng tài khoản email cá nhân. Nhưng nếu không sử dụng PGP thường xuyên, có thể thi thoảng bạn lại đưa khóa PGP vào các email quan trọng, và đó cũng là chuyện đã xảy ra với Snowden. Anh đã quên đưa khóa công khai của mình vào email để Lee có thể trả lời.

Không có cách nào an toàn để liên lạc với con người bí ẩn này, Lee đành phản hồi bằng email văn bản bình thường, chưa mã hóa, trong đó yêu cầu Snowden cung cấp khóa công khai, và Snowden làm theo yêu cầu đó.

Một lần nữa Lee, một bên thứ ba đáng tin cậy, lại phải can thiệp. Từ kinh nghiệm cá nhân, tôi có thể khẳng định rằng việc xác minh danh tính của người đang có liên lạc bí mật với bạn là hết sức quan trọng, tốt nhất là thông qua một người bạn chung – nhưng nhớ phải kiểm tra kỹ để chắc chắn rằng bạn đang liên lạc với người bạn đó chứ không phải kẻ mạo danh.

Tôi biết điều này là quan trọng do trước đây tôi từng vào vai kẻ mạo danh, trong đó đối tác không nghi ngờ về danh tính thực sự của tôi hoặc khóa công khai mà tôi đã gửi. Lần đó, tôi muốn liên lạc với Neill Clift, một sinh viên sau đại học chuyên ngành hóa hữu cơ tại Đại học Leeds, Anh, đồng thời là chuyên gia tìm kiếm các lỗ hổng an ninh trong hệ điều hành VMS của công ty Digital

Equipment Corporation (DEC). Tôi muốn Clift gửi cho tôi thông tin về tất cả các lỗ hổng an ninh mà anh đã báo cáo cho DEC. Để làm được điều đó, tôi phải làm sao để anh ta nghĩ rằng tôi thực sự làm việc cho DEC.

Đầu tiên, tôi mạo danh một người tên là Dave Hutchins để gửi email cho anh ta. Trước đó, tôi đã mạo danh Derrell Piper thuộc bộ phận kỹ thuật VMS để gọi cho Clift, vì vậy lúc này tôi (trong vai Hutchins) viết trong email rằng Piper muốn trao đổi qua email với Clift về một dự án. Tìm kiếm trong hệ thống email của DEC, tôi biết rằng trước đây Clift và Piper thật đã gửi email cho nhau, nên yêu cầu mới này cũng không có gì lạ lùng cả. Sau đó, tôi gửi một email giả mạo địa chỉ email của Piper.

Để khiến Clift tin tưởng hơn nữa, tôi còn đề nghị anh ta sử dụng mã hóa PGP để một kẻ như Kevin Mitnick không thể đọc được email. Chẳng bao lâu sau, Clift và "Piper" đã trao đổi thông tin về khóa công khai và mã hóa nội dung liên lạc – các nội dung mà tôi, trên cương vị Piper, có thể đọc được. Sai lầm của Clift là không nghi ngờ về danh tính của Piper. Tương tự, khi nhận được một cuộc gọi bất ngờ từ ngân hàng yêu cầu cung cấp số An sinh Xã hội hoặc thông tin về tài khoản của bạn, hãy gác máy và đích thân gọi đến ngân hàng – làm sao mà bạn biết được người vừa chủ động liên hệ với mình là ai chứ.

Do tầm quan trọng của những bí mật mà họ sắp chia sẻ với nhau, Snowden và Poitras không thể sử dụng địa chỉ email thường dùng được. Tại sao vậy? Tài khoản email cá nhân của họ chứa các thông tin đặc thù – chẳng hạn như sở thích, danh sách liên lạc – có thể xác định danh tính của họ. Thay vào đó, Snowden và Poitras quyết định tạo tài khoản email mới.

Vấn đề duy nhất lúc này là làm sao để họ biết địa chỉ email mới của nhau? Nói cách khác, nếu cả hai bên đều hoàn toàn ẩn danh, vậy thì làm thế nào để họ có thể biết ai là ai và ai là người có thể tin tưởng? Chẳng hạn, làm sao Snowden có thể yên tâm loại trừ khả năng NSA hoặc ai đó khác mạo danh tài khoản email mới của Poitras? Khóa công khai rất dài, vì vậy, dù có thể sử dụng đường

dây điện thoại an toàn, bạn cũng không thể nhấc máy lên gọi rồi đọc to từng ký tự của khóa cho phía bên kia chép lại được. Cần phải có một kênh trao đổi email an toàn.

Bằng cách lại nhờ đến Micah Lee một lần nữa, Snowden và Poitras có thể giao phó niềm tin của mình vào một người khi thiết lập tài khoản email mới và ẩn danh. Đầu tiên, Poitras cho Lee biết khóa công khai mới của mình. Nhưng khóa mã hóa PGP tương đối dài (không đến mức vô hạn định như số Pi[23], nhưng dài), và điều gì sẽ xảy ra nếu tài khoản email của Lee cũng đang bị người khác theo dõi? Vì thế, Lee không dùng khóa thực mà dùng từ viết tắt gồm 40 ký tự (hay còn gọi là dấu vân tay) của khóa công khai của Poitras, và anh đăng thông tin này lên Twitter, một website công khai.

[23] Số Pi (giá trị xấp xỉ bằng 3,1415926535897): Một số có độ dài vô hạn.

Đôi khi bạn phải sử dụng cái hữu hình để trở nên vô hình.

Lúc này, Snowden có thể lẳng lặng đọc tweet[24] của Lee và so sánh khóa rút gọn này với thông điệp anh nhận được. Nếu hai dữ liệu không khớp nhau, Snowden sẽ biết rằng không nên tin tưởng vào email đó, vì có thể nội dung email đã bị xâm phạm, hoặc người gửi là NSA.

[24] Tweet: Từ chỉ một bài đăng trên mạng xã hội Twitter.

Trong trường hợp này, hai dữ liệu trên khớp với nhau.

Bây giờ, một số yêu cầu về danh tính trên mạng – và vị trí ngoài đời thực của họ – đã được loại bỏ, Snowden và Poitras đã có thể sẵn sàng cho kênh liên lạc ẩn danh và an toàn qua email. Cuối cùng, Snowden gửi cho Poitras một email mã hóa, trong đó anh chỉ đề tên mình là "Citizenfour[25]." Chữ ký này về sau trở thành tiêu đề cho bộ phim tài liệu nói về chiến dịch bảo vệ quyền riêng tư của bà và giành được giải Oscar.

[25] Citizenfour (công dân 4): Snowden sử dụng số 4 vì trước anh,

đã có ba người tìm cách tiết lộ hoạt động giám sát người dân của NSA. Trong mắt anh, anh là người thứ tư.

Mọi chuyện tưởng chừng như xong xuôi – bây giờ họ đã có thể liên lạc một cách an toàn qua email mã hóa – nhưng không phải vậy. Đó mới chỉ là khởi đầu.

Sau vụ tấn công khủng bố năm 2015 ở Paris, nhiều chính phủ đã tính đến chuyện xây dựng cửa hậu hoặc các phương thức khác giúp người của chính phủ có thể giải mã các email, văn bản, và tin nhắn điện thoại được mã hóa từ những kẻ bị tình nghi là khủng bố nước ngoài. Tất nhiên, điều này sẽ đánh bại mục đích của mã hóa. Nhưng thực ra, các chính phủ không cần phải tận mắt đọc nội dung mã hóa trong email mới biết đích xác bạn đang liên lạc với ai và với tần suất như thế nào – tôi sẽ trình bày điều này ở ngay sau đây.

Như tôi đã nói, mục đích của mã hóa là mã hóa thông điệp của bạn sao cho chỉ người có đúng khóa mới có thể giải mã được. Sức mạnh của phép toán và độ dài của khóa là hai yếu tố quyết định mức độ khó dễ của việc giải mã khi không có khóa.

Các thuật toán mã hóa được sử dụng ngày nay đều là công khai. Đó là điều hợp lý. Hãy cẩn thận với các thuật toán mã hóa độc quyền và không công khai. Các thuật toán công khai đều đã được kiểm định, có nghĩa là nhiều người đã tìm cách phá giải chúng. Khi một thuật toán công khai bị phá giải hoặc trở nên suy yếu, nó sẽ bị gỡ bỏ và các thuật toán mới hơn, mạnh hơn sẽ thế chỗ. Các thuật toán cũ vẫn tồn tại, nhưng không nên tiếp tục sử dụng chúng.

Nhìn chung, các khóa thuộc quyền kiểm soát của bạn, do đó, việc quản lý chúng là rất quan trọng. Nếu bạn tạo một khóa mã hóa, thì bạn – và không ai khác – sẽ có khóa đó lưu trong thiết bị của mình. Nếu bạn cho phép một công ty thực hiện mã hóa trên đám mây, thì sau khi chia sẻ khóa cho bạn, công ty này vẫn có thể giữ lại nó. Điều đáng lo ngại ở đây là công ty này có thể buộc phải chia sẻ khóa đó với cơ quan thực thi pháp luật hoặc cơ quan chính

phủ theo lệnh của tòa án mà không đến lý do xác đáng. Bạn nên đọc kỹ chính sách bảo mật của dịch vụ mã hóa mà bạn sử dụng và tìm hiểu xem ai sở hữu các khóa.

Nếu bạn muốn mã hóa một thông điệp – một email, văn bản, hoặc cuộc điện thoại – hãy sử dụng mã hóa đầu cuối[26]. Tức là thông điệp của bạn sẽ ở trạng thái không thể đọc được cho tới khi nó đến tay người nhận. Với mã hóa đầu cuối, chỉ bạn và người nhận mới có khóa để giải mã thông điệp. Các công ty viễn thông, chủ sở hữu website, hay nhà phát triển ứng dụng – tức những bên có thể bị các cơ quan thực thi pháp luật hay chính phủ yêu cầu giao nộp thông tin về bạn – sẽ không có được đặc quyền ấy. Làm sao để biết liệu dịch vụ mã hóa bạn đang sử dụng có phải là mã hóa đầu cuối không? Hãy tìm kiếm trên Google cụm từ "end-to-end encryption voice call" (mã hóa đầu cuối cuộc gọi thoại). Đừng chọn ứng dụng hoặc dịch vụ nào không sử dụng mã hóa đầu cuối.

[26] Mã hóa đầu cuối (end-to-end encryption – E2EE): Phương thức mã hóa theo đó chỉ những người giao tiếp với nhau mới có thể hiểu được thông điệp mã hóa.

Nếu những điều này nghe có vẻ phức tạp, đó là bởi vì bản chất chúng như vậy. Nhưng hiện đã có các plugin[27] PGP dành cho trình duyệt Chrome và Firefox, giúp quá trình mã hóa được dễ dàng hơn. Một trong số đó là Mailvelope, phần mềm xử lý khéo léo các khóa mã hóa công khai và bí mật của PGP. Bạn chỉ cần nhập cụm mật khẩu để tạo khóa. Sau đó, hễ khi nào bạn viết email trên nền web rồi chọn người nhận, và nếu người nhận đó cũng có khóa công khai, thì chương trình sẽ đưa ra một lựa chọn để bạn có thể gửi nội dung mã hóa cho họ.

[27] Plugin: Phần mềm hỗ trợ, bổ sung tính năng cụ thể cho một chương trình lớn hơn.

Nhưng ngay cả khi bạn đã mã hóa nội dung email bằng PGP, bất kỳ ai cũng vẫn có thể đọc một phần nhỏ nhưng chứa nhiều thông tin trong đó. Biện hộ trước những tiết lộ của Snowden, chính phủ

Mỹ đã nhiều lần khẳng định rằng họ không thu thập nội dung thực sự của các email – mà với mã hóa PGP, nội dung email sẽ ở trạng thái không thể đọc được. Thay vào đó, chính phủ Mỹ cho biết họ chỉ thu thập các siêu dữ liệu của email.

Siêu dữ liệu email là gì? Là thông tin trong các trường "To" (người nhận) và "From" (người gửi), cũng như địa chỉ IP của các máy chủ đã xử lý email từ người gửi đến người nhận. Siêu dữ liệu cũng bao gồm dòng tiêu đề – mà thông tin ở dòng tiêu đề nhiều khi có thể cho biết cả nội dung mã hóa của email. Vốn là một di sản tồn tại từ những ngày đầu của Internet, siêu dữ liệu vẫn xuất hiện trong mọi email gửi và nhận, nhưng người dùng hiện đại đã biết cách ẩn đi các thông tin này.

PGP, dù ở dạng nào, không thực hiện mã hóa siêu dữ liệu – tức các trường "Người nhận," "Người gửi," dòng tiêu đề, và nhãn thời gian. Các thông tin này vẫn ở dạng văn bản, dù bạn có nhìn thấy chúng hay không. Các bên thứ ba vẫn có thể nhìn thấy siêu dữ liệu ở email mã hóa, và như vậy họ sẽ biết được rằng vào ngày X bạn đã gửi email cho người Y, và rằng hai ngày sau, bạn lại gửi một email khác cho người đó,…

Điều đó nghe có vẻ vô hại, vì các bên thứ ba không thực sự đọc được nội dung email, mà có lẽ bạn cũng không quan tâm đến cơ chế di chuyển của email – các địa chỉ máy chủ và nhãn thời gian – nhưng bạn sẽ ngạc nhiên khi thấy lượng thông tin có thể rút ra được từ hai yếu tố đơn giản là đường đi và tần suất của email.

Trở lại thập niên 1990, trước khi bị FBI săn lùng, tôi đã thực hiện một phân tích siêu dữ liệu đối với tài liệu ghi thông tin các cuộc gọi điện thoại. Đầu tiên, tôi xâm nhập vào PacTel Cellular, một nhà cung cấp dịch vụ di động ở Los Angeles để lấy các hồ sơ ghi chi tiết cuộc gọi (CDR) của những người cung cấp thông tin mà FBI đang sử dụng để tìm hiểu về các hoạt động của tôi.

CDR rất giống với siêu dữ liệu mà tôi đang nói đến ở đây; chúng cho biết thời gian cuộc gọi được thực hiện, số điện thoại gọi đến, thời lượng cuộc gọi, và số lần gọi cho một số điện thoại cụ thể –

tất cả đều là những thông tin rất hữu ích.

Bằng cách tìm kiếm trong các cuộc gọi qua PacTel Cellular đến đường dây điện thoại cố định của người cung cấp thông tin, tôi đã xây dựng được một danh sách số điện thoại di động của những người đã gọi cho anh ta. Phân tích hóa đơn điện thoại của người gọi, tôi thấy rằng họ là thành viên thuộc đội chống tội phạm cổ cồn trắng[28] của FBI, hoạt động bên ngoài văn phòng Los Angeles. Quả nhiên, một vài số mà họ gọi đi là trong mạng nội bộ, đến văn phòng FBI ở Los Angeles, văn phòng công tố viên, và các văn phòng chính phủ khác. Một vài cuộc gọi có thời lượng trao đổi rất dài, và khá thường xuyên.

[28] Tội phạm cổ cồn trắng: Chỉ các vụ án có động cơ về tài chính, phi bạo lực, do những người hoạt động trong lĩnh vực kinh doanh/chính phủ gây ra.

Hễ khi nào họ chuyển người cung cấp thông tin đến một nhà an toàn[29] mới, tôi đều lấy được số điện thoại cố định ở đó bởi vì các đặc vụ sẽ gọi đến đó sau khi liên lạc với người cung cấp thông tin qua máy nhắn tin. Sau khi đã có số điện thoại cố định của người cung cấp thông tin, vận dụng social engineering, tôi còn có thể lấy được địa chỉ thực – chẳng hạn, tôi giả vờ làm nhân viên của Pacific Bell, một công ty cung cấp dịch vụ tại các nhà an toàn.

[29] Nhà an toàn: Chỉ một nơi bí mật, dùng để che giấu người khỏi nguy hiểm hay các mối đe dọa.

Social engineering là kỹ thuật tấn công sử dụng mánh khóe, lừa gạt, và gây ảnh hưởng để khiến đối tượng mục tiêu phải thực hiện theo yêu cầu. Thông thường, mọi người sẽ bị lừa để cung cấp thông tin nhạy cảm. Trong trường hợp này, vì biết số điện thoại nội bộ ở công ty điện thoại, nên tôi đóng giả một kỹ thuật viên, biết sử dụng đúng thuật ngữ và biệt ngữ chuyên ngành – đây là điều quan trọng giúp thu thập thông tin nhạy cảm.

Như vậy, mặc dù việc ghi lại siêu dữ liệu trong email khác với việc ghi lại nội dung email thực tế, nhưng từ quan điểm về quyền

riêng tư, đó cũng là hành vi xâm phạm trái phép.

Nếu nhìn vào siêu dữ liệu từ bất kỳ email nào gần đây, bạn sẽ thấy địa chỉ IP của các máy chủ đã chuyển email đó đi vòng quanh thế giới trước khi đến tay bạn. Mỗi máy chủ – giống như mỗi người truy cập Internet – đều có một địa chỉ IP riêng là giá trị số học được tính toán bằng cách sử dụng thông tin về quốc gia nơi bạn đang sống và nhà cung cấp Internet của bạn. Mỗi quốc gia có các khối địa chỉ IP riêng, và mỗi nhà cung cấp dịch vụ lại có khối phụ riêng, được chia nhỏ hơn theo loại hình dịch vụ, như quay số, cáp, hoặc di động. Nếu bạn mua địa chỉ IP tĩnh, nó sẽ được gắn với tài khoản thuê bao và địa chỉ nhà riêng của bạn, nếu không, địa chỉ IP bên ngoài sẽ được tạo ra từ vùng địa chỉ gán cho nhà cung cấp dịch vụ Internet của bạn. Ví dụ: một người gửi – tức là người đang gửi email cho bạn – có thể có địa chỉ IP 27.126.148.104, là địa chỉ nằm ở Victoria, Úc.

Hoặc địa chỉ đó có thể là 175.45.176.0, một trong những địa chỉ IP của Bắc Triều Tiên. Trong trường hợp địa chỉ thứ hai này, tài khoản email của bạn có thể bị gắn cờ để chính phủ kiểm tra. Ai đó trong chính phủ Mỹ có thể muốn biết tại sao bạn lại liên lạc với người ở Bắc Triều Tiên, ngay cả khi dòng tiêu đề email là "Chúc mừng sinh nhật."

Có thể bạn vẫn cho rằng địa chỉ máy chủ không chứa thông tin gì thú vị. Nhưng tần suất liên lạc có thể cho bạn biết rất nhiều điều. Ngoài ra, nếu xác định rõ từng thành phần – người gửi, người nhận, và vị trí của họ – bạn có thể suy luận ra tình hình. Ví dụ, khi kết hợp siêu dữ liệu với các cuộc gọi điện thoại – thời lượng gọi, thời gian gọi,… – bạn có thể phỏng đoán được sức khỏe tâm thần của một người. Một cuộc gọi kéo dài 10 phút vào lúc 10 giờ đêm đến đường dây nóng hỗ trợ các vấn đề bạo lực gia đình, hoặc một cuộc gọi kéo dài 20 phút vào lúc nửa đêm từ cầu Brooklyn đến đường dây nóng ngăn chặn tự tử có thể mang lại rất nhiều thông tin. Đại học Dartmouth đã phát triển một ứng dụng để phát hiện ra các xu hướng stress, trầm cảm, và cô đơn trong dữ liệu người dùng. Hoạt động của người dùng cũng có mối tương

quan với thành tích điểm số của sinh viên ở trường.

Bạn vẫn không thấy có gì nguy hại khi siêu dữ liệu email của mình bị lộ? Immersion, một chương trình được tạo ra ở Viện Công nghệ Massachusetts, có thể vạch ra các mối quan hệ giữa người gửi và người nhận của tất cả các email mà bạn lưu trữ trong tài khoản email của mình chỉ bằng cách sử dụng siêu dữ liệu. Công cụ này là một cách giúp bạn định lượng trực quan những người quan trọng nhất đối với mình. Thậm chí nó còn có thang thời gian di động, giúp bạn thấy vai trò của những người mà mình quen biết thay đổi lên xuống ra sao theo thời gian. Có thể bạn nghĩ rằng bạn hiểu rõ các mối quan hệ của mình, nhưng khi nhìn hình ảnh biểu diễn chúng bằng đồ họa, biết đâu bạn sẽ có được một cái nhìn khách quan hơn. Có thể qua đó bạn mới chợt nhận ra rằng mình hay gửi email cho một người mới chỉ thân sơ, hoặc mình quá lười gửi email cho một người thân thiết. Với công cụ Immersion, bạn có thể tùy chọn việc có tải dữ liệu lên hay không, và bạn cũng có thể xóa thông tin sau khi đồ thị đã hoàn tất.

Theo Snowden, các siêu dữ liệu email, văn bản, và điện thoại của chúng ta đang bị NSA và các cơ quan khác thu thập. Nhưng chính phủ không thể thu thập siêu dữ liệu của tất cả mọi người được, phải không? Về mặt kỹ thuật là không. Tuy nhiên, từ năm 2001 tới nay đã có xu hướng gia tăng mạnh trong hoạt động thu tập thông tin "hợp pháp."

Được sự hậu thuẫn của Đạo luật Giám sát Tình báo Nước ngoài (FISA) năm 1978 của Mỹ, Tòa án Giám sát Tình báo Nước ngoài (viết tắt là FISC, hoặc Tòa án FISA) quản lý tất cả các yêu cầu xin lệnh giám sát đối với các cá nhân nước ngoài tại Mỹ. Nhìn bề ngoài, việc cơ quan thực thi pháp luật phải có lệnh của tòa án mới được phép can thiệp vào một cá nhân nghe có vẻ hợp lý. Nhưng thực tế lại hơi khác. Chỉ tính riêng trong năm 2012, có 1.856 yêu cầu được trình lên tòa và cả 1.856 yêu cầu được phê duyệt – điều này cho thấy rằng quy trình phê duyệt hiện nay của chính phủ Mỹ hầu như chỉ mang tính hình thức. Sau khi Toà án FISA ra yêu

cầu, cơ quan thực thi pháp luật có thể buộc các công ty tư nhân phải giao nộp mọi dữ liệu về bạn mà họ có.

Để có thể thực sự ẩn mình trong thế giới số, bạn sẽ phải làm nhiều việc hơn, chứ không chỉ đơn thuần là mã hóa email. Sau đây là những việc cần làm:

Xóa địa chỉ IP thực: Đây là vị trí bạn kết nối với Internet, là dấu vân tay của bạn. Nó có thể cho biết bạn đang ở đâu (chi tiết đến tận địa chỉ nhà bạn) và đang sử dụng nhà cung cấp nào.

Che thông tin về phần cứng và phần mềm mà bạn đang sử dụng: Khi bạn kết nối trực tuyến với một website, website đó có thể chụp nhanh thông tin về phần cứng và phần mềm mà bạn đang sử dụng. Họ có thể sử dụng một số thủ thuật để tìm hiểu xem bạn đang cài đặt phần mềm nào, chẳng hạn Adobe Flash. Phần mềm trình duyệt báo cho website đó biết bạn đang sử dụng hệ điều hành nào, phiên bản nào, và bạn đang chạy các phần mềm nào khác trên máy tính vào thời điểm đó.

Bảo vệ tính ẩn danh của bạn: Việc chỉ ra mối liên hệ giữa hoạt động trên mạng và ngoài đời thực là rất khó. Rất khó để chứng minh rằng vào thời điểm một sự kiện diễn ra, bạn đang ngồi ở bàn phím. Tuy nhiên, nếu bạn xuất hiện trước camera trước khi vào mạng tại quán cà phê Starbucks, hoặc nếu bạn vừa mua một ly cà phê ở Starbucks bằng thẻ tín dụng, thì có thể liên hệ những hành động này với sự hiện diện trực tuyến của bạn vài phút sau đó.

Như chúng ta đã biết, mỗi khi bạn kết nối với Internet, kết nối đó sẽ được gán cho một địa chỉ IP. Nếu bạn muốn ẩn mình trên mạng thì đây là một vấn đề: bạn có thể đổi tên (hoặc không cung cấp tên), nhưng địa chỉ IP vẫn sẽ tiết lộ bạn đang ở đâu, bạn sử dụng nhà cung cấp nào, và danh tính của người thanh toán cho dịch vụ Internet (có thể là bạn hoặc không phải là bạn). Tất cả các thông tin này đều được đưa vào trường siêu dữ liệu của email và sau này có thể được dùng để xác định ra bạn. Bất kỳ hoạt động giao tiếp nào, dù là email hay không, đều có thể được dùng để

nhận diện bạn dựa trên địa chỉ IP gán cho bộ định tuyến mà bạn đang sử dụng – có thể là ở nhà, nơi làm việc, hoặc ở nhà bạn.

Tất nhiên, có thể giả mạo địa chỉ IP trong email. Một người có thể sử dụng địa chỉ proxy – tức không phải địa chỉ IP thực của người đó mà là địa chỉ của người khác – để khiến email đó có vẻ như bắt nguồn từ một địa điểm khác. Proxy đóng vai trò như một phiên dịch viên – bạn nói với người phiên dịch, rồi người phiên dịch nói lại cho đối tác ngoại quốc của bạn – chỉ có thông điệp là vẫn giữ nguyên. Vấn đề ở đây là một người có thể sử dụng proxy từ Trung Quốc hoặc thậm chí Đức để tránh bị phát hiện qua một email có nguồn gốc thực sự ở Bắc Triều Tiên.

Thay vì lưu trữ proxy riêng, bạn có thể sử dụng một dịch vụ gọi là anonymous remailer[30] để giấu địa chỉ IP của email. Anonymous remailer chỉ thay đổi địa chỉ email của người gửi rồi chuyển email đến cho người nhận. Người nhận có thể trả lời thông qua dịch vụ remailer này. Đó là phiên bản đơn giản nhất.

[30] Anonymous remailer (chuyển tiếp thư ẩn danh): Là máy chủ nhận email có nhúng các hướng dẫn về nơi cần gửi tiếp email đi, và thực hiện chuyển tiếp mà không để lộ nguồn gốc của email.

Ngoài ra còn có các biến thể khác. Một số remailer loại I và II không cho phép trả lời email; chúng chỉ đơn thuần là hình thức liên lạc một chiều. Remailer loại III, hay còn gọi là Mixminion, cung cấp dịch vụ trọn gói: trả lời, chuyển tiếp, và mã hóa. Nếu bạn chọn phương thức liên lạc ẩn danh này, hãy tìm hiểu xem remailer của mình cung cấp dịch vụ nào.

Một cách nữa để giấu địa chỉ IP là sử dụng bộ định tuyến kiểu củ hành (Tor)[31] – đây là cách mà Snowden và Poitras đã áp dụng.

[31] Tor (The Onion Router – Định tuyến kiểu củ hành): Cũng giống như củ hành tây gồm nhiều lớp, Tor sử dụng một mạng lưới các máy tính cá nhân lồng vào nhau, gọi là nút, làm nhiệm vụ định tuyến và mã hóa lưu lượng truy cập Internet đi qua Internet.

Chương trình mã nguồn mở Tor do Phòng Thí nghiệm Nghiên

cứu Hải quân Hoa Kỳ phát triển vào năm 2004 nhằm giúp người của quân đội thực hiện hoạt động tìm kiếm mà không để lộ vị trí thực của mình, và từ đó được mở rộng ra. Tor được thiết kế để giúp những người sống trong các thể chế hà khắc tránh được sự kiểm duyệt đối với các phương tiện truyền thông và dịch vụ đại chúng, đồng thời ngăn chặn người khác theo dõi những cụm từ khóa tìm kiếm mà họ sử dụng. Hiện nay, Tor vẫn miễn phí và dành cho bất cứ ai, ở bất cứ nơi đâu – kể cả bạn.

Tor hoạt động như thế nào? Nó đảo ngược mô hình truy cập website thông thường.

Thông thường, khi vào mạng, bạn mở trình duyệt Internet và nhập tên của website muốn truy cập. Một yêu cầu được chuyển tới website đó và một phần nghìn giây sau, trình duyệt của bạn nhận được phản hồi cùng với website. Dựa trên địa chỉ IP, website này biết nhà cung cấp dịch vụ là ai, và đôi khi còn biết được cả vị trí của bạn do suy từ vị trí nhà cung cấp hoặc độ trễ của các bước nhảy từ thiết bị của bạn đến website. Ví dụ, nếu thiết bị của bạn hiển thị vị trí ở Mỹ, nhưng thời gian và số bước nhảy mà yêu cầu của bạn cần trải qua để đến được đích lại cho thấy bạn đang ở một nơi khác, thì một số website – đặc biệt là các website trò chơi – sẽ coi đó là dấu hiệu gian lận.

Khi bạn sử dụng Tor, đường nối trực tiếp giữa bạn và website mà bạn truy cập sẽ được che khuất bởi một loạt các nút bổ sung, và sau mỗi 10 giây, chuỗi nút mạng kết nối bạn với website đó sẽ thay đổi mà không gây gián đoạn cho bạn. Các nút mạng kết nối bạn với một website giống như các lớp trong một củ hành tây vậy. Nói cách khác, nếu có người muốn từ website đích lần ngược lại để tìm bạn, đó là điều bất khả thi vì đường dẫn sẽ liên tục thay đổi. Kết nối của bạn sẽ được ẩn danh, trừ khi điểm đăng nhập và điểm thoát ra của bạn có mối liên hệ nào đó.

Với Tor, yêu cầu mở một website của bạn – ví dụ, mitnicksecurity.com – sẽ không được gửi trực tiếp đến máy chủ đó mà trước tiên được gửi đến một nút Tor khác. Và để làm cho mọi việc trở nên phức tạp hơn, nút mạng này lại tiếp tục chuyển

yêu cầu trên đến một nút khác, cuối cùng mới kết nối với mitnicksecurity.com. Như vậy, có một nút đăng nhập, một nút ở giữa, và nút thoát ra. Nếu muốn nhìn xem ai đang truy cập vào website của công ty mình, tôi sẽ chỉ nhìn thấy địa chỉ IP và thông tin từ nút thoát ra, tức nút cuối cùng trong chuỗi, chứ không thấy được nút đầu tiên, tức nút đăng nhập của bạn. Bạn có thể xây dựng cấu hình cho Tor để nó sử dụng nút thoát ra ở một quốc gia cụ thể, chẳng hạn Tây Ban Nha, hoặc thậm chí còn chi tiết hơn, ví dụ Honolulu.

Để sử dụng Tor, bạn phải lấy trình duyệt Firefox sửa đổi từ website Tor (torproject.org). Hãy tìm các trình duyệt Tor phù hợp cho hệ điều hành của bạn trên website dự án Tor. Đừng sử dụng website của bên thứ ba. Đối với các hệ điều hành Android, Orbot trên Google Play là một ứng dụng Tor miễn phí phù hợp, vừa thực hiện mã hóa lưu lượng truy cập vừa ẩn địa chỉ IP của bạn. Trên các thiết bị iOS (iPad, iPhone), hãy cài đặt trình duyệt Onion, một ứng dụng phù hợp từ cửa hàng ứng dụng iTunes.

Có thể bạn đang thắc mắc, tại sao không tạo luôn một máy chủ email ngay trong Tor? Có người đã làm rồi. Tor Mail là dịch vụ được lưu trữ trên một website dành riêng cho các trình duyệt Tor. Tuy nhiên, FBI[32] đã thu giữ máy chủ đó trong một vụ án không liên quan và chiếm được quyền truy cập vào tất cả các email mã hóa lưu trong Tor Mail. Đây là một câu chuyện cảnh giác cho thấy ngay cả khi bạn đinh ninh rằng thông tin của mình là an toàn và không có sơ hở, nhưng thực tế có thể không phải là như vậy.

[32] FBI: Cục Điều tra Liên bang Mỹ.

Tuy Tor sử dụng mạng đặc biệt, nhưng bạn vẫn có thể truy cập Internet từ đó, chỉ có điều tốc độ tải trang sẽ chậm hơn nhiều. Tuy nhiên, ngoài việc cho phép bạn lướt các website ở phần có thể tìm kiếm được trên Internet, Tor còn giúp bạn truy cập vào một thế giới website không thể tìm kiếm được theo cách thông thường, gọi là web tối . Đây là những website không mang tên

thông thường như Google.com mà có đuôi là .onion. Một số website ẩn này có thể chào mời, bán, hoặc cung cấp các sản phẩm và dịch vụ bất hợp pháp. Một số khác là các website hợp pháp của những người sống ở các khu vực bị áp bức.

Dẫu vậy, bạn cũng nên lưu ý đến một số điểm yếu của Tor:

- - Bạn không có quyền kiểm soát các nút thoát ra – có thể chúng thuộc quyền kiểm soát của chính phủ hoặc các cơ quan thực thi pháp luật;
- - Thông tin về bạn vẫn có thể bị thu thập và bạn vẫn có thể được nhận dạng;
- - Tor rất chậm.

Nhưng nếu vẫn quyết định sử dụng Tor, bạn không nên chạy nó trên cùng một thiết bị thường dùng để duyệt web. Nói cách khác, hãy dùng một máy tính xách tay để duyệt web và một thiết bị riêng cho Tor (ví dụ, một máy tính mini Raspberry Pi chạy phần mềm Tor). Mục đích ở đây là nếu có người xâm nhập được vào máy tính xách tay của bạn, họ vẫn sẽ không thể bóc tầng giao vận Tor của bạn vì nó chạy trên một thiết bị khác.

Trong trường hợp của Snowden và Poitras, như tôi đã nói, việc liên lạc qua email mã hóa là không đủ bảo mật. Sau khi Poitras tạo khóa công khai mới cho tài khoản email ẩn danh của mình, bà có thể gửi nó đến địa chỉ email trước kia của Snowden, nhưng nếu có người đang theo dõi tài khoản đó, thì danh tính mới của bà sẽ bị lộ. Một nguyên tắc hết sức cơ bản ở đây là bạn phải cách ly hoàn toàn các tài khoản ẩn danh khỏi bất kỳ thứ gì có thể liên quan đến danh tính thực của bạn.

Để tàng hình, bạn phải bắt đầu từ đầu cho mỗi liên hệ bảo mật mới mà bạn thực hiện. Các tài khoản email cũ có thể được kết nối theo nhiều cách khác nhau đến các khía cạnh khác trong cuộc sống của bạn – bạn bè, sở thích, công việc. Để giao tiếp bí mật, bạn phải tạo tài khoản email mới bằng Tor để địa chỉ IP thiết lập tài khoản không có bất kỳ mối liên hệ nào với danh tính thực của

bạn.

Tạo địa chỉ email ẩn danh là khó nhưng có thể làm được.

Bạn có thể sử dụng các dịch vụ email cá nhân. Nhưng nếu thanh toán cho các dịch vụ đó, bạn sẽ để lại dấu vết, nên tốt hơn, hãy sử dụng dịch vụ web miễn phí. Một rắc rối nhỏ: Gmail, Microsoft, Yahoo và các nhà cung cấp khác đều yêu cầu bạn cung cấp số điện thoại để xác minh danh tính. Rõ ràng bạn không thể sử dụng số điện thoại di động thật vì nó có thể liên quan đến tên và địa chỉ thật của bạn. Bạn có thể thiết lập một số điện thoại Skype nếu nó có tính năng xác thực bằng giọng nói thay vì xác thực bằng tin nhắn; tuy nhiên, bạn vẫn sẽ cần đến một tài khoản email hiện có và một thẻ quà tặng trả trước để thiết lập một số điện thoại Skype. Nếu bạn nghĩ chỉ cần sử dụng điện thoại di động trả trước là danh tính sẽ không bị lộ, thì bạn nhầm rồi. Nếu bạn từng sử dụng điện thoại trả trước để thực hiện các cuộc gọi có mối liên hệ với danh tính thực của mình, việc tìm ra bạn là ai đơn giản như trò chơi dành cho trẻ em.

Hãy sử dụng điện thoại dùng một lần. Một số người nghĩ điện thoại ẩn danh[33] là thiết bị chỉ dành cho những kẻ khủng bố, buôn người, và buôn bán ma túy, nhưng thực ra chúng có rất nhiều công dụng hợp pháp. Ví dụ, do muốn tìm hiểu xem ai là người đã tiết lộ các thông tin quan trọng trong ban lãnh đạo công ty, hãng Hewlett-Packard đã thuê thám tử tư điều tra và họ đến lục lọi thùng rác ở nhà một phóng viên kinh doanh; phóng viên này sau đó chuyển sang sử dụng điện thoại ẩn danh để họ khó xác định các cuộc gọi của cô hơn. Kể từ sau vụ việc này, cô chỉ trao đổi với nguồn cung cấp thông tin của mình trên điện thoại ẩn danh.

[33] Điện thoại ẩn danh (burner phone): Loại điện thoại di động giá rẻ, được thiết kế để sử dụng tạm thời, thường được vứt bỏ sau khi sử dụng. Điện thoại ẩn danh sử dụng dịch vụ trả trước tính theo phút, không có hợp đồng với nhà cung cấp dịch vụ điện thoại nào.

Tương tự, một người phụ nữ muốn tránh bị chồng/bạn trai cũ quấy rầy có thể sử dụng loại điện thoại không yêu cầu phải ký hợp đồng sử dụng hoặc không cần đến tài khoản Google hay Apple. Điện thoại ẩn danh thường có tính năng Internet hạn chế, chủ yếu cung cấp dịch vụ thoại, tin nhắn, và email – nhưng đôi khi đó là tất cả những gì chúng ta cần. Tuy nhiên, bạn vẫn có thể lấy được dữ liệu vì có thể kết nối điện thoại ẩn danh với máy tính xách tay rồi dùng nó để lướt Internet. (Ở phần sau của cuốn sách, tôi sẽ nêu cách thay đổi địa chỉ MAC[34] trên máy tính xách tay sao cho mỗi khi bạn kết nối với điện thoại ẩn danh, nó lại có vẻ như là một thiết bị mới.)

[34] MAC (media access control – kiểm soát truy cập phương tiện truyền thông): Là một tầng con trong tầng liên kết dữ liệu (DLL) trong mô hình tham chiếu OSI bảy tầng. Chức năng cơ bản của MAC là cung cấp cơ chế xác định địa chỉ và truy cập kênh sao cho mỗi nút trên một mạng lưới đều có thể giao tiếp với các nút khác trên cùng mạng hoặc khác mạng.

Tuy nhiên, việc giấu danh tính của bạn khi mua một chiếc điện thoại ẩn danh cũng rất khó khăn. Có thể lấy các hành động trong thế giới thực để nhận dạng bạn trong thế giới ảo. Dĩ nhiên, tôi có thể đến những cửa hàng như Walmart để mua điện thoại ẩn danh và 100 phút gọi bằng tiền mặt. Như vậy thì ai mà biết được chứ? Thực ra, rất nhiều người sẽ biết đấy.

Trước tiên, tôi đến Walmart bằng cách nào? Bắt xe Uber hay taxi? Tất cả những thông tin này đều có thể bị tòa yêu cầu cung cấp.

Tôi có thể lái xe riêng, nhưng cơ quan thực thi pháp luật hiện đã triển khai sử dụng công nghệ nhận dạng biển số tự động (ALPR) tại các bãi đỗ xe công cộng lớn để tìm kiếm xe bị mất/trộm cũng như để tìm kiếm những người đang có lệnh truy nã. Tòa án có thể yêu cầu giao nộp các dữ liệu từ ALPR.

Nhưng dù đi bộ đến Walmart, thì ngay khi tôi bước vào cửa hàng, hệ thống camera an ninh trong cửa hàng sẽ ghi lại khuôn mặt tôi, và video đó có thể bị tòa yêu cầu giao nộp.

Được rồi, vậy giả sử tôi cử người đi mua hộ – một người mà tôi không biết, ví dụ tôi thuê một người vô gia cư tình cờ gặp trên phố. Người đó đi vào cửa hàng rồi dùng tiền mặt để mua điện thoại ẩn danh cùng vài tấm thẻ cào. Đây là phương pháp an toàn nhất. Bạn có thể thu xếp gặp người này ở một nơi cách xa cửa hàng sau khi họ mua xong. Như vậy, bạn sẽ không có liên đới với giao dịch mua bán thực tế. Trong trường hợp này, mắt xích yếu nhất vẫn có thể là người mà bạn cử đi – anh ta đáng tin cậy đến mức nào? Nếu số tiền thù lao mà bạn trả lớn hơn giá trị của chiếc điện thoại, có lẽ anh ta sẽ giao lại chiếc điện thoại như đã hứa.

Để kích hoạt điện thoại trả trước, bạn phải gọi đến bộ phận dịch vụ khách hàng của nhà mạng hoặc thực hiện kích hoạt trên website của họ. Nhưng để tránh cuộc gọi bị ghi âm nhằm "giúp chúng tôi bảo đảm chất lượng dịch vụ," hãy kích hoạt trên web. Biện pháp bảo vệ tối thiểu ở đây là sau khi thay đổi địa chỉ MAC, hãy sử dụng Tor thông qua mạng không dây mở. Các thông tin thuê bao bạn nhập vào website đều nên là thông tin ngụy tạo. Về địa chỉ, hãy tìm kiếm trên Google địa chỉ của một khách sạn lớn và sử dụng thông tin đó. Bịa ra một ngày sinh nào đó và nhập mã PIN dễ nhớ để đề phòng trường hợp sau này phải liên lạc với dịch vụ khách hàng của nhà mạng.

Có một số dịch vụ email không yêu cầu xác minh, và nếu không phải lo lắng về các nhà chức trách, bạn có thể sử dụng số Skype để đăng ký tài khoản Google hoặc các dịch vụ tương tự, nhưng để minh họa, chúng ta hãy giả sử rằng sau khi bạn sử dụng Tor để ngẫu nhiên hóa địa chỉ IP, và sau khi tạo được một tài khoản Gmail không liên quan đến số điện thoại thực của bạn, Google gửi đến điện thoại của bạn mã xác minh hoặc cuộc gọi thoại. Lúc này, bạn đã có một tài khoản Gmail gần như không thể lần dấu.

Như vậy, bây giờ chúng ta đã có một địa chỉ email ẩn danh được thiết lập bằng các dịch vụ quen thuộc và phổ biến. Chúng ta có thể gửi đi các email tương đối an toàn, có địa chỉ IP ẩn danh nhờ Tor (mặc dù bạn không có quyền kiểm soát các nút thoát ra) và có nội dung mà chỉ người nhận mới đọc được nhờ PGP.

Xin lưu ý, tài khoản này chỉ có thể được giữ ẩn danh khi bạn truy cập nó thông qua Tor để địa chỉ IP của bạn không có mối liên hệ gì với nó. Ngoài ra, trong thời gian đăng nhập vào tài khoản Gmail ẩn danh này, bạn không nên thực hiện bất kỳ hoạt động tìm kiếm nào trên Internet, vì biết đâu bạn lại vô tình tìm kiếm một thông tin gì đó có liên quan đến danh tính thật của mình. Ngay cả việc tìm kiếm thông tin về thời tiết cũng có thể tiết lộ vị trí của bạn.

Như bạn có thể thấy, quá trình ẩn mình và duy trì sự vô hình này đòi hỏi tinh thần kỷ luật nghiêm khắc và sự cẩn trọng thường trực. Nhưng đó là cái giá xứng đáng để được vô hình.

Các kết luận quan trọng nhất ở đây là: Trước tiên, hãy nhận thức được tất cả những cách mà người khác có thể dùng để nhận diện bạn, ngay cả khi bạn chỉ thực hiện một số chứ không phải tất cả các biện pháp phòng ngừa mà tôi đã mô tả. Và nếu đã áp dụng tất cả các biện pháp này, bạn vẫn cần lưu ý đề phòng mỗi khi sử dụng các tài khoản ẩn danh. Không có ngoại lệ nào trong trường hợp này cả đâu.

Cũng cần phải nhắc lại rằng mã hóa đầu cuối – tức phương thức mã hóa sao cho email được an toàn và không ai có thể đọc được nó ngoại trừ người nhận, chứ không phải mã hóa đơn thuần – là rất quan trọng. Có thể sử dụng mã hóa đầu cuối cho các mục đích khác, chẳng hạn như mã hóa cuộc gọi và tin nhắn – chúng ta sẽ bàn đến vấn đề này ở hai chương tiếp theo.

Chương 3: NGHE TRỘM – NHỮNG ĐIỀU CẦN BIẾT

Hằng ngày bạn dành vô số thời gian trên điện thoại di động, trò chuyện, nhắn tin, lướt Internet. Nhưng bạn có thực sự biết điện thoại của mình hoạt động như thế nào không?

Dịch vụ điện thoại di động vận hành không dây và dựa vào các tháp di động, hay trạm cơ sở. Để duy trì kết nối, điện thoại di động phải liên tục gửi tín hiệu đến tháp hoặc các tháp gần nhất. Tín hiệu phản hồi từ các tháp được chuyển thành số lượng các "cột sóng" trên điện thoại – không có cột sóng nào nghĩa là không có tín hiệu.

Để bảo vệ phần nào danh tính của người dùng, các tín hiệu từ điện thoại di động sử dụng số nhận dạng thuê bao di động quốc tế (IMSI), một số riêng biệt được gán cho thẻ SIM của bạn. Số này ra đời từ thời các mạng di động cần biết khi nào bạn sử dụng tháp của họ, và khi nào bạn chuyển vùng (tức sử dụng tháp di động của nhà cung cấp dịch vụ khác). Phần đầu tiên của mã IMSI xác định nhà mạng, và phần còn lại xác định điện thoại.

Các cơ quan thực thi pháp luật đã tạo ra các thiết bị có thể giả vờ làm các trạm cơ sở nhằm chặn tin nhắn thoại và tin nhắn văn bản. Tại Mỹ, các cơ quan thực thi pháp luật và cơ quan tình báo cũng sử dụng nhiều thiết bị khác để bắt IMSI. IMSI được chụp ngay lập tức, trong vòng chưa đầy một giây, và không hề có cảnh báo trước. Thông thường, thiết bị bắt IMSI được sử dụng trong các cuộc biểu tình lớn, giúp các cơ quan thực thi pháp luật sau này có thể tìm ra những người đã tham gia, đặc biệt là những người tích cực kêu gọi người khác cùng tham gia.

Các dịch vụ và ứng dụng vận tải cũng có thể sử dụng những thiết bị này để tạo báo cáo về lưu lượng giao thông. Ở đây, số tài khoản thực tế, hay IMSI, không quan trọng, điều quan trọng là tốc độ di

chuyển từ tháp này đến tháp khác hoặc từ khu vực địa lý này đến khu vực địa lý khác của điện thoại. Lượng thời gian cần thiết để một chiếc điện thoại di động đến và đi khỏi mỗi tháp sẽ xác định tình trạng của tín hiệu giao thông: đỏ, vàng, hay xanh.

Khi có pin, thiết bị di động kết nối với một loạt tháp phát sóng. Tháp gần nhất chịu trách nhiệm xử lý cuộc gọi, tin nhắn, hoặc phiên truy cập Internet của bạn. Khi bạn di chuyển, điện thoại của bạn sẽ ping[35] tháp gần nhất và, nếu cần, cuộc gọi của bạn sẽ được chuyển từ tháp này sang tháp khác trong khi vẫn duy trì tính nhất quán. Tất cả các tháp lân cận khác đều ở chế độ chờ, sao cho khi bạn di chuyển từ điểm A đến điểm B và rơi vào vùng phủ sóng của một tháp khác, thì quá trình chuyển giao sẽ diễn ra suôn sẻ và bạn không bị rớt cuộc gọi.

[35] Ping (Packet Internet Grouper): Một công cụ cho mạng máy tính sử dụng trên các mạng TCP/IP (chẳng hạn như Internet) để kiểm tra xem có thể kết nối tới một máy chủ cụ thể nào đó hay không, và ước lượng khoảng thời gian trễ trọn vòng để gửi gói dữ liệu cũng như tỉ lệ các gói dữ liệu có thể bị mất giữa hai máy.

Thiết bị di động của bạn phát ra một chuỗi số riêng biệt được ghi lại trên một số tháp di động. Như vậy, khi nhìn vào nhật ký của một tháp, người ta sẽ thấy số nhận dạng trạm di động tạm thời (TMSI) của tất cả những người xung quanh khu vực đó vào bất kỳ thời điểm nào, cho dù họ có thực hiện cuộc gọi hay không. Các cơ quan thực thi pháp luật có thể, và trên thực tế là đã yêu cầu các nhà mạng cung cấp thông tin này, bao gồm cả dữ liệu nhận dạng tài khoản back-end[36] của chủ sở hữu.

[36] Back-end: Là phần trong một hệ thống phần mềm hoặc dịch vụ trực tuyến mà người dùng không tương tác, thường chỉ có các lập trình viên hoặc quản trị viên hệ thống mới tiếp cận được.

Thông thường, nếu bạn chỉ xem nhật ký của một tháp di động, có thể dữ liệu chỉ cho thấy rằng có người đã đi ngang qua đó và thiết bị của họ đã liên lạc với một tháp di động khác ở chế độ chờ. Nếu phát sinh cuộc gọi hoặc trao đổi dữ liệu, nhật ký cũng ghi lại cuộc

gọi đó và thời lượng gọi.

Tuy nhiên, có thể sử dụng dữ liệu từ nhật ký của các tháp di động để định vị người dùng. Hầu hết các thiết bị di động đều ping ba hoặc nhiều tháp cùng một lúc. Sử dụng nhật ký từ các tháp này, dựa trên cường độ tương đối của mỗi ping, người ta có thể định vị một người dùng điện thoại khá chính xác. Như vậy, về bản chất, chiếc điện thoại mà bạn mang theo người hằng ngày chính là một thiết bị theo dõi.

Làm thế nào để tránh bị theo dõi?

Khi ký hợp đồng với nhà mạng, bạn phải cung cấp tên, địa chỉ, và số An sinh Xã hội. Ngoài ra, họ còn kiểm tra tín dụng để đảm bảo rằng bạn có khả năng thanh toán hóa đơn hằng tháng. Nếu chọn nhà mạng thương mại thì bạn không thể tránh được thủ tục này.

Điện thoại ẩn danh có vẻ là một lựa chọn hợp lý. Điện thoại di động trả trước, có lẽ là loại mà bạn thay thế thường xuyên (chẳng hạn hằng tuần hoặc thậm chí hằng tháng), sẽ không để lại nhiều dấu vết. Số TMSI của bạn sẽ hiển thị trong nhật ký tháp di động, sau đó biến mất. Nếu bạn mua điện thoại một cách kín đáo, không ai có thể truy ngược lại tài khoản thuê bao. Dịch vụ di động trả trước vẫn là tài khoản thuê bao, vì vậy mỗi tài khoản đều được gán một số IMSI. Do đó, tính ẩn danh của một người phụ thuộc vào cách người đó mua thiết bị ẩn danh.

Chúng ta hãy thử tranh luận một chút. Giả sử bạn đã loại bỏ được mọi dấu vết cá nhân liên quan đến việc mua một chiếc điện thoại ẩn danh. Bạn đã làm theo các hướng dẫn của tôi, nhờ một người lạ dùng tiền mặt mua hộ điện thoại cho mình. Phải chăng như vậy có nghĩa là không ai có thể theo dõi được việc sử dụng chiếc điện thoại dùng một lần này? Câu trả lời ngắn gọn là không.

Sau đây là một câu chuyện cảnh giác: Một buổi chiều trong năm 2007, chiếc xe container chở lượng thuốc lắc trị giá 500 triệu đô-la xuất phát từ một cảng ở Melbourne, Úc rồi bị mất tích. Pat Barbaro, chủ nhân của chiếc container, đồng thời là một tay buôn bán ma túy khét tiếng, thò tay vào chiếc túi đựng 12 chiếc điện

thoại di động và lấy ra một chiếc để gọi cho Nick McKenzie, một phóng viên trong vùng – phóng viên này chỉ biết người gọi tên là Stan. Sau đó, Barbaro dùng một chiếc điện thoại ẩn danh khác để nhắn tin cho McKenzie hòng moi thông tin từ phóng viên điều tra này về container bị mất tích. Nhưng như chúng ta sẽ thấy, mánh khóe này không hiệu quả.

Trái với suy nghĩ của nhiều người, điện thoại ẩn danh không thực sự là vô danh. Theo Đạo luật Hỗ trợ Truyền thông để Củng cố Luật pháp của Mỹ (CALEA), tất cả các số IMSI kết nối với điện thoại ẩn danh đều phải được báo cáo giống như các thuê bao ký hợp đồng với các nhà mạng lớn. Nói cách khác, từ sổ nhật ký, cơ quan thực thi pháp luật có thể phát hiện ra điện thoại ẩn danh một cách dễ dàng như đối với điện thoại hợp đồng đã đăng ký. Tuy số IMSI không xác định được chủ sở hữu, nhưng hoạt động sử dụng điện thoại có thể cho biết điều đó.

Úc không có Đạo luật CALEA, song cơ quan thực thi pháp luật ở đây vẫn có thể theo dõi những chiếc điện thoại của Barbaro bằng các phương pháp truyền thống. Ví dụ, có thể họ thấy một cuộc gọi phát sinh từ điện thoại riêng của hắn, và sau đó một vài giây lại thấy một cuộc gọi hoặc tin nhắn phát sinh từ một trong những chiếc điện thoại ẩn danh của hắn cũng trong vùng phủ sóng của một tháp điện thoại. Dần dần, xuất phát từ thực tế là các số IMSI này thường xuyên xuất hiện cùng nhau trong cùng một vùng phủ sóng, người ta có thể suy ra rằng chúng là của cùng một người.

Việc Barbaro sử dụng nhiều điện thoại di động có một vấn đề: Dù hắn dùng loại gì, cá nhân hay ẩn danh, chỉ cần hắn vẫn ở yên một chỗ, tín hiệu từ điện thoại vẫn sẽ tìm đến cùng một tháp di động. Các cuộc gọi bằng điện thoại ẩn danh sẽ luôn xuất hiện bên cạnh các cuộc gọi bằng điện thoại mà hắn đã đăng ký. Và chiếc điện thoại đã đăng ký với nhà mạng là hoàn toàn có thể theo dõi được, từ đó giúp cơ quan thực thi pháp luật xác định danh tính của hắn. Nó trở thành bằng chứng vững chắc chống lại hắn, đặc biệt là vì hành vi này được lặp đi lặp lại ở các địa điểm khác nữa. Nhờ vậy,

chính quyền Úc có thể kết án Barbaro về tội thực thi một cuộc vận chuyển thuốc lắc thuộc loại lớn nhất lịch sử nước Úc.

McKenzie kết luận: “Kể từ lúc chiếc điện thoại trong túi tôi đổ chuông vào ngày hôm đó, và ‘Stan’ xuất hiện chớp nhoáng trong cuộc đời tôi, tôi trở nên đặc biệt quan tâm đến việc hoạt động giao tiếp của một người để lại dấu vết như thế nào, cho dù họ có cẩn thận đến đâu đi nữa.”

Tất nhiên, bạn có thể dùng một chiếc điện thoại ẩn danh duy nhất. Nhưng thi thoảng bạn sẽ phải kín đáo mua thêm phút gọi bằng thẻ trả trước hoặc Bitcoin. Để làm được điều này, bạn có thể sử dụng Wi-Fi công cộng sau khi thay đổi địa chỉ MAC trên thẻ không dây, và không bị ghi hình trong chiếc camera nào. Hoặc, như được đề cập ở chương trước, bạn có thể thuê người lạ cầm tiền mặt đến cửa hàng để mua điện thoại trả trước và một số thẻ nạp. Tuy mất thêm chi phí, và có lẽ mọi việc cũng phiền hà thêm một chút, nhưng bạn sẽ có một điện thoại thực sự ẩn danh.

Thoạt nghe, nhiều người có thể nghĩ rằng di động là một công nghệ hoàn toàn mới mẻ, song nó đã có tuổi đời hơn 40 năm rồi, và cũng giống như các hệ thống điện thoại sử dụng dây đồng, nó sử dụng nhiều công nghệ cũ, có thể gây tổn hại đến sự riêng tư của bạn.

Mỗi thế hệ công nghệ điện thoại di động ra đời lại mang đến những tính năng mới, chủ yếu nhằm mục đích di chuyển thêm nhiều dữ liệu hơn một cách hiệu quả hơn. Điện thoại thế hệ đầu tiên, hay 1G, phổ biến công nghệ điện thoại trong những năm 1980. Các mạng và thiết bị cầm tay 1G ban đầu này vận hành dựa trên công nghệ analog[37], và chúng sử dụng nhiều tiêu chuẩn di động đến nay đã lỗi thời. Năm 1991, mạng kỹ thuật số thế hệ thứ hai (2G) ra đời và mang đến hai tiêu chuẩn: hệ thống thông tin di động toàn cầu (GSM) và đa truy nhập phân chia theo mã (CDMA). Mạng 2G cũng mang đến dịch vụ tin nhắn ngắn (SMS), dữ liệu dịch vụ bổ sung phi cấu trúc (USSD), và các giao thức liên lạc đơn giản khác hiện vẫn đang được sử dụng. Ngày nay, chúng ta đang ở vào giai đoạn giữa của công nghệ 4G/LTE và đang trên đường

hướng tới thế hệ 5G.

[37] Công nghệ analog (tương tự): Công nghệ có đầu ra tương ứng hoặc tương tự với đầu vào. Điều này đối lập với công nghệ số ra đời về sau, trong đó đầu ra không có mối liên hệ với mã nhị phân ở đầu vào.

Dù nhà mạng sử dụng công nghệ thế hệ nào (2G, 3G, 4G, hoặc 4G/LTE), ở tầng nền vẫn là một giao thức tín hiệu quốc tế gọi là hệ thống báo hiệu (SS). Một trong những vai trò của giao thức hệ thống báo hiệu (hiện đang là phiên bản 7) là duy trì kết nối cho các cuộc gọi di động trong khi bạn lái xe trên xa lộ và di chuyển từ tháp di động này sang tháp di động khác. Cũng có thể sử dụng giao thức này cho mục đích giám sát. Về cơ bản, hệ thống báo hiệu 7 (SS7) có thể thực hiện mọi việc cần thiết để định tuyến một cuộc gọi, chẳng hạn như:

- Thiết lập kết nối mới cho cuộc gọi
- Xóa kết nối khi cuộc gọi kết thúc
- Tính phí cho bên thực hiện cuộc gọi
- Quản lý các tính năng bổ sung như chuyển tiếp cuộc gọi, hiển thị tên và số của bên gọi đến, gọi ba chiều, và các dịch vụ mạng thông minh (IN) khác
- Các cuộc gọi toll-free[38] (800 và 888) và gọi đường dài (900)
- Các dịch vụ không dây, bao gồm nhận dạng thuê bao, nhà cung cấp, và chuyển vùng trên thiết bị di động.

[38] Toll-free: Dịch vụ gọi điện có cước phí được tính cho bên nhận cuộc gọi.

Phát biểu tại Hội nghị Truyền thông Hỗn loạn, một hội nghị thường niên của các hacker được tổ chức tại Berlin, Đức, Tobias Engel, nhà sáng lập Sternraute, và Karsten Nohl, khoa học gia trưởng của Phòng Thí nghiệm Nghiên cứu An ninh, cho biết họ không chỉ định vị được người gọi mà còn có thể nghe được nội

dung trao đổi trong các cuộc gọi đó. Và nếu không nghe theo thời gian thực, họ có thể ghi lại các cuộc gọi và tin nhắn được mã hóa để thực hiện giải mã sau đó.

Về khía cạnh an ninh, mức độ bảo mật của bạn chỉ tương đương với liên kết yếu nhất. Engel và Nohl phát hiện ra rằng tuy các nước phát triển ở Bắc Mỹ và châu Âu đã đầu tư hàng tỉ đô-la để xây dựng các mạng 3G và 4G tương đối an toàn và riêng tư, song họ vẫn phải sử dụng SS7 làm giao thức nền tảng.

SS7 xử lý quá trình thực hiện các chức năng thiết lập cuộc gọi, tính cước phí, định tuyến, và trao đổi thông tin. Điều đó có nghĩa là nếu tiếp cận được SS7, bạn có thể điều khiển được cuộc gọi. SS7 cho phép kẻ tấn công sử dụng một nhà mạng nhỏ, giả dụ ở Nigeria, để truy cập các cuộc gọi được thực hiện ở châu Âu hoặc Mỹ. Engel nói: “Điều này giống như việc bạn bảo vệ cửa trước của ngôi nhà, nhưng lại để ngỏ cửa hậu vậy.”

Hai nhà nghiên cứu trên đã thử nghiệm một phương pháp trong đó kẻ tấn công sử dụng chức năng chuyển tiếp cuộc gọi và SS7 để chuyển tiếp các cuộc gọi đi của mục tiêu cho hắn trước khi thực hiện cuộc gọi hội nghị (gọi ba chiều) với người nhận.

Sau khi tiếp cận được, kẻ tấn công có thể nghe tất cả các cuộc gọi do nạn nhân thực hiện từ bất cứ đâu trên thế giới.

Một cách khác là kẻ tấn công thiết lập ăng-ten vô tuyến để thu thập tất cả các cuộc gọi và tin nhắn di động thực hiện trong một khu vực. Với các cuộc gọi 3G mã hóa, hắn có thể yêu cầu SS7 cung cấp khóa giải mã.

“Tất cả đều được thực hiện tự động, chỉ cần một nút bấm,” Nohl nói. “Tôi nghĩ việc ghi lại và giải mã hầu như bất kỳ mạng lưới nào là một khả năng gián điệp hoàn hảo... Cách này phát huy hiệu quả với mọi mạng lưới mà chúng tôi đã thử nghiệm.” Sau đó, ông liệt kê ra tổng cộng khoảng 20 nhà mạng lớn ở Bắc Mỹ và châu Âu.

Nohl và Engel cũng thấy rằng họ có thể định vị bất kỳ người dùng

điện thoại di động nào bằng cách sử dụng một hàm SS7 gọi là anytime interrogation query (truy vấn bất kỳ lúc nào). Nhưng tính năng này đã bị hủy bỏ từ đầu năm 2015. Tuy nhiên, vì tất cả các nhà mạng đều phải theo dõi người dùng để cung cấp dịch vụ, nên SS7 vẫn có các chức năng khác cho phép thực hiện giám sát từ xa. Nhưng từ sau khi nghiên cứu của Nohl và Engel được công bố, các nhà mạng đã có động thái giảm bớt hầu hết các lỗi sai mà hai nhà nghiên cứu đã chỉ ra.

Bạn có thể nghĩ rằng mã hóa sẽ giúp bảo vệ sự riêng tư cho các cuộc gọi bằng điện thoại di động. Bắt đầu từ 2G, các cuộc gọi thực hiện nền tảng GSM đã được mã hóa. Tuy nhiên, các phương pháp mã hóa cuộc gọi ban đầu trong 2G rất yếu và đều bị phá vỡ. Thật không may, chi phí nâng cấp mạng lưới lên 3G là quá tầm với của nhiều nhà mạng, vì vậy công nghệ 2G yếu ớt vẫn được sử dụng cho đến khoảng năm 2010.

Mùa hè năm 2010, một nhóm nghiên cứu do Nohl phụ trách đã chia tất cả các khóa mã hóa có thể được các mạng 2G GSM sử dụng cho các mạng này và thực hiện tính toán rồi xây dựng nên bảng cầu vồng, tức danh sách các khóa hoặc mật khẩu được tính toán trước. Họ công bố bảng này để chứng minh cho các nhà mạng trên thế giới thấy rằng việc mã hóa 2G bằng GSM là không an toàn. Mỗi gói thoại, tin nhắn, hay dữ liệu – hay còn gọi là đơn vị dữ liệu giữa nguồn và đích – gửi qua 2G GSM đều có thể được giải mã trong vòng vài phút bằng cách sử dụng bảng khóa trên. Đây là một trường hợp cực đoan, nhưng nhóm nghiên cứu cho rằng như vậy là cần thiết vì trước đó, khi Nohl và những người khác trình bày phát hiện của mình cho các nhà mạng, những lời cảnh báo của họ đều bị bỏ ngoài tai. Bằng cách chứng minh rằng họ có thể phá giải mã hóa 2G GSM, phần nào họ cũng đã khiến các nhà mạng phải thay đổi.

Điều quan trọng cần lưu ý ở đây là 2G hiện vẫn tồn tại, và các nhà mạng đang cân nhắc việc bán quyền truy cập vào các mạng 2G cũ để sử dụng cho các thiết bị Internet Vạn vật (tức các thiết bị khác ngoài máy tính có thể kết nối Internet, chẳng hạn ti-vi và tủ

lạnh) vốn chỉ cần truyền dữ liệu với tần suất không thường xuyên. Nếu điều này xảy ra, chúng ta sẽ phải làm sao để đảm bảo rằng bản thân các thiết bị đó có mã hóa đầu cuối, bởi chúng ta biết rằng mã hóa 2G là không đủ mạnh.

Tất nhiên, hoạt động nghe trộm đã tồn tại trước khi phổ biến các thiết bị di động. Đối với Anita Busch, cơn ác mộng bắt đầu vào sáng ngày 20 tháng 6 năm 2002, khi cô thức giấc vì tiếng gõ cửa dồn dập của hàng xóm. Có người đã bắn vỡ kính chắn gió trên xe của cô, lúc này đang đỗ ở lối vào nhà. Không chỉ vậy, họ để lại cho Busch một bông hồng, một chiếc đầu cá, và một lời nhắn gọn lỏn – "Dừng lại" – trên mui xe. Về sau, cô biết được rằng điện thoại của mình đã bị nghe lén, và không phải do cơ quan thực thi pháp luật.

Dường như có cơ sở cho sự tương đồng giữa cảnh lỗ đạn và con cá chết ở đây với một phân cảnh trong một bộ phim về xã hội đen của Hollywood. Khi đó, Busch, một phóng viên dày dạn kinh nghiệm, mới tham gia được vài tuần vào một dự án làm riêng cho tờ Los Angeles Times nhằm miêu tả lại sức ảnh hưởng ngày càng gia tăng của giới tội phạm có tổ chức ở Hollywood. Cô đang điều tra Steven Seagal và đối tác kinh doanh cũ của diễn viên này, Julius R. Nasso, người đã bị truy tố vì thông đồng với giới mafia ở New York để tống tiền Seagal.

Sau lời nhắn trên xe là một loạt tin nhắn điện thoại. Có vẻ người gọi muốn chia sẻ một số thông tin về Seagal. Rất lâu sau đó, Busch mới biết rằng người gọi được thuê bởi Anthony Pellicano, một cựu thám tử tư nổi tiếng ở Los Angeles; vào thời điểm xe của Busch bị phá, Pellicano đang bị FBI nghi ngờ về hoạt động nghe trộm bất hợp pháp, hối lộ, trộm cắp danh tính, và cản trở pháp luật. Pellicano đã cài thiết bị nghe lén vào điện thoại sử dụng dây cáp đồng của Busch, nhờ đó biết rằng cô đang viết một bài báo về các khách hàng của mình. Chiếc đầu cá trên mui xe là dấu hiệu cảnh báo cô dừng lại.

Hoạt động nghe trộm thường được liên tưởng đến các cuộc gọi điện thoại, nhưng các luật về nghe trộm ở Mỹ còn bao gồm cả

hoạt động nghe lén đối với email và tin nhắn. Bây giờ, tôi sẽ tập trung vào hoạt động nghe trộm truyền thống qua đường dây điện thoại cố định.

Điện thoại cố định là điện thoại có dây sử dụng trong gia đình hoặc công ty, và hoạt động nghe lén ở đây ý chỉ việc can thiệp vào đường dây trực tiếp. Trước kia, mỗi công ty điện thoại đều có vô số thiết bị chuyển mạch để thực hiện nghe trộm. Tức là công ty điện thoại có thiết bị đặc dụng để các công nghệ khung kết nối chúng với số điện thoại mục tiêu trên máy tính lớn đặt ở văn phòng trung tâm. Ngoài ra còn có thêm thiết bị nghe trộm thực hiện thao tác quay số vào thiết bị này và được sử dụng để theo dõi mục tiêu. Ngày nay, cách nghe trộm trên không còn được dùng nữa, và các công ty điện thoại phải tuân thủ các yêu cầu kỹ thuật do CALEA quy định.

Tuy hiện nay ngày càng có nhiều người chuyển sang dùng điện thoại di động, nhưng nhiều người vẫn tiếp tục sử dụng điện thoại cố định vì dây đồng đáng tin cậy. Cũng có người sử dụng công nghệ truyền giọng nói qua giao thức Internet (VoIP), tức là gọi điện qua Internet, vốn thường đi kèm với dịch vụ cáp hoặc Internet ở nhà riêng hoặc công ty. Các cơ quan thực thi pháp luật có khả năng nghe trộm cuộc gọi, dù là với công nghệ chuyển mạch vật lý tại công ty điện thoại hay công nghệ chuyển mạch số.

Đạo luật CALEA ra đời năm 1994 yêu cầu các nhà sản xuất và nhà cung cấp dịch vụ viễn thông phải điều chỉnh thiết bị của họ để cơ quan thực thi pháp luật có thể nghe trộm đường dây. Như vậy, trên lý thuyết theo Đạo luật CALEA, bất kỳ cuộc gọi điện thoại cố định nào ở Mỹ đều có thể bị chặn. Và cũng theo CALEA, cơ quan thực thi pháp luật muốn nghe trộm phải có lệnh điều tra theo Mục III[39]. Như vậy, việc một công dân bình thường thực hiện nghe trộm là bất hợp pháp – Anthony Pellicano đã vi phạm pháp luật khi bí mật theo dõi Anita Busch và những người khác. Danh sách các nạn nhân bị ông ta nghe trộm bao gồm cả những nhân vật nổi tiếng ở Hollywood như Sylvester Stallone, David

Carradine, Kevin Nealon,...

[39] Lệnh điều tra theo Mục III: Tên gọi dành cho các lệnh điều tra cho phép công tố viên thực hiện điều tra hoạt động tội phạm hình sự.

Trong danh sách đó có cả Erin Finn bạn tôi – người bạn trai cũ kiên quyết đeo bám và muốn theo dõi nhất cử nhất động của cô. Do đường dây điện thoại của cô bị nghe lén, nên khi gọi cho cô, chính tôi cũng bị theo dõi. Chuyện hay nhất ở đây là AT&T[40] đã trả cho tôi hàng nghìn đô-la để dàn xếp một vụ kiện tập thể vì Pellicano đã nghe lén các cuộc gọi của tôi với Finn. Điều đó có phần hơi mỉa mai, bởi vì vào một dịp khác, tôi lại chính là người đi nghe trộm. Có lẽ mục đích nghe trộm của Pellicano đen tối hơn mục đích của tôi; ông ta muốn khống chế để buộc các nhân chứng không được đứng ra làm chứng hoặc khai thông tin theo cách khác.

[40] AT&T: Một công ty viễn thông đa quốc gia có trụ sở tại Mỹ.

Thời điểm giữa những năm 1990, thiết bị nghe lén phải do kỹ thuật viên cài đặt. Vì vậy, Pellicano, hoặc người của ông ta, thuê người ở công ty điện thoại PacBell can thiệp vào đường dây điện thoại của Busch và Finn. Kỹ thuật viên có thể thiết lập các phần mở rộng cho các máy điện thoại mục tiêu tại văn phòng của Pellicano ở Beverly Hills. Trong trường hợp này, các thiết bị nghe trộm không được đặt tại hộp nối hoặc thiết bị đầu cuối gắn ở bên cạnh nhà hoặc khu chung cư, mặc dù điều này cũng khả thi.

Trong cuốn sách Ghost in the Wires (Bóng ma trên mạng)[41], tôi có kể chuyện một lần lái xe từ căn hộ của cha tôi ở Calabasas đến Long Beach để cài đặt thiết bị nghe trộm trên đường dây điện thoại của Kent, bạn của anh tôi khi đó mới qua đời. Có nhiều nghi vấn xung quanh cái chết của anh tôi, kể cả khả năng sử dụng ma túy quá liều, và tôi cho rằng Kent dự phần vào cái chết đó (nhưng về sau phát hiện ra rằng anh ấy không hề liên quan). Trong nhà kho của khu chung cư nơi Kent sống, tôi sử dụng kỹ thuật social engineering, giả vờ làm một kỹ thuật viên đường dây gọi đến một

đơn vị thuộc GTE42 để tìm ra nơi đặt cáp và cặp dây nối với điện thoại của Kent. Nhưng hóa ra đường dây điện thoại của Kent chạy qua một tòa chung cư khác. Tôi lại lật đật chạy sang nhà kho ở đó và cuối cùng cũng đặt được máy ghi âm mini kích hoạt bằng giọng nói vào đường dây điện thoại của anh ta ở hộp đầu cuối (là nơi các kỹ thuật viên của công ty điện thoại kết nối các đường dây với từng căn hộ).

[41] Cuốn sách này thuộc bộ "An toàn thông tin trong kỷ nguyên số" do Alpha Books phát hành.

[42] GTE: Một công ty điện thoại của Mỹ.

Sau đó, hễ khi nào Kent gọi điện, tôi có thể ghi âm lại cuộc trao đổi ở cả hai đầu mà anh ấy không hay biết – nhưng tôi không nghe trực tiếp ngay trong lúc quá trình ghi âm diễn ra. Trong 10 ngày tiếp theo đó, ngày nào tôi cũng lái xe 60 phút đến nhà Kent rồi mới quay về ngồi nghe băng ghi âm. Thật không may, tôi không tìm được thông tin gì trong số đó cả. Nhiều năm sau, tôi mới biết được rằng có lẽ chú tôi mới là người chịu trách nhiệm về cái chết của anh tôi.

Từ việc Pellicano và tôi có thể dễ dàng nghe trộm các cuộc trao đổi riêng tư trên điện thoại như vậy, có thể bạn sẽ băn khoăn không biết làm thế nào để ẩn mình trong đường dây cáp đồng của điện thoại cố định vốn rất dễ bị theo dõi. Thực ra, bạn không thể ẩn mình được đâu, nếu không có thiết bị đặc dụng. Những người đa nghi đến độ hoang tưởng có thể sử dụng loại điện thoại cố định thực hiện mã hóa tất cả các cuộc trao đổi qua dây cáp đồng. Chúng giải quyết được vấn đề nghe trộm, nhưng với điều kiện cả hai đầu dây đều sử dụng mã hóa; nếu không, việc theo dõi vẫn có thể diễn ra dễ dàng. Đối với những người bình thường chúng ta, có một số lựa chọn cơ bản giúp tránh bị nghe trộm.

Sự chuyển dịch sang công nghệ điện thoại kỹ thuật số đã và đang khiến cho hoạt động giám sát càng trở nên dễ dàng hơn. Ngày nay, việc nghe trộm trên đường dây điện thoại kỹ thuật số có thể được thực hiện từ xa. Máy tính đảo mạch chỉ cần tạo ra một luồng

dữ liệu thứ hai chạy song song, không cần đến thiết bị theo dõi. Như vậy, việc xác định xem liệu một đường dây điện thoại có bị nghe trộm không càng trở nên khó khăn hơn nhiều. Và hầu hết các vụ nghe trộm đều chỉ được phát hiện tình cờ.

Năm 2004, một thời gian ngắn sau khi Hy Lạp tổ chức Thế Vận hội Mùa hè, các kỹ sư tại Vodafone-Panafon[43] đã gỡ bỏ một số phần mềm lừa đảo bị phát hiện hoạt động trong mạng di động của công ty này suốt hơn một năm. Trên thực tế, cơ quan thực thi pháp luật chặn tất cả các dữ liệu thoại và văn bản đi qua bất kỳ mạng di động nào thông qua một hệ thống điều khiển từ xa gọi là RES – có thể coi đây là phiên bản kỹ thuật số của một thiết bị nghe trộm analog. Khi đối tượng bị giám sát thực hiện một cuộc gọi trên điện thoại di động, RES sẽ tạo ra một luồng dữ liệu thứ hai đi thẳng đến cơ quan thực thi pháp luật.

[43] Vodafone-Panafon: Tên một công ty cung cấp các sản phẩm và dịch vụ viễn thông ở Hy Lạp.

Phần mềm lừa đảo bị phát hiện ở Hy Lạp đã can thiệp vào hệ thống RES của Vodafone, có nghĩa là ai đó không thuộc cơ quan thực thi pháp luật đã nghe trộm các cuộc trao đổi diễn ra trên mạng di động của hãng này; trong trường hợp này, kẻ nghe trộm quan tâm đến các quan chức chính phủ. Trong thời gian Thế Vận hội diễn ra, một số quốc gia như Mỹ và Nga cung cấp hệ thống liên lạc riêng để phục vụ các cuộc trao đổi cấp nhà nước. Nguyên thủ các quốc gia khác và các lãnh đạo doanh nghiệp đến từ khắp nơi trên thế giới đều sử dụng hệ thống Vodafone lúc này đang bị xâm nhập.

Theo thông tin điều tra, các cuộc trao đổi của thủ tướng Hy Lạp và phu nhân – cũng như của thị trưởng Athens, ủy viên Liên minh châu Âu tại Hy Lạp, và các bộ trưởng bộ quốc phòng, ngoại giao, hải quân, và tư pháp – đều bị theo dõi trong kỳ Thế Vận hội. Ngoài ra, thành viên của các tổ chức dân quyền, các nhóm chống toàn cầu hóa, đảng Dân chủ Mới cầm quyền, các sĩ quan Hải quân Hy Lạp, các nhà hoạt động vì hòa bình, và một nhân viên người

Mỹ gốc Hy Lạp tại Đại sứ quán Hoa Kỳ ở Athens cũng bị nghe trộm điện thoại.

Hoạt động gián điệp lẽ ra còn tiếp diễn lâu hơn nữa, nếu như Vodafone không gọi Ericsson, nhà cung cấp thiết bị phần cứng cho hệ thống RES của hãng, để điều tra một vụ khiếu nại khác liên quan đến tỉ lệ gửi tin nhắn không thành công cao hơn so với mức thông thường. Sau khi tìm hiểu vấn đề, Ericsson thông báo với Vodafone rằng họ vừa tìm thấy phần mềm lừa đảo.

Đáng tiếc là, hơn một thập kỷ sau, đến bây giờ chúng ta vẫn không biết ai đã làm việc này. Hay tại sao họ làm như vậy. Hay mức độ phổ biến của hoạt động này là như thế nào. Tệ hơn, cách xử lý cuộc điều tra của Vodafone có vẻ khá vụng về. Thứ nhất, các file nhật ký quan trọng liên quan đến vụ việc trên đã bị mất. Thứ hai, sau khi phát hiện ra vụ việc, lẽ ra phải để chương trình lừa đảo trên tiếp tục chạy – như cách làm thông thường trong các cuộc điều tra tội phạm máy tính – Vodafone lại đột ngột gỡ bỏ nó khỏi hệ thống; động thái này có thể đã đánh động cho kẻ xâm phạm, tạo cơ hội để chúng che đậy dấu vết.

Trường hợp của Vodafone là một lời nhắc nhở đáng lo ngại rằng điện thoại di động của chúng ta dễ bị nghe trộm đến mức nào. Nhưng vẫn có cách giúp bạn ẩn mình với điện thoại kỹ thuật số.

Ngoài điện thoại di động và điện thoại cố định kiểu cũ, còn có một lựa chọn thứ ba là công nghệ truyền giọng nói qua giao thức Internet (VoIP). VoIP rất phù hợp với các thiết bị không dây không được tích hợp sẵn phương tiện thực hiện cuộc gọi điện thoại, ví dụ: iPod Touch của Apple; nó giống với việc lướt Internet hơn là thực hiện cuộc gọi truyền thống. Điện thoại cố định đòi hỏi dây cáp đồng. Điện thoại di động sử dụng tháp phát sóng di động. VoIP chỉ đơn giản là truyền giọng nói của bạn qua Internet – bằng cách sử dụng các dịch vụ Internet có dây hoặc không dây. VoIP cũng hoạt động trên các thiết bị di động, chẳng hạn như máy tính xách tay và máy tính bảng, bất kể chúng có dịch vụ di động hay không.

Để tiết kiệm tiền, nhiều gia đình và văn phòng đã chuyển sang dùng các hệ thống VoIP do các nhà cung cấp dịch vụ mới và các công ty cáp hiện tại cung cấp. VoIP cũng sử dụng cáp đồng trục truyền tải video và Internet tốc độ cao tới từng hộ gia đình.

Tin tốt là các hệ thống điện thoại VoIP có sử dụng mã hóa, cụ thể là các mô tả an ninh trong Giao thức Mô tả Phiên (SDES). Tin xấu là chính bản thân SDES cũng không hẳn an toàn.

Một phần vấn đề của SDES là khóa mã hóa không được chia sẻ qua giao thức mã hóa mạng an toàn là SSL/TLS, tức là khóa được gửi đi một cách lộ liễu. Thay vì mã hóa bất đối xứng, SDES sử dụng mã hóa đối xứng, có nghĩa là bằng cách nào đó, khóa do người gửi tạo ra phải được chuyển cho người nhận để giải mã cuộc gọi.

Giả sử Bob muốn gọi điện cho Alice đang ở Trung Quốc. Điện thoại VoIP được mã hóa SDES của Bob tạo ra một khóa mới cho cuộc gọi này. Bằng cách nào đó, Bob phải chuyển được khóa mới tạo cho Alice để thiết bị VoIP của cô có thể giải mã cuộc gọi của anh và họ có thể trò chuyện. Giải pháp của SDES là gửi khóa cho nhà mạng của Bob để họ chuyển nó cho nhà mạng của Alice, rồi họ sẽ chia sẻ cho cô.

Bạn đã nhìn ra sai sót ở đây chưa? Bạn còn nhớ những gì tôi đã nói về mã hóa đầu cuối trong chương trước không? Nội dung liên lạc được giữ an toàn cho đến khi người nhận mở nó ra. Nhưng SDES lại chia sẻ khóa của Bob cho nhà mạng của Bob và, nếu Alice sử dụng nhà mạng khác, cuộc gọi lại được mã hóa từ nhà mạng của Alice rồi chuyển tới Alice. Việc lỗ hổng này có phải là vấn đề nghiêm trọng không vẫn còn là điều cần bàn luận. Skype và Google Voice cũng áp dụng cách tương tự. Khóa mới được tạo ra mỗi khi phát sinh cuộc gọi, nhưng sau đó các khóa này lại bị chuyển giao cho Microsoft và Google. Như vậy thì không thể có cuộc trao đổi nào là riêng tư cả.

May mắn thay, có nhiều cách để thực hiện mã hóa đầu cuối đối với VoIP.

Signal, một ứng dụng của Open Whisper Systems (OWS)44, là một hệ thống VoIP mã nguồn mở miễn phí dùng cho điện thoại di động, có chức năng thực hiện mã hóa đầu cuối cho cả iPhone và Android.

44 Open Whisper Systems (OWS): Một tổ chức phần mềm, nhà phát triển giao thức mã hóa đầu cuối Signal và ứng dụng liên lạc mã hóa Signal, hoạt động chủ yếu nhờ tiền quyên góp và mọi sản phẩm của họ đều là sản phẩm phần mềm mã nguồn mở miễn phí. (DG)

Ưu điểm chính khi sử dụng Signal là việc quản lý khóa thuộc về các bên tham gia cuộc gọi, không thông qua bất kỳ bên thứ ba nào. Điều đó có nghĩa là, như trong SDES, khóa mới được tạo ra cho từng cuộc gọi; tuy nhiên, bản sao của khóa chỉ được lưu trữ trên thiết bị của người dùng. Vì CALEA cho phép cơ quan thực thi pháp luật tiếp cận bản ghi nhật ký của mọi cuộc gọi, nên trong trường hợp này, họ sẽ chỉ thấy dữ liệu lưu lượng mã hóa trên đường dây của nhà mạng, tức là loại thông tin không thể đọc được. Và OWS, tổ chức phi lợi nhuận tạo ra Signal, không giữ khóa, nên dẫu tòa án phát lệnh điều tra cũng vô ích. Khóa chỉ tồn tại trên các thiết bị ở hai đầu của cuộc gọi. Và khi cuộc gọi kết thúc, khóa sử dụng cho phiên gọi đó sẽ bị tiêu hủy.

Hiện tại, phạm vi áp dụng của Đạo luật CALEA chưa mở rộng đến người dùng cuối hoặc thiết bị của họ.

Có thể bạn cho rằng thực hiện mã hóa trên điện thoại di động sẽ làm hao pin. Đúng là như vậy, nhưng không hao nhiều. Signal sử dụng thông báo đẩy45, các ứng dụng WhatsApp và Telegram cũng vậy. Do đó, bạn sẽ chỉ nhìn thấy cuộc gọi đang đến, nhờ đó làm giảm mức tiêu hao pin trong lúc bạn đang nghe các cuộc gọi mới. Các ứng dụng Android và iOS cũng sử dụng thuật toán codec46 và buffer47 âm thanh dành cho mạng di động, như vậy, một lần nữa, quá trình mã hóa không tiêu hao nhiều điện năng trong khi bạn đang thực hiện cuộc gọi.

45 Thông báo đẩy: Là thông báo xuất hiện trên một thiết bị di

động. Đơn vị phát hành ứng dụng này có thể gửi thông báo đẩy đi vào bất kỳ thời điểm nào; người dùng không nhất thiết phải đang sử dụng ứng dụng hay thiết bị di động mới nhận được chúng.

[46] Codec (viết tắt của thuật ngữ Coder-Decoder – mã hóa- giải mã): Lý do người ta phải dùng đến các Codec là để làm giảm dung lượng các tập tin video hay âm thanh để tiện lợi hơn trong việc lưu trữ hay trao đổi qua mạng Internet. Yêu cầu chính của một Codec là phải giữ nguyên, hoặc làm suy giảm không đáng kể, phần chất lượng hình ảnh, âm thanh của tập tin sau khi mã hóa. Người ta có thể dùng phần cứng, hay phần mềm để tạo ra các bộ Codec này. Codec phần cứng đạt tốc độ xử lý nhanh, nhưng bộ giải mã bằng phần mềm sẽ uyển chuyển, dễ cải tiến và nâng cấp hơn.

[47] Buffer: Là dữ liệu tạm thời và thường được lưu trữ trong bộ nhớ tạm (RAM).

Ngoài mã hóa đầu cuối, Signal cũng sử dụng tính năng chuyển tiếp bí mật hoàn hảo (perfect forwarding secrecy – PFS). PFS là gì? Đó là hệ thống sử dụng khóa mã hóa khác nhau cho mọi cuộc gọi, vì vậy dù có người lấy được cuộc gọi mã hóa cùng với khóa giải mã cuộc gọi đó của bạn, nhưng các cuộc gọi khác vẫn sẽ an toàn. Tất cả các khóa PFS đều được tạo ra từ một khóa gốc duy nhất, nhưng điều quan trọng ở đây là nếu có kẻ lấy được một khóa, chưa chắc họ đã xâm nhập được vào các nội dung liên lạc khác của bạn.

Chương 4: KHÔNG MÃ HÓA NGHĨA LÀ CÓ SƠ HỞ

Bây giờ, nếu có người nhặt được điện thoại di động của bạn (trong tình trạng không khóa), người đó sẽ có thể truy cập được vào email, tài khoản Facebook, thậm chí cả tài khoản Amazon của bạn. Với thiết bị di động, chúng ta không đăng nhập riêng lẻ vào từng dịch vụ như với máy tính xách tay và máy tính để bàn; thiết bị di động có các ứng dụng dành riêng, và khi chúng ta đăng nhập vào đó, chúng sẽ duy trì chế độ mở. Ngoài các dữ liệu hình ảnh và âm nhạc, điện thoại di động còn có các tính năng riêng biệt khác, chẳng hạn như tin nhắn văn bản SMS. Tất cả đều sẽ bị sơ hở nếu có người lấy được thiết bị di động đã mở khóa của bạn.

Hãy xem xét trường hợp này: Năm 2009, Daniel Lee ở Longview, Washington, bị bắt giữ vì bị tình nghi buôn bán ma túy. Cảnh sát kiểm tra chiếc điện thoại di động không có mật khẩu của ông ta và ngay lập tức phát hiện ra một số tin nhắn liên quan đến ma túy, trong đó có một mục trao đổi với một người tên là Z-Jon.

Nội dung tin nhắn đó như sau: “Tôi có 130 ứng với 1/60 khoản tôi nợ anh tối qua.” Theo lời khai tại tòa án, cảnh sát Longview không chỉ đọc tin nhắn của Z-Jon gửi cho Lee mà còn chủ động phản hồi, thu xếp giao dịch mua bán ma túy với hắn. Đóng giả là Lee, cảnh sát gửi cho Z-Jon một tin nhắn để hỏi liệu hắn có “cần thêm” không. Z-Jon trả lời: “Có, còn gì bằng.” Khi Z-Jon (tên thật là Jonathan Roden) đến nơi hẹn, cảnh sát Longview bắt giữ hắn vì tội tàng trữ heroin.

Cảnh sát cũng thấy một mục trao đổi tin nhắn khác trên điện thoại của Lee và bắt giữ Shawn Daniel Hinton với kịch bản tương tự.

Cả hai đều kháng cáo, và vào năm 2014, với sự giúp đỡ của Liên minh Tự do Dân sự Mỹ, Tòa án Tối cao Bang Washington đã hủy bỏ các phán quyết của một tòa án cấp thấp hơn đối với Roden và

Hinton, đồng thời khẳng định rằng cảnh sát đã vi phạm kỳ vọng của các bị cáo về quyền riêng tư.

Các thẩm phán của bang Washington cho hay, nếu Lee đọc được các tin nhắn của Roden và Hinton trước hoặc hướng dẫn cảnh sát trả lời với nội dung rằng: "Daniel không có ở đây," thì điều đó có lẽ sẽ làm thay đổi tiến trình cơ bản của cả hai trường hợp. "Tin nhắn văn bản có thể liên quan đến các chủ đề thân mật giống như trong các cuộc gọi điện thoại, thư niêm phong, và các hình thức giao tiếp truyền thống khác vốn luôn được bảo vệ nghiêm ngặt theo luật pháp của Washington," Thẩm phán Steven Gonzalez viết trong vụ án của Hinton.

Các thẩm phán đã ra phán quyết rằng kỳ vọng về quyền riêng tư sẽ được mở rộng từ kỷ nguyên giấy sang kỷ nguyên số. Tại Mỹ, cơ quan thực thi pháp luật không được phép mở thư đã được niêm phong khi chưa có sự cho phép của người nhận. Kỳ vọng về quyền riêng tư là một phép thử về pháp lý. Nó được sử dụng để xác định xem liệu các các biện pháp bảo vệ quyền riêng tư trong Tu chính án thứ tư của Hiến pháp Mỹ có được áp dụng hay không. Tuy nhiên, vẫn còn phải chờ xem liệu các tòa án sẽ phán quyết các vụ án trong tương lai như thế nào, và họ có đưa phép thử về pháp lý này vào không.

Công nghệ văn bản – còn được gọi là dịch vụ tin nhắn ngắn, hay SMS – đã có từ khoảng năm 1992. Điện thoại di động, thậm chí cả điện thoại phổ thông (tức không phải điện thoại thông minh), cho phép gửi tin nhắn văn bản ngắn. Tin nhắn văn bản không nhất thiết di chuyển theo đường trực tiếp: nói cách khác, tin nhắn không di chuyển từ điện thoại này sang điện thoại khác. Giống như email, tin nhắn bạn gõ trên điện thoại được gửi đi trong trạng thái chưa được mã hóa đến một trung tâm dịch vụ tin nhắn ngắn (SMSC) là một phần của mạng di động được thiết kế để lưu trữ, chuyển tiếp, và gửi SMS – đôi khi là vài giờ sau đó.

Tin nhắn văn bản gốc trên điện thoại di động – tức tin nhắn được khởi tạo từ điện thoại chứ không phải từ ứng dụng – đi qua một SMSC của nhà mạng, nơi các tin nhắn có thể được lưu trữ hoặc

không. Các nhà mạng viễn thông nói rằng họ chỉ lưu tin nhắn trong vài ngày. Sau thời gian đó, họ khẳng định rằng tin nhắn chỉ còn được lưu trữ trên các thiết bị điện thoại đã thực hiện gửi và nhận chúng, và số lượng tin nhắn được lưu trữ này phụ thuộc vào từng loại điện thoại. Tuy họ nói vậy, nhưng tôi cho rằng tất cả các nhà mạng ở Mỹ đều giữ lại các tin nhắn văn bản, dù cho họ có cam đoan điều gì trước công chúng đi nữa.

Có một số nghi ngờ xung quanh lời khẳng định này của các nhà mạng. Các tài liệu do Edward Snowden tiết lộ cho thấy mối quan hệ chặt chẽ giữa NSA và ít nhất một nhà mạng là AT&T. Theo tạp chí Wired, bắt đầu từ năm 2002 – không lâu sau ngày 11/9[48] – NSA đã tiếp cận AT&T và đặt vấn đề yêu cầu xây dựng các phòng bí mật tại một số cơ sở của họ, bao gồm một phòng ở Bridgeton, Missouri và một phòng khác ở đường Folsom thuộc trung tâm thành phố San Francisco, và cuối cùng mở rộng ra các thành phố khác là Seattle, San Jose, Los Angeles, và San Diego. Nhiệm vụ của các phòng bí mật này là chuyển mọi lưu lượng dữ liệu trên Internet, email, và điện thoại đi qua một bộ lọc đặc biệt để tìm kiếm các từ khóa. Cho đến nay, vẫn chưa rõ tin nhắn văn bản có nằm trong danh sách này không, nhưng theo suy luận logic thì là có. Chúng ta cũng không được biết sau sự kiện Snowden, liệu hoạt động này hiện còn tồn tại ở AT&T hoặc bất kỳ nhà mạng nào khác hay không.

[48] 11/9: Tức ngày 11 tháng Chín năm 2001, thời điểm diễn ra cuộc tấn công của nhóm khủng bố Hồi giáo cực đoan al-Qaeda vào nước Mỹ, làm thiệt mạng gần 3.000 người.

Một bằng chứng cho thấy rằng hoạt động này đã bị ngưng lại.

Năm 2015, trong giải AFC[49] để tranh vé vào trận Super Bowl XLIX[50], đội New England Patriots đã châm ngòi cho cuộc tranh cãi về chiến thắng 45-7 của họ trước đội Indianapolis Colts. Trọng tâm cuộc tranh cãi xoay quanh nghi vấn có phải đội New England đã cố tình làm xì hơi bóng của mình hay không. Liên đoàn Bóng bầu dục Quốc gia (NFL) có những quy định nghiêm

ngặt về độ căng của bóng, và sau trận playoff[51], người ta xác định được rằng bóng của đội New England không đáp ứng các tiêu chuẩn đã đề ra. Tâm điểm cuộc điều tra là các tin nhắn văn bản của Tom Brady, hậu vệ ngôi sao của New England.

[49] AFC: Giải bóng bầu dục Mỹ.

[50] Super Bowl: Trận tranh chức vô địch thường niên của Liên đoàn Bóng bầu dục Quốc gia của Mỹ.

[51] Playoff: Trận đấu quyết định đội thắng cuộc.

Brady lên tiếng phủ nhận vai trò của mình trong vụ việc này. Để chứng minh, anh chỉ cần cung cấp cho các nhà điều tra những tin nhắn mà anh đã trao đổi trong thời gian trước và trong khi trận đấu diễn ra. Thật không may, đúng vào ngày đến gặp cơ quan điều tra, Brady đột ngột đổi điện thoại; anh bỏ chiếc điện thoại đã sử dụng trong khoảng giai đoạn từ tháng 11 năm 2014 đến ngày 6 tháng 3 năm 2015 để chuyển sang một chiếc điện thoại hoàn toàn mới. Sau đó, Brady báo với ủy ban điều tra rằng anh đã phá hủy chiếc điện thoại cũ cùng với tất cả dữ liệu lưu trong đó, bao gồm cả tin nhắn. Kết quả là Brady bị NFL phạt treo giò bốn trận – án phạt này sau đó được tòa án dỡ bỏ.

NFL cho biết: “Trong thời gian bốn tháng sử dụng chiếc điện thoại di động đó, Brady đã trao đổi gần 10.000 tin nhắn, và hiện nay tất cả đều không thể khôi phục được. Sau buổi điều trần kháng cáo, đại diện của Brady đưa ra một lá thư từ nhà cung cấp dịch vụ điện thoại di động của Brady xác nhận rằng các tin nhắn được trao đổi trên chiếc điện thoại bị phá hủy là không thể phục hồi được nữa.”

Như vậy, nếu Tom Brady nhận được lưu ý từ nhà mạng rằng tất cả các tin nhắn của anh đều bị hủy, và bản thân các nhà mạng khẳng định rằng họ không lưu giữ chúng, thì cách duy nhất để kéo dài tuổi thọ của tin nhắn là sao lưu thiết bị di động vào đám mây. Nếu bạn sử dụng một dịch vụ của nhà mạng, hoặc thậm chí của Google hay Apple, thì các công ty này có thể có quyền truy

cập vào tin nhắn của bạn. Có vẻ như Tom Brady đã không kịp sao lưu các nội dung trong điện thoại cũ lên đám mây trước khi thực hiện nâng cấp khẩn cấp.

Quốc hội Mỹ chưa giải quyết vấn đề lưu trữ dữ liệu nói chung và dữ liệu điện thoại di động nói riêng. Trên thực tế, trong những năm gần đây Quốc hội đã và đang tranh luận về việc liệu có cần yêu cầu tất cả các nhà mạng phải lưu trữ tin nhắn văn bản trong thời gian hai năm hay không. Nước Úc đã quyết định thực hiện điều này vào năm 2015, chúng ta hãy cùng chờ xem cách làm của họ có hiệu quả không.

Vậy làm thế nào để giữ sự riêng tư cho tin nhắn? Trước hết, không sử dụng dịch vụ tin nhắn gốc đi qua nhà cung cấp dịch vụ không dây. Thay vào đó, hãy sử dụng ứng dụng của một bên thứ ba. Nhưng chọn ứng dụng nào?

Để che giấu danh tính của mình trên mạng – để được tha hồ lướt Internet một cách ẩn danh – chúng ta cần phải tin tưởng một số phần mềm và dịch vụ phần mềm. Rất khó xác thực niềm tin này. Nhìn chung, các tổ chức mã nguồn mở và phi lợi nhuận có lẽ cung cấp các phần mềm và dịch vụ an toàn nhất, bởi vì có hàng nghìn cặp mắt cùng săm soi nghiên cứu từng dòng mã lập trình và cảnh báo ngay khi có điều gì sơ hở hoặc đáng ngờ. Nếu sử dụng phần mềm độc quyền, bạn sẽ phải ít nhiều tin tưởng vào lời hứa của nhà cung cấp.

Bản thân các đánh giá phần mềm có thể cung cấp cho bạn rất nhiều thông tin – chẳng hạn như cách vận hành của một tính năng giao diện. Những người đánh giá nghiên cứu phần mềm trong vài ngày rồi ghi lại những ấn tượng của họ. Họ không thực sự sử dụng phần mềm, cũng không thể cho biết về những gì sẽ xảy ra trong thời gian dài. Họ chỉ ghi lại những ấn tượng ban đầu của mình mà thôi.

Ngoài ra, những người đánh giá cũng không khẳng định bạn có thể tin tưởng phần mềm này hay không. Họ không thẩm định khía cạnh an ninh và quyền riêng tư của sản phẩm. Và không thể

chắc chắn rằng sản phẩm của một thương hiệu nổi tiếng là an toàn. Trên thực tế, chúng ta nên cảnh giác với các thương hiệu phổ biến bởi vì họ có thể mang lại ảo tưởng về sự an toàn. Bạn không nên tin vào lời nói của nhà cung cấp.

Hồi những năm 1990, khi cần mã hóa chiếc máy tính xách tay Windows 95, tôi đã chọn Norton Diskreet, một sản phẩm tiện ích của Norton nay đã ngừng sản xuất. Peter Norton là một lập trình viên thiên tài. Tiện ích máy tính đầu tiên của ông giúp tự động hóa quá trình lấy lại một tập tin đã bị xóa. Sau đó, ông tiếp tục tạo ra rất nhiều tiện ích hệ thống tuyệt vời khác trong thập niên 1980, thời điểm vẫn còn rất ít người hiểu được một dòng lệnh. Nhưng rồi ông bán lại công ty cho Symantec, và người ta bắt đầu viết phần mềm dưới danh nghĩa của ông.

Vào thời điểm tôi mua Diskreet, mã hóa DES 56 bit (DES là viết tắt của "data encryption standard," nghĩa là "tiêu chuẩn mã hóa dữ liệu") là ghê gớm lắm rồi, vì nó là loại mã hóa mạnh nhất thời bấy giờ. Để bạn dễ hình dung hơn, ngày nay chúng ta sử dụng mã hóa AES 256-bit (AES là viết tắt của "advanced encryption standard," nghĩa là "tiêu chuẩn mã hóa nâng cao"). Mỗi bit mã hóa mới sẽ bổ sung một lượng khóa mã hóa theo cấp số nhân và do đó bảo mật hơn. Mã hóa DES 56 bit được coi là an toàn và tối tân cho đến khi nó bị phá giải vào năm 1998.

Quay trở lại câu chuyện trên, tôi muốn kiểm tra xem liệu chương trình Diskreet có đủ mạnh để giấu dữ liệu không. Tôi cũng muốn thách thức FBI nếu họ từng chiếm đoạt máy tính của tôi. Sau khi mua Diskreet, tôi tấn công vào Symantec và tìm kiếm mã nguồn của chương trình. Sau khi phân tích hoạt động và cách thức vận hành của nó, tôi phát hiện ra rằng Diskreet chỉ sử dụng 30 bit của khóa 56 bit – phần còn lại chỉ là chuỗi các số 0. Cách này thậm chí còn kém an toàn hơn loại khóa 40 bit được phép xuất khẩu ra ngoài nước Mỹ.

Điều đó có nghĩa là người khác – như NSA, cơ quan thực thi pháp luật, hoặc ai đó có máy tính tốc độ cao – có thể bẻ khóa Diskreet dễ dàng hơn nhiều so với những gì họ quảng cáo về sản phẩm

này, vì nó không hề sử dụng mã hóa 56 bit. Ấy vậy mà hãng này vẫn quảng cáo rằng nó sử dụng mã hóa 56 bit. Tôi quyết định chuyển sang phương án khác.

Làm thế nào để công chúng biết được điều này? Họ không biết.

Theo dữ liệu từ website xếp hạng Niche.com, tuy các mạng xã hội như Facebook, Snapchat, và Instagram xếp hạng cao nhất về mức độ phổ biến đối với các thanh thiếu niên, nhưng ở cấp độ tổng quan, tin nhắn văn bản vẫn đứng ở vị trí thống lĩnh. Một nghiên cứu gần đây cho thấy 87% thanh thiếu niên gửi tin nhắn hằng ngày, trong khi chỉ có 61% sử dụng Facebook, sự lựa chọn phổ biến thứ hai của họ. Cũng theo nghiên cứu trên, mỗi tháng các cô gái gửi trung bình khoảng 3.952 tin nhắn và các chàng trai gần 2.815 tin nhắn.

Tin vui là ngày nay tất cả các ứng dụng nhắn tin phổ biến đều cung cấp một số dạng mã hóa khi gửi và nhận tin nhắn – tức là chúng bảo vệ "dữ liệu đang di chuyển." Tin không vui là không phải tất cả các phương thức mã hóa hiện đang sử dụng đều mạnh. Năm 2014, nhà nghiên cứu Paul Jauregui thuộc hãng bảo mật Praetorian phát hiện ra rằng có thể phá vỡ mã hóa của WhatsApp để thực hiện một cuộc tấn công MitM[52], trong đó kẻ tấn công chặn các tin nhắn giữa nạn nhân với người nhận và có thể đọc mọi tin nhắn. " NSA thích thứ này," Jauregui nhận xét. Vào thời điểm tôi đang viết cuốn sách này, WhatsApp đã cập nhật phương thức mã hóa của họ, và sử dụng mã hóa đầu cuối trên cả các thiết bị iOS và Android. Và công ty mẹ của WhatsApp là Facebook cũng bổ sung mã hóa cho 900 triệu người dùng ứng dụng Messenger của mình, dù rằng đó chỉ là một phương án tùy chọn, nghĩa là muốn sử dụng, bạn phải đặt sang cấu hình "Secret Conversations" (trao đổi bí mật).

[52] Trong mật mã học và an ninh máy tính, tấn công xen giữa, còn được gọi theo tiếng Anh là tấn công MITM (Man-in-the-middle), là cuộc tấn công trong đó kẻ tấn công bí mật chuyển tiếp và có thể làm thay đổi giao tiếp giữa hai bên mà họ tin rằng họ đang

trực tiếp giao tiếp với nhau.

Tin tệ hơn là những gì có thể xảy ra với dữ liệu được lưu trữ, hay còn gọi là "dữ liệu nghỉ." Hầu hết các ứng dụng tin nhắn trên thiết bị di động đều không mã hóa dữ liệu lưu trữ, dù là lưu trữ trên thiết bị của bạn hay trên hệ thống của bên thứ ba. Các ứng dụng như AIM, BlackBerry Messenger, và Skype đều lưu trữ tin nhắn mà không mã hóa chúng. Điều đó có nghĩa là nhà cung cấp dịch vụ có thể đọc được nội dung (nếu lưu trữ trên đám mây) và sử dụng nội dung đó để phục vụ mục đích quảng cáo. Điều đó cũng có nghĩa là nếu cơ quan thực thi pháp luật hoặc hacker tội phạm chiếm được thiết bị, họ cũng có thể đọc những tin nhắn đó.

Một vấn đề khác là lưu trữ dữ liệu dài hạn, vấn đề mà chúng ta đã bàn tới ở phần trước – dữ liệu nghỉ được nghỉ trong bao lâu? Nếu các ứng dụng như AIM và Skype lưu trữ tin nhắn không mã hóa, thì chúng sẽ giữ tin nhắn trong bao lâu? Microsoft, công ty chủ quản của Skype, tuyên bố, "Skype sử dụng chức năng quét tự động trong tin nhắn tức thời (IM) và tin nhắn ngắn (SMS) để (a) xác định tin nhắn rác tình nghi và/hoặc (b) xác định các URL[53] trước đó đã bị gắn cờ là các liên kết rác, gian lận, hoặc lừa đảo." Điều này nghe có vẻ giống như hoạt động quét để chống phần mềm độc hại mà các công ty thực hiện đối với các email của chúng ta. Tuy nhiên, chính sách bảo mật trên của Microsoft tiếp tục: "Skype sẽ giữ lại thông tin của bạn trong thời gian cần thiết để: (1) đáp ứng bất kỳ mục đích nào (theo định nghĩa trong Điều 2 của Chính sách Bảo mật này) hoặc (2) tuân thủ luật pháp, các yêu cầu pháp lý và các lệnh liên quan từ các tòa án có thẩm quyền."

[53] URL (Uniform Resource Locator – Định vị Tài nguyên thống nhất): Dùng để tham chiếu tới tài nguyên trên Internet.

Như vậy là không hay rồi. "Trong thời gian cần thiết" là trong bao lâu?

Instant Messenger của AOL (AIM) có thể là dịch vụ tin nhắn tức thời đầu tiên mà chúng ta từng sử dụng. Nó xuất hiện từ khá lâu

rồi. Được thiết kế cho máy tính để bàn hoặc máy tính cá nhân truyền thống, ban đầu AIM có dạng cửa sổ nhỏ xuất hiện ở góc dưới bên phải màn hình. Ngày nay, phần mềm này còn có phiên bản ứng dụng di động. Nhưng từ góc độ sự riêng tư, cần phải cảnh giác với AIM ở một số khía cạnh. Thứ nhất, AIM lưu trữ tất cả các tin nhắn được gửi qua đó. Thứ hai, giống như Skype, ứng dụng này cũng quét nội dung các tin nhắn. Thứ ba, AOL lưu trữ bản ghi của các tin nhắn trên đám mây đề phòng trường hợp bạn muốn truy cập lịch sử trò chuyện từ các thiết bị khác với thiết bị mà bạn dùng để thực hiện phiên hoạt động gần nhất.

Dữ liệu trò chuyện trên AOL không được mã hóa và bất kỳ thiết bị đầu cuối nào cũng có thể tiếp cận vì nó được lưu trữ trong đám mây, do vậy, cơ quan thực thi pháp luật và hacker mũ đen có thể dễ dàng lấy được một bản sao. Ví dụ, tài khoản AOL của tôi từng bị tấn công bởi một hacker non tay có biệt danh Virus, tên thật là Michael Nieves. Anh ta sử dụng kỹ thuật tấn công social-engineering (nói cách khác là gọi điện thoại và tỉ tê) đối với AOL và giành được quyền truy cập vào hệ thống cơ sở dữ liệu khách hàng nội bộ của họ, gọi là Merlin, nhờ đó thay đổi được địa chỉ email của tôi thành địa chỉ liên kết với một tài khoản riêng do anh ta kiểm soát. Sau đó, anh ta cài đặt lại mật khẩu của tôi và đọc được tất cả các tin nhắn trước đây. Năm 2007, Nieves bị khởi tố với bốn trọng tội và một tội nhẹ vì đã xâm nhập vào "các mạng máy tính và cơ sở dữ liệu nội bộ của AOL, bao gồm hóa đơn thanh toán, địa chỉ, và thông tin thẻ tín dụng của khách hàng."

Như Tổ chức Biên giới điện tử đã nói, "không có nhật ký nào là nhật ký tốt cả." Và AOL có nhật ký.

Các ứng dụng tin nhắn ngoại lai có thể tuyên bố chúng có mã hóa, nhưng mã hóa đó có thể không mạnh hoặc có sai sót. Nên chọn loại nào? Hãy chọn ứng dụng tin nhắn có mã hóa đầu cuối, tức là không bên thứ ba nào có quyền tiếp cận khóa. Khóa chỉ nên tồn tại trên từng thiết bị. Cũng cần lưu ý rằng nếu một trong các thiết bị tham gia liên lạc bị phần mềm độc hại xâm phạm, thì dù sử dụng bất kỳ loại mã hóa nào cũng trở thành vô nghĩa.

Các ứng dụng tin nhắn có ba loại cơ bản:

- Ứng dụng hoàn toàn không có mã hóa – nghĩa là ai cũng có thể đọc tin nhắn của bạn.
- Ứng dụng có mã hóa, nhưng không phải mã hóa đầu cuối – nghĩa là liên lạc có thể bị chặn bởi các bên thứ ba như nhà cung cấp dịch vụ, bởi họ biết khóa mã hóa.
- Ứng dụng có mã hóa đầu cuối – nghĩa là bên thứ ba không thể đọc được nội dung liên lạc vì khóa được lưu trữ trên thiết bị.

Thật không may, các ứng dụng nhắn tin phổ biến nhất như AIM đều không thực sự riêng tư. Ngay cả Whisper và Secret cũng vậy. Whisper được hàng triệu người sử dụng và bản thân hãng cung cấp cũng tự quảng bá rằng dịch vụ này thực sự là ẩn danh, nhưng các nhà nghiên cứu đã chỉ ra những lỗ hổng trong lời tuyên bố này. Whisper theo dõi người dùng của mình, còn danh tính của người dùng Secret đôi khi cũng bị tiết lộ.

Telegram là một ứng dụng nhắn tin khác có chức năng mã hóa, và nó được coi là một lựa chọn phổ biến ngang ngửa với WhatsApp. Ứng dụng này chạy trên các thiết bị Android, iOS và Windows. Tuy nhiên, các nhà nghiên cứu đã phát hiện ra rằng có thể tấn công các máy chủ của Telegram và giành quyền tiếp cận những dữ liệu quan trọng. Họ cũng nhận thấy có thể dễ dàng lấy lại tin nhắn mã hóa của Telegram, ngay cả sau khi chúng đã bị xóa khỏi thiết bị.

Vậy là chúng ta vừa thanh lọc một số lựa chọn phổ biến, bây giờ còn lại những gì?

Rất nhiều. Bạn hãy vào cửa hàng ứng dụng hoặc Google Play rồi tìm các ứng dụng có chức năng nhắn tin bí mật (off-the-record – OTR). Đây là giao thức mã hóa đầu cuối tiêu chuẩn cao hơn dùng cho tin nhắn văn bản và hiện đã được tích hợp trong một số sản phẩm.

Ứng dụng tin nhắn lý tưởng cũng cần phải có tính năng chuyển

tiếp bí mật hoàn hảo (PFS), sử dụng khóa phiên hoạt động ngẫu nhiên được thiết kế để có khả năng phục hồi trong tương lai. Điều đó có nghĩa là nếu một khóa bị bẻ gãy, không thể sử dụng khóa đó để đọc các tin nhắn sau này của bạn.

Một số ứng dụng sử dụng cả OTR và PFS.

ChatSecure là ứng dụng nhắn tin bảo mật hoạt động trên cả Android và iPhones. Ứng dụng này cũng cung cấp một cơ chế gọi là certificate pinning (chứng thư bảo mật), tức là nó bao gồm một chứng chỉ về bằng chứng nhận dạng được lưu trữ trên thiết bị. Ở từng phiên liên hệ với các máy chủ tại ChatSecure, chứng chỉ trong ứng dụng trên thiết bị của bạn sẽ được so sánh với chứng chỉ tại trạm chính. Nếu chứng chỉ được lưu trữ không khớp, phiên hoạt động sẽ bị ngừng lại. Một chi tiết thú vị nữa là ChatSecure cũng mã hóa nhật ký các cuộc trao đổi lưu trữ trên thiết bị – tức là phần dữ liệu nghỉ.

Có lẽ phương án mã nguồn mở tốt nhất là Signal của OWS, hoạt động trên cả iOS và Android.

Một ứng dụng nhắn tin khác có thể cân nhắc là Cryptocat, có thể dùng cho iPhone và hầu hết các trình duyệt chính trên máy tính cá nhân truyền thống. Tuy nhiên, ứng dụng này không phục vụ Android.

Và vào thời điểm tôi viết cuốn sách này, dự án Tor, đang vận hành trình duyệt Tor, cũng vừa phát hành Tor Messenger. Giống như trình duyệt Tor, ứng dụng mới này ẩn danh địa chỉ IP của người dùng, tức là sẽ khó theo dõi được các tin nhắn (tuy nhiên, xin lưu ý, giống như với trình duyệt Tor, theo cài đặt mặc định, các nút thoát ra không thuộc tầm kiểm soát của bạn). Tin nhắn tức thời được mã hóa bằng phương pháp mã hóa đầu cuối. Giống như với Tor, ứng dụng này hơi khó cho người dùng lần đầu, nhưng nó có thể bảo đảm sự riêng tư thực sự cho tin nhắn.

Ngoài ra, còn có các ứng dụng thương mại cũng cung cấp mã hóa đầu cuối. Tôi chỉ có một lời cảnh báo duy nhất ở đây là phần mềm của họ là độc quyền, mà nếu thiếu đi những đánh giá độc lập, thì

không thể xác nhận được tính an toàn và toàn vẹn của các phần mềm đó. Silent Phone cung cấp tính năng mã hóa đầu cuối tin nhắn văn bản. Tuy nhiên, phần mềm này lại lưu trữ một số dữ liệu, nhưng chỉ nhằm mục đích cải thiện các dịch vụ của mình. Khóa mã hóa được lưu trữ trên thiết bị – có nghĩa là chính phủ hoặc cơ quan thực thi pháp luật không thể buộc nhà sản xuất của phần mềm này là Silent Circle giao nộp khóa mã hóa của bất kỳ người dùng nào.

Vừa rồi tôi đã nói đến dữ liệu di chuyển và dữ liệu nghỉ, cũng như việc sử dụng mã hóa đầu cuối, PFS, và OTR. Còn các dịch vụ không dựa trên ứng dụng, chẳng hạn như webmail, thì sao? Mật khẩu thì sao?

Chương 5: THOẮT ẨN THOẮT HIỆN

Tháng Tư năm 2013, Khairullozhon Matanov, một cựu tài xế taxi 22 tuổi đến từ Quincy, Massachusetts, đi ăn tối với hai người bạn, thực ra là một cặp anh em. Trong câu chuyện, ba người nhắc đến sự kiện mới diễn ra trong ngày: một người đã đặt các nồi cơm điện bên trong chứa đầy đinh, thuốc súng, và thiết bị bấm giờ ở vị trí gần vạch đích của cuộc thi chạy Boston Marathon. Vụ nổ đã cướp đi ba mạng sống và làm bị thương hơn 200 người. Cặp anh em ngồi ăn cùng Matanov, Tamerlan và Dzhokhar Tsarnaev, về sau được xác định là nghi phạm chính.

Sau này, Matanov nói rằng anh không được biết thông tin trước về vụ đánh bom, nhưng anh bị cáo buộc là đã rời khỏi một cuộc họp sớm với các viên chức thực thi pháp luật sau sự kiện đánh bom trên và vội vàng xóa lịch sử trình duyệt trên máy tính cá nhân. Chỉ riêng hành động đơn giản đó – xóa lịch sử trình duyệt của máy tính xách tay – đã dẫn đến những cáo buộc chống lại Matanov.

Xóa lịch sử trình duyệt cũng là một trong những cáo buộc chống lại David Kernell, sinh viên đã tấn công tài khoản email của Sarah Palin. Điều thú vị nằm ở chỗ, khi xóa lịch sử trình duyệt, chạy trình chống phân mảnh[54] đĩa, và xóa các file ảnh của Palin đã tải về, Kernell chưa hề bị điều tra. Thông điệp rút ra ở đây là ở Mỹ, bạn không được phép xóa bất cứ hoạt động gì từng thực hiện trên máy tính của mình. Các công tố viên muốn xem toàn bộ lịch sử trình duyệt của bạn.

[54] Chống phân mảnh (defragmentation): Quá trình hợp nhất các file bị phân mảnh trên ổ cứng của người dùng.

Các cáo buộc chống lại Matanov và Kernell xuất phát từ một luật gần 15 năm tuổi đời – Luật Cải cách Kiểm toán trong Công ty Đại chúng và Bảo vệ Nhà đầu tư (theo cách gọi ở Thượng viện), hoặc

Đạo luật Doanh nghiệp và Trách nhiệm và Giải trình Kiểm toán (theo cách gọi ở Hạ viện), hoặc theo lối gọi dân dã là Đạo luật Sarbanes-Oxley năm 2002. Luật này là kết quả trực tiếp ra đời sau những hoạt động quản lý yếu kém ở Enron, một hãng cung cấp khí đốt bị phát hiện là gian lận và lừa gạt các nhà đầu tư cũng như chính phủ Hoa Kỳ. Các nhà điều tra phát hiện ra rằng rất nhiều dữ liệu đã bị xóa ngay từ khi bắt đầu cuộc điều tra, khiến các công tố viên khó biết được chính xác những gì đã xảy ra trong công ty này. Kết quả là, Thượng nghị sĩ Paul Sarbanes và Đại biểu bang Ohio là Michael G. Oxley đã đỡ đầu cho sự ra đời của đạo luật liên quan đến bảo tồn dữ liệu, trong đó có yêu cầu giữ lại lịch sử trình duyệt.

Theo một bản cáo trạng của đại bồi thẩm đoàn, Matanov đã xóa lịch sử trình duyệt Google Chrome của mình một cách có chọn lọc, theo đó chỉ để lại dữ liệu về các hoạt động trong một số ngày nhất định trong tuần xung quanh ngày 15 tháng 4 năm 2013. Matanov chính thức bị truy tố về hai tội: "(1) phá hủy, thay đổi, và làm sai lệch hồ sơ, tài liệu, và các vật thể hữu hình trong một cuộc điều tra liên bang, và (2) khai nhận sai sự thật, bịa đặt, và gian lận trong một cuộc điều tra liên bang liên quan đến khủng bố quốc tế và trong nước." Matanov bị kết án 30 tháng tù giam.

Trước đây, điều khoản về lịch sử trình duyệt trong Đạo luật Sarbanes-Oxley hiếm khi được sử dụng để chống lại các doanh nghiệp hoặc cá nhân. Và Matanov là trường hợp bất thường, một vụ án an ninh quốc gia nghiêm trọng. Tuy nhiên, sau sự kiện này, các công tố viên đã nhận ra được tiềm năng của nó và bắt đầu dùng đến nó thường xuyên hơn.

Nếu bạn không thể ngăn người khác theo dõi email, điện thoại, và tin nhắn của mình, và nếu pháp luật không cho phép bạn xóa lịch sử trình duyệt, vậy bạn có thể làm gì? Có lẽ ngay từ đầu bạn đừng thu thập những dữ liệu lịch sử làm gì.

Các trình duyệt như Firefox của Mozilla, Chrome của Google, Safari của Apple và Internet Explorer của Microsoft và Edge đều có sẵn tính năng tìm kiếm ẩn danh trên mọi thiết bị, từ máy tính

cá nhân truyền thống cho đến thiết bị di động. Trong mỗi phiên tìm kiếm, trình duyệt sẽ mở một cửa sổ mới và không lưu lại các thông tin bạn đã tìm kiếm hay địa chỉ mà bạn truy cập. Khi bạn đóng cửa sổ trình duyệt riêng tư đó, mọi dấu vết về các trang bạn đã truy cập sẽ biến mất khỏi thiết bị. Đổi lại, nếu không đánh dấu (bookmark) website nào trong khi sử dụng trình duyệt riêng tư, bạn sẽ không thể nhớ đường quay lại đó; không có lịch sử nào cả – ít nhất là không có trên máy của bạn.

Có thể bạn cảm thấy yên tâm khi sử dụng cửa sổ riêng tư trên Firefox hay chế độ ẩn danh trên Chrome, nhưng yêu cầu truy cập riêng tư của bạn vẫn phải đi qua nhà cung cấp dịch vụ Internet, tức công ty mà bạn bỏ tiền ra để mua dịch vụ Internet hoặc di động – và nhà cung cấp này có thể chặn bất kỳ thông tin nào gửi đi mà không được mã hóa. Nếu bạn truy cập một website sử dụng mã hóa, thì nhà cung cấp có thể lấy được siêu dữ liệu – tức các thông tin cho biết vào ngày A giờ B bạn truy cập website C.

Khi trình duyệt Internet – trên máy tính cá nhân truyền thống hoặc thiết bị di động – kết nối với một website, trước tiên nó sẽ tìm hiểu xem có mã hóa không, và nếu có thì là mã hóa loại nào. Giao thức cho các hoạt động giao tiếp qua web được gọi là http, đặt trước địa chỉ website, nghĩa là một URL điển hình có thể trông giống như sau: http://www.mitnicksecurity.com. Trong một số trường hợp, cụm “www” là không cần thiết.

Khi bạn sử dụng mã hóa để kết nối với một website, giao thức sẽ thay đổi một chút. Thay vì “http,” bạn sẽ thấy “https,” như vậy địa chỉ website lúc này sẽ là https://www.mitnicksecurity.com. Kết nối https này an toàn hơn, một phần vì đây là kết nối điểm-tới-điểm, nhưng với điều kiện bạn phải kết nối trực tiếp với chính website đó. Ngoài ra còn có rất nhiều Mạng Phân phối Nội dung (Content Delivery Network – CDN) lưu trữ lại các trang để máy khách cung cấp chúng nhanh hơn, bất kể bạn ở đâu trên thế giới, và do đó tạo thành một hàng rào ngăn bạn với website bạn muốn truy cập.

Cũng xin lưu ý rằng nếu bạn đăng nhập vào các tài khoản Google,

Yahoo hoặc Microsoft, các tài khoản này có thể ghi lại lưu lượng web trên máy tính cá nhân hoặc thiết bị di động của bạn – có lẽ là để xây dựng kho dữ liệu về hành vi trực tuyến của bạn nhằm giúp họ hiển thị những quảng cáo phù hợp hơn. Để tránh điều này, hãy đăng xuất khỏi các tài khoản Google, Yahoo, và Microsoft khi sử dụng xong và khi nào cần sử dụng tiếp hãy đăng nhập lại.

Ngoài ra còn có các trình duyệt mặc định được tích hợp vào thiết bị di động – xin lưu ý đây không phải là các trình duyệt tốt. Chúng là rác thì đúng hơn, vì đó phiên bản mini của các trình duyệt trên máy tính để bàn và máy tính xách tay, do đó thiếu đi một số biện pháp an ninh và bảo vệ quyền riêng tư của các phiên bản mạnh hơn. Ví dụ, iPhone cài sẵn Safari, nhưng bạn nên vào cửa hàng Apple trực tuyến để tải phiên bản Chrome hoặc Firefox dành cho thiết bị di động, các trình duyệt này được thiết kế riêng cho môi trường di động. Các phiên bản Android mới hơn đều được cài đặt sẵn Chrome. Tất cả các trình duyệt trên thiết bị di động ít nhất đều hỗ trợ duyệt web riêng tư.

Và nếu sử dụng Kindle Fire, bạn không nên tải xuống Firefox hay Chrome qua Amazon. Thay vào đó, hãy sử dụng một vài thủ thuật thủ công để cài đặt Firefox hoặc Chrome qua trình duyệt Silk của Amazon. Để cài đặt Firefox trên Kindle Fire, hãy mở trình duyệt Silk và truy cập website Mozilla FTP. Chọn “Go,” sau đó chọn file có đuôi .apk.

Hoạt động duyệt web riêng tư không tạo ra các file tạm thời, do đó không để lại lịch sử duyệt web trên máy tính xách tay hoặc thiết bị di động. Liệu một bên thứ ba có thể vẫn thấy sự tương tác của bạn với các website không? Có, trừ khi tương tác đó được mã hóa ngay từ đầu. Để thực hiện điều này, Tổ chức Biên giới Điện tử đã xây dựng plugin HTTPS Everywhere dành cho các trình duyệt Firefox và Chrome trên máy tính cá nhân truyền thống và trình duyệt Firefox trên thiết bị Android. Tại thời điểm viết cuốn sách này, chưa có phiên bản dành cho iOS. Nhưng HTTPS Everywhere có thể mang đến một lợi thế độc đáo: giả dụ rằng trong vài giây đầu tiên của phiên kết nối, trình duyệt và website đàm phán về

loại bảo mật sẽ sử dụng. Bạn muốn sử dụng PFS mà tôi đã nói đến ở chương trước. Nhưng không phải mọi website đều sử dụng PFS. Và không phải mọi cuộc đàm phán đều cho ra kết quả là PFS – dù rằng nó được đề xuất. HTTPS Everywhere có thể bắt buộc sử dụng https bất cứ khi nào có thể, ngay cả khi không có PFS.

Đây là một tiêu chí nữa đối với một kết nối an toàn: mọi website phải có chứng chỉ, tức sự đảm bảo của một bên thứ ba rằng khi bạn kết nối, ví dụ với website của ngân hàng Bank of America, thì đó thực sự là website của ngân hàng này chứ không phải là website lừa đảo. Các trình duyệt hiện đại làm việc với các bên thứ ba này, gọi là nhà chứng thực, để có các danh sách cập nhật. Khi bạn kết nối với một website không được chứng thực một cách hợp lệ, trình duyệt sẽ đưa ra cảnh báo hỏi xem bạn có tin tưởng website đó và tiếp tục truy cập hay không. Bạn được tự do đặt ra ngoại lệ. Nhưng nhìn chung, đừng tạo ngoại lệ, trừ khi bạn biết website đó.

Ngoài ra, trên Internet không chỉ có một loại chứng chỉ, mà có nhiều cấp độ chứng chỉ. Loại phổ biến nhất mà lúc nào bạn cũng thấy chỉ xác định tên miền thuộc về người đã yêu cầu chứng chỉ thông qua hình thức xác minh qua email. Người yêu cầu có thể là bất kỳ ai, nhưng điều đó không quan trọng, vì điều quan trọng là website đó có chứng chỉ được trình duyệt của bạn công nhận. Điều này cũng đúng với loại chứng chỉ thứ hai là chứng chỉ tổ chức. Tức là website đó dùng chung chứng chỉ với các website khác có liên quan đến cùng một tên miền – nói cách khác, tất cả các tên miền phụ trên mitnicksecurity.com sẽ dùng chung một chứng chỉ.

Cấp xác thực chứng chỉ nghiêm ngặt nhất là là chứng chỉ xác thực mở rộng (extended verification certificate). Trên tất cả các trình duyệt, khi chứng chỉ xác thực mở rộng được cấp, một số phần của URL sẽ chuyển sang màu xanh (thông thường là màu xám). Khi nhấp chuột vào địa chỉ website – https://www.mitnicksecurity.com – bạn sẽ thấy có thêm các thông tin chi tiết về chứng chỉ và chủ sở hữu chứng chỉ, thường

là tên thành phố và tiểu bang đặt máy chủ cung cấp website. Việc xác thực sự tồn tại trong thế giới thực này hàm ý rằng công ty đang giữ URL này là hợp pháp và đã được xác thực bởi một đơn vị chứng thực thứ ba đáng tin cậy.

Có thể bạn đã biết rằng trình duyệt trên thiết bị di động có thể theo dõi vị trí của bạn, nhưng hẳn là bạn sẽ ngạc nhiên khi biết trình duyệt trên máy tính cá nhân truyền thống cũng làm như vậy. Đúng là thế đấy. Bằng cách nào?

Bạn còn nhớ phần tôi giải thích về việc siêu dữ liệu email chứa địa chỉ IP của tất cả các máy chủ xử lý email trên đường di chuyển đến bạn không? Một lần nữa, địa chỉ IP đến từ trình duyệt của bạn có thể xác định nhà cung cấp mà bạn đang sử dụng và khoanh vùng khu vực mà bạn đang ở.

Lần đầu tiên bạn truy cập một website yêu cầu cung cấp thông tin cụ thể về vị trí của bạn (chẳng hạn một website thời tiết), trình duyệt sẽ hỏi bạn có muốn chia sẻ dữ liệu đó với website trên hay không. Lợi ích của việc chia sẻ dữ liệu là website có thể tùy chỉnh danh mục cho bạn. Ví dụ: trên trang washingtonpost.com, có thể bạn sẽ thấy quảng cáo của các doanh nghiệp trong vùng nơi bạn đang sinh sống thay vì ở nơi khác.

Bạn không nhớ trước kia đã trả lời câu hỏi đó của trình duyệt hay chưa? Vậy hãy vào trang kiểm tra ở địa chỉ http://benwerd.com/lab/geo.php. Đây là một trong nhiều website kiểm tra cho bạn biết liệu trình duyệt bạn đang dùng có báo cáo vị trí của bạn hay không. Nếu có nhưng bạn muốn ẩn danh, hãy tắt tính năng này. Điều may mắn là bạn có thể tắt tính năng theo dõi vị trí của trình duyệt. Với Firefox, gõ chữ “about: config” vào thanh địa chỉ URL. Kéo xuống mục “geo” (địa lý) và thay đổi cài đặt thành “disable” (tắt). Lưu những thay đổi của bạn. Với Chrome, vào phần Options>Under the Hood[55]>Content Settings>Location (Tùy chọn>Nâng cao>Cài đặt nội dung>Vị trí). Tùy chọn “Do not allow any site to track my physical location” (Không cho phép bất kỳ trang nào theo dõi vị trí thực của tôi) sẽ tắt tính năng định vị trong Chrome. Các trình duyệt khác cũng có

các tùy chọn cấu hình tương tự.

[55] Phiên bản Chrome mới hiện đã thay mục “Under the Hood” thành “Show advanced settings” ở cuối trang cài đặt.

Nếu muốn vui chơi một chút, bạn cũng có thể giả mạo vị trí của mình. Nếu muốn gửi đi thông tin tọa độ giả – ví dụ Nhà Trắng – trong Firefox, bạn có thể cài đặt một plugin có tên là Geolocator. Với Google Chrome, hãy vào mục cài đặt sẵn có tên “emulate geolocation coordinates” (Mô phỏng tọa độ vị trí địa lý) của plugin. Với Chrome, nhấn tổ hợp Ctrl+Shift+I trên Windows hoặc Cmd+Option+I trên Mac để mở Chrome Developer Tools (Công cụ nhà phát triển Chrome). Cửa sổ bảng điều khiển sẽ mở ra, và bạn có thể nhấp vào biểu tượng ba dấu chấm xếp theo chiều dọc ở phía trên cùng bên phải bảng điều khiển, sau đó chọn more tools>sensors (thêm công cụ>cảm biến). Một thẻ cảm biến sẽ xuất hiện để bạn có thể xác định vĩ độ và kinh độ cụ thể muốn chia sẻ. Bạn có thể sử dụng dữ liệu vị trí của một địa điểm nổi tiếng hoặc một vị trí nào đó giữa đại dương. Website sẽ không thể biết thực sự bạn đang ở đâu.

Bạn không những có thể giấu vị trí thực mà còn giấu được cả địa chỉ IP. Ở phần trước, tôi đã nói rằng Tor thực hiện ngẫu nhiên hóa địa chỉ IP hiển thị cho website mà bạn đang truy cập. Nhưng không phải website nào cũng chấp nhận lưu lượng Tor. Chính Facebook mãi đến gần đây mới chấp nhận. Đối với những website không chấp nhận các kết nối Tor, bạn có thể sử dụng proxy.

Một proxy mở là một máy chủ xen giữa bạn và Internet. Ở chương 2, tôi đã giải thích rằng proxy có vai trò như một người phiên dịch – bạn nói với người phiên dịch, rồi anh ta nói lại cho người nói tiếng nước ngoài nghe, nhưng nội dung thông điệp vẫn giữ nguyên. Tôi đã sử dụng từ này để nói về khả năng một người ở một quốc gia thù địch gửi cho bạn một email giả vờ là từ một quốc gia thân cận.

Bạn cũng có thể sử dụng proxy để truy cập vào các website bị giới hạn địa lý – ví dụ, trong trường hợp bạn sống ở một quốc gia giới

hạn khả năng tiếp cận Google để tìm kiếm. Hoặc có lẽ bạn phải ẩn danh để tải xuống những nội dung bất hợp pháp hoặc đã có bản quyền thông qua BitTorrent.

Tuy nhiên, proxy không phải là hoàn hảo. Khi sử dụng proxy, hãy lưu ý rằng mỗi trình duyệt phải được đặt cấu hình theo cách thủ công để trỏ đến dịch vụ proxy. Và ngay cả các website proxy tốt nhất cũng thừa nhận rằng các thủ thuật Flash hoặc JavaScript thông minh vẫn có thể phát hiện địa chỉ IP ẩn của bạn – tức địa chỉ mà bạn sử dụng để kết nối với proxy ngay từ đầu. Bạn có thể hạn chế hiệu quả của các thủ thuật này bằng cách chặn hoặc giới hạn việc sử dụng Flash và JavaScript trong trình duyệt đang dùng. Nhưng cách tốt nhất để ngăn chặn sự theo dõi của JavaScript qua trình duyệt là sử dụng plug-in HTTPS Everywhere.

Có rất nhiều dịch vụ proxy thương mại. Nhưng hãy nhớ đọc kỹ chính sách riêng tư của bất kỳ dịch vụ nào mà bạn đăng ký sử dụng. Hãy chú ý đến cách dịch vụ đó xử lý việc mã hóa dữ liệu di chuyển, đồng thời xem nó có tuân thủ pháp luật và các yêu cầu của chính phủ về thông tin hay không.

Ngoài ra còn có một số proxy miễn phí, nhưng cái giá của sự miễn phí này là vô số những quảng cáo vô dụng. Lời khuyên của tôi là hãy cẩn thận với các proxy miễn phí. Trong bài thuyết trình tại hội nghị DEF CON 20, Chema Alonso, chuyên gia an ninh và cũng là bạn tôi, đã làm thí nghiệm lập ra một proxy; vì muốn thu hút những kẻ có ý đồ xấu tìm đến với proxy này, anh cho quảng cáo địa chỉ của nó trên trang xroxy.com. Sau vài ngày đã có hơn 5.000 người sử dụng proxy "ẩn danh" miễn phí này, tuy phần lớn đều dùng nó làm công cụ lừa đảo.

Nhưng đổi lại, Alonso có thể dễ dàng sử dụng proxy miễn phí này để đẩy phần mềm độc hại vào trình duyệt của kẻ xấu và theo dõi hoạt động của họ nhờ vào khung khai thác trình duyệt BeEF. Anh cũng sử dụng một thỏa thuận cấp phép người dùng cuối (end user license agreement – EULA) mà người dùng phải chấp nhận để cho phép anh làm điều đó. Nhờ vậy, anh có thể đọc các email

gửi qua proxy này để xác định xem có lưu lượng dữ liệu nào liên quan đến hoạt động tội phạm hay không. Bài học rút ra ở đây là tiền nào của nấy.

Nếu bạn sử dụng proxy với giao thức https, cơ quan thực thi pháp luật hoặc chính phủ sẽ chỉ nhìn thấy địa chỉ IP của proxy chứ không thấy các hoạt động trên website mà bạn truy cập, vì dữ liệu này sẽ được mã hóa. Như đã nói, lưu lượng Internet http thông thường không được mã hóa; do đó bạn cũng phải sử dụng HTTPS Everywhere (vâng, đây là câu trả lời của tôi để phòng tránh hầu hết các thảm họa về trình duyệt).

Để thuận tiện, mọi người thường đồng bộ hóa cài đặt trình duyệt trên nhiều thiết bị khác nhau. Ví dụ, khi bạn đăng nhập vào trình duyệt Chrome hoặc vào một chiếc Chromebook, tất cả các đánh dấu trang, thẻ tab, lịch sử, và các tùy chọn trình duyệt khác của bạn đều được đồng bộ hóa qua tài khoản Google. Các cài đặt này sẽ được tải tự động mỗi khi bạn sử dụng Chrome, dù là trên máy tính cá nhân hay thiết bị di động. Hãy vào trang cài đặt trên trình duyệt Chrome để chọn các thông tin bạn muốn đồng bộ hóa với tài khoản của mình. Trang Dashboard (trang tổng quan) của Google cho bạn toàn quyền kiểm soát trong việc giữ lại hay loại bỏ các thông tin đã được đồng bộ hóa. Không nên đặt chế độ tự động đồng bộ hóa đối với các thông tin nhạy cảm. Firefox của Mozilla cũng có tùy chọn đồng bộ hóa.

Nhược điểm ở đây là kẻ tấn công chỉ cần dụ bạn đăng nhập vào tài khoản Google trên trình duyệt Chrome hoặc Firefox, khi đó tất cả lịch sử tìm kiếm của bạn sẽ được di chuyển sang thiết bị của chúng. Giả sử một người bạn sử dụng máy tính của bạn và đăng nhập vào trình duyệt trong máy. Lúc này, lịch sử, dấu trang,... của người bạn đó sẽ được đồng bộ hóa. Tức là giờ đây có thể xem được lịch sử lướt web cùng nhiều thông tin khác của người bạn đó trên máy tính của bạn. Ngoài ra, nếu bạn đăng nhập vào tài khoản trình duyệt được đồng bộ hóa trên thiết bị công cộng và quên đăng xuất, thì người tiếp theo sử dụng thiết bị đó sẽ thấy được hết các dấu trang và lịch sử trình duyệt của bạn. Nếu bạn

đăng nhập vào Google Chrome, thì ngay cả lịch Google, YouTube, và các khía cạnh khác trong tài khoản Google của bạn đều sẽ bị lộ. Nếu phải sử dụng thiết bị công cộng, hãy nhớ đăng xuất trước khi rời đi.

Một nhược điểm khác của đồng bộ hóa là tất cả các thiết bị được kết nối với nhau sẽ hiển thị cùng một nội dung. Nếu bạn sống một mình thì không sao. Nhưng nếu bạn dùng chung tài khoản iCloud, những chuyện dở khóc dở cười có thể xảy ra. Ví dụ, việc cha mẹ cho phép con cái sử dụng chiếc iPad chung của gia đình có thể vô tình khiến trẻ nhìn thấy các nội dung dành cho người lớn.

Trong một cửa hàng Apple ở Denver, Colorado, Elliot Rodriguez, một chuyên viên chăm sóc khách hàng đăng ký máy tính bảng mới mua với tài khoản iCloud hiện tại của mình. Ngay lập tức, trên thiết bị mới của anh đã sẵn sàng tất cả các file ảnh, tin nhắn, âm nhạc, và video mà anh đã tải về. Sự tiện lợi này giúp tiết kiệm thời gian, anh không phải sao chép và lưu các tài liệu đó vào nhiều thiết bị khác nhau theo cách thủ công nữa. Nó cũng cho phép anh truy cập vào các file này từ mọi thiết bị.

Sau đó, Elliot đưa chiếc máy tính bảng công nghệ cũ cho cô con gái tám tuổi. Việc con gái được kết nối với các thiết bị của bố cũng có một số ích lợi ban đầu. Thi thoảng, trên chiếc máy tính bảng mới, Elliot lại thấy xuất hiện thông báo về một ứng dụng mới mà con gái vừa tải về máy của mình. Cũng có khi hai bố con chia sẻ với nhau những tấm ảnh chụp gia đình. Rồi một lần, Elliot bay đến thành phố New York, nơi anh vẫn thường xuyên công tác.

Trong lúc vô tư, Elliot rút chiếc iPhone ra và chụp một vài bức ảnh ghi lại khoảnh khắc tình tứ với cô nhân tình của mình ở đây. Những bức ảnh này đã tự động đồng bộ hóa với chiếc iPad của con gái anh ở Colorado. Và tất nhiên, cô bé chạy đi hỏi mẹ xem người phụ nữ ở cùng bố là ai. Chuyện về sau thế nào chắc bạn cũng đoán được, Elliot đã gặp phải một phen điêu đứng khi trở về nhà.

Tiếp đến là những rắc rối xung quanh chuyện quà sinh nhật. Nếu bạn chia sẻ các thiết bị hoặc tài khoản đồng bộ hóa, thì dữ liệu truy cập website của bạn sẽ trở thành dấu hiệu để người nhận quà đoán được họ sắp nhận quà gì trong ngày sinh nhật. Hay tệ hơn, lẽ ra họ suýt được tặng quà gì. Vậy là chúng ta lại có thêm một lý do nữa để giải thích tại sao việc cả gia đình cùng dùng chung máy tính cá nhân hoặc máy tính bảng có thể gây ra những vấn đề liên quan đến sự riêng tư.

Một cách để tránh rắc rối trên là thiết lập người dùng khác nhau – một bước tương đối đơn giản trong Windows. Bạn hãy giữ đặc quyền quản trị viên để có thể thêm phần mềm vào hệ thống và thiết lập thêm tài khoản chung cho cả gia đình hoặc tài khoản riêng cho từng thành viên. Tất cả người dùng sẽ đăng nhập bằng mật khẩu riêng và chỉ có quyền truy cập vào nội dung, dấu trang, và lịch sử trình duyệt riêng của mình.

Apple cũng có tính năng phân chia quyền sử dụng tương tự trong các hệ điều hành OSX. Tuy nhiên, không có nhiều người nhớ đến việc phân chia không gian trong iCloud. Và đôi khi, công nghệ phản bội chúng ta không vì lý do nào cả.

Sau nhiều năm hẹn hò với một vài người, cuối cùng Dylan Monroe, một nhà sản xuất truyền hình tại Los Angeles, cũng tìm được ý trung nhân nên quyết định ổn định cuộc sống. Vị hôn phu chuyển đến ở cùng anh, và hân hoan trước cuộc sống mới, anh vô tư kết nối người vợ tương lai với tài khoản iCloud của mình.

Trước ngưỡng cửa lập gia đình mới, ai cũng muốn kết nối tất cả mọi người lại trong một tài khoản chung để chia sẻ với nhau những video, tin nhắn, và âm nhạc. Nhưng đó là việc ở thời hiện tại. Còn quá khứ của bạn được công nghệ số lưu lại thì sao?

Đôi khi, việc sử dụng dịch vụ sao lưu đám mây tự động như iCloud cũng đồng nghĩa với việc chúng ta tích lũy các file hình ảnh, tin nhắn, và âm nhạc trong suốt nhiều năm, và không khỏi có những file đã rơi vào quên lãng, như chúng ta vẫn không nhớ có gì bên trong những chiếc hộp cũ kỹ để trong nhà kho.

Những bức ảnh là thứ gần gũi nhất với kỷ niệm. Suốt bao nhiêu thế hệ nay, những người vợ, người chồng trong các gia đình đều có lúc vô tình bắt gặp những chiếc hộp giày, bên trong đựng chồng ảnh và thư từ cũ. Nhưng các phương tiện kỹ thuật số giúp bạn dễ dàng lưu hàng nghìn bức ảnh có độ phân giải cao sẽ mang đến vô vàn rắc rối mới. Đột nhiên, những kỷ niệm cũ của Dylan – trong đó có một số kỷ niệm hết sức riêng tư – quay trở về ám ảnh anh trong hình hài của những file ảnh lúc này đang nằm gọn trong iPhone và iPad của người vợ sắp cưới.

Vậy là một số đồ đạc trong nhà đành phải ra đi vì trước đây đã có những người phụ nữ khác lả lơi với anh ở chiếc ghế sofa kia, cái bàn nọ, hay chiếc giường đó. Có những nhà hàng mà vị hôn thê của anh kiên quyết không đặt chân đến vì nàng đã thấy những bức ảnh anh chụp chung với những người phụ nữ khác ở đó, bên chiếc bàn cạnh cửa sổ hay trong một góc phòng ấm cúng.

Dylan ân cần làm theo ý muốn của vị hôn thê, chấp nhận cả khi nàng yêu cầu ở anh sự hy sinh cao nhất: bán nhà ngay sau khi hai người kết hôn. Tất cả chỉ bởi vì anh đã kết nối iPhone của hai người với nhau.

Đám mây mang đến một vấn đề thú vị khác. Ngay cả khi bạn xóa lịch sử trình duyệt trên máy tính để bàn, máy tính xách tay, hay thiết bị di động, thì một bản sao lịch sử tìm kiếm của bạn vẫn còn trên đám mây. Do được lưu trữ trên máy chủ của công ty cung cấp công cụ tìm kiếm, nên lịch sử của bạn sẽ khó xóa hơn và khả năng cao là sẽ được lưu lại. Đây chỉ là một ví dụ cho thấy việc thu thập dữ liệu lén lút, bỏ qua bối cảnh thích hợp có thể dễ dàng bị hiểu sai vào một thời điểm khác về sau. Một tập hợp dữ liệu tìm kiếm vô tội và trong sáng hoàn toàn có thể bị bóp méo theo một chiều hướng khác.

Một buổi sáng cuối hè năm 2013, vài tuần sau vụ đánh bom trong cuộc đua marathon ở Boston, chồng của Michele Catalano nhìn thấy hai chiếc xe SUV màu đen đỗ trước cửa nhà họ ở Long Island. Khi anh mở cửa, các đặc vụ liên bang hỏi danh tính rồi yêu cầu lục soát nhà anh. Tuy không hiểu vì sao họ lại đến,

nhưng vì cũng không có gì để che giấu, nên anh cho phép họ vào bên trong. Sau một vòng ngó nghiêng các phòng, họ đi vào vấn đề chính.

“Trong nhà này có ai tìm kiếm thông tin về nồi áp suất không?”

“Trong nhà này có ai tìm kiếm thông tin về ba lô không?”

Có vẻ như các hoạt động tìm kiếm trực tuyến của gia đình họ qua Google đã khiến Bộ An ninh Nội địa phải thực hiện một cuộc điều tra sớm. Tuy không biết mục đích của cuộc điều tra này, nhưng người ta cũng có thể đoán được rằng trong những tuần sau vụ đánh bom trên, một số hoạt động tìm kiếm trực tuyến khi được kết hợp lại với nhau sẽ chỉ ra khả năng khủng bố, do đó chúng được gắn cờ cảnh báo. Trong vòng hai giờ, gia đình Catalano đã được minh oan. Về sau, Michele viết về sự kiện này trên tờ Medium như một lời cảnh báo rằng những gì bạn tìm kiếm ngày hôm nay có thể quay trở lại ám ảnh bạn vào ngày mai.

Trong bài viết của mình, Catalano cho rằng có lẽ các nhà điều tra đã bỏ qua những nội dung tìm kiếm khác của cô như, “Tôi có thể làm cái quái gì với hạt diêm mạch?” và “A-Rod[56] đã bị treo giò chưa?” Cô tìm kiếm thông tin về nồi áp suất chẳng qua chỉ để tìm hiểu cách nấu hạt diêm mạch. Còn chuyện chiếc ba lô thì sao? Chồng cô muốn có một chiếc.

[56] A-Rod: Biệt danh của Alexander Emmanuel Rodriguez, cầu thủ bóng chày của Mỹ.

Ít nhất một công ty công cụ tìm kiếm là Google đã tạo ra một số công cụ bảo mật cho phép bạn chỉ định những thông tin bạn đồng ý giữ lại. Chẳng hạn, bạn có thể tắt tính năng theo dõi quảng cáo cá nhân hóa để khi tìm kiếm thông tin về Patagonia (một vùng ở Nam Mỹ), bạn sẽ không thấy những quảng cáo về du lịch Nam Mỹ. Bạn cũng có thể tắt toàn bộ lịch sử tìm kiếm của mình. Hoặc bạn có thể không đăng nhập vào Gmail, YouTube hay bất kỳ tài khoản Google nào trong khi tìm kiếm trực tuyến.

Ngay cả khi bạn không đăng nhập vào tài khoản Microsoft,

Yahoo, hay Google, thì địa chỉ IP của bạn vẫn bị ràng buộc với từng yêu cầu bạn gõ trong công cụ tìm kiếm. Để tránh điều này, bạn có thể sử dụng startpage.com hoặc DuckDuckGo.

DuckDuckGo hiện đã là một tùy chọn mặc định trong Firefox và Safari. Khác với Google, Yahoo, và Microsoft, DuckDuckGo không cung cấp tài khoản người dùng, và công ty này cho biết họ không lưu lại địa chỉ IP của người dùng. DuckDuckGo cũng vận hành nút thoát ra của Tor, có nghĩa là bạn có thể tìm kiếm DuckDuckGo trong khi sử dụng Tor mà không bị trễ mạng.

Vì DuckDuckGo không theo dõi hoạt động của bạn nên kết quả tìm kiếm của bạn sẽ không được lọc qua các nội dung tìm kiếm trước kia. Hầu hết mọi người không nhận ra điều này, nhưng các kết quả bạn thấy trong Google, Yahoo, và Bing đều được lọc dựa theo mọi thứ mà bạn từng tìm kiếm trên đó trong quá khứ. Ví dụ, nếu thấy bạn muốn tìm kiếm website liên quan đến các vấn đề về sức khỏe, công cụ tìm kiếm sẽ tiến hành lọc và đẩy các kết quả liên quan đến sức khỏe lên đầu. Tại sao? Bởi vì rất ít người trong chúng ta nhấp chuột mở sang trang thứ hai trong kết quả tìm kiếm. Có một câu chuyện vui trên Internet nói rằng nơi tốt nhất để giấu xác chết là trang thứ hai trong kết quả tìm kiếm.

Một số người có thể thích sự thuận tiện khi không phải cuộn chuột qua các kết quả tìm kiếm không liên quan, nhưng việc này cũng đồng thời hỗ trợ cho công cụ tìm kiếm ra quyết định về những gì bạn có thể quan tâm hoặc không quan tâm. DuckDuckGo cũng trả về các kết quả tìm kiếm có liên quan, nhưng được lọc theo chủ đề chứ không theo lịch sử tìm kiếm trước đây của bạn.

Trong chương tiếp theo, tôi sẽ nói chi tiết về các biện pháp được các website sử dụng nhằm ngăn cản bạn ẩn mình trước chúng và bạn có thể làm gì để lướt web ẩn danh.

Chương 6: BẠN BỊ THEO DÕI Ở TỪNG CÚ NHẤP CHUỘT

Hãy hết sức cẩn trọng với những gì bạn tìm kiếm trên Internet. Không chỉ công cụ tìm kiếm mà mọi website bạn truy cập cũng đang theo dõi các thói quen trực tuyến của bạn. Và bạn sẽ thấy lẽ ra một số website không nên tiết lộ các vấn đề cá nhân cho người khác thấy. Ví dụ, một báo cáo năm 2015 cho thấy rằng "70% URL của các website về sức khỏe chứa thông tin tiết lộ chi tiết về bệnh, tình trạng, và biện pháp điều trị."

Nói cách khác, nếu tôi truy cập vào website y tế WebMD và tìm kiếm về "nấm da chân," thì cụm từ nấm da chân không mã hóa sẽ xuất hiện trong URL hiển thị trên thanh địa chỉ ở trình duyệt của tôi. Điều đó có nghĩa là tất cả – từ trình duyệt, nhà cung cấp Internet, cho đến nhà mạng điện thoại của tôi – đều biết tôi tìm kiếm thông tin về nấm da chân. HTTPS Everywhere sẽ mã hóa nội dung của website mà bạn truy cập – giả dụ website đó hỗ trợ https – nhưng nó không mã hóa URL. Đến Tổ chức Biên giới điện tử cũng phải đưa ra lời cảnh báo rằng https không được thiết kế để che giấu thông tin nhận dạng của các website mà bạn truy cập.

Thêm vào đó, nghiên cứu trên còn chỉ ra rằng 91% các website liên quan tới sức khỏe thực hiện tham vấn tới các bên thứ ba. Các tham vấn này được nhúng trong bản thân các website, và chúng gọi về những hình ảnh tí hon (hiển thị hoặc không hiển thị trên trang trình duyệt) làm nhiệm vụ thông báo cho các website bên thứ ba rằng bạn đang truy cập một website cụ thể nào đó. Khi bạn tìm kiếm "nấm da chân," có đến 20 đối tượng khác nhau – từ công ty dược cho tới Facebook, Pinterest, Twitter, và Google – sẽ được liên hệ ngay khi kết quả tìm kiếm xuất hiện trên trình duyệt của bạn. Lúc này, tất cả các bên thứ ba đó đều biết bạn đang tìm kiếm thông tin về nấm da chân.

Họ sử dụng thông tin này để hiển thị quảng cáo trực tuyến cho

bạn. Ngoài ra, nếu bạn đăng nhập vào website trên, họ còn có thể lấy được địa chỉ email của bạn nữa. Thật may, tôi có thể giúp bạn ngăn chặn họ tìm hiểu thêm về bạn. Trên các website về sức khỏe được phân tích trong nghiên cứu trên, mười bên thứ ba hàng đầu là Google, comScore, Facebook, AppNexus, AddThis, Twitter, Quantcast, Amazon, Adobe, và Yahoo – trong đó có một số, như comScore, AppNexus, và Quantcast, thực hiện đo lường lưu lượng website như Google. Cũng trong số trên, Google, Facebook, Twitter, Amazon, Adobe, và Yahoo do thám hoạt động của bạn nhằm mục đích thương mại, chẳng hạn hiển thị quảng cáo về các phương pháp chữa nấm bàn chân trong các phiên tìm kiếm sau này của bạn.

Nghiên cứu này còn nhắc đến các bên thứ ba Experian và Axiom, vốn chỉ đơn thuần là các kho dữ liệu (data warehouse), thu thập tối đa dữ liệu về một người. Rồi họ bán dữ liệu đó. Bạn có nhớ các câu hỏi bảo mật và câu trả lời sáng tạo mà tôi khuyên dùng không? Thường thì các công ty như Experian và Axiom thu thập, cung cấp, và sử dụng các câu hỏi bảo mật đó để xây dựng thành những hồ sơ trực tuyến giá trị cho các nhà tiếp thị muốn nhắm mục tiêu đến phân khúc khách hàng phù hợp.

Chuyện này diễn ra như thế nào?

Dù bạn gõ tay URL hay sử dụng công cụ tìm kiếm, mọi website trên Internet đều có hostname[57]và địa chỉ IP bằng số (một số website chỉ tồn tại dưới dạng địa chỉ số). Nhưng bạn hầu như không bao giờ thấy địa chỉ bằng số này. Trình duyệt sẽ ẩn nó đi và sử dụng dịch vụ tên miền (DNS) để dịch hostname của website thành địa chỉ cụ thể, ví dụ Google thành https://74.125.224.72/.

[57] Hostname: Cụm ký tự gán cho một thiết bị kết nối với mạng máy tính, dùng để xác định thiết bị đó trong các hình thức liên lạc điện tử khác nhau, như mạng diện rộng World Wide Web.

DNS giống như danh bạ điện thoại toàn cầu, tham chiếu chéo hostname với địa chỉ số của máy chủ cung cấp website mà bạn yêu cầu. Khi bạn gõ chữ “Google.com” vào trình duyệt, DNS sẽ

liên hệ với máy chủ của họ tại https://74.125.224.72. Sau đó, bạn sẽ thấy màn hình màu trắng quen thuộchiện ra, với biểu tượng Google Doodle[58] trong ngày bên trên một trường tìm kiếm trống. Về lý thuyết, mọi trình duyệt web đều hoạt động theo cách này. Nhưng trên thực tế có nhiều điều để nói hơn.

[58] Google Doodle: Biểu tượng đặc biệt, thay thế tạm thời cho biểu tượng trên trang chủ của Google để chào mừng các ngày lễ, sự kiện, nhân vật…

Sau khi đã được xác định thông qua địa chỉ số, website sẽ gửi thông tin trở lại trình duyệt web của bạn để "xây dựng" nên website mà bạn nhìn thấy. Khi trang được trả về trình duyệt, bạn sẽ thấy các phần tử theo đúng kỳ vọng của mình – các thông tin mà bạn muốn truy xuất, mọi hình ảnh có liên quan, và các cách để điều hướng đến những phần khác của website. Nhưng thông thường, một số phần tử được trả về trình duyệt lại gọi tới các website khác để yêu cầu thêm hình ảnh hoặc tập lệnh. Một số – nếu không phải là tất cả – tập lệnh này phục vụ cho mục đích theo dõi, và hầu hết là bạn không cần đến chúng.

Gần như mọi công nghệ kỹ thuật số đều tạo ra siêu dữ liệu, và các trình duyệt cũng không phải là ngoại lệ. Trình duyệt có thể tiết lộ thông tin về cấu hình máy tính của bạn nếu bị website mà bạn đang truy cập truy vấn – ví dụ, bạn đang sử dụng trình duyệt và hệ điều hành nào, phiên bản bao nhiêu; trình duyệt đó có những tiện ích bổ sung nào; và trong khi tìm kiếm, bạn chạy những chương trình nào khác trên máy tính (chẳng hạn các sản phẩm của Adobe). Nó thậm chí còn có thể tiết lộ thông tin chi tiết về phần cứng máy tính của bạn, chẳng hạn độ phân giải màn hình và dung lượng bộ nhớ tích hợp. Khi đọc tới đây, có thể bạn sẽ yên chí rằng mình đã có những bước tiến lớn trong việc trở thành vô hình trên mạng. Vâng, đúng là như vậy. Nhưng vẫn còn việc phải làm đấy.

Hãy dành chút thời gian vào trang Panopticlick.com. Đây là website do Tổ chức Biên giới Điện tử xây dựng, có thể chỉ ra mức

độ phổ biến trong cách cài đặt cấu hình trên trình duyệt của bạn so với người khác dựa trên những gì đang được chạy trên hệ điều hành và các plugin trong thiết bị. Nói cách khác, bạn có plugin nào có thể dùng để giới hạn hoặc bảo vệ các thông tin mà Panopticlick có thể thu thập được từ trình duyệt của bạn hay không?

Nếu trong kết quả kiểm tra nhận về từ Panopticlick, thông số ở bên tay trái có giá trị lớn – ví dụ sáu chữ số – thì trường hợp của bạn là tương đối độc đáo, vì tỉ lệ gặp được cấu hình trình duyệt của bạn là chưa đến 1 trong 100.000 máy tính. Xin chúc mừng. Tuy nhiên, nếu thông số này thấp – ví dụ dưới ba chữ số – thì cấu hình trình duyệt của bạn là khá phổ biến với tỉ lệ gặp là 1 trong một vài trăm máy tính. Điều đó có nghĩa là nếu muốn nhắm mục tiêu vào bạn – để cung cấp quảng cáo hay phần mềm độc hại – tôi sẽ không phải mất nhiều công sức, vì bạn có cấu hình trình duyệt rất phổ biến.

Có thể bạn nghĩ rằng cấu hình phổ biến sẽ giúp bạn trở nên vô hình, vì bạn là một phần của đám đông, bạn lẫn trong đám đông. Nhưng từ góc độ kỹ thuật, điều này sẽ khiến bạn dễ trở thành đối tượng tấn công của những hoạt động ác ý. Hacker tội phạm không muốn tốn nhiều công sức. Nếu một ngôi nhà để cửa mở còn nhà bên cạnh khóa cửa, bạn nghĩ kẻ trộm sẽ đột nhập vào đâu? Nếu hacker tội phạm biết bạn có cấu hình phổ biến, thì có lẽ bạn cũng thiếu một số biện pháp bảo vệ để tăng cường an ninh.

Tôi biết, tôi vừa nhảy cóc từ chỗ đang nói đến chuyện các nhà tiếp thị muốn theo dõi hoạt động trực tuyến của bạn sang bàn chuyện hacker tội phạm sử dụng thông tin cá nhân để đánh cắp nhận dạng của bạn. Hai vấn đề này là rất khác nhau. Nhà tiếp thị thu thập thông tin để tạo quảng cáo giúp mang lại lợi nhuận cho các website. Nếu không có quảng cáo, một số website sẽ không thể tiếp tục tồn tại. Tuy nhiên, giới tiếp thị, hacker tội phạm, và cả chính phủ đều tìm cách lấy được những thông tin mà bạn có thể không muốn cung cấp, và tất cả thường tham gia sôi nổi vào các cuộc tranh luận về sự xâm phạm quyền riêng tư.

Một cách giúp bạn vừa là một phần của số đông vừa ngăn chặn được hoạt động nghe trộm trực tuyến là sử dụng máy ảo (virtual machine – VM) – đây là một hệ điều hành như Mac OSX chạy trên hệ điều hành Windows ở cương vị phần mềm khách. Bạn có thể cài đặt VMware trên máy tính và dùng nó để chạy một hệ điều hành khác. Khi xong việc, bạn chỉ cần tắt nó đi. Hệ điều hành này và mọi thứ bạn đã làm trong đó sẽ biến mất. Tuy nhiên, các file mà bạn lưu lại vẫn sẽ ở nguyên tại vị trí mà bạn đã lưu.

Tuy nhiên, một điều cần cảnh giác ở đây là các nhà tiếp thị cũng như hacker tội phạm đều biết thông tin về khách truy cập website thông qua file hình ảnh 1 pixel, hay còn gọi là bọ web (web bug). Giống như một cửa sổ pop-up[59] trống trên trình duyệt, đây là một hình ảnh có kích cỡ 1 x 1 pixel được đặt ở đâu đó trên một website, và tuy vô hình nhưng truy vấn lại cho website của bên thứ ba đã đặt nó ở đó. Máy chủ đầu cuối ghi lại địa chỉ IP đã cố gắng hiển thị hình ảnh đó. Hình ảnh 1 pixel đặt ở một website về sức khỏe có thể thông báo cho một hãng dược phẩm biết rằng tôi quan tâm đến các cách chữa trị nấm da chân.

[59] Cửa sổ pop-up (pop-up window): Cửa sổ đột nhiên xuất hiện (pop-up) khi bạn ấn vào một phím chức năng nào đó.

Nghiên cứu năm 2015 mà tôi nhắc tới từ đầu chương này phát hiện ra rằng gần một nửa các truy vấn của bên thứ ba chỉ hiển thị các cửa sổ pop-up không chứa bất kỳ nội dung nào. Các cửa sổ "trống" này âm thầm tạo ra các truy vấn http tới máy chủ của bên thứ ba vốn chỉ dùng cho mục đích theo dõi. Bạn có thể tránh điều này bằng cách đặt lệnh yêu cầu trình duyệt không cho phép hiển thị cửa sổ pop-up (và điều này cũng sẽ loại bỏ những quảng cáo phiền toái đó).

Theo nghiên cứu trên, gần một phần ba số truy vấn còn lại của bên thứ ba có chứa các dòng mã nhỏ, các file JavaScript, vốn chỉ thực thi các hình động trên website. Thông thường, website có thể xác định được máy tính truy cập vào nó bằng cách đọc địa chỉ IP đang yêu cầu file JavaScript.

Ngay cả khi không có hình ảnh 1 pixel hay cửa sổ pop-up trống, hoạt động lướt web của bạn vẫn có thể bị theo dõi bởi các website mà bạn truy cập. Ví dụ, Amazon có thể biết rằng lần gần đây nhất bạn truy cập một website về sức khỏe, vì vậy website Amazon sẽ hiển thị đề xuất cho bạn là các sản phẩm chăm sóc sức khỏe. Có thể Amazon biết thông tin này là do nó đã thực sự nhìn thấy website mà bạn truy cập gần đây nhất trong truy vấn trình duyệt của bạn.

Amazon thực hiện điều này bằng cách sử dụng các referrer bên thứ ba – tức là dữ liệu trong một truy vấn gọi website thông báo cho trang mới biết truy vấn này bắt nguồn từ đâu. Ví dụ, nếu tôi đang đọc một bài viết trên tạp chí Wired và nó chứa một liên kết, khi tôi nhấp vào liên kết đó, website mới sẽ biết rằng trước đó tôi đã ở trên một trang thuộc Wired.com. Bạn có thể thấy hoạt động theo dõi của bên thứ ba này có thể ảnh hưởng đến quyền riêng tư của mình như thế nào chưa?

Để tránh điều này, hãy vào Google.com trước tiên, như thế website mà bạn muốn truy cập sẽ không biết trước đó bạn ở đâu. Tôi không cho rằng referrer bên thứ ba là một vấn đề lớn, trừ khi bạn đang cần che giấu danh tính. Đây là một ví dụ nữa về sự đánh đổi giữa cái tiện lợi (chỉ cần truy cập vào website tiếp theo) và tính ẩn danh (luôn bắt đầu từ Google.com).Plugin NoScript của Firefox là một trong những cơ chế phòng thủ tốt nhất chống lại hoạt động theo dõi của bên thứ ba. Tiện ích bổ sung này ngăn chặn hiệu quả gần như mọi thứ bị coi là có hại cho máy tính và trình duyệt của bạn, cụ thể là Flash và JavaScript. Việc thêm các plugin bảo mật sẽ mang đến cho bạn một trải nghiệm khác khi lướt web của bạn, tuy nhiên, bạn có thể chọn và kích hoạt các tính năng cụ thể hoặc đặt chế độ tin tưởng vĩnh viễn một số website.

Khi bật NoScript, website bạn truy cập sẽ không có quảng cáo và referrer của bên thứ ba. Hệ quả của việc chặn này là trang web trông có phần xấu và tẻ nhạt hơn so với phiên bản không có NoScript. Tuy nhiên, nếu muốn xem một video flash, bạn có thể

cho phép hiển thị video đó trong khi vẫn tiếp tục chặn mọi phần tử khác. Hoặc, nếu cảm thấy tin tưởng một website, bạn có thể cho phép – tạm thời hoặc vĩnh viễn – tải tất cả các phần tử trên trang đó; chẳng hạn, bạn có thể đặt cơ chế này với các website ngân hàng.

Chrome cũng có ScriptBlock để ngăn chặn việc sử dụng các tập lệnh trên website. Đây là một tính năng hữu ích đối với trẻ nhỏ, bởi trong lúc vào mạng, có thể chúng truy cập vào một website cho phép hiển thị các nội dung quảng cáo pop-up dành cho người lớn.

Việc chặn các phần tử có khả năng gây hại (và chắc chắn là xâm phạm quyền riêng tư) trên các website sẽ giúp máy tính của bạn không bị nhiễm các phần mềm độc hại tạo quảng cáo. Chẳng hạn, có lẽ bạn từng thấy quảng cáo xuất hiện trên trang chủ Google của mình. Thực ra, trang chủ Google không có quảng cáo nào cả. Nếu bạn thấy chúng, thì có lẽ máy tính và trình duyệt của bạn đã bị tấn công (có thể là mới giây lát trước đó), nên bạn mới thấy quảng cáo của bên thứ ba, và chúng có thể chứa các Trojan horse[60] – chẳng hạn các keylogger[61] ghi lại mọi phím mà bạn gõ, và nhiều phần mềm độc hại khác – nếu bạn nhấn vào. Ngay cả khi quảng cáo không chứa phần mềm độc hại, nhà quảng cáo vẫn được tính doanh thu dựa trên số lần nhấp chuột mà họ nhận được. Càng nhiều người bị lừa nhấp chuột, họ càng kiếm được nhiều tiền hơn.

[60] Trojan horse (ngựa thành Troy): Tên gọi một loại phần mềm độc hại.

[61] Keylogger: Một dạng phần mềm theo dõi mà khi được cài đặt vào một hệ thống, có thể ghi lại mọi hoạt động gõ phím thực hiện trên phần mềm đó.

Tuy hiệu quả, song NoScript và ScriptBlock không thể chặn được mọi thứ. Để có sự bảo vệ hoàn toàn trước các mối đe dọa đến từ trình duyệt, hãy cài đặt Adblock Plus. Vấn đề duy nhất ở đây là Adblock ghi lại mọi thứ: công ty này cũng theo dõi lịch sử lướt

web của bạn, dù rằng bạn sử dụng tính năng duyệt web riêng tư. Tuy nhiên, trong trường hợp này, mặt tốt (ngăn chặn các quảng cáo tiềm ẩn nguy hiểm) trội hơn so với mặt xấu (họ biết bạn ở đâu trên mạng).

Một plugin hữu ích khác là Ghostery, dùng được cho cả Chrome và Firefox. Ghostery nhận diện tất cả các chương trình theo dõi lưu lượng web (như DoubleClick và Google AdSense) mà các website sử dụng để theo dõi hoạt động của bạn. Giống như NoScript, Ghostery cho bạn quyền kiểm soát chi tiết đối với từng trình theo dõi mà bạn muốn cho phép hoạt động trên mỗi trang. Website của plugin này viết, "Việc chặn trình theo dõi là để chúng không chạy trong trình duyệt của bạn, nhờ đó kiểm soát được hoạt động theo dõi dữ liệu hành vi của bạn. Hãy nhớ rằng một số trình theo dõi có thể hữu ích, chẳng hạn như các tiện ích nguồn cấp dữ liệu trên mạng xã hội hoặc các trò chơi trên trình duyệt. Việc chặn có thể mang lại những tác động ngoài ý muốn đối với các website mà bạn truy cập." Có nghĩa là khi cài đặt Ghostery, một số website sẽ không còn hoạt động được. Thật may, bạn có thể chọn tắt plugin này theo từng trang.

Ngoài việc sử dụng plugin để ngăn các website nhận ra mình, bạn cũng có thể tung hỏa mù cho hacker bằng cách sử dụng nhiều địa chỉ email khác nhau dùng cho các mục đích cá nhân. Ví dụ, ở Chương 2, tôi đã hướng dẫn các cách tạo tài khoản email ẩn danh để liên lạc mà không bị phát hiện. Tương tự, đối với hoạt động lướt web đơn giản hằng ngày, bạn cũng nên tạo nhiều tài khoản email – mục đích ở đây không phải để ẩn danh mà nhằm bớt thu hút sự chú ý của các bên thứ ba trên Internet. Việc có nhiều hồ sơ cá nhân trực tuyến sẽ làm giảm bớt tác động đối với quyền riêng tư so với việc chỉ có một địa chỉ có thể nhận dạng được. Nó sẽ gây khó khăn cho bất kỳ ai muốn xây dựng hồ sơ trực tuyến về bạn.

Giả sử bạn muốn mua đồ trên mạng. Hãy tạo một địa chỉ email dành riêng cho việc mua sắm. Đừng dùng địa chỉ nhà mà hãy dùng địa chỉ hòm thư để đăng ký nhận các món đồ bạn mua bằng

email này. Ngoài ra, thi thoảng bạn có thể tải thẻ quà tặng để mua hàng.

Bằng cách này, công ty bán sản phẩm cho bạn sẽ chỉ có địa chỉ email không chính thức, địa chỉ nhận không chính thức, và thẻ quà tặng dùng một lần của bạn. Nếu dữ liệu của công ty đó bị xâm phạm, ít nhất kẻ tấn công sẽ không có địa chỉ email thực, địa chỉ nhà thực, hay số thẻ tín dụng của bạn. Cách chặt đứt sợi dây liên hệ với hoạt động mua hàng trực tuyến như thế này là một biện pháp an ninh hữu hiệu.

Bạn cũng nên tạo một địa chỉ email không chính thức khác để dùng cho các mạng xã hội. Có thể lấy đây là địa chỉ email "công khai" để liên lạc với người lạ hoặc người quen sơ. Lợi thế của việc này là, một lần nữa, mọi người sẽ không biết được nhiều thông tin về bạn. Ít nhất là không biết theo cách trực tiếp. Bạn có thể làm thêm động tác bảo vệ nữa là đặt tên người dùng riêng cho từng địa chỉ không chính thức, có thể là một biến thể khác trong tên gọi thực của bạn hay một tên khác hoàn toàn.

Hãy cẩn thận nếu bạn chọn phương án sử dụng biến thể tên thực. Đừng dùng tên đệm – hay nếu bạn thường dùng tên đệm thì đừng dùng họ. Ngay cả một thông tin vô hại như JohnQDoe@xyz.com cũng có thể tiết lộ rằng bạn có tên đệm và tên đệm đó bắt đầu bằng chữ Q. Đây là một ví dụ về việc cung cấp thông tin cá nhân khi không cần thiết. Hãy nhớ rằng ở đây mục đích của bạn là hòa mình vào môi trường chứ không phải kêu gọi sự chú ý về mình.

Nếu bạn sử dụng một từ hoặc cụm từ không liên quan đến tên mình, hãy làm sao để nó tiết lộ càng ít thông tin về bạn càng tốt. Nếu địa chỉ email của bạn là snowboarder@xyz.com, chúng tôi có thể không biết bạn tên gì, nhưng ít nhất chúng tôi biết một sở thích của bạn[62]. Tốt hơn hết, hãy chọn một tên chung chung, như silverfox@xyz.com[63].

[62] Snow boarder: Nghĩa là người trượt tuyết.

[63] Silver fox: Cáo bạc.

Tất nhiên, bạn cũng nên có một địa chỉ email cá nhân, nhưng hãy chỉ chia sẻ nó với bạn bè thân thiết và gia đình. Nhưng các phương pháp an toàn nhất thường đi kèm với những phần thưởng tốt đẹp: bạn sẽ thấy rằng việc không sử dụng địa chỉ email cá nhân để mua hàng trực tuyến sẽ giúp bạn chặn được hàng tấn thư rác.

Điện thoại di động cũng không miễn nhiễm khỏi sự theo dõi của các công ty. Mùa hè năm 2015, một nhà nghiên cứu tinh mắt đã phát hiện ra rằng hai hãng viễn thông AT&T và Verizon cài thêm mã vào mọi truy vấn website thực hiện qua trình duyệt trên thiết bị di động. Đây không phải là IMSI – số nhận dạng thuê bao di động quốc tế – như tôi đã bàn đến trong Chương 3, mà là một mã nhận dạng duy nhất được gửi kèm với mỗi truy vấn website, gọi là tiêu đề nhận dạng duy nhất (unique identifier header – UIDH). Đây là số sê-ri tạm thời mà nhà quảng cáo có thể dùng để nhận ra bạn trên web. Nhà nghiên cứu trên phát hiện ra điều đó khi ông cài đặt cấu hình điện thoại di động để ghi lại tất cả các lưu lượng web (không nhiều người thực hiện việc này). Sau đó, ông nhận thấy có dữ liệu bổ sung gắn vào khách hàng của Verizon và AT&T.

Vấn đề nằm ở chỗ khách hàng không được thông báo về đoạn mã bổ sung này. Chẳng hạn, những người sử dụng AT&T hoặc Verizon khi tải xuống ứng dụng Firefox dành cho thiết bị di động và dùng plugin để tăng cường sự riêng tư sẽ bị các mã UIDH này theo dõi.

Nhờ các mã UIDH này, Verizon và AT&T có thể thu thập được thông tin về lưu lượng truy cập liên kết với các truy vấn web của bạn và dùng nó để xây dựng hồ sơ về hoạt động trực tuyến qua thiết bị di động của bạn nhằm phục vụ mục đích quảng cáo trong tương lai hoặc đơn giản là bán dữ liệu thô cho các bên khác.

Hiện nay, AT&T đã tạm ngừng hoạt động đó. Verizon thì đưa nó trở thành một tùy chọn cho người dùng cuối cài đặt cấu hình. Xin

lưu ý: nếu không chọn không tham gia, nghĩa là bạn đồng ý để Verizon tiếp tục. Ngay cả khi bạn đã tắt JavaScript, các website vẫn có thể chuyển một file văn bản có dữ liệu gọi là http cookie trở lại trình duyệt của bạn. Cookie này có thể được lưu trữ trong một thời gian dài. Thuật ngữ cookie là cách gọi ngắn gọn của magic cookie, chỉ một đoạn văn bản được gửi đi từ một website và được lưu trữ trong trình duyệt của người dùng để theo dõi, chẳng hạn các món đồ trong giỏ hàng, hoặc thậm chí để xác thực người dùng. Cookie được Netscape[64] sử dụng lần đầu tiên trên web với ý định ban đầu là hỗ trợ tạo ra giỏ hàng ảo và các chức năng thương mại điện tử. Cookie thường được lưu trữ trong trình duyệt trên máy tính cá nhân truyền thống và có ngày hết hạn, nhưng thời hạn này có thể là hàng thập niên trong tương lai.

[64] Netscape: Tên một hãng viễn thông của Mỹ, xây dựng nên Netscape, một trong những trình duyệt web ban đầu, về sau được hãng AOL mua lại vào năm 1999.

Cookie có nguy hiểm không? Không, ít nhất là bản thân chúng thì không nguy hiểm. Tuy nhiên, cookie có thể cung cấp cho bên thứ ba thông tin về tài khoản và các sở thích cụ thể của bạn, chẳng hạn thành phố yêu thích của bạn trên một website thời tiết hoặc hãng hàng không yêu thích của bạn trên một website du lịch. Lần tiếp theo khi trình duyệt của bạn kết nối với website đó, nếu đã tồn tại cookie, website sẽ nhớ bạn và có thể nói, “Xin chào, người quen.” Và nếu đó là website thương mại, nó cũng có thể nhớ một số lần mua hàng gần nhất của bạn.

Cookie không thực sự lưu trữ thông tin này trên máy tính cá nhân hoặc thiết bị di động của bạn. Giống như điện thoại di động dùng IMSI làm proxy, cookie chứa proxy cho dữ liệu lưu ở phần backend[65] của website. Khi trình duyệt tải một website đính kèm cookie, dữ liệu bổ sung được kéo ra từ website đó sẽ liên quan cụ thể đến bạn.

[65] Front-end và back-end (trong kỹ thuật phần mềm): Front-end là phần tương tác trực tiếp với người dùng (hệ thống các giao

diện người dùng và lập trình phía người dùng), back-end là phần lập trình trên máy chủ, gồm có các thành phần để xử lý thông tin từ front-end.

Cookie không chỉ lưu trữ các tùy chọn cá nhân của bạn ở trang web mà còn cung cấp các dữ liệu theo dõi có giá trị cho trang web nơi chúng bắt nguồn. Ví dụ, nếu bạn là khách hàng tiềm năng của một công ty và trước đây bạn từng nhập địa chỉ email hay các thông tin khác để tải xuống một file tài liệu, thì khả năng cao là trong trình duyệt của bạn có cookie cho website của công ty đó làm nhiệm vụ khớp thông tin về bạn trong một hệ thống quản lý hồ sơ khách hàng (CRM) – ví dụ như Salesforce hoặc HubSpot – ở phần back-end. Từ nay, mỗi khi bạn truy cập website của công ty đó, bạn sẽ được nhận diện thông qua cookie trong trình duyệt của bạn, và phiên truy cập đó sẽ được ghi lại trong CRM.

Cookie được phân đoạn, nghĩa là website A không thể xem nội dung của cookie cho website B. Cũng có ngoại lệ, nhưng thông thường các thông tin được giữ riêng biệt và tương đối bảo mật. Tuy nhiên, từ góc độ riêng tư mà nói, cookie không khiến bạn thật sự trở nên vô hình.

Bạn chỉ có thể truy cập các cookie trong cùng một tên miền, tức một tập hợp tài nguyên được gán cho một nhóm người cụ thể. Các hãng quảng cáo khắc phục hạn chế này bằng cách tải cookie có thể theo dõi hoạt động của bạn trên một số website vốn thuộc về mạng lưới rộng hơn của họ. Mặc dù vậy, nhìn chung cookie của website này không thể tiếp cận cookie của website khác. Các trình duyệt hiện đại có thể giúp người dùng kiểm soát cookie. Ví dụ: nếu bạn lướt web bằng tính năng duyệt web ẩn danh hoặc riêng tư, trình duyệt sẽ không lưu lại lịch sử truy cập website, và bạn cũng sẽ không có cookie mới cho phiên hoạt động đó. Nhưng nếu bạn đã có cookie từ phiên truy cập trước, thì cookie vẫn sẽ được áp dụng ở chế độ riêng tư. Mặt khác, nếu sử dụng tính năng duyệt web bình thường, thi thoảng bạn phải xóa bằng thao tác thủ công một số hoặc tất cả các cookie đã tích lũy được qua nhiều năm.

Xin lưu ý, không nên xóa tất cả cookie. Để xóa bỏ dấu vết cá nhân trên Internet, bạn có thể chọn xóa các cookie liên quan đến những lượt truy cập một lần vào các website bạn không thực sự quan tâm đến. Chẳng hạn, các website mà bạn truy cập lại sẽ không thể nhìn thấy bạn. Nhưng đối với một số website, chẳng hạn website thời tiết, việc phải nhập mã bưu chính mỗi lần truy cập sẽ trở nên phiền hà trong khi chỉ cần duy trì một cookie đơn giản là đủ.

Để xóa cookie, bạn có thể dùng tiện ích bổ sung hoặc vào phần cài đặt hay tùy chọn của trình duyệt, ở đó thường có tùy chọn xóa một hoặc nhiều (thậm chí là tất cả) cookie.

Một số nhà quảng cáo sử dụng cookie để theo dõi thời gian bạn ở lại trên các website mà họ đặt quảng cáo. Một số thậm chí còn ghi lại lượt truy cập của bạn vào các website trước đó, gọi là website referrer (website tham chiếu). Bạn nên xóa các cookie này ngay lập tức. Có thể dễ dàng nhận ra chúng vì tên của chúng không chứa tên của các website bạn đã truy cập. Ví dụ, thay vì "CNN," một cookie referrer lại có tên là "Ad321." Bạn cũng có thể nghĩ đến chuyện sử dụng công cụ phần mềm làm sạch cookie, chẳng hạn công cụ trên piriform.com/ccleaner, để giúp quản lý cookie dễ dàng hơn.

Tuy nhiên, có một số cookie không chịu ảnh hưởng bởi bất kỳ quyết định nào bạn đưa ra ở phía trình duyệt. Đây được gọi là siêu cookie, vì chúng tồn tại trên máy tính của bạn, tức là bên ngoài trình duyệt. Siêu cookie truy cập các tùy chọn và dữ liệu theo dõi của website bất kể bạn sử dụng trình duyệt nào (ngày hôm nay là Chrome, ngày mai là Firefox). Và bạn nên xóa siêu cookie khỏi trình duyệt, bởi nếu không, vào lần tới khi trình duyệt truy cập website đó, máy tính cá nhân truyền thống của bạn sẽ tìm cách tạo lại cookie http từ bộ nhớ.

Có hai siêu cookie chạy bên ngoài trình duyệt mà bạn có thể xóa: Flash của Adobe, và Silverlight của Microsoft. Hai siêu cookie này không có thời hạn tồn tại. Và nhìn chung, việc xóa chúng là khá an toàn.

Nhưng còn một cookie khác, mạnh nhất trong tất cả các cookie. Samy Kamkar, từng nổi tiếng với sâu Samy phát tán nhanh chóng khắp trang mạng xã hội MySpace, đã tạo ra Evercookie, một cookie có sức sống bền bỉ. Kamkar đạt được sự bền bỉ ấy bằng cách lưu dữ liệu cookie ở rất nhiều hệ thống lưu trữ của các trình duyệt trong hệ điều hành Windows. Chỉ cần một trong những trang lưu trữ vẫn còn nguyên vẹn, Evercookie sẽ tìm cách khôi phục cookie ở mọi nơi khác. Vì vậy, chỉ xóa một Evercookie khỏi bộ nhớ cache lưu trữ cookie của trình duyệt là chưa đủ. Giống như trò chơi đập chuột của trẻ em, các Evercookie sẽ liên tục xuất hiện. Để giành phần thắng, bạn phải xóa chúng hoàn toàn khỏi thiết bị của mình.Nếu lấy số lượng cookie có thể tồn tại trên trình duyệt nhân với số lượng các vùng lưu trữ trên thiết bị, có thể bạn sẽ mất gần cả ngày chỉ để xóa cookie.

Không chỉ các website và các nhà mạng di động muốn theo dõi hoạt động trực tuyến của bạn. Facebook đã trở nên phổ biến khắp nơi – và đây là một nền tảng vượt ra ngoài phạm vi mạng truyền thông xã hội đơn thuần. Bạn có thể đăng nhập vào Facebook rồi sử dụng phiên đăng nhập Facebook đó để đăng nhập vào rất nhiều ứng dụng khác.

Thói quen này phổ biến như thế nào? Ít nhất một báo cáo tiếp thị cho biết 88% người tiêu dùng Mỹ từng đăng nhập vào một trang web hoặc ứng dụng di động thông qua danh tính của họ từ một mạng xã hội như Facebook, Twitter, và Google Plus.

Sự tiện lợi này có cả ưu và nhược điểm, tóm gọn trong cái gọi là OAuth, một giao thức xác thực cho phép website tin tưởng bạn ngay cả khi bạn không nhập mật khẩu. Một mặt, đó là lối tắt: bạn có thể nhanh chóng truy cập website mới bằng mật khẩu mạng xã hội hiện tại. Mặt khác, điều này cho phép trang mạng xã hội thu thập thông tin về bạn để xây dựng kho hồ sơ phục vụ mục đích tiếp thị. Nó không chỉ biết về lượt truy cập của bạn vào một website riêng lẻ, mà còn biết về tất cả các website, tất cả các thương hiệu mà bạn sử dụng thông tin đăng nhập của nó để kết nối. Khi sử dụng OAuth, chúng ta sẽ từ bỏ rất nhiều sự riêng tư để

đổi lấy sự thuận tiện.

Facebook có lẽ là nền tảng truyền thông xã hội "đeo bám" dai dẳng nhất. Khi bạn đăng xuất khỏi Facebook, trình duyệt của bạn sẽ không còn quyền truy cập vào Facebook và các ứng dụng web của nó nữa. Ngoài ra, Facebook còn cài thêm các trình theo dõi để giám sát hoạt động người dùng ngay cả sau khi bạn đăng xuất; các trình này yêu cầu những thông tin như vị trí địa lý, website bạn truy cập, những phần bạn nhấp vào trên từng trang, và tên người dùng của bạn trên Facebook. Các nhóm hoạt động vì quyền riêng tư đang bày tỏ lo ngại trước việc Facebook dự định theo dõi thông tin từ một số website và ứng dụng mà người dùng của họ đang truy cập để hiển thị nhiều quảng cáo phù hợp hơn.

Vấn đề ở đây là Facebook, cũng giống như Google, muốn có dữ liệu về bạn. Nhưng nó không hỏi trực tiếp mà lại tìm cách để lấy được thông tin đó. Nếu bạn liên kết tài khoản Facebook của mình với các dịch vụ khác, Facebook sẽ có thông tin về bạn và dịch vụ đó. Giả sử bạn dùng Facebook để truy cập vào tài khoản ngân hàng, nó sẽ biết bạn đang sử dụng tổ chức tài chính nào. Chỉ sử dụng một xác thực có nghĩa là nếu có người vào được tài khoản Facebook của bạn, người đó sẽ có quyền truy cập vào mọi trang web khác liên kết với tài khoản ấy, kể cả tài khoản ngân hàng. Trong công tác bảo mật, điểm gây lỗi duy nhất[66] không bao giờ là một ý tưởng hay. Tuy sẽ mất thêm vài giây nữa, nhưng bạn chỉ nên đăng nhập vào Facebook khi cần và đăng nhập riêng vào từng ứng dụng.

[66] Điểm gây lỗi duy nhất (single point of failure – SPOF): Một phần trong một hệ thống mà nếu thất bại sẽ khiến toàn bộ hệ thống ngừng hoạt động. SPOF là sự cố không mong muốn đối với bất kỳ hệ thống nào có mục tiêu hoạt động đáng tin cậy.

Thêm vào đó, Facebook đã cố tình không tuân theo tín hiệu "không theo dõi" do Internet Explorer gửi đi, lấy lý do là nó "không có sự đồng thuận của toàn ngành." Trình theo dõi của Facebook có các hình thức cổ điển: cookie, JavaScript, ảnh 1 pixel,

và iframe. Điều này cho phép các nhà quảng cáo có thể quét và truy cập các cookie cũng như các trình theo dõi cụ thể của trình duyệt để phân phối sản phẩm, dịch vụ, và quảng cáo, cả trong và ngoài Facebook.

May mắn là có các tiện ích mở rộng trình duyệt giúp chặn các dịch vụ Facebook trên các website của bên thứ ba, ví dụ như Facebook Disconnect dành cho Chrome và Facebook Privacy List trên Adblock Plus (hoạt động với cả Firefox và Chrome). Mục tiêu cuối cùng của tất cả các công cụ plugin này là mang đến cho bạn quyền kiểm soát những gì bạn chia sẻ với Facebook cũng như bất kỳ mạng xã hội nào khác thay vì để bạn phải khoanh tay ngồi nhìn các dịch vụ bạn sử dụng chi phối những điều đó.

Với những gì Facebook biết về 1,65 tỉ thuê bao của mình, công ty này khá tử tế – cho đến nay là như vậy. Họ có hàng tấn dữ liệu, nhưng cũng giống như Google, họ đã quyết định không hành động trên tất cả số dữ liệu đó. Nhưng điều đó không có nghĩa là họ sẽ không làm gì.

Không giấu diếm như cookie – nhưng khả năng ký sinh cũng bền bỉ không kém – là các thanh công cụ (toolbar). Thanh công cụ bổ sung mà bạn thấy ở phần đầu trình duyệt trên máy tính cá nhân truyền thống có thể ghi tên YAHOO, MCAFEE, ASK, hoặc tên của bất kỳ công ty nào khác. Rất có thể bạn không nhớ làm thế nào mà thanh công cụ này lại xuất hiện ở đó. Bạn cũng không bao giờ sử dụng nó. Và bạn cũng không biết cách xóa bỏ nó.

Những thanh công cụ như thế này thu hút sự chú ý của bạn, khiến bạn quên mất thanh công cụ đi kèm với trình duyệt của bạn. Thanh công cụ gốc cho phép bạn chọn công cụ tìm kiếm mặc định. Thanh công cụ ký sinh sẽ đưa bạn đến trang tìm kiếm riêng của mình, và kết quả trả về có thể chứa đầy các nội dung được tài trợ. Điều này đã xảy ra với Gary More, một cư dân ở Tây Hollywood. Anh gặp thanh công cụ Ask.com mà không có cách nào để gỡ bỏ nó. “Nó hệt như một khách trọ xấu tính vậy,” More nói. “Nó không chịu rời đi.”

Nếu bạn có thanh công cụ thứ hai hoặc thứ ba, có thể là do bạn đã tải xuống phần mềm mới hoặc vừa cập nhật phần mềm hiện tại. Ví dụ, nếu bạn mới cài đặt Java, nhà cung cấp Java là Oracle sẽ tự động bổ sung một thanh công cụ trừ khi bạn yêu cầu không cài. Khi nhấp chuột trên màn hình tải xuống hoặc cập nhật, có thể bạn không để ý thấy ô đánh dấu nhỏ mặc định cho biết bạn đã đồng ý cài đặt thanh công cụ. Điều này không có gì là bất hợp pháp; bạn đã đồng ý, dù rằng điều đó có nghĩa là bạn cũng chọn cài đặt nó tự động. Nhưng thanh công cụ đó cho phép công ty khác theo dõi thói quen duyệt web của bạn và có thể thay đổi công cụ tìm kiếm mặc định của bạn sang dịch vụ riêng của nó.

Cách tốt nhất để loại bỏ thanh công cụ là gỡ cài đặt theo cách gỡ các chương trình trên máy tính cá nhân truyền thống. Nhưng một số thanh công cụ gan lỳ có thể yêu cầu bạn phải tải xuống công cụ gỡ, và thường quá trình gỡ cài đặt này có thể để lại đủ thông tin để các đại lý quảng cáo liên quan đến thanh công cụ đó thực hiện cài đặt lại nó.

Khi cài đặt phần mềm mới hoặc cập nhật phần mềm hiện tại, hãy để ý đến tất cả các ô chọn. Bạn có thể tránh được rất nhiều rắc rối nếu không đồng ý cài đặt các thanh công cụ này ngay từ đầu.

Điều gì sẽ xảy ra nếu bạn sử dụng tính năng duyệt web riêng tư, dùng NoScript, HTTPS Everywhere, và định kỳ xóa các cookie trình duyệt và thanh công cụ bổ sung? Liệu bạn sẽ an toàn hay không? Không. Bạn vẫn có thể bị theo dõi trực tuyến.

Các website được mã hóa bằng ngôn ngữ đánh dấu siêu văn bản, hay HTML. Phiên bản hiện hành, HTML5, có nhiều tính năng mới, trong đó có những tính năng giúp loại bỏ các siêu cookie Silverlight và Flash nhanh hơn – đây là một điều tốt. Tuy nhiên, có lẽ do vô tình, HTML5 lại cho phép các công nghệ theo dõi mới.

Một trong số đó là canvas fingerprinting, một công cụ theo dõi trực tuyến tuyệt vời theo cách rất đáng sợ. Canvas fingerprinting sử dụng phần tử canvas[67] của HTML5 để vẽ một hình ảnh đơn giản. Chỉ như vậy là xong. Quá trình vẽ diễn ra bên trong trình

duyệt và không hiển thị cho bạn thấy. Tất cả chỉ mất một phần nhỏ của một giây. Nhưng kết quả sẽ hiển thị trên website truy vấn.

[67] Canvas: Thẻ <canvas> được dùng để vẽ đồ họa thông qua JavaScript.

Ý tưởng ở đây là phần cứng và phần mềm của bạn, khi được kết hợp thành tài nguyên của trình duyệt, sẽ hiển thị hình ảnh đó một cách riêng biệt, không giống với bất kỳ hình ảnh nào khác. Hình ảnh này – có thể là một loạt các hình dạng có màu sắc khác nhau – sau đó được chuyển đổi thành một số duy nhất, gần giống như mật khẩu. Số này tiếp tục được đối chiếu với các trường hợp mà nó được nhìn thấy trên các website khác trong Internet. Và từ đó – từ số lượng các địa điểm mà số duy nhất đó được nhìn thấy – hồ sơ về các website bạn đã truy cập sẽ được hình thành. Có thể dùng số này, hay còn gọi là canvas fingerprinting, để xác định trình duyệt của bạn khi nó quay trở lại website yêu cầu nó, ngay cả khi bạn đã xóa tất cả cookie hoặc chặn việc cài đặt cookie trong tương lai, vì nó sử dụng một phần tử đã được tích hợp vào chính bản thân HTML5.

Canvas fingerprinting là một tiến trình chạy ngầm tự động; nó không yêu cầu bạn phải bấm hoặc làm bất cứ điều gì mà chỉ đơn giản là xem một trang web. May mắn thay, có một số plugin trên trình duyệt có thể chặn nó. Đối với Firefox có CanvasBlocker. Đối với Google Chrome có CanvasFingerprintBlock. Ngay cả dự án Tor cũng mới bổ sung công nghệ chống canvas cho trình duyệt của mình.

Nếu bạn sử dụng các plugin này và làm theo tất cả những lời khuyên khác của tôi, có thể bạn sẽ nghĩ rằng cuối cùng mình cũng không còn bị theo dõi trực tuyến nữa. Nhưng bạn sai rồi.

Các công ty như Drawbridge, Tapad, và Crossswise của Oracle, đã nâng kỹ thuật theo dõi trực tuyến lên một bước nữa. Họ tuyên bố sở hữu các công nghệ có thể theo dõi sở thích của bạn trên nhiều thiết bị, bao gồm cả những website bạn chỉ truy cập trên điện

thoại di động và máy tính bảng.

Một số kỹ thuật theo dõi kiểu này là kết quả của việc ứng dụng máy học và logic mờ[68]. Ví dụ: nếu thiết bị di động và máy tính cá nhân truyền thống đều liên hệ với một website qua cùng một địa chỉ IP, thì rất có thể chúng có chung một chủ sở hữu. Chẳng hạn, nếu bạn dùng điện thoại di động để tìm kiếm một món quần áo, rồi khi về nhà sử dụng máy tính cá nhân truyền thống, bạn sẽ thấy món đồ đó trong phần "đã xem gần đây" trên website của nhà bán lẻ. Kết quả tốt hơn nữa là bạn mua món đồ trên bằng máy tính cá nhân. Càng có nhiều kết quả tương đồng giữa các thiết bị khác nhau, khả năng chúng có chung một người sử dụng càng cao. Drawbridge tuyên bố trong năm 2015, họ đã liên kết 1,2 tỉ người dùng qua 3,6 tỉ thiết bị khác nhau.

[68] Logic mờ (fuzzy logic): Một hình thức logic đa trị, dùng để xử lý khái niệm về sự thật một phần, trong đó giá trị đúng có thể dao động từ hoàn toàn đúng sang hoàn toàn sai thay vì logic Bolean truyền thống chỉ có giá trị đúng hoặc sai (0 hay 1).

Tất nhiên, Google, Apple, và Microsoft cũng làm vậy. Điện thoại Android yêu cầu sử dụng tài khoản Google. Các thiết bị Apple sử dụng ID Apple. Dù người dùng có điện thoại thông minh hay máy tính xách tay, lưu lượng truy cập web được tạo ra từ mỗi thiết bị đều được liên kết với một người dùng cụ thể. Và các hệ điều hành mới nhất của Microsoft đều yêu cầu tài khoản Microsoft để có thể tải xuống các ứng dụng hoặc lưu trữ ảnh và tài liệu bằng dịch vụ đám mây của hãng này.

Điểm khác biệt lớn ở đây là Google, Apple, và Microsoft cho phép bạn tắt một số hoặc tất cả các hoạt động thu thập dữ liệu này và xóa dữ liệu đã thu thập trước đó. Drawbridge, Crosswise, và Tapad khiến cho quá trình vô hiệu hóa và xóa này trở nên mập mờ hơn. Hoặc có khi họ không có các tính năng đó.

Proxy hoặc Tor là các phương pháp thuận tiện giúp che giấu vị trí thực của bạn khi truy cập Internet, xong điều này có thể mang đến những rắc rối thú vị, thậm chí gây phản tác dụng, bởi vì đôi

khi việc theo dõi trực tuyến là hợp lý, đặc biệt khi một công ty thẻ tín dụng muốn tìm cách chống gian lận. Ví dụ, vài ngày trước khi Edward Snowden xuất hiện công khai, anh muốn tạo một trang web hỗ trợ các quyền trực tuyến. Tuy nhiên, anh gặp rắc rối khi dùng thẻ tín dụng để trả phí đăng ký cho công ty cung cấp dịch vụ máy chủ.

Vào thời điểm đó, Snowden vẫn sử dụng tên thật, địa chỉ email thật, và thẻ tín dụng cá nhân – điều này diễn ra ngay trước khi anh tiết lộ các tài liệu. Anh cũng sử dụng Tor – điều này đôi khi khiến các hãng thẻ tín dụng phải cảnh giác khi họ muốn xác minh danh tính của bạn và không thể khớp một số thông tin bạn cung cấp với những gì họ có trong hồ sơ. Ví dụ, nếu tài khoản thẻ tín dụng cho biết bạn sống ở New York, vậy tại sao nút thoát Tor lại chỉ ra bạn đang ở Đức? Sự khác biệt về vị trí địa lý như thế này thường là dấu hiệu cho thấy ý định mua bán bất hợp pháp, do đó khiến họ phải nghiên cứu kỹ hơn.

Chắc chắn các công ty thẻ tín dụng cũng theo dõi chúng ta trên mạng. Họ biết tất cả các hoạt động mua sắm của chúng ta. Họ biết chúng ta đăng ký thuê bao ở đâu. Họ biết khi nào chúng ta ra nước ngoài. Và họ biết khi nào chúng ta sử dụng một thiết bị mới để mua hàng trực tuyến.

Theo Micah Lee của Tổ chức Biên giới Điện tử, có lần Snowden ở trong phòng một khách sạn đặt ở Hồng Kông để trao đổi các bí mật của chính phủ với Laura Poitras và Glenn Greenwald, một phóng viên của tờ Guardian, và đồng thời liên lạc với bộ phận hỗ trợ khách hàng tại DreamHost, một nhà cung cấp Internet có trụ sở tại Los Angeles. Snowden giải thích với DreamHost rằng anh đang ở nước ngoài và không tin tưởng vào dịch vụ Internet ở đây, vì thế anh mới phải sử dụng Tor. Cuối cùng, DreamHost chấp nhận thẻ tín dụng của anh qua Tor.

Để tránh rắc rối này với Tor, bạn có thể cấu hình file torrec config để sử dụng các nút thoát đặt ở quốc gia của bạn. Điều đó sẽ khiến cho các công ty thẻ tín dụng vui vẻ. Ngược lại, nếu liên tục sử dụng các nút thoát giống nhau, danh tính của bạn rốt cuộc sẽ bị

tiết lộ. Có tin cho rằng các cơ quan chính phủ có thể kiểm soát một số nút thoát ra, vì vậy nên sử dụng các nút khác nhau.

Một phương pháp thanh toán khác không để lại dấu vết là sử dụng Bitcoin, một loại tiền ảo. Giống như hầu hết các loại tiền tệ, giá trị của nó biến động dựa trên niềm tin của người dùng.

Bitcoin là một thuật toán cho phép mọi người tạo ra – hay nói theo thuật ngữ Bitcoin là "đào" tiền cho mình. Nhưng nếu việc đào tiền dễ dàng, hẳn ai cũng sẽ làm. Vì vậy, nó không hề dễ dàng. Quá trình này đòi hỏi công suất tính toán rất lớn, và phải mất một thời gian dài mới tạo ra được một Bitcoin. Như vậy, mỗi ngày chỉ có một lượng Bitcoin hữu hạn – thực tế này cộng với niềm tin của người tiêu dùng tạo thành yếu tố tác động đến giá trị của Bitcoin.

Mỗi Bitcoin có một chữ ký mã hóa để xác định nó là bản gốc và duy nhất. Các giao dịch thực hiện với chữ ký mã hóa đó có thể được truy nguyên về đồng tiền, nhưng phương pháp lấy tiền có thể bị che khuất – ví dụ, bằng cách thiết lập địa chỉ email ẩn danh rồi dùng nó để thiết lập một ví Bitcoin ẩn danh bằng mạng Tor.

Bạn có thể mua Bitcoin trực tiếp hoặc mua ẩn danh trên mạng bằng cách sử dụng thẻ quà tặng trả trước, hoặc tìm ATM Bitcoin không có camera giám sát. Tùy thuộc vào yếu tố giám sát nào có khả năng tiết lộ danh tính thực sự của mình, bạn phải cân nhắc đến mọi rủi ro trong quá trình chọn phương thức mua hàng. Sau đó, bạn có thể đưa các Bitcoin này cho một bên cung cấp dịch vụ trộn tiền (tumbler). Dịch vụ này sẽ lấy một ít Bitcoin từ tôi, một ít từ bạn, và một ít từ những người khác được chọn ngẫu nhiên rồi trộn tất cả lại với nhau. Sau khi trừ đi phí trộn tiền, bạn sẽ nhận về số Bitcoin của mình – chỉ có điều chữ ký mã hóa của mỗi đồng Bitcoin có thể khác nhau sau khi trộn. Nhờ vậy mà hệ thống được ẩn danh ở mức độ nào đó.

Lưu trữ Bitcoin bằng cách nào? Vì không có ngân hàng Bitcoin và vì Bitcoin không phải là tiền vật lý, nên bạn sẽ phải dùng ví Bitcoin được thiết lập ẩn danh bằng cách sử dụng các hướng dẫn

chi tiết sẽ được mô tả ở phần sau trong cuốn sách này.

Sau khi đã mua và lưu trữ Bitcoin, bạn sử dụng đồng tiền này như thế nào? Các sàn giao dịch cho phép bạn đầu tư vào Bitcoin và đổi nó sang các loại tiền tệ khác, chẳng hạn như đô-la Mỹ, hoặc mua hàng hóa trên các website như Amazon. Giả sử bạn có một Bitcoin, trị giá 618 đô-la. Nếu chỉ mua một món đồ trị giá 80 đô-la, thì sau giao dịch, bạn sẽ giữ lại một tỉ lệ phần trăm nhất định của giá trị ban đầu, tùy thuộc vào tỉ giá trao đổi.

Các giao dịch được xác minh trong một sổ cái kế toán công khai gọi là blockchain và được xác định theo địa chỉ IP. Nhưng như chúng ta đã thấy, địa chỉ IP là có thể thay đổi hoặc làm giả. Và mặc dù các điểm bán hàng đã bắt đầu chấp nhận Bitcoin, nhưng phí dịch vụ vốn thường do đơn vị bán hàng thanh toán lại được chuyển sang người mua. Hơn nữa, không giống như thẻ tín dụng, Bitcoin không cho phép hoàn tiền.

Bạn có thể tích lũy nhiều Bitcoin như tích lũy tiền thực. Nhưng tuy đạt được thành công về mặt tổng thể (anh em nhà Winklevoss, nổi tiếng với vụ kiện Mark Zuckerberg về việc thành lập Facebook, là những nhà đầu tư lớn trong Bitcoin), hệ thống này cũng vấp phải một số thất bại lịch sử. Năm 2014, Mt. Gox, một sàn giao dịch Bitcoin tại Tokyo, tuyên bố phá sản sau khi thông báo rằng Bitcoin của sàn này đã bị đánh cắp. Cũng đã có những báo cáo về hành vi trộm cắp khác trong các sàn giao dịch Bitcoin, nhưng khác với tài khoản ngân hàng, loại tài sản này không được bảo hiểm.

Nhưng dẫu sao, tuy trước đây đã có nhiều ý tưởng về tiền ảo, song Bitcoin đã trở thành tiền tệ ẩn danh tiêu chuẩn của Internet. Bitcoin vẫn còn nhiều điều cần hoàn thiện, nhưng nó là một lựa chọn cho những ai tìm kiếm sự riêng tư. Đến đây, có lẽ bạn nghĩ mình đã có thể vô hình được rồi – nào là giấu địa chỉ IP bằng Tor, rồi mã hóa email và tin nhắn bằng PGP và Signal. Tuy nhiên, tôi chưa nói nhiều về phần cứng – thứ có thể được dùng vừa để tìm bạn vừa để giấu bạn trên Internet.

Chương 7: THANH TOÁN HAY LÀ KHÔNG!

Cơn ác mộng bắt đầu trên mạng và kết thúc với việc các đặc vụ liên bang xông vào một ngôi nhà ở ngoại ô Blaine, Minnesota. Họ chỉ có một địa chỉ IP liên quan đến các lượt tải về những nội dung khiêu dâm trẻ em và một lời đe dọa ám sát đối với Phó Tổng thống Mỹ Joe Biden. Qua liên hệ với nhà cung cấp dịch vụ Internet gắn với địa chỉ IP đó, các đặc vụ nắm được địa chỉ nhà của người dùng đó. Phương pháp theo dõi này từng rất thành công trước kia, khi mọi người vẫn còn dùng kết nối có dây với modem hoặc bộ định tuyến. Khi ấy, mỗi địa chỉ IP đều có thể được truy về một máy.

Nhưng ngày nay, hầu hết mọi người đều sử dụng kết nối không dây. Mạng không dây cho phép mọi người di chuyển tự do trong nhà, chỉ cần mang theo thiết bị di động là vẫn kết nối được với Internet. Và nếu bạn không cẩn thận, hàng xóm cũng có thể kết nối vào tín hiệu nhà bạn. Trong trường hợp này, các đặc vụ liên bang đã gõ nhầm cửa. Nơi cần đến là ngôi nhà bên cạnh.

Năm 2010, Barry Vincent Ardolf nhận các tội danh xâm phạm máy tính trái phép, trộm cắp thông tin nhận dạng, sở hữu nội dung khiêu dâm trẻ em, và đe dọa Phó Tổng thống Biden. Hồ sơ của tòa án cho thấy xung đột giữa Ardolf và người hàng xóm nảy sinh khi người hàng xóm, vốn là một luật sư, gửi đơn khiếu nại cho cảnh sát với nội dung cáo buộc Ardolf đã "đụng chạm và hôn với thái độ không phù hợp" vào miệng của một em bé đang tuổi tập đi, cũng là con của vị luật sư trên.

Sau đó, Ardolf sử dụng địa chỉ IP của bộ định tuyến không dây ở nhà người hàng xóm và lấy danh tính đó để mở tài khoản Yahoo và Myspace. Chính từ những tài khoản giả mạo này mà Ardolf đã rắp tâm bôi xấu và gây rắc rối pháp lý cho vị luật sư đó.

Ngày nay, nhiều nhà cung cấp dịch vụ Internet tích hợp sẵn tính

năng không dây cho các bộ định tuyến tại nhà. Một số nhà cung cấp, chẳng hạn như Comcast, còn tạo dịch vụ Wi-Fi mở thứ hai trong đó bạn có quyền kiểm soát hạn chế. Ví dụ, bạn có thể thay đổi một vài cài đặt như khả năng tắt thiết bị đi. Bạn nên biết về điều này. Ai đó ngồi trong một chiếc xe tải đỗ ở trước cửa nhà bạn có thể đang sử dụng mạng không dây miễn phí của bạn đấy. Mặc dù việc sử dụng ké này không tốn thêm tiền, nhưng nếu tín hiệu thứ hai bị sử dụng nhiều, tốc độ Wi-Fi sẽ giảm xuống một chút. Bạn có thể tắt Xfinity Home Hotspot của Comcast nếu không cần chia sẻ mạng Internet với khách đến chơi nhà.

Tuy mạng không dây tích hợp giúp bạn bắt kịp với dịch vụ công nghệ mới, nhưng thường thì các bộ định tuyến băng thông rộng này không được cấu hình đúng cách và có thể mang lại rắc rối khi chúng không được bảo mật. Một nguyên nhân là vì truy cập không dây không an toàn có thể là điểm xâm nhập vào nhà bạn, như trường hợp của Ardolf. Mặc dù kẻ xâm nhập có thể không nhắm mục tiêu vào các file số của bạn, nhưng biết đâu chúng lại có ý đồ gây rối khác.

Ardolf không phải là thiên tài máy tính. Hắn khai trước tòa rằng hắn không biết sự khác biệt giữa mã hóa WEP (bảo mật tương đương với mạng có dây) mà bộ định tuyến của vị luật sư hàng xóm sử dụng, và mã hóa WPA (truy cập Wi-Fi được bảo vệ) vốn an toàn hơn rất nhiều. Hắn chỉ hành động vì giận dữ. Vậy là lại thêm một lý do để bạn dành thời gian xem xét sự an toàn của mạng không dây ở nhà mình. Làm sao biết khi nào một người hàng xóm vì xung đột với bạn mà rắp tâm dùng mạng của nhà bạn để làm hại bạn?

Nếu có người phá hoại mạng nhà bạn, vẫn có một số biện pháp bảo vệ cho chủ sở hữu các bộ định tuyến. Theo Tổ chức Biên giới Điện tử, các thẩm phán liên bang đã từ chối nhiều vụ kiện nhắm vào BitTorrent của các chủ sở hữu bản quyền vì hãng này đã chứng minh được rằng có người dùng mạng không dây của họ để tải phim. Tổ chức Biên giới Điện tử tuyên bố rằng địa chỉ IP không phải là người, nghĩa là chủ thuê bao không dây có thể không phải

chịu trách nhiệm về hành động của người khác trên mạng không dây của họ.Mặc dù ngành pháp y máy tính sẽ minh oan cho người vô tội có Wi-Fi bị kẻ khác lợi dụng để thực hiện hành vi phạm tội – như trong trường hợp của vị luật sư ở Minnesota – nhưng tại sao phải trải qua những thủ tục phiền hà như vậy?

Ngay cả khi bạn sử dụng modem quay số dựa trên điện thoại bàn hoặc bộ định tuyến trên cáp ASM (nguồn phát đa hướng) do Cisco, Belkin, cùng nhiều hãng khác cung cấp, song các thiết bị này cũng đều ít nhiều có vấn đề về phần mềm và cấu hình.

Trước tiên và quan trọng nhất, hãy tải xuống firmware mới nhất (firmware là phần mềm được cài đặt trong thiết bị phần cứng) bằng cách truy cập màn hình cấu hình của bộ định tuyến (xem bên dưới) hoặc truy cập website của nhà sản xuất và tìm kiếm các bản cập nhật cho bản mà thiết bị của bạn đang dùng. Hãy thực hiện động tác cập nhật này càng thường xuyên càng tốt. Một cách dễ làm là mỗi năm mua một bản mới. Cách này có thể tốn kém, nhưng nó sẽ đảm bảo rằng bạn có firmware mới nhất và tốt nhất. Thứ hai, hãy cập nhật các cài đặt cấu hình của bộ định tuyến. Đừng sử dụng những cài đặt mặc định.

Nhưng trước tiên: trong cái tên có gì? Nhiều hơn bạn nghĩ đấy. Điểm chung giữa bộ định tuyến của nhà cung cấp mạng Internet và bộ định tuyến mà bạn mua tại Best Buy là ở việc đặt tên. Theo mặc định, tất cả các bộ định tuyến không dây đều phát bộ định danh thiết lập dịch vụ (service set identifier – SSID). SSID thường là tên và model của bộ định tuyến, ví dụ: “Linksys WRT54GL.” Nếu nhìn vào các kết nối không dây trong khu vực mình ở, bạn sẽ hiểu ý tôi muốn nói.

Việc phát SSID mặc định ra ngoài có thể che giấu điểm xuất nguồn của tín hiệu Wi-Fi, nhưng nó cũng cho phép một người lạ ở ngoài đường biết gia đình bạn đang dùng bộ định tuyến của hãng nào và model nào. Tại sao điều đó không tốt? Vì người đó cũng có thể biết các sơ hở của model đó để tìm cách khai thác.

Vậy làm thế nào để thay đổi tên bộ định tuyến và cập nhật

firmware của nó?

Có thể dễ dàng truy cập vào bộ định tuyến từ trình duyệt Internet. Nếu không có hướng dẫn cho bộ định tuyến của mình, bạn có thể tìm trên mạng danh sách các URL, nó sẽ cho bạn biết cần phải nhập nội dung gì vào cửa sổ trình duyệt để kết nối trực tiếp với bộ định tuyến trên mạng của nhà mình. Sau khi nhập URL cục bộ (xin lưu ý, bạn chỉ đang nói chuyện với bộ định tuyến mà thôi, không phải với cả mạng Internet rộng lớn), bạn sẽ thấy một màn hình đăng nhập. Tên người dùng và mật khẩu đăng nhập là gì?

Hóa ra trên Internet còn có cả một danh sách các đăng nhập mặc định. Trong ví dụ Linksys ở trên, tên người dùng để trống và mật khẩu là "admin." Sau khi tiếp cận được màn hình cấu hình của bộ định tuyến, bạn nên thay đổi mật khẩu mặc định ngay lập tức theo các hướng dẫn của tôi về cách tạo mật khẩu mạnh và độc đáo hoặc sử dụng một chương trình quản lý mật khẩu.

Hãy nhớ lưu lại mật khẩu này trong trình quản lý mật khẩu hoặc ghi ra giấy, vì có thể bạn sẽ không cần truy cập bộ định tuyến thường xuyên. Nếu bạn lỡ quên mật khẩu (bạn thực sự không cần truy cập nhiều vào màn hình cấu hình cho bộ định tuyến đâu), đừng lo lắng. Có một phím reset cứng giúp khôi phục cài đặt mặc định. Tuy nhiên, khi thực hiện reset cứng, hay khôi phục cài đặt gốc, bạn vẫn sẽ phải nhập lại tất cả các cài đặt cấu hình mà tôi sắp giải thích bên dưới. Vì vậy, hễ khi nào thiết lập cài đặt cho bộ định tuyến khác với cài đặt gốc, hãy ghi lại các nội dung cài đặt hoặc chụp ảnh màn hình rồi in ra. Những ảnh chụp màn hình này sẽ phát huy giá trị khi bạn cần cấu hình lại bộ định tuyến.

Tôi khuyên bạn nên thay đổi "Linksys WRT54GL" thành một cái tên vô thưởng vô phạt, chẳng hạn như "HP Inkjet" (máy in phun HP), như vậy người lạ sẽ không dễ dàng biết tín hiệu Wi-Fi xuất phát từ ngôi nhà nào. Tôi thường dùng tên chung chung, chẳng hạn như tên của khu chung cư nơi tôi sống, thậm chí là tên người hàng xóm của tôi.

Ngoài ra còn có một tùy chọn để ẩn hoàn toàn SSID của bạn, nghĩa là những người khác sẽ không thể dễ dàng nhìn thấy nó trong danh sách các kết nối mạng không dây.

Ở phần cài đặt cấu hình bộ định tuyến cơ bản, bạn có thể cân nhắc một số loại bảo mật không dây vốn không được kích hoạt theo mặc định. Và không phải tất cả mã hóa không dây đều được tạo ra đồng đều như nhau, và cũng không được hỗ trợ bởi tất cả các thiết bị.

Hình thức cơ bản nhất của mã hóa không dây, tức WEP, là vô dụng. Đừng coi nó là một sự lựa chọn – thậm chí đừng nghĩ đến nó. WEP đã bị bẻ khóa từ nhiều năm nay nên không còn được khuyên dùng nữa. Chỉ có các thiết bị và bộ định tuyến cũ là vẫn đưa nó ra làm một tùy chọn. Thay vào đó, hãy chọn một trong những tiêu chuẩn mã hóa mới hơn, mạnh hơn, như WPA. WPA2 thậm chí còn an toàn hơn.

Bật chế độ mã hóa tại bộ định tuyến có nghĩa là các thiết bị kết nối với nó cũng sẽ phải phù hợp với các cài đặt mã hóa. Hầu hết các thiết bị mới đều tự động nhận dạng loại mã hóa đang được sử dụng, nhưng các model cũ vẫn yêu cầu bạn nêu đích danh mức độ mã hóa đang sử dụng. Hãy luôn sử dụng mức mã hóa cao nhất có thể. Mức độ an toàn của bạn chỉ ngang với liên kết yếu nhất mà bạn có, vì vậy hãy đảm bảo tối đa hóa mức độ mã hóa trên thiết bị cũ nhất.

Nếu sử dụng WPA2, thì khi kết nối máy tính xách tay hoặc thiết bị di động, bạn cũng sẽ phải đặt nó ở chế độ WPA2, mặc dù một số hệ điều hành mới sẽ tự động nhận dạng loại mã hóa này. Các hệ điều hành hiện đại trên điện thoại hoặc máy tính xách tay sẽ xác định Wi-Fi khả dụng trong khu vực bạn đang đứng. Phát sóng SSID của bạn (lúc này đang là “HP Inkjet”) sẽ xuất hiện ở đầu hoặc gần đầu danh sách. Biểu tượng ổ khóa trong danh sách các kết nối Wi-Fi khả dụng (thường nằm đè lên trên biểu tượng độ mạnh của từng kết nối) cho biết kết nối Wi-Fi nào yêu cầu mật khẩu (cột sóng của bạn giờ đây cũng sẽ hiển thị biểu tượng ổ khóa).

Từ danh sách các kết nối có sẵn, hãy nhấp vào SSID của bạn. Bạn sẽ được nhắc nhập mật khẩu – hãy đảm bảo rằng mật khẩu của bạn có ít nhất 15 ký tự. Hoặc sử dụng trình quản lý mật khẩu để tạo mật khẩu phức tạp. Để kết nối với Wi-Fi được bảo vệ bằng mật khẩu, bạn sẽ phải nhập mật khẩu ít nhất một lần trên mỗi thiết bị, vì vậy trình quản lý mật khẩu có thể không hoạt động trong mọi trường hợp, đặc biệt là khi bạn phải nhớ mật khẩu phức tạp để sau này tự nhập nó. Mỗi thiết bị – bao gồm cả tủ lạnh "thông minh" và ti-vi kỹ thuật số – đều sẽ sử dụng một mật khẩu bộ định tuyến do bạn chọn khi đặt mã hóa trên bộ định tuyến. Bạn sẽ phải thực hiện thao tác này một lần cho mọi thiết bị truy cập Wi-Fi tại nhà hoặc văn phòng của bạn, và sẽ không phải tiếp tục làm thế, trừ khi bạn thay đổi mật khẩu mạng hoặc mua thiết bị mới.

Cũng có thể giới hạn kết nối Wi-Fi ở các thiết bị do bạn chỉ định – đây được gọi là danh sách trắng (whitelist). Với quy trình này, bạn cấp quyền truy cập (danh sách trắng) cho một số thiết bị và cấm mọi thiết bị khác (danh sách đen, hay blacklist). Để thực hiện điều này, bạn phải nhập địa chỉ kiểm soát truy cập phương tiện truyền thông, hay địa chỉ MAC, của thiết bị. Như vậy, khi nâng cấp điện thoại di động, bạn sẽ phải bổ sung nó vào địa chỉ MAC trong bộ định tuyến thì nó mới kết nối được. Địa chỉ này là riêng biệt cho mọi thiết bị; ba bộ ký tự đầu tiên (octet) là mã nhà sản xuất, và ba bộ ký tự cuối cùng là dành riêng cho sản phẩm. Bộ định tuyến sẽ từ chối bất kỳ thiết bị nào có MAC phần cứng chưa được lưu trước đó. Cũng cần biết rằng, có một công cụ xâm nhập gọi là aircrack-ng có thể phát hiện địa chỉ MAC hợp lệ của người dùng để kẻ tấn công có thể giả mạo địa chỉ đó để kết nối với bộ định tuyến không dây. Cũng giống như các SSID không dây ẩn, việc tránh bộ lọc địa chỉ MAC là chuyện nhỏ.

Việc tìm địa chỉ MAC trên thiết bị của bạn tương đối dễ dàng. Trong Windows, hãy vào nút Start, gõ "CMD," nhấp vào "Command Prompt," và tại dấu nháy ngược, gõ "IPCONFIG." Máy sẽ trả về một danh sách dài dữ liệu, trong đó có địa chỉ MAC bao gồm 12 ký tự hệ thập lục phân, cứ hai ký tự lại được ngăn cách

nhau bằng dấu hai chấm. Đối với các sản phẩm của Apple, việc này thậm chí còn dễ dàng hơn. Hãy đi đến biểu tượng Apple, chọn "System Preferences," rồi đến "Network." Sau đó, nhấp vào thiết bị mạng trên bảng điều khiển bên trái và đi đến Advanced> Hardware, ở đó bạn sẽ thấy địa chỉ MAC. Đối với một số sản phẩm Apple cũ hơn, quy trình thực hiện sẽ là: Biểu tượng Apple>Tùy chọn hệ thống>Mạng>Ethernet tích hợp. Bạn có thể tìm thấy địa chỉ MAC cho iPhone bằng cách chọn Cài đặt>Chung>Giới thiệu và tìm trong "Địa chỉ Wi-Fi." Đối với điện thoại Android, đi tới Cài đặt>Giới thiệu về điện thoại>Trạng thái và xem trong "Địa chỉ MAC Wi-Fi." Hướng dẫn này có thể thay đổi tùy theo thiết bị và model máy mà bạn đang sử dụng.

Sau khi có được những địa chỉ MAC 12 chữ số này, bạn phải cho bộ định tuyết biết rằng nó chỉ được chấp nhận những thiết bị này và chặn mọi thiết bị khác. Có một vài nhược điểm ở đây. Nếu khách đến chơi muốn kết nối với mạng nhà riêng của bạn, bạn sẽ phải đưa cho người đó một trong những thiết bị của mình kèm mật khẩu, hoặc tắt tính năng lọc địa chỉ MAC bằng cách nhập lại màn hình cấu hình bộ định tuyến. Ngoài ra, có thể có những lúc bạn muốn thay đổi địa chỉ MAC của một thiết bị; nếu không thay đổi về như cũ, bạn sẽ không kết nối được với mạng Wi-Fi đã đặt chế độ hạn chế MAC ở nhà hoặc nơi làm việc. May mắn là, trong hầu hết các trường hợp, chỉ cần khởi động lại thiết bị là địa chỉ MAC ban đầu sẽ được khôi phục.

Để khiến cho việc kết nối thiết bị mới với bộ định tuyến tại nhà trở nên dễ dàng hơn, Liên minh Wi-Fi, một nhóm các nhà cung cấp mong muốn quảng bá việc sử dụng các công nghệ Wi-Fi, đã tạo ra thiết lập Wi-Fi bảo mật (Wi-Fi protected setup – WPS). WPS được giới thiệu là một phương pháp giúp bất kỳ ai – tôi nhấn mạnh là bất kỳ ai – có thể thiết lập thiết bị di động ở nhà hoặc tại văn phòng một cách an toàn. Mặc dù vậy, trên thực tế, cách này cũng không hẳn là an toàn.

WPS thường là một nút trên bộ định tuyến, hoặc sử dụng mã PIN và giao tiếp trường gần (near field communication – NFC). Chỉ

cần nhấn nút, bạn sẽ kích hoạt tính năng WPS, và nó giao tiếp với bất kỳ thiết bị mới nào trong nhà hoặc văn phòng của bạn, tự động đồng bộ hóa chúng để làm việc với mạng Wi-Fi ở đó.

Nghe có vẻ tuyệt vời. Tuy nhiên, nếu bộ định tuyến ở khu vực "công cộng," ví dụ trong phòng khách, thì bất kỳ ai cũng có thể chạm vào nút WPS và truy cập mạng nhà riêng của bạn.

Ngay cả khi không thể tiếp cận trực tiếp với thiết bị, kẻ tấn công trên mạng vẫn có thể sử dụng thuật toán vét cạn để đoán mã PIN WPS của bạn. Có thể mất vài giờ, nhưng đây vẫn là một phương pháp tấn công khả thi, và bạn nên tự vệ bằng cách ngay lập tức tắt WPS trên bộ định tuyến.

Một phương pháp tấn công WPS khác là Pixie Dust. Đây là kiểu tấn công ngoại tuyến và chỉ ảnh hưởng đến một số nhà sản xuất chip, bao gồm Ralink, Realtek và Broadcom. Pixie Dust hoạt động bằng cách giúp hacker chiếm mật khẩu trên các bộ định tuyến không dây. Về cơ bản, công cụ này rất đơn giản và có thể truy cập vào thiết bị chỉ sau vài giây hoặc vài giờ, tùy thuộc vào độ phức tạp của mã PIN WPS. Ví dụ, một chương trình tương tự là Reaver có thể bẻ khóa một bộ định tuyến hỗ trợ WPS trong vòng vài giờ.

Nhìn chung, nên tắt WPS. Bạn có thể kết nối từng thiết bị di động mới với mạng bằng cách nhập mật khẩu đã đặt để truy cập.

Như vậy, thông qua việc sử dụng mã hóa và mật khẩu mạnh, bạn đã ngăn chặn được người khác sử dụng mạng định tuyến không dây tại nhà của mình. Liệu điều đó có đồng nghĩa với việc không ai có thể xâm nhập vào mạng gia đình của bạn hay nhòm ngó vào nhà bạn qua công cụ kỹ thuật số không? Không hoàn toàn.

Khi Blake Robbins, cậu học sinh lớp 10 của một trường trung học ở khu vực ngoại ô Philadelphia, bị gọi vào văn phòng hiệu trưởng, cậu không biết mình sắp bị khiển trách vì "hành vi không đúng đắn" – ở nhà. Trước đó, Học khu69 Hạ Merion ở ngoại ô Philadelphia đã trang bị máy tính xách tay MacBook mới cho tất cả các học sinh trung học, bao gồm Robbins, để sử dụng trong kỳ học. Nhưng họ không cho biết rằng phần mềm được thiết kế để

lấy lại thiết bị trong trường hợp bị mất cũng được dùng để theo dõi hành vi của tất cả 2.300 học sinh khi ở trong phạm vi quan sát của webcam gắn trên máy.

[69] Học khu: Khu vực mà tất cả các trường học trong đó đều nằm dưới sự quản lý của một cấp chức trách.

Robbins bị cáo buộc tội gì? Cắn thuốc lắc. Thông qua luật sư, gia đình Robbins khẳng định rằng cậu bé chỉ vừa làm bài tập vừa ăn kẹo của hãng Mike & Ike.

Vậy tại sao vấn đề này lại bị làm rùm beng lên?

Học khu này khẳng định rằng họ chỉ kích hoạt phần mềm theo dõi hành vi trộm cắp sau khi một thiết bị của họ bị đánh cắp. Phần mềm theo dõi trộm cắp hoạt động như sau: khi người sử dụng phần mềm báo cáo rằng máy tính xách tay của mình bị đánh cắp, nhà trường có thể đăng nhập vào một website và xem các hình ảnh chụp từ webcam của chiếc máy bị đánh cắp, họ còn nghe được âm thanh từ micro. Khi đó, một viên chức trong trường có thể theo dõi chiếc máy này và chụp ảnh nếu cần. Bằng cách này, họ có thể định vị được thiết bị, xác định được kẻ trộm, và thu lại máy về. Tuy nhiên, trong trường hợp này, người ta cho rằng các quản lý của nhà trường đã bật tính năng trên để theo dõi học sinh ở nhà.

Webcam trên chiếc máy tính Mac mà nhà trường giao cho Robbins đã chụp lại hàng trăm bức ảnh của cậu, trong đó có những bức chụp cảnh cậu đang ngủ trên giường. Đối với các học sinh khác, tình hình còn tồi tệ hơn. Theo lời khai tại tòa, nhà trường thậm chí còn giữ nhiều hình ảnh hơn của một số học sinh khác, một vài trong số đó là "khỏa thân một phần." Hoạt động này lẽ ra còn tiếp diễn mà học sinh không hay biết nếu như Robbins không bị khiển trách vì điều mà cậu bị cho rằng đã làm ở nhà.

Robbins cùng với Jalil Hasan, một cựu học sinh cùng trường bị chụp lén gần 500 bức ảnh cá nhân và 400 ảnh chụp màn hình cho biết hoạt động trực tuyến của cậu và các website mà cậu truy

cập, đã đệ đơn kiện học khu. Robbins nhận được 175.000 đô-la và Hasan nhận được 10.000 đô-la bồi thường. Học khu này cũng phải bỏ ra gần nửa triệu đô-la để trang trải chi phí pháp lý cho hai người. Tổng cộng số tiền học khu phải trả qua hãng bảo hiểm là khoảng 1,4 triệu đô-la.

Phần mềm độc hại có thể dễ dàng kích hoạt webcam và micro trên máy tính cá nhân truyền thống mà người dùng không hề hay biết. Và điều này cũng đúng đối với thiết bị di động. Trong trường hợp trên, đó là một hành động có chủ ý. Nhưng thường thì tất cả lại xuất phát từ sự vô tình. Một cách khắc phục nhanh là dán băng dính che webcam trên máy tính và chỉ tháo ra khi cần sử dụng.

Mùa thu năm 2014, Sophie Curtis, một phóng viên của tờ Telegraph có trụ sở ở London, nhận được yêu cầu kết bạn trên LinkedIn qua một email có vẻ từ một đồng nghiệp. Vốn quen nhận được cá email như thế này nên cô cũng không đắn đo mà chấp nhận yêu cầu kết bạn trên. Vài tuần sau, cô nhận được một email có vẻ từ một tổ chức tố giác tội phạm ẩn danh đang sắp sửa công bố các tài liệu nhạy cảm. Là một phóng viên từng đưa tin về các nhóm như Anonymous và WikiLeaks, trước đây cô cũng đã nhận được những email như thế này, nên email mới không khỏi khiến cô tò mò. File đính kèm trông không có gì đáng ngờ, vậy là cô nhấn chuột để mở xem.

Ngay lập tức cô nhận ra sai lầm của mình. Windows Defender, chương trình bảo mật đi kèm với mọi bản Windows, bắt đầu phát cảnh báo trên máy tính, và các cảnh báo cứ liên tiếp xuất hiện chồng chất trên màn hình.

Như rất nhiều người khác ngày nay, Curtis đã bị lừa nhấp vào một file đính kèm mà cô nghĩ là thông thường. File này giả vờ chứa thông tin mà cô muốn xem, nhưng nó lại tải xuống và giải nén một loạt các file khác cho phép kẻ tấn công từ xa kiểm soát hoàn toàn máy tính của cô. Phần mềm độc hại này thậm chí còn chụp ảnh Curtis bằng chính webcam của cô khi cô đang hốt hoảng và bối rối tìm hiểu xem tại sao kẻ khác lại có thể kiểm soát

được thiết bị của mình.

Thực ra, Curtis biết rõ kẻ xâm phạm. Vài tháng trước đó, để thử nghiệm, cô đã thuê một chuyên gia kiểm định an ninh – một người làm công việc giống như tôi. Các cá nhân và doanh nghiệp thường thuê hacker chuyên nghiệp tấn công vào mạng máy tính của mình để tìm ra các điểm sơ hở cần tăng cường phòng vệ. Trong trường hợp của Curtis, quá trình này kéo dài vài tháng.

Khi bắt đầu những công việc như thế này, tôi luôn cố gắng thu thập càng nhiều thông tin về khách hàng càng tốt. Tôi tìm hiểu về cuộc sống và thói quen trực tuyến, đồng thời theo dõi các bài đăng công khai của họ trên Twitter, Facebook, thậm chí cả LinkedIn. Người kiểm định cho Sophie Curtis cũng làm như vậy. Giữa tất cả các email cô nhận được là một thông điệp được xây dựng cẩn thận – email đầu tiên là của người kiểm định mà cô thuê. Người này biết rằng cô là phóng viên và khá cởi mở trong việc tiếp nhận các email mời chào từ người lạ. Theo những gì Curtis viết về sau này, email đầu tiên không cung cấp đủ thông tin để cô cảm thấy muốn phỏng vấn một người nào đó rồi viết thành bài báo. Nhưng cô rất ấn tượng với khối lượng nghiên cứu mà hacker và các đồng nghiệp của anh tại hãng tư vấn an ninh đã thực hiện.

Curtis nói: “Họ có thể dùng Twitter để tìm ra địa chỉ email công việc của tôi cũng như một số địa điểm tôi mới ghé thăm gần đây và cả tên của buổi giao lưu tối mà tôi hay tham dự với các nhà báo khác. Từ bối cảnh nền trong một bức ảnh mà tôi đăng trên Twitter, họ có thể phát hiện ra loại điện thoại di động mà tôi sử dụng, rằng vị hôn thê của tôi thường hút thuốc lá cuộn (đó là một bức ảnh cũ), và rằng anh ấy thích đạp xe.” Mỗi chi tiết trên lại trở thành cơ sở để họ viết một email khác.

Ngoài ra, theo công bố tại Hội nghị DEF CON năm 2016, có một công cụ nữa giúp phân tích tweet của đối tượng cần theo dõi. Sau đó, nó sẽ xây dựng một email lừa đảo mạo danh dựa trên sở thích cá nhân của họ. Vì vậy, hãy cẩn thận khi nhấp vào các liên kết chứa trong tweet.

Thực ra, thường là những điều nhỏ nhặt – những bình luận vô thưởng vô phạt mà thi thoảng bạn đăng ở đâu đó, món đồ lặt vặt độc đáo đặt trên cái kệ phía sau lưng bạn trong một bức ảnh, chiếc áo phông từ một sự kiện bạn từng tham dự – sẽ cung cấp những thông tin cá nhân quan trọng mà bạn không bao giờ có ý định chia sẻ công khai. Chúng ta có thể coi những khoảnh khắc thoắt đến thoắt đi này là vô hại, nhưng càng biết thêm thông tin về bạn, kẻ tấn công càng có thể lừa bạn mở các file đính kèm trong email và khống chế thế giới trên mạng của bạn.

Curtis cho biết nhóm kiểm định chỉ dừng cuộc tấn công ở đó. Nếu có ý đồ xấu thực sự, trò vui có lẽ còn tiếp diễn trong một thời gian dài, có thể là rốt cuộc kẻ xấu sẽ giành được quyền truy cập vào các tài khoản của cô trên mạng xã hội, mạng lưới văn phòng của cô tại Telegraph, thậm chí cả các tài khoản ngân hàng. Và khả năng cao là một cuộc tấn công như vậy sẽ diễn ra khi Curtis không hề hay biết; hầu hết các cuộc tấn công không ngay lập tức kích hoạt Windows Defender hoặc phần mềm chống virus. Một số kẻ tấn công còn xâm nhập và hoạt động lén lút trong nhiều tháng hoặc nhiều năm trước khi bị người dùng phát hiện. Và vấn đề không chỉ giới hạn ở máy tính xách tay: một cuộc tấn công bằng email cũng có thể bắt nguồn từ iPhone hoặc một thiết bị di động Android bị bẻ khóa.

Mặc dù Google và các nhà cung cấp dịch vụ email khác có thực hiện quét email để ngăn chặn việc lan truyền phần mềm độc hại và các nội dung khiêu dâm – đồng thời cũng là để thu thập dữ liệu quảng cáo – nhưng không nhất thiết là họ quét email để phát hiện các hoạt động lừa đảo. Như tôi đã nói, tiêu chuẩn riêng tư ở mỗi người mỗi khác, thì ở đây cũng vậy, rất khó định lượng sự lừa đảo. Và chúng ta không phải lúc nào cũng nhận ra nó, ngay cả khi nó đang ở trước mặt chúng ta.

Trong nội dung email mời kết bạn LinkedIn giả mạo mà Curtis nhận được chứa một hình ảnh cỡ 1x1 pixel, một chấm hình ảnh tí hon mà mắt thường không nhìn ra, thứ mà tôi đã nói là có thể tìm thấy trên các website và được dùng để theo dõi bạn trên

mạng. Khi dấu chấm nhỏ đó gọi ra ngoài, nó sẽ báo cho máy chủ theo dõi ở xa, có thể là bất kỳ nơi nào trên thế giới, thời gian bạn mở email, thời gian email hiển thị trên màn hình, và thiết bị dùng để mở email. Nó cũng có thể cho biết bạn đã lưu, chuyển tiếp, hay xóa email. Ngoài ra, nếu kịch bản mà nhóm kiểm định trên sử dụng là thực, thì kẻ tấn công có thể còn gửi kèm một liên kết dẫn đến trang LinkedIn giả mạo, giống hệt trang thực, ngoại trừ một điểm là nó được lưu trữ trên một máy chủ khác, có lẽ ở một quốc gia khác.

Đối với nhà quảng cáo, con bọ web này có thể dùng để thu thập thông tin về người nhận. Đối với kẻ tấn công, có thể dùng nó để lấy các chi tiết kỹ thuật cần để thiết kế cuộc tấn công tiếp theo nhằm xâm nhập vào tận bên trong máy tính của bạn. Ví dụ, nếu bạn đang chạy phiên bản cũ của một trình duyệt, có thể có một số sơ hở để chúng khai thác.

Email thứ hai mà Curtis nhận được từ đội kiểm định chứa file đính kèm là một tài liệu được nén nhằm khai thác lỗ hổng trong phần mềm dùng để mở file (ví dụ, Adobe Acrobat). Khi nhắc đến phần mềm độc hại, hầu hết mọi người sẽ nghĩ về các loại virus máy tính xuất hiện vào đầu những năm 2000, khi một email bị nhiễm độc có thể phát tán các email bị nhiễm độc khác cho tất cả mọi người trong danh sách liên hệ. Ngày nay, hình thức tấn công lây nhiễm hàng loạt này ít phổ biến hơn, một phần là do những thay đổi đối với bản thân phần mềm email. Phần mềm độc hại nguy hiểm nhất hiện nay tinh vi hơn và thường được nhắm mục tiêu cũng như tùy chỉnh cho phù hợp với từng cá nhân – tương tự như trong trường hợp của Sophie Curtis. Đội kiểm định đã sử dụng một hình thức lừa đảo đặc biệt gọi là lừa đảo có mục tiêu (spear phishing)[70], được thiết kế để nhắm vào một người cụ thể.

[70] Spear phishing: Hình thức lừa đảo theo đó kẻ tấn công gửi email trên danh nghĩa một người gửi có vẻ là đáng tin cậy để lừa nạn nhân tiết lộ các thông tin nhạy cảm. Phishing là cách chơi chữ từ chữ fishing, nghĩa là câu cá.

Phishing là quá trình lừa đảo hình sự trong đó kẻ tấn công tìm cách lấy các thông tin nhạy cảm như tên người dùng, mật khẩu, và thông tin thẻ tín dụng hoặc ngân hàng. Phương thức này đã được sử dụng để tấn công vào các giám đốc tài chính, lừa gạt họ chuyển khoản những lượng tiền lớn vì vị "giám đốc điều hành" đã ủy quyền cho họ. Thông thường, email hoặc tin nhắn lừa đảo dạng phishing sẽ chứa một mục tác vụ như nhấp vào liên kết hoặc mở file đính kèm. Trong trường hợp của Curtis, ý định của đội kiểm định là cài phần mềm độc hại trên máy tính của cô để cô thấy việc này dễ dàng như thế nào.

Một trong những kế hoạch lừa đảo phishing nổi tiếng nhất là Chiến dịch Aurora, trong đó kẻ tấn công gửi email lừa đảo cho các nhân viên người Trung Quốc của Google. Ý định ở đây là lây nhiễm cho máy móc của hãng này ở Trung Quốc nhằm chiếm quyền truy cập vào mạng nội bộ tại trụ sở chính của Google ở Mountain View, California. Kẻ tấn công đã tiếp cận gần mã nguồn công cụ tìm kiếm của Google. Nhưng không chỉ Google là nạn nhân. Các công ty như Adobe cũng thông báo những vụ xâm nhập tương tự. Kết quả là Google phải tạm thời rút các hoạt động của mình khỏi Trung Quốc.

Khi nhận được yêu cầu từ LinkedIn hoặc Facebook, chúng ta thường ít cảnh giác. Có lẽ bởi vì chúng ta tin tưởng các website đó và email của họ. Tuy nhiên, như đã thấy, bất kỳ ai cũng có thể tạo ra một email trông có vẻ hợp pháp. Khi tiếp xúc trực tiếp, chúng ta có thể cảm nhận được nếu người đối diện đeo râu giả, cấy tóc, hay nói giọng không tự nhiên; với bản năng tiến hóa từ hàng thế kỷ nay, chúng ta có thể đánh hơi được sự lừa dối trong chớp mắt. Nhưng bản năng đó không áp dụng được trên mạng, ít nhất là đối với hầu hết chúng ta. Sophie Curtis là phóng viên; công việc yêu cầu ở cô sự hiếu kỳ và hoài nghi để lần theo các manh mối và kiểm chứng dữ liệu. Lẽ ra cô nên nhìn qua danh sách nhân viên của Telegraph để xem người mời cô kết bạn trên LinkedIn là ai, đồng thời kiểm tra xem email đó là thật hay giả. Nhưng cô đã không làm thế. Và thực tế là hầu hết chúng ta đều hớ hênh như nhau.

Kẻ tấn công phishing (gọi là phisher) sẽ có một số, nhưng không phải tất cả, thông tin cá nhân của bạn – nhưng một chút đó cũng đủ để hắn dùng làm mồi câu. Ví dụ, phisher có thể gửi cho bạn một email chứa bốn số cuối trong số thẻ tín dụng của bạn để tạo sự tin tưởng, sau đó tiếp tục hỏi thêm thông tin. Đôi khi bốn chữ số này cũng không chính xác, và phisher sẽ yêu cầu bạn gửi email phản hồi và sửa lại chỗ chưa đúng. Đừng làm theo yêu cầu đó. Nói ngắn gọn, đừng tương tác với phisher. Nhìn chung, không trả lời bất kỳ yêu cầu nào về thông tin cá nhân, ngay cả khi yêu cầu đó có vẻ đáng tin cậy. Thay vào đó, hãy liên hệ với người yêu cầu bằng một email riêng (nếu bạn có địa chỉ) hoặc tin nhắn (nếu bạn có số điện thoại di động).

Loại tấn công phishing đáng lo ngại hơn là lừa mục tiêu thực hiện một hành động có thể trực tiếp khai thác sơ hở trên máy tính của họ, từ đó mang lại quyền kiểm soát hoàn toàn cho kẻ tấn công. Đó là cách tôi vẫn làm trong các cuộc tấn công social engineering. Thu thập thông tin xác thực cũng là một loại tấn công phổ biến, trong đó kẻ tấn công thu thập tên người dùng và mật khẩu, nhưng mối nguy thực sự của spear phishing là giành quyền truy cập vào hệ thống và mạng máy tính của mục tiêu.

Điều gì sẽ xảy ra nếu bạn tương tác với phisher và bị mất tất cả dữ liệu trên thiết bị – tất cả những bức ảnh cá nhân và tài liệu riêng tư? Đó là điều đã xảy ra với mẹ của nhà văn Alina Simone. Viết trên tờ New York Times, Simone kể chuyện mẹ cô – vốn không sành công nghệ – gặp phải một kẻ tấn công tinh vi sử dụng cái gọi là ransomware[71].

[71] Ransomware (mã độc tống tiền): Một loại phần mềm độc hại được thiết kế nhằm ngăn chặn quyền truy cập vào một hệ thống máy tính cho đến khi nạn nhân trả tiền chuộc.

Năm 2014, trên Internet tràn lan các mã độc tống tiền nhắm vào cả cá nhân và tổ chức. Cryptowall là một ví dụ. Nó mã hóa toàn bộ ổ cứng của bạn, ngăn bạn tiếp cận mọi file cho đến khi bạn trả tiền cho kẻ tấn công để mua khóa mở file. Nếu không có bản sao

lưu đầy đủ, bạn sẽ không thể tiếp cận được các nội dung trong máy của mình cho đến khi trả khoản tiền chuộc.

Bạn không muốn trả tiền? Bức thư của kẻ tống tiền xuất hiện trên màn hình hiển thị thông báo rằng chìa khóa để mở file sẽ bị phá hủy sau một khoảng thời gian nhất định. Thường thì thông báo này sẽ đi kèm với một đồng hồ đếm ngược. Nếu bạn không trả tiền, thời hạn đôi khi sẽ được kéo dài hơn, nhưng mức tiền chuộc sẽ gia tăng theo từng lần trì hoãn. Nói chung, bạn nên tránh nhấp vào các file đính kèm email (trừ khi bạn mở file trong Google Quick View hoặc Google Documents). Tuy nhiên, Cryptowall có những cách lây lan khác – chẳng hạn qua banner quảng cáo trên các website. Chỉ cần bạn xem một trang có banner quảng cáo bị nhiễm độc, máy tính cá nhân truyền thống của bạn cũng có thể bị nhiễm độc theo – hình thức này được gọi là drive-by[72], bởi vì bạn không chủ động nhấp vào quảng cáo. Đây chính là nơi phát huy hiệu quả của các plugin loại bỏ quảng cáo trong trình duyệt như Adblock Plus.

[72] Drive-by (đi xe bắn súng): Nghĩa gốc chỉ một hành vi phạm tội, ví dụ bắn súng, được thực hiện từ một phương tiện đang di chuyển.

Trong sáu tháng đầu năm 2015, Trung tâm Khiếu nại Tội phạm Internet của FBI (IC3) đã ghi nhận gần 1.000 trường hợp nhiễm độc Cryptowall 3.0 với thiệt hại ước tính khoảng 18 triệu đô-la, bao gồm số tiền chuộc đã thanh toán, chi phí cho các phòng ban kỹ thuật và các cửa hàng sửa chữa, và thiệt hại về năng suất lao động. Trong một số trường hợp, các file mã hóa chứa thông tin nhận dạng cá nhân như số An sinh Xã hội, vì thế cuộc tấn công liên quan sẽ trở thành vụ xâm phạm dữ liệu, do đó thiệt hại sẽ cao hơn.

Chi phí mua chìa khóa mở file trọn gói thường dao động từ 500 đến 1.000 đô-la, nhưng các nạn nhân thường lại thử các phương pháp khác, chẳng hạn như tự phá mã để loại bỏ ransomware. Mẹ của Simone cũng làm như vậy. Đến khi bà buộc phải gọi điện cầu

cứu con gái, thời hạn gần như sắp hết.

Hầu như tất cả những người cố gắng phá mã hóa ransomware đều thất bại. Đó là loại mã hóa mạnh, để phá giải được nó cần đến các loại máy tính mạnh và tốn nhiều thời gian hơn so với khả năng đáp ứng của phần lớn mọi người. Vì vậy, các nạn nhân thường phải trả tiền. Theo Simone, tháng 11 năm 2014, văn phòng cảnh sát trưởng Tennessee quận Dickson đã trả tiền một khoản tiền chuộc cho Cryptowall để mở khóa 72.000 báo cáo khám nghiệm tử thi, bản ghi lời khai của nhân chứng, ảnh chụp hiện trường vụ án, và các tài liệu khác.

Hacker thường yêu cầu thanh toán bằng Bitcoin, có nghĩa là việc trả tiền chuộc sẽ rất gian nan đối với nhiều người bình thường. Như đã nói, Bitcoin là một loại tiền ảo ngang hàng phi tập trung, và hầu hết chúng ta đều không có sẵn ví Bitcoin để rút tiền.

Từ đầu đến cuối bài viết trên tờ Times, Simone nhắc nhở độc giả rằng không nên trả tiền chuộc – nhưng rốt cuộc chính cô lại phải làm việc đó. Thực ra, hiện nay chính FBI cũng khuyên những người có máy tính bị nhiễm ransomware trả tiền chuộc. Joseph Bonavolonta, trợ lý đặc vụ phụ trách chương trình không gian mạng và phản gián của FBI ở Boston, nói: “Thành thật mà nói, chúng tôi thường khuyên mọi người nên trả tiền chuộc.” Anh cho biết đến FBI cũng không thể bẻ khóa mã hóa siêu bảo mật mà các tác giả của ransomware sử dụng, và anh cũng nói thêm rằng do có rất nhiều người trả tiền chuộc, nên mức giá 500 đô-la vẫn được duy trì ổn định qua nhiều năm. Về sau, FBI cũng công khai phát ngôn rằng việc trả tiền chuộc hay nhờ các chuyên gia an ninh can thiệp là tùy vào quyết định của từng công ty bị nhiễm độc.

Mẹ của Simone, vốn chưa bao giờ mua ứng dụng nào, gọi cho con gái 11 giờ sau khi cuộc tấn công diễn ra vì bà không biết cách thanh toán bằng tiền ảo. Simone kể lại rằng cô tìm được một máy ATM Bitcoin ở Manhattan, và sau một trục trặc về phần mềm và một cuộc gọi cho chủ sở hữu máy ATM đó, cuối cùng cô cũng thực hiện được thanh toán. Tại tỉ giá trao đổi của ngày hôm đó,

mỗi Bitcoin có giá hơn 500 đô-la.

Dù kẻ tống tiền nhận Bitcoin hay tiền mặt, chúng vẫn duy trì được sự ẩn danh, mặc dù về mặt kỹ thuật, có nhiều cách để truy tìm tung tích của cả hai hình thức thanh toán trên. Có thể tìm ra đường dây liên kết giữa các giao dịch trực tuyến bằng Bitcoin với người mua – nhưng đó không phải là việc dễ làm. Câu hỏi đặt ra là, ai sẽ dành ra thời gian và nỗ lực để theo đuổi những tên tội phạm này?

Trong chương tiếp theo, tôi sẽ nói về những gì có thể xảy ra khi bạn kết nối với Internet thông qua Wi-Fi công cộng. Từ quan điểm riêng tư, sự ẩn danh của Wi-Fi công cộng là điều tốt, nhưng nó cũng đồng nghĩa với việc bạn phải thực hiện những biện pháp đề phòng.

Chương 8: TIN TẤT CẢ, NHƯNG ĐỪNG TRÔNG CHỜ VÀO BẤT KỲ ĐIỀU GÌ

Khi mới ra đời, điện thoại được nối dây vào nhà và có lẽ được đặt trong một cái hộc nào đó trên tường. Gia đình nào có đường dây điện thoại thứ hai được coi là có vị thế lắm. Tương tự, các buồng điện thoại công cộng cũng được xây dựng để giữ gìn sự riêng tư. Đến cả dãy điện thoại trả tiền trong hành lang khách sạn cũng có vách ngăn âm thanh ở giữa để tạo ra ảo giác về sự riêng tư.

Với điện thoại di động, cảm thức về sự riêng tư đó đã hoàn toàn biến mất. Bây giờ ra ngõ là thấy cảnh mọi người vừa đi đường vừa oang oang nói chuyện điện thoại từ những việc hết sức cá nhân, hay tệ hơn là vô tư đọc số thẻ tín dụng đến người qua đường cũng nghe rành rọt không sót một câu. Sống trong nền văn hóa cởi mở và chia sẻ này, chúng ta cần phải suy nghĩ thận trọng về những gì mình chia sẻ.

Đôi khi cả thế giới cùng lắng nghe bạn đấy. Tôi chỉ nói vậy thôi.

Giả sử bạn cũng giống tôi, thích ngồi làm việc trong quán cà phê gần nhà. Họ có Wi-Fi miễn phí. Chuyện đó tốt mà, phải không? Tôi không muốn làm bạn thất vọng, nhưng không tốt chút nào cả đâu. Trong lúc tạo ra Wi-Fi công cộng, người ta không nghĩ đến ngân hàng trực tuyến hay thương mại điện tử. Nó chỉ đơn thuần là sự thuận tiện, và nó cũng rất không an toàn. Nhưng không phải tất cả sự không an toàn đó đều xuất phát từ khía cạnh kỹ thuật. Một phần trong đó bắt đầu – và hy vọng là kết thúc – với bạn.

Làm thế nào để biết bạn đang sử dụng mạng Wi-Fi công cộng? Thứ nhất, bạn sẽ không phải nhập mật khẩu để kết nối với điểm truy cập không dây. Để chứng minh sự sơ hở của bạn trên Wi-Fi công cộng, các nhà nghiên cứu thuộc công ty bảo mật và an ninh

mạng F-Secure đã tiến hành xây dựng điểm truy cập riêng, hay điểm phát sóng (hotspot). Họ triển khai thí nghiệm tại hai địa điểm khác nhau ở trung tâm London, một là quán cà phê và một là khu vực công cộng. Kết quả thu về khiến nhiều người phải sửng sốt.

Thí nghiệm đầu tiên được thực hiện tại một quán cà phê ở một khu vực nhộn nhịp của London. Khi các khách quen của quán duyệt qua danh sách các mạng khả dụng, điểm phát sóng của F-Secure hiển thị với tín hiệu mạng vừa mạnh vừa miễn phí. Các nhà nghiên cứu cũng gửi kèm một banner xuất hiện trên trình duyệt của người dùng, trong đó nêu rõ các điều khoản và điều kiện. Có lẽ bạn cũng từng thấy banner như thế này trong quán cà phê gần nhà với nội dung quy định những gì bạn được phép và không được phép làm khi sử dụng dịch vụ của họ. Tuy nhiên, trong thí nghiệm này, điều khoản sử dụng Wi-Fi miễn phí yêu cầu người dùng phải giao nộp đứa con đầu lòng hoặc thú cưng của mình. Sáu người nhấn nút đồng ý. Nói công bằng, hầu hết mọi người đều không dành thời gian đọc những văn bản có cỡ chữ nhỏ li ti mà chỉ muốn được sử dụng dịch vụ. Tuy nhiên, ít nhất bạn cũng nên lướt qua các điều khoản và điều kiện đó. Trong trường hợp này, về sau F-Secure cho biết rằng họ và các luật sư của họ không muốn nhận trẻ em hay thú cưng làm gì.

Vấn đề thực sự nằm ở những gì mà các bên thứ ba có thể nhìn thấy khi bạn sử dụng Wi-Fi công cộng. Kết nối không dây ở nhà của bạn cần được mã hóa bằng WPA2. Điều đó có nghĩa là nếu có kẻ rình mò, hắn sẽ không thể biết được bạn đang làm gì trên mạng. Nhưng khi bạn sử dụng mạng Wi-Fi công cộng tại một quán cà phê hoặc sân bay, lưu lượng truy cập ở đó sẽ không được bảo vệ.

Một lần nữa, bạn có thể hỏi, vậy thì sao chứ? Trước hết, bạn không biết ai đang ở đầu bên kia của kết nối. Trong trường hợp này, nhóm nghiên cứu của F-Secure đã tiêu hủy những dữ liệu mà họ thu thập được, nhưng tội phạm có thể sẽ không làm như vậy. Chúng sẽ bán địa chỉ email của bạn cho các công ty để họ gửi

thư rác nhằm gạ bạn mua hàng hoặc lây nhiễm phần mềm độc hại cho máy tính của bạn. Và chúng thậm chí có thể sử dụng nội dung trong các email không mã hóa của bạn để thực hiện các cuộc tấn công lừa đảo spear phishing.

Trong thí nghiệm thứ hai, nhóm nghiên cứu đặt điểm phát sóng trên một ban công gần Nhà Quốc hội là trụ sở của các đảng Lao động và Bảo thủ, và Cơ quan Tội phạm Quốc gia. Trong vòng 30 phút, điểm phát sóng này có tổng cộng 250 người kết nối, đa phần đều do các thiết bị mà họ sử dụng tự động kết nối. Nói cách khác, người dùng không chủ động chọn mạng mà thiết bị đã chọn mạng cho họ.

Có một vài vấn đề ở đây. Trước tiên, chúng ta hãy cùng tìm hiểu xem tại sao các thiết bị di động lại tự động kết nối mạng Wi-Fi, và chúng thực hiện điều đó như thế nào.

Máy tính cá nhân truyền thống và tất cả các thiết bị di động của bạn nhớ một số kết nối Wi-Fi gần nhất – cả công cộng và riêng tư. Điều này là tốt vì nó giúp bạn bớt đi sự phiền hà khi phải liên tục xác thực lại một điểm truy cập Wi-Fi thường dùng, như ở nhà hoặc nơi làm việc. Nhưng điều này cũng không tốt vì nếu bước vào một quán cà phê mới, một nơi bạn chưa từng đến trước đây, có thể bạn sẽ đột nhiên thấy rằng mình có kết nối không dây ở đó. Tại sao điều đó lại không tốt? Vì bạn có thể được kết nối với một số thứ khác chứ không phải với mạng không dây ở quán cà phê.

Khả năng là thiết bị di động của bạn đã phát hiện ra một điểm truy cập khớp với một hồ sơ đã có trong danh sách kết nối gần đây nhất của bạn. Có thể bạn thấy không yên tâm về việc kết nối Wi-Fi tự động ở một nơi chưa từng đến, nhưng mọi người xung quanh đang mải mê việc của họ nên bạn cũng tặc lưỡi cho qua.

Quá trình kết nối Wi-Fi tự động diễn ra như thế nào? Như tôi đã giải thích trong chương trước, có thể ở nhà bạn sử dụng dịch vụ Comcast Internet, và gói dịch vụ đó có thể bao gồm một SSID công cộng không mã hóa gọi là Xfinity. Thiết bị của bạn, lúc này đang bật chế độ bắt Wi-Fi, có thể đã kết nối với nó một lần trước

đây. Nhưng làm sao bạn có thể cam đoan rằng anh chàng có máy tính xách tay ngồi ở bàn trong góc quán kia không phát sóng một điểm truy cập không dây giả mạo có tên là Xfinity?

Giả sử bạn không kết nối với mạng không dây của quán cà phê mà với mạng của kẻ khả nghi kia. Trước tiên, bạn vẫn có thể lướt net bình thường. Tuy nhiên, mọi gói dữ liệu không mã hóa mà bạn gửi và nhận qua Internet đều không thoát khỏi tầm mắt của kẻ khả nghi này thông qua điểm truy cập không dây giả mạo trên máy tính xách tay của hắn.

Nếu hắn mất công thiết lập điểm truy cập không dây giả mạo, thì rất có khả năng hắn thu thập các gói dữ liệu trên bằng một ứng dụng miễn phí như Wireshark. Tôi vẫn sử dụng ứng dụng này khi kiểm định để theo dõi các hoạt động mạng đang diễn ra xung quanh. Tôi có thể thấy địa chỉ IP của các website mà mọi người đang kết nối cũng như thời lượng truy cập của họ. Nếu kết nối không có mã hóa, việc chặn lưu lượng dữ liệu là hợp pháp vì nó dành cho công chúng. Chẳng hạn, trên cương vị quản trị viên IT, tôi muốn biết các hoạt động diễn ra trên mạng lưới mà mình quản lý.

Có lẽ kẻ khả nghi ngồi trong góc quán cà phê kia chỉ đang đánh hơi sục sạo, theo dõi nơi bạn truy cập nhưng không tác động đến lưu lượng của bạn. Hoặc có thể hắn đang chủ động tác động đến lưu lượng truy cập Internet của bạn. Điều này sẽ phục vụ cho nhiều mục đích khác nhau.

Có thể hắn đang chuyển hướng kết nối của bạn đến một proxy để cấy keylogger javascript vào trình duyệt của bạn, và như vậy, khi bạn truy cập vào Amazon, mọi thao tác gõ bàn phím tương tác với website này sẽ bị ghi lại. Có thể hắn được thuê để thu thập các thông tin xác thực của bạn như tên người dùng và mật khẩu. Hãy nhớ rằng thẻ tín dụng của bạn có thể được liên kết với Amazon và các nhà bán lẻ khác.

Trong các buổi thuyết trình, tôi thường có phần minh họa cho thấy tôi có thể chặn tên người dùng và mật khẩu của nạn nhân

khi truy cập vào các website sau khi họ kết nối với điểm truy cập giả mạo của mình. Do đứng ở vị trí giữa trong luồng tương tác giữa nạn nhân và website, nên tôi có thể cài JavaScript và khiến các thông báo cập nhật Adobe giả xuất hiện trên màn hình của họ – nếu họ cài đặt theo yêu cầu, máy tính của nạn nhân sẽ bị nhiễm phần mềm độc hại. Mục đích ở đây thường là lừa bạn cài đặt bản cập nhật giả để chiếm quyền kiểm soát máy tính của bạn.

Khi gã khả nghi ngồi ở góc quán cà phê kia tác động đến luồng truy cập Internet, hành vi đó được gọi là tấn công xen giữa (MITM). Kẻ tấn công điều hướng các gói dữ liệu của bạn qua các trang web thực thụ, nhưng chặn hoặc cấy dữ liệu dọc đường di chuyển của chúng.

Vậy là bạn đã biết rằng mình có thể vô tình kết nối với một điểm truy cập Wi-Fi mờ ám, làm thế nào để ngăn chặn điều đó? Máy tính xách tay sẽ thực hiện quá trình tìm kiếm mạng không dây ưu tiên rồi kết nối. Nhưng một số máy tính xách tay và thiết bị di động tự động chọn mạng để tham gia – phương án này nhằm hỗ trợ cho quá trình di chuyển thiết bị di động từ địa điểm này sang địa điểm khác diễn ra suôn sẻ tối đa. Nhưng như tôi đã nói, sự thuận tiện không phải không đi kèm với những nhược điểm.

Theo Apple, các sản phẩm của họ sẽ tự động kết nối mạng theo thứ tự ưu tiên như sau:

1. mạng riêng tư mà thiết bị kết nối gần đây nhất,

2. một mạng riêng tư khác, và

3. một điểm phát sóng (hotspot).

Thật may là máy tính xách tay có phương tiện xóa các kết nối Wi-Fi lỗi thời – chẳng hạn Wi-Fi ở khách sạn mà bạn kết nối vào mùa hè năm ngoái trong một chuyến công tác. Với máy tính xách tay sử dụng Windows, hãy bỏ chọn trường “Connect Automatically” (Kết nối tự động) bên cạnh tên mạng trước khi bạn kết nối. Hoặc đi đến Control Panel>Network and Sharing Center (Bảng điều khiển>Trung tâm mạng và chia sẻ) và nhấp vào tên mạng. Nhấp

vào “Wireless Properties” (Thuộc tính không dây), rồi bỏ chọn “Connect automatically when this network is in range” (Tự động kết nối khi mạng này ở trong phạm vi phủ sóng). Với máy Mac, chuyển đến System Preferences (Tùy chọn hệ thống), đến Network (Mạng), đánh dấu Wi-Fi trên bảng điều khiển bên trái, và nhấp vào “Advanced” (Nâng cao). Sau đó, bỏ chọn “Remember networks this computer has joined” (Nhớ các mạng mà máy tính này đã kết nối). Bạn cũng có thể xóa từng mạng bằng cách chọn tên mạng và nhấn dấu trừ bên dưới.

Các thiết bị Android và iOS cũng có hướng dẫn xóa các kết nối Wi-Fi đã sử dụng trước đây. Với iPhone hoặc iPod, đi tới phần cài đặt, chọn “Wi-Fi,” nhấp vào biểu tượng “i” bên cạnh tên mạng, và chọn “Forget this Network” (Quên mạng này). Với điện thoại Android, đi tới phần cài đặt, chọn “Wi-Fi,” nhấn và giữ ở tên mạng, và chọn “Forget Network” (Quên mạng).

Nói nghiêm túc, nếu bạn thực sự cần phải làm điều gì đó nhạy cảm bên ngoài nhà, tôi khuyên bạn nên sử dụng kết nối di động trên thiết bị di động thay vì mạng không dây tại sân bay hoặc quán cà phê. Bạn cũng có thể kết nối mạng bằng thiết bị di động cá nhân thông qua USB, Bluetooth, hoặc Wi-Fi. Nếu sử dụng Wi-Fi, hãy cài đặt cấu hình bảo mật WPA2 theo hướng dẫn ở phần trước. Một phương án khác là mua thiết bị phát sóng cá nhân (portable hotspot) để sử dụng khi di chuyển. Cũng xin lưu ý rằng cách này sẽ không làm cho bạn vô hình, nhưng là phương án thay thế tốt hơn so với sử dụng Wi-Fi công cộng. Nhưng nếu bạn cần giữ sự riêng tư trước con mắt của nhà mạng di động – ví dụ để tải xuống một bảng tính nhạy cảm – hãy sử dụng HTTPS Everywhere hoặc Giao thức truyền file bảo mật (Secure File Transfer Protocol – SFTP). SFTP được hỗ trợ bằng ứng dụng Transmit trên máy Mac và ứng dụng Tunnelier trên Windows.

Mạng riêng ảo (virtual private network – VPN) là một “đường hầm” bảo mật mở rộng mạng riêng (từ nhà, văn phòng, hoặc nhà cung cấp dịch vụ VPN) đến thiết bị của bạn trên mạng công cộng. Bạn có thể vào Google tìm kiếm các nhà cung cấp VPN và đăng ký

mua dịch vụ với giá khoảng 60 đô-la một năm. Các mạng mà bạn tìm thấy tại quán cà phê gần nhà, sân bay, hoặc ở những nơi công cộng khác đều không đáng tin cậy – bởi vì chúng là mạng công cộng. Nhưng bằng cách sử dụng VPN, bạn có thể luồn qua mạng công cộng để quay về với một mạng riêng và an toàn. Mọi hoạt động của bạn trong VPN đều được bảo vệ bằng mã hóa, vì tất cả lưu lượng truy cập Internet của bạn lúc này đều được thực hiện qua mạng công cộng. Đó là lý do tại sao việc sử dụng nhà cung cấp VPN đáng tin cậy là rất quan trọng – bởi họ có thể thấy luồng truy cập Internet của bạn. Khi bạn sử dụng VPN ở quán cà phê, gã khả nghi ngồi ở góc phòng kia chỉ có thể thấy rằng bạn vừa kết nối với một máy chủ VPN và không thấy gì nữa cả – hoạt động của bạn và các website mà bạn truy cập được che giấu hoàn toàn sau lớp mã hóa khó phá giải.

Tuy nhiên, bạn vẫn sẽ tiếp xúc với Internet bằng địa chỉ IP có thể truy nguyên trực tiếp về bạn, trong trường hợp này là địa chỉ IP từ nhà hoặc văn phòng của bạn. Như vậy, bạn vẫn chưa thực sự tàng hình, ngay cả khi sử dụng VPN. Đừng quên, nhà cung cấp VPN biết địa chỉ IP gốc của bạn. Chúng ta sẽ bàn về cách khiến kết nối này tàng hình ở phần sau.

Nhiều công ty trang bị VPN cho nhân viên, cho phép họ kết nối từ mạng công cộng (tức là Internet) tới mạng nội bộ riêng của công ty. Nhưng những người như chúng ta thì sao?

Hiện nay có nhiều dịch vụ VPN thương mại. Nhưng làm thế nào để biết là họ đáng tin cậy? Công nghệ VPN cơ bản là giao thức bảo mật Internet (Internet protocol security – IPsec) tự động bao gồm PFS; nhưng không phải tất cả các dịch vụ – ngay cả dịch vụ dành cho doanh nghiệp – chịu cấu hình nó. OpenVPN, một dự án mã nguồn mở, có cung cấp PFS, như vậy bạn có thể suy luận rằng khi một sản phẩm thông báo rằng nó sử dụng OpenVPN thì nó cũng đồng thời sử dụng PFS, nhưng điều này không phải lúc nào cũng đúng. Sản phẩm có thể không được cấu hình OpenVPN đúng cách. Hãy tìm hiểu để chắc chắn rằng dịch vụ mà bạn sẽ sử dụng có bao gồm PFS.

Một điểm bất lợi là các VPN đắt hơn proxy. Và do các dịch vụ VPN thương mại được dùng chung, nên tốc độ của chúng có thể tương đối chậm, hoặc trong một số trường hợp, bạn phải chờ người khác dùng xong mới có được một cổng VPN để dùng riêng. Một phiền toái khác là trong một số trường hợp, Google sẽ hiển thị CAPTCHA yêu cầu bạn nhập các ký tự có trên màn hình rồi mới cho phép bạn sử dụng công cụ tìm kiếm của nó vì nó muốn đảm bảo bạn là con người chứ không phải là bot[73]. Cuối cùng, nếu nhà cung cấp VPN lưu nhật ký, hãy đọc chính sách bảo mật của họ để đảm bảo rằng dịch vụ này không lưu lại lưu lượng truy cập hoặc nhật ký kết nối của bạn – kể cả những nội dung đã được mã hóa – và rằng họ không dễ dàng chấp nhận chia sẻ dữ liệu với cơ quan thực thi pháp luật. Bạn có thể tìm hiểu điều này trong các điều khoản dịch vụ và chính sách bảo mật. Nếu họ có thể báo cáo các hoạt động cho cơ quan thực thi pháp luật, tức là họ có ghi nhật ký các phiên kết nối VPN.

[73] Bot: Một chương tình máy tính vận hành tự động, đặc biệt nhằm tìm kiếm thông tin trên Internet.

Hành khách đi máy bay sử dụng dịch vụ Internet hàng không như GoGo cũng có nguy cơ tương tự như khi họ vào mạng trong quán cà phê Starbucks hoặc phòng chờ sân bay, và VPN không phải lúc nào cũng là giải pháp tuyệt vời. Vì muốn ngăn chặn Skype hay các ứng dụng gọi thoại khác, GoGo và các dịch vụ mạng hàng không khác hạn chế các gói UDP[74], khiến hầu hết các dịch vụ VPN đều trở nên rất chậm vì UDP là giao thức được sử dụng nhiều nhất theo mặc định. Tuy nhiên, chất lượng mạng sẽ cải thiện đáng kể nếu bạn chọn một dịch vụ VPN sử dụng giao thức TCP thay vì UDP, chẳng hạn như TorGuard hoặc ExpressVPN. Cả hai dịch vụ VPN này cho phép người dùng đặt TCP hoặc UDP làm giao thức ưu tiên.

[74] UDP (User Datagram Protocol – Giao thức dữ liệu người dùng): Một phần trong Giao thức Internet (IP), được các chương trình chạy trên nhiều máy tính khác nhau trên một mạng sử dụng. UDP được dùng để gửi các tin nhắn ngắn gọi là datagram.

Một vấn đề cần lưu tâm khác với VPN là chính sách bảo mật. Cho dù bạn sử dụng VPN thương mại hay VPN do công ty cung cấp, lưu lượng dữ liệu của bạn đều di chuyển qua mạng của VPN đó – đây là lý do tại sao lại cần sử dụng https để nhà cung cấp VPN không thể xem nội dung các liên lạc của bạn.

Nếu bạn làm việc trong một văn phòng, rất có thể công ty bạn sẽ trang bị VPN để nhân viên có thể làm việc từ xa. Trong một ứng dụng trên máy tính cá nhân truyền thống, bạn nhập tên người dùng và mật khẩu (thứ mà bạn biết). Ứng dụng này cũng chứa một chứng chỉ xác minh danh tính do phòng IT đưa vào (thứ bạn đã có), hoặc nó có thể gửi cho bạn một tin nhắn trên điện thoại do công ty trang bị (cũng là thứ bạn đã có). Ứng dụng này có thể kết hợp cả ba kỹ thuật trên thành một quá trình gọi là xác thực đa yếu tố (multifactor authentication).

Bây giờ, bạn có thể ngồi ở một quán Starbucks hoặc phòng chờ sân bay và làm việc như thể bạn đang sử dụng một dịch vụ Internet riêng tư. Tuy nhiên, không nên thực hiện các công việc cá nhân ở đây, chẳng hạn ngân hàng từ xa, trừ khi phiên truy cập được mã hóa bằng phần mở rộng HTTPS Everywhere.

Cách duy nhất để tin tưởng một nhà cung cấp VPN là ẩn danh ngay từ đầu. Nếu bạn thực sự muốn ẩn danh hoàn toàn, đừng bao giờ sử dụng kết nối Internet có thể được liên kết với bạn (tức là các kết nối bắt nguồn từ nhà, văn phòng, nhà bạn bè, phòng khách sạn do bạn đứng tên đặt chỗ, hay bất kỳ thứ gì khác liên quan đến bạn). Hồi những năm 1990, tôi bị bắt khi FBI lần theo tín hiệu điện thoại di động dẫn đến nơi ẩn náu của tôi ở Raleigh, Bắc Carolina. Vì vậy, nếu bạn muốn tránh các cơ quan chính phủ, đừng bao giờ truy cập thông tin cá nhân bằng điện thoại ẩn danh ở cùng một địa điểm. Để tàng hình được, mọi hoạt động thực hiện trên thiết bị ẩn danh phải được tách biệt hoàn toàn. Nghĩa là không có siêu dữ liệu nào từ thiết bị đó có thể liên kết với danh tính thực của bạn.

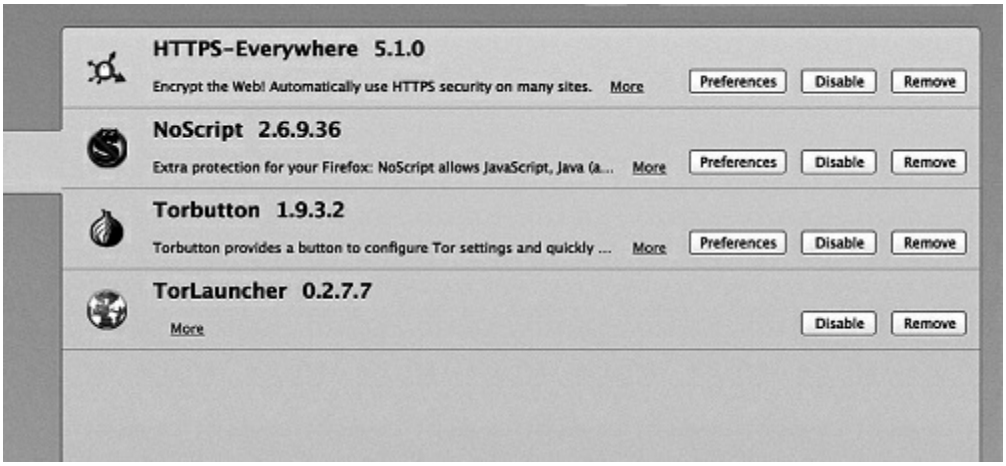
Bạn cũng có thể cài đặt VPN trên thiết bị di động. Cả Apple và Android đều có hướng dẫn cách làm.

Nếu bạn làm theo lời khuyên của tôi trong cuốn sách cho đến lúc này, tức là bạn đã làm tốt hơn nhiều so với người bình thường rồi đấy. Hầu hết các hoạt động sử dụng Internet của bạn bây giờ sẽ được an toàn, không bị nghe lén hay chịu sự thao túng của kẻ xấu.

Tài khoản mạng xã hội của bạn cũng vậy. Facebook sử dụng https cho tất cả các phiên truy cập.

Email thì sao? Google cũng vừa mới chuyển sang chỉ dùng https. Phần lớn các dịch vụ webmail và dịch vụ nhắn tin tức thời cũng đã và đang làm theo họ. Thực ra, hầu hết các website lớn – Amazon, eBay, Dropbox – bây giờ đều đã sử dụng https.

Để ẩn danh, tốt nhất là nên bảo vệ quyền riêng tư của bạn theo nhiều lớp. Nguy cơ lưu lượng dữ liệu của bạn bị người lạ nhìn thấy trong một mạng công cộng sẽ giảm xuống tỉ lệ thuận với số lớp bảo mật bổ sung mà bạn sử dụng. Ví dụ, từ mạng Wi-Fi công cộng, hãy truy cập dịch vụ VPN trả phí, sau đó truy cập Tor bằng tiện ích HTTPS Everywhere được cài đặt mặc định trong trình duyệt Firefox.



Như vậy, mọi hoạt động trên mạng của bạn sẽ được mã hóa và rất khó theo dõi.

Giả sử bạn chỉ muốn xem dự báo thời tiết và không có hoạt động gì liên quan đến tài chính hay các vấn đề cá nhân, và bạn đang sử dụng máy tính xách tay cá nhân bên ngoài mạng nhà riêng – điều

đó sẽ an toàn, đúng không? Một lần nữa, không hẳn. Bạn vẫn cần phải thực hiện một số biện pháp phòng ngừa đấy.

Trước tiên, hãy tắt Wi-Fi đi. Tôi nói nghiêm túc đấy. Nhiều người có thói quen để Wi-Fi trên máy tính xách tay ở chế độ bật ngay cả khi không có nhu cầu sử dụng. Theo các tài liệu do Edward Snowden công bố, Cơ quan An ninh Truyền thông Canada (CSEC) có thể xác định được danh tính của du khách đi qua các sân bay Canada chỉ bằng cách ghi lại địa chỉ MAC của họ, vốn là thứ mà bất kỳ máy tính nào đang tìm kiếm yêu cầu dò mạng từ các thiết bị không dây đều có thể đọc được. Ngay cả khi bạn không kết nối, địa chỉ MAC vẫn có thể bị thu thập. Vì vậy, nếu không có nhu cầu sử dụng Wi-Fi, hãy tắt nó đi. Như chúng ta đã thấy, sự tiện lợi thường là kẻ thù của sự riêng tư và an toàn.

Tới lúc này, chúng ta vẫn chưa bàn sâu về một vấn đề quan trọng – địa chỉ MAC. Địa chỉ này là duy nhất đối với bất kỳ thiết bị nào bạn đang sử dụng. Và nó không phải là vĩnh viễn; bạn có thể thay đổi nó.

Tôi sẽ cho bạn một ví dụ.

Trong Chương 2, tôi đã nói về việc mã hóa email bằng PGP. Nhưng điều gì sẽ xảy ra nếu bạn không muốn thực hiện quy trình phiền phức ấy, hay nếu người nhận không có khóa PGP công khai để bạn sử dụng? Có một cách bí mật khác để trao đổi qua email: sử dụng thư mục nháp trong tài khoản email dùng chung.

Đây là cách liên lạc giữa cựu giám đốc CIA David Petraeus với Paula Broadwell, tình nhân đồng thời là người viết tiểu sử cho ông. Vụ bê bối này bị lộ sau khi Petraeus kết thúc mối quan hệ tình cảm ngoài luồng này và nhận thấy có người gửi email hăm dọa đến một người bạn của ông. Khi FBI điều tra, họ không chỉ phát hiện ra rằng những lời đe dọa đó đến từ Broadwell, mà còn biết được rằng cô có gửi cho Petraeus những thông điệp tình tứ.

Điều thú vị ở đây là các thông điệp giữa Broadwell và Petraeus không được gửi đi mà nằm ở thư mục nháp của tài khoản email "ẩn danh." Trong trường hợp này, email không đi qua các máy

chủ khác để đến tay người nhận, vì vậy không có cơ hội chặn email. Và về sau, nếu có người truy cập được vào tài khoản này, sẽ không có bằng chứng nào cả, nếu như bạn xóa email và dọn sạch thùng rác từ trước đó.

Broadwell cũng dùng một máy tính riêng để đăng nhập vào tài khoản email "ẩn danh" của mình. Cô không truy cập website email từ địa chỉ IP ở nhà riêng. Như thế sẽ quá lộ liễu. Thay vào đó, cô đến nhiều khách sạn khác nhau để thực hiện liên lạc.

Tuy đã vất vả giấu mình như vậy, song Broadwell vẫn không thể tàng hình. Theo tờ New York Times, "vì tài khoản của người gửi đã được đăng ký ẩn danh, nên các nhà điều tra phải sử dụng các kỹ thuật pháp y máy tính – bao gồm kiểm tra các tài khoản email khác đã được truy cập từ cùng một địa chỉ máy tính trên – để xác định người viết email."

Các nhà cung cấp dịch vụ email như Google, Yahoo, và Microsoft lưu lại bản ghi về các phiên đăng nhập của người dùng trong hơn một năm, và những thông tin này tiết lộ địa chỉ IP cụ thể mà người dùng đã đăng nhập. Ví dụ, nếu bạn từng sử dụng Wi-Fi công cộng ở Starbucks, địa chỉ IP sẽ tiết lộ vị trí thực của cửa hàng đó. Mỹ hiện cho phép các cơ quan thực thi pháp luật thu giữ những bản ghi này từ các nhà cung cấp dịch vụ email – tất cả chỉ với một trát hầu tòa, chưa cần đến thẩm phán.

Như vậy, các nhà điều tra nắm được vị trí của từng địa chỉ IP đã liên hệ với tài khoản email "ẩn danh" trên, sau đó đem khớp với thông tin về địa chỉ MAC của thiết bị mà Broadwell sử dụng được lưu trong nhật ký kết nối của bộ định tuyến tại các địa điểm đó.

Nhờ sự hậu thuẫn là quyền lực của FBI (đây là một vấn đề lớn, bởi vì khi đó Petraeus vẫn đang là Giám đốc CIA), các đặc vụ có thể tìm kiếm trong tất cả các file nhật ký của bộ định tuyến cho từng khách sạn để xem địa chỉ MAC của Broadwell xuất hiện khi nào. Hơn nữa, họ còn có thể chỉ ra rằng vào những ngày cụ thể, Broadwell là một khách đăng ký. Các nhà điều tra cũng lưu ý rằng tuy đăng nhập vào các tài khoản email này, song Broadwell chưa

bao giờ thực sự gửi một email nào đi cả.

Khi bạn kết nối với mạng không dây, thiết bị mạng không dây sẽ tự động ghi lại địa chỉ MAC trên máy tính của bạn. Địa chỉ MAC tương tự như một số sê-ri được gán cho card mạng[75] của bạn. Để ẩn danh, trước khi kết nối với bất kỳ mạng không dây nào, bạn phải thay đổi địa chỉ MAC thành một địa chỉ không liên quan đến bạn.

[75] Card mạng (network card): Hay còn gọi là card giao tiếp mạng (network interface card), là một bản mạch cung cấp khả năng truyền thông mạng cho một máy tính.

Để ẩn danh, bạn phải thay đổi địa chỉ MAC mỗi lần kết nối với mạng không dây, như vậy việc tìm ra mối tương quan giữa bạn với các phiên truy cập Internet của bạn sẽ trở nên khó khăn. Trong quá trình này, không nên truy cập vào bất kỳ tài khoản trực tuyến cá nhân nào vì điều đó có thể ảnh hưởng tới tính ẩn danh của bạn.

Các hướng dẫn thay đổi địa chỉ MAC tùy thuộc vào từng hệ điều hành – Windows, Mac OS, Linux, thậm chí cả Android và iOS. Mỗi khi kết nối với mạng công cộng (hoặc riêng tư), hãy nhớ thay đổi địa chỉ MAC của mình. Sau khi khởi động lại, máy sẽ được trả về địa chỉ MAC ban đầu.

Giả sử bạn không có máy tính xách tay và buộc phải sử dụng máy tính công cộng – có thể là ở một quán cà phê, thư viện, hay thậm chí là ở khu dịch vụ văn phòng trong một khách sạn cao cấp. Bạn cần làm gì để bảo vệ bản thân?

Khi đi cắm trại, tôi tuân theo quy tắc "không để lại dấu vết" – nghĩa là nơi hạ trại phải trông giống như khi tôi mới đến. Điều này cũng đúng với các thiết bị máy tính công cộng. Sau khi bạn rời đi, không ai được biết bạn từng ở đó.

Điều này đặc biệt đúng ở các triển lãm thương mại. Một năm nọ, tôi tới dự Triển lãm Điện tử Dân dụng thường niên và thấy một dãy máy tính công cộng xếp hàng để khách tham gia có thể vào

kiểm tra email trong thời gian ở đây. Tôi còn thấy cả cảnh này trong hội nghị an ninh RSA thường niên ở San Francisco. Nhưng đây là một ý tưởng tồi, vì một số lý do.

Thứ nhất, đây là những máy tính đi thuê, được đem đi sử dụng từ sự kiện này đến sự kiện khác. Có thể người ta đã làm sạch máy, cài đặt lại hệ điều hành, nhưng có khi là chưa.

Thứ hai, chúng thường vận hành với quyền quản trị viên, có nghĩa là người tham dự hội nghị có thể cài đặt bất kỳ phần mềm nào tùy ý – kể cả những phần mềm độc hại như keylogger, có thể lưu trữ thông tin tên người dùng và mật khẩu của bạn. Trong công tác bảo mật, chúng tôi có nguyên tắc "đặc quyền tối thiểu," nghĩa là máy chỉ cấp cho người dùng những đặc quyền tối thiểu mà họ cần để thực hiện công việc. Việc đăng nhập vào máy công cộng với quyền quản trị hệ thống, vốn là chế độ mặc định ở một số máy công cộng, là vi phạm nguyên tắc đặc quyền tối thiểu và sẽ chỉ càng làm gia tăng nguy cơ rằng bạn đang sử dụng một thiết bị đã bị nhiễm phần mềm độc hại. Giải pháp duy nhất ở đây là hãy sử dụng tài khoản khách với các đặc quyền hạn chế, nhưng hầu hết mọi người đều không biết cách thực hiện điều này ra sao.

Nhìn chung, tôi khuyên bạn đừng bao giờ tin tưởng vào một thiết bị công cộng. Giả sử người sử dụng lần cuối đã cố ý hoặc vô tình cài đặt phần mềm độc hại vào đó. Nếu bạn đăng nhập vào Gmail trên máy tính công cộng đã bị cài keylogger, thì lúc này một bên thứ ba từ xa nào đó sẽ nắm được tên người dùng và mật khẩu của bạn. Nếu bạn đăng nhập vào tài khoản ngân hàng – tốt nhất đừng nghĩ tới chuyện này. Hãy nhớ bật 2FA trên mọi website bạn truy cập để kẻ tấn công tuy có tên người dùng và mật khẩu của bạn nhưng không thể mạo danh bạn được. Xác thực hai yếu tố sẽ làm giảm đáng kể khả năng tài khoản của bạn bị tấn công trong trường hợp có người lấy được thông tin về tên người dùng và mật khẩu của bạn.

Số lượng người sử dụng máy tính công cộng tại các hội nghị liên quan đến máy tính như CES và RSA không khỏi khiến tôi sửng sốt. Tóm lại, nếu bạn đang ở một triển lãm thương mại, hãy sử

dụng điện thoại hay máy tính bảng có hỗ trợ mạng di động, điểm phát sóng cá nhân, hoặc đợi cho đến khi quay về nhà.

Nếu phải dùng Internet cách xa nhà hoặc văn phòng, hãy sử dụng điện thoại thông minh. Nếu bắt buộc phải sử dụng máy tính công cộng, thì bằng bất cứ giá nào cũng không được đăng nhập vào bất kỳ tài khoản cá nhân nào, kể cả webmail. Chẳng hạn, nếu muốn tìm kiếm một nhà hàng, hãy chỉ truy cập những website không yêu cầu xác thực, ví dụ Yelp. Nếu thi thoảng bạn lại phải sử dụng máy tính công cộng, hãy thiết lập một tài khoản email dùng riêng cho thiết bị công cộng, và chỉ chuyển tiếp email từ tài khoản chính thức tới địa chỉ "dùng một lần" này khi đang ở bên ngoài. Khi đã về nhà, đừng chuyển tiếp email như vậy nữa – điều này sẽ làm giảm thiểu lượng thông tin có thể tìm thấy theo địa chỉ email kia.

Tiếp theo, hãy kiểm tra để chắc chắn rằng các website mà bạn truy cập từ thiết bị công cộng đều https trong URL. Nếu không thấy https (hoặc nếu có thấy nhưng bạn nghi ngờ rằng có người đã đặt nó ở đó để tạo cảm giác an toàn giả cho bạn), thì có lẽ bạn nên xem xét lại việc truy cập các thông tin nhạy cảm từ thiết bị công cộng này.

Giả sử bạn có URL https hợp lệ. Nếu đang ở trên trang đăng nhập, hãy tìm hộp chọn có nội dung "Keep me logged in" (Giữ cho tôi đăng nhập). Hãy bỏ tích chọn. Lý do thì đã rõ ràng: đây không phải là máy tính cá nhân của bạn. Nhiều người khác cũng sử dụng nó. Nếu duy trì trạng thái đăng nhập, bạn sẽ tạo ra một cookie trên máy đó. Bạn không muốn người tiếp theo sử dụng chiếc máy này nhìn thấy email của bạn hoặc có thể gửi email từ địa chỉ của bạn, đúng không nào?

Như tôi đã lưu ý, đừng đăng nhập vào các website tài chính hoặc y tế từ một thiết bị công cộng. Nếu bạn đăng nhập vào một website (Gmail hay các trang khác), thì khi sử dụng xong, hãy nhớ đăng xuất, thậm chí sau đó có thể thay đổi mật khẩu tài khoản trên đó từ máy tính hoặc thiết bị di động riêng của bạn để đảm bảo an toàn. Khi ở nhà, bạn không cần phải thường xuyên

đăng xuất khỏi các tài khoản của mình, nhưng hãy luôn nhớ thực hiện thao tác này khi sử dụng máy tính của người khác.

Sau khi đã gửi email (hoặc làm bất kỳ điều gì cần làm) và đăng xuất, hãy xóa lịch sử trình duyệt để người tiếp theo không biết bạn đã ở đâu. Nếu có thể, hãy xóa luôn các cookie. Và nhớ đừng tải xuống các file cá nhân. Nếu buộc phải làm vậy, sau khi xong việc hãy xóa file khỏi màn hình nền hay thư mục tải về.

Mặc dù vậy, thật không may, chỉ xóa file thôi thì vẫn chưa đủ. Tiếp theo, bạn phải dọn sạch thùng rác nữa. Nhưng như thế vẫn chưa gỡ bỏ được hoàn toàn file đã xóa khỏi máy tính – nếu muốn, tôi vẫn có thể gọi lại file đó sau khi bạn rời đi. Thật may, hầu hết mọi người đều không có khả năng thực hiện điều đó, và thường thì bạn chỉ cần xóa và dọn sạch thùng rác là đủ rồi. Tất cả các bước này là cần thiết để bạn được vô hình trên một thiết bị công cộng.

Chương 9: BẠN KHÔNG CÓ QUYỀN RIÊNG TƯ Ư? HÃY QUÊN CHUYỆN ĐÓ ĐI!

Trong thời gian sinh sống ở Belize[76] để trốn tránh chính quyền, cựu lập trình viên sáng tạo ra phần mềm chống virus John McAfee lập một blog. Hãy tin lời tôi: Nếu bạn đang muốn cắt đứt mọi liên lạc và biến mất hoàn toàn, đừng bao giờ lập blog. Vì một lẽ, kiểu gì bạn cũng sẽ phạm sai lầm.

[76] Belize: Một quốc gia ở Trung Mỹ.

McAfee là người thông minh. Từ những ngày đầu của Thung lũng Silicon, ông đã gây dựng được cơ đồ nhờ tiên phong trong hoạt động nghiên cứu chống virus. Sau đó, ông bán công ty cùng tất cả các tài sản riêng ở Mỹ để chuyển đến sống trong một tư dinh ngoài khơi ở Belize suốt gần bốn năm, từ 2008 đến 2012. Vào cuối giai đoạn đó, chính phủ Belize đặt ông dưới sự giám sát gần như liên tục, tấn công vào tư dinh của ông và cáo buộc ông tội chiêu mộ quân đội riêng và buôn bán ma túy.

McAfee phủ nhận cả hai tội danh trên. Ông cho hay chính ông cũng tham gia chiến đấu chống lại các trùm ma túy trên đảo. Ví dụ, ông nói từng mua một chiếc ti-vi màn hình phẳng cho một người buôn bán cần sa nhỏ lẻ với điều kiện người đó phải cam kết ngừng bán ma túy. Người ta cũng vài lần thấy ông bắt những chiếc xe mà ông nghi đang chở các trùm ma túy phải dừng lại.

Thực ra, đúng là McAfee có một phòng thí nghiệm ma túy, nhưng không nhất thiết nhằm mục đích nghiên cứu các loại ma túy phục vụ thú tiêu khiển. McAfee tuyên bố ông đang tạo ra một thế hệ ma túy "hữu ích" mới. Vì vậy mà ông ngày càng nghi ngờ rằng những chiếc xe chở đầy những người da trắng lượn lờ bên ngoài tư dinh của mình là gián điệp từ các hãng dược phẩm như GlaxoSmithKline. Ông còn nói rằng các cuộc tấn công của cảnh

sát địa phương là do chính các hãng đó xúi giục.

McAfee sử dụng một số người và đàn chó 11 con để bảo vệ tư dinh của mình. Greg Faull, một người hàng xóm ở cách đó hai ngôi nhà về phía nam, thường xuyên phàn nàn với chính quyền về việc đàn chó sủa vào ban đêm. Rồi một đêm vào tháng 11 năm 2012, một vài con chó của McAfee bị đầu độc. Và sau đó trong cùng tuần, Faull bị bắn; người ta tìm thấy anh ta trong tư thế nằm úp mặt trong một vũng máu trong nhà.

Như một lẽ hiển nhiên, các nhà chức trách Belize coi McAfee là một nghi phạm trong cuộc điều tra của họ. Theo thông tin McAfee thuật lại trên blog, khi được quản gia thông báo cảnh sát muốn nói chuyện với ông, ông đã chạy đi. Ông trở thành một kẻ chạy trốn.

Nhưng blog không phải là nguyên nhân cuối cùng khiến cơ quan thực thi pháp luật tìm ra McAfee. Mà là một bức ảnh. Và đó thậm chí không phải là ảnh của ông.

Một nhà nghiên cứu bảo mật tên là Mark Loveless (được giới bảo mật quen gọi là Simple Nomad – người du mục giản dị) trông thấy một bức ảnh chụp McAfee được tạp chí Vice đăng trên Twitter vào đầu tháng 12 năm 2012. Trong ảnh, biên tập viên của Vice đứng cạnh McAfee ở một khu vực nhiệt đới – có thể là Belize hoặc nơi nào khác.

Biết rằng các bức ảnh kỹ thuật số lưu giữ rất nhiều thông tin về thời gian, địa điểm, và cách chúng được chụp như thế nào, Loveless muốn xem bức ảnh trên chứa những thông tin gì. Ảnh kỹ thuật số lưu trữ file dữ liệu hình ảnh có thể trao đổi, hay EXIF. Đây là siêu dữ liệu ảnh, và nó chứa các thông tin chi tiết khô khan như lượng bão hòa màu để có thể sao chép lại hay in lại ảnh một cách chính xác. Nếu camera có trang bị tính năng phù hợp, ảnh còn có thể chứa dữ liệu chính xác về kinh độ và vĩ độ của nơi chụp ảnh.

Rõ ràng, bức ảnh của McAfee với biên tập viên tạp chí Vice được chụp bằng camera từ một chiếc iPhone 4S. Một số điện thoại di

động khi bán ra đã tự động bật sẵn tính năng định vị. Loveless đã gặp may: hình ảnh được đăng trong file trực tuyến bao gồm thông tin về vị trí địa lý chính xác của John McAfee, lúc đó đang ở gần Guatemala.Trong một bài đăng tiếp theo trên blog, McAfee cho biết ông đã giả mạo dữ liệu trên, nhưng thực tế có vẻ không phải vậy. Sau đó, ông nói ông cố tình tiết lộ vị trí của mình, nhưng có lẽ do lười thì đúng hơn.

Kể tóm tắt câu chuyện dài, cảnh sát Guatemala bắt giữ McAfee và không chịu để ông rời khỏi đất nước họ. Sau đó, ông phải nhập viện vì vấn đề sức khỏe nên cuối cùng được phép trở về Mỹ.

Vụ án giết Greg Faull cho đến nay vẫn chưa được phá giải. McAfee hiện đang sống ở Tennessee, và vào năm 2015, ông quyết định tranh cử tổng thống để ủng hộ cho nhiều chính sách thân thiện với không gian mạng hơn trong chính phủ Mỹ. Và ông cũng ít viết blog hơn.

Giả sử bạn là một lính thánh chiến trẻ tuổi đầy tham vọng đang rất đỗi tự hào khi được giao đứng gác ở một trụ sở quân sự mới thành lập của ISIS[77]. Điều đầu tiên bạn sẽ làm là gì? Rút điện thoại ra và chụp ảnh tự sướng. Tệ hơn nữa, ngoài bức ảnh tự sướng tại nơi ở mới, bạn còn đăng kèm một vài câu nhận xét về các thiết bị tinh vi được trang bị ở đó.

[77] ISIS (hay Daesh/ISIL): Tên một tổ chức Hồi giáo cực đoan dòng Sunni.

Cách đó nửa vòng Trái đất, các phi công trinh sát tại sân bay Hurlburt Field ở Florida đang tìm kiếm trên các phương tiện truyền thông xã hội thì bắt gặp bức ảnh này. “Chúng ta có tay trong đây rồi,” một người nói. Quả nhiên, vài giờ sau, ba quả bom JDAM đã san bằng tòa nhà quân sự mới còn chưa bay hết mùi vữa. Tất cả chỉ vì một bức ảnh tự sướng.

Không phải lúc nào chúng ta cũng nghĩ đến những thứ khác lọt vào trong khung ảnh tự sướng vừa chụp – trong điện ảnh, đây được gọi là mise-en-scène, dịch từ tiếng Pháp có nghĩa là “những gì có trong bối cảnh.” Trong bức ảnh của bạn có thể thấy cảnh

một đường chân trời nơi thành phố đông đúc và Tháp Tự do lấp ló bên ngoài cửa sổ căn hộ. Ngay cả một bức ảnh chụp bạn trong khung cảnh thôn dã – có thể là một đồng cỏ trải dài tít tắp tới đường chân trời – cũng có thể cung cấp cho tôi những thông tin giá trị về nơi bạn sinh sống. Những hình ảnh này chứa các manh mối tí hon về địa điểm cho người nào muốn tìm bạn.

Trong trường hợp của người lính thánh chiến trẻ tuổi trên, những gì có trong bối cảnh là một trụ sở quân sự.

Trong siêu dữ liệu của bức ảnh tự sướng đó còn có kinh độ và vĩ độ chính xác – hay vị trí địa lý – của nơi chụp ảnh. Tướng Hawk Carlisle, người đứng đầu Bộ Tư lệnh Không quân Hoa Kỳ, ước tính chỉ mất 24 tiếng đồng hồ kể từ khi bức ảnh tự sướng được đăng lần đầu tiên trên mạng xã hội cho đến khi trụ sở đó bị tiêu diệt hoàn toàn.

Dĩ nhiên, có thể dùng siêu dữ liệu trong file hình ảnh để định vị bạn. Dữ liệu EXIF trong một hình ảnh kỹ thuật số chứa thông tin về ngày và giờ chụp, nhà sản xuất và model của máy ảnh, kinh độ và vĩ độ của nơi chụp (nếu bạn bật tính năng định vị trên máy). Chính từ thông tin này trong file mà quân đội Mỹ có thể tìm ra trụ sở của Daesh giữa sa mạc mênh mông, cũng như Mark Loveless đã sử dụng dữ liệu EXIF để xác định vị trí của John McAfee. Công cụ này có sẵn trong chương trình kiểm tra file trên hệ điều hành OSX của Apple và trong các công cụ tải xuống như FOCA cho Windows và Metagoofil cho Linux, do đó bất kỳ ai cũng có thể sử dụng nó để truy cập vào trường siêu dữ liệu lưu trữ trong các bức ảnh và tài liệu.

Đôi khi, thủ phạm tiết lộ vị trí của bạn không phải file ảnh mà là một ứng dụng. Mùa hè năm 2015, trùm ma túy Joaquin “El Chapo” Guzman trốn thoát khỏi Altiplano, một nhà tù được tăng cường an ninh mức độ cao nhất ở Mexico, và lập tức biến mất. Liệu có phải như vậy?

Hai tháng sau đó, Jesus Alfredo Guzman Salazar, người con trai 29 tuổi của El Chapo, đăng một hình ảnh lên Twitter. Mặc dù hai

người đàn ông ngồi ở bàn ăn với Salazar bị che đi bằng các biểu tượng cảm xúc, nhưng hình dáng người ngồi bên trái rất giống với El Chapo. Hơn nữa, Salazar còn chú thích cho bức ảnh này là, "Tháng 8 ở đây, với ai thì các bạn đã biết rồi đấy." Các tweet cũng chứa dữ liệu về vị trí của người đăng – Costa Rica – tức là con trai của El Chapo đã không tắt chức năng tự động gắn thẻ trên ứng dụng điện thoại thông minh của Twitter.

Dù gia đình bạn không có tù nhân trốn trại, nhưng bạn vẫn cần nhận thức được rằng các thông tin và hình ảnh kỹ thuật số ẩn giấu trong ảnh của mình (đôi khi mắt thường cũng thấy được) có thể tiết lộ rất nhiều điều cho một người không biết bạn, và nó có thể quay trở lại ám ảnh bạn.

Ảnh trực tuyến có thể cung cấp nhiều thông tin hơn chứ không chỉ dừng lại ở việc tiết lộ vị trí của bạn. Khi kết hợp với một số chương trình phần mềm nhất định, chúng có thể hé mở các thông tin cá nhân về bạn.

Năm 2011, Alessandro Acquisti, một nhà nghiên cứu ở Đại học Carnegie Mellon, đưa ra một giả thiết đơn giản: "Tôi muốn xem liệu từ một khuôn mặt trên đường phố có thể suy luận ra một số An sinh Xã hội hay không." Và câu trả lời là có. Bằng cách chụp qua webcam hình ảnh một người tình nguyện tham gia vào nghiên cứu trên, Acquisti và nhóm của anh đã có đủ dữ liệu để thu thập thông tin cá nhân về người đó.

Hãy nghĩ về điều đó. Bạn có thể chụp ảnh một người đi trên đường rồi dùng phần mềm nhận dạng khuôn mặt để xác định danh tính của họ. Nếu không có xác nhận từ chính người đó, một số kết quả bạn tìm ra có thể là sai. Nhưng khả năng cao là phần lớn các "kết quả khớp dữ liệu" sẽ xác định được cho bạn một cái tên cụ thể.

Chia sẻ với tờ Threatpost, Acquisti nói: "Có sự pha trộn giữa dữ liệu trực tuyến và dữ liệu ngoại tuyến, và khuôn mặt chính là đường dẫn – là mối liên kết thực sự giữa hai thế giới này. Tôi nghĩ bài học rút ra ở đây khá là u ám. Chúng ta phải đối diện với thực

tế rằng khái niệm về sự riêng tư của chúng ta đang bị xói mòn. Bạn không còn riêng tư trên đường phố hoặc trong đám đông nữa. Sự kết hợp của tất cả các công nghệ này đang thách thức kỳ vọng của chúng ta về sự riêng tư."

Nhóm nghiên cứu của Acquisti đến Đại học Carnegie Mellon nhờ các sinh viên điền vào một bảng câu hỏi khảo sát trực tuyến. Webcam trên máy tính xách tay chụp lại ảnh từng người khi họ trả lời bảng câu hỏi, và những bức ảnh này được tham chiếu chéo ngay trên mạng bằng phần mềm nhận dạng khuôn mặt. Khi họ thực hiện gần xong bảng câu hỏi, một số ảnh được truy xuất đã xuất hiện trên màn hình. Acquisti cho biết 42% số ảnh đã được xác định chính xác và liên kết tới các hồ sơ của sinh viên trên Facebook.

Nếu sử dụng Facebook, có lẽ bạn đã biết về công nghệ nhận dạng khuôn mặt tương đối hạn chế của họ. Khi bạn tải ảnh lên, Facebook sẽ cố gắng gắn thẻ những người trong mạng lưới của bạn, những người có trong danh sách bạn bè của bạn. Bạn có một chút quyền kiểm soát trong chuyện này. Ở mục cài đặt, bạn có thể yêu cầu Facebook thông báo mỗi khi người khác đăng ảnh có mặt bạn và quyết định xem có nên cho phép họ gắn thẻ bạn không. Bạn cũng có thể chọn đăng bức ảnh đó lên tường hoặc dòng thời gian của mình sau khi có thông báo.

Để ẩn các ảnh được gắn thẻ trong Facebook, hãy mở tài khoản và đi tới "Private Settings" (Cài đặt riêng tư). Có nhiều tùy chọn khác nhau, bao gồm giới hạn hình ảnh cho dòng thời gian riêng tư. Ngoài ra, Facebook vẫn chưa cung cấp tùy chọn để ngăn người khác gắn thẻ bạn mà chưa xin phép.

Các công ty như Google và Apple cũng tích hợp công nghệ nhận diện khuôn mặt trong một số ứng dụng như Google Photo và iPhoto. Bạn nên xem phần cài đặt cấu hình cho các ứng dụng và dịch vụ đó để giới hạn những gì mà công nghệ nhận diện khuôn mặt có thể thực hiện. Cho đến nay, Google vẫn khá dè dặt trong việc đưa công nghệ nhận diện khuôn mặt vào tính năng tìm kiếm hình ảnh của mình (được biểu thị bằng biểu tượng máy ảnh

trong cửa sổ tìm kiếm của Google). Bạn có thể tải lên một hình ảnh đã có, và Google sẽ tìm kiếm bức ảnh đó, nhưng nó sẽ không tìm kiếm các bức ảnh khác cũng có người trong ảnh. Trong nhiều tuyên bố khác nhau, Google đã nhiều lần khẳng định rằng việc để người dùng xác định người lạ bằng khuôn mặt là hành động "vượt qua những ranh giới đáng sợ."

Mặc dù vậy, một số chính phủ đàn áp đã làm điều đó. Họ chụp ảnh người tham gia trong các cuộc biểu tình lớn chống chính phủ rồi đưa ảnh lên mạng. Trong trường hợp này, thực ra họ không sử dụng phần mềm nhận diện hình ảnh mà sử dụng lợi thế của đám đông (crowdsource) cho quá trình nhận dạng. Ngoài ra, một số tiểu bang của Mỹ cũng đã bắt đầu sử dụng cơ sở dữ liệu hìnhảnh của các Sở Quản lý xe Cơ giới để xác định nghi phạm trong các vụ án hình sự. Nhưng đó là những hoạt động phức tạp ở cấp độ tiểu bang. Một nhà nghiên cứu đơn độc có thể làm được gì?

Acquisti và nhóm nghiên cứu của anh muốn tìm hiểu xem có thể tham chiếu chéo trực tuyến bao nhiêu lượng thông tin trích xuất từ hình ảnh về một người. Để tìm câu trả lời, họ sử dụng một công nghệ nhận diện khuôn mặt gọi là Pittsburgh Pattern Recognition, hoặc PittPatt, hiện thuộc sở hữu của Google. Các thuật toán được sử dụng trong PittPatt đã được cấp phép cho nhiều công ty bảo mật và tổ chức chính phủ khác nhau. Ngay sau khi mua lại công nghệ này, Google đã chính thức tuyên bố ý định của mình: "Như chúng tôi vẫn khẳng định trong hơn một năm qua, chúng tôi sẽ không bổ sung tính năng nhận diện khuôn mặt cho Google cho đến khi nào tìm ra mô hình bảo mật đủ mạnh cho nó. Và đến giờ chúng tôi vẫn chưa tìm ra mô hình đó." Hãy hy vọng rằng công ty này sẽ tiếp tục giữ lời.

Tại thời điểm thực hiện nghiên cứu trên, Acquisti có thể sử dụng PittPatt kết hợp với các hình ảnh Facebook khai thác được (qua dữ liệu) từ các hồ sơ cá nhân mà nhóm nghiên cứu cho rằng có thể tìm kiếm công khai, ví dụ những hình ảnh cá nhân mà các sinh viên ở Carnegie Mellon đã đăng lên cùng với một chút ít thông tin nào đó. Sau đó, họ khớp tập hợp các khuôn mặt đã biết

này với tập hợp các khuôn mặt "ẩn danh" trên một website hẹn hò trực tuyến. Ở đó, các nhà nghiên cứu có thể xác định được 15% trong số các tài khoản được cho là "ẩn danh" này.

Tuy nhiên, thí nghiệm đáng sợ nhất là liên kết khuôn mặt của một người với số An sinh Xã hội của người đó. Acquisti và nhóm nghiên cứu thực hiện tìm kiếm các hồ sơ trên Facebook có thông tin về ngày sinh và quê quán của một người. Trước đây, năm 2009, cũng nhóm nghiên cứu này đã chứng minh rằng chỉ riêng thông tin này cũng đủ để họ lấy được số An Sinh Xã Hội của một người (số này được cấp tuần tự theo công thức riêng của từng tiểu bang, và từ năm 1989, nó được cấp vào ngày sinh hoặc gần ngày sinh của mỗi người, do đó việc đoán bốn chữ số cuối cùng trở nên dễ dàng hơn).

Sau một số tính toán ban đầu, các nhà nghiên cứu gửi một bảng khảo sát bổ sung, hỏi các sinh viên Carnegie Mellon xem năm chữ số đầu tiên trong số An sinh Xã hội của họ do thuật toán phỏng đoán có đúng không. Và phần lớn đều trả lời là đúng.

Tôi cá rằng có một số bức ảnh mà bạn không muốn xuất hiện trên mạng nữa. Nhưng khả năng cao là bạn sẽ không thể lấy lại tất cả, dù rằng đã xóa chúng khỏi các trang mạng xã hội. Điều này một phần là vì sau khi bạn đăng một nội dung lên mạng xã hội, nó sẽ thuộc về quyền sở hữu của mạng đó và rời khỏi tay bạn. Và bạn đã đồng ý như vậy trong các điều khoản dịch vụ.

Nếu sử dụng ứng dụng phổ biến là Google Photos, thì dù bạn đã xóa ảnh ở đó cũng không nhất thiết có nghĩa là nó đã biến mất. Nhiều khách hàng nhận thấy hình ảnh vẫn ở đó ngay cả khi họ xóa ứng dụng khỏi thiết bị di động. Tại sao? Bởi vì một khi hình ảnh chạm tới đám mây, nó sẽ tồn tại độc lập với ứng dụng, nghĩa là các ứng dụng khác có thể tiếp cận và tiếp tục hiển thị hình ảnh bạn đã xóa.

Điều này mang lại những hệ quả trong cuộc sống thực. Giả sử bạn đăng một số chú thích ngu ngốc lên ảnh của một người hiện làm việc tại công ty mà bạn đang nộp hồ sơ xin việc. Hoặc bạn đăng

chụp chung với người mà bạn không muốn vợ/chồng hiện nay của mình biết. Mặc dù nó có thể là tài khoản cá nhân của bạn, nhưng nó cũng là dữ liệu của mạng xã hội.

Có lẽ bạn chưa từng dành thời gian đọc các điều khoản sử dụng của bất kỳ website nào nơi bạn đăng các dữ liệu cá nhân, trải nghiệm hằng ngày, suy nghĩ, ý kiến, câu chuyện, thông tin, khiếu nại,... hoặc nơi bạn mua sắm, chơi, học, và tương tác – có lẽ là với tần suất hằng ngày, thậm chí hằng giờ. Hầu hết các website mạng xã hội đều yêu cầu người dùng phải đồng ý với các điều khoản và điều kiện của họ trước khi sử dụng dịch vụ. Điều đáng tranh cãi là, các điều khoản này thường chứa các điều mục cho phép họ lưu trữ dữ liệu thu được từ người dùng và thậm chí chia sẻ nó với các bên thứ ba.

Nhiều năm qua, Facebook đã thu hút sự chú ý của công luận vì các chính sách lưu trữ dữ liệu của họ, bao gồm cả việc website này gây khó khăn cho việc xóa tài khoản. Và Facebook không phải là trường hợp cá biệt. Nhiều website có lối nói hệt như nhau trong phần điều khoản sử dụng, có thể khiến bạn sợ hãi mà tránh xa nếu bạn chịu đọc nó trước khi đăng ký. Dưới đây là một ví dụ, từ Facebook, tại thời điểm ngày 30 tháng 1 năm 2015:

Bạn sở hữu tất cả nội dung và thông tin bạn đăng trên Facebook và bạn có thể kiểm soát cách thức nội dung và thông tin được chia sẻ thông qua cài đặt bảo mật và ứng dụng của mình. Ngoài ra:

1. Đối với nội dung thuộc quyền sở hữu trí tuệ, như ảnh và video (nội dung sở hữu trí tuệ), bạn đặc biệt cho chúng tôi quyền sau, tùy thuộc vào cài đặt riêng tư và ứng dụng của bạn: bạn cấp phép cho chúng tôi Giấy phép không độc quyền, có thể chuyển nhượng, có thể cấp phép phụ, miễn phí bản quyền, giấy phép toàn cầu để sử dụng bất kỳ nội dung sở hữu trí tuệ nào mà bạn đăng hoặc liên quan đến Facebook (Giấy phép sở hữu trí tuệ). Giấy phép sở hữu trí tuệ này kết thúc khi bạn xóa nội dung sở hữu trí tuệ hoặc tài khoản của mình trừ khi nội dung của bạn được chia sẻ với người khác và họ chưa xóa nó.

Nói cách khác, Facebook có quyền sử dụng bất kỳ thứ gì bạn đăng trên website này, theo bất kỳ cách nào họ muốn. Thậm chí họ còn có thể bán các hình ảnh, ý kiến, bài viết, hoặc bất cứ điều gì khác mà bạn đăng lên, kiếm tiền từ sự đóng góp của bạn mà không phải trả cho bạn một xu. Họ có thể sử dụng các bình luận, nội dung chỉ trích, phỉ báng, vu khống của bạn (nếu có), và những chi tiết mang tính cá nhân nhất mà bạn đăng về con cái, cấp trên, hay nhân tình của bạn. Và họ không phải làm điều đó lén lút: nếu bạn đã sử dụng tên thật của mình, thì họ cũng có thể sử dụng tên thật của bạn.

Một trong những kết luận rút ra được ở đây là những hình ảnh mà bạn đăng lên Facebook cũng có thể xuất hiện ở các website khác. Để tìm xem trên mạng có lưu giữ hình ảnh nhạy cảm nào của mình không, bạn có thể thực hiện tìm kiếm hình ảnh ngược trong Google. Hãy nhấp vào biểu tượng máy ảnh nhỏ trong cửa sổ tìm kiếm của Google và tải lên ảnh từ ổ cứng của bạn. Sau vài phút, bạn sẽ thấy mọi bản sao có thể tìm thấy của hình ảnh đó trên mạng. Về lý thuyết, nếu đó là ảnh của bạn, bạn sẽ biết tất cả các website xuất hiện trong kết quả tìm kiếm. Tuy nhiên, nếu bạn thấy có người đăng ảnh của mình lên một website mà bạn không thích, thì bạn không có nhiều sự lựa chọn đâu.

Công nghệ tìm kiếm hình ảnh ngược chỉ giới hạn ở những gì đã được đăng tải. Nói cách khác, nếu trên mạng có hình ảnh tương tự nhưng không giống hệt, Google sẽ không tìm. Nó chỉ tìm đúng hình ảnh bạn yêu cầu, kể cả các phiên bản ảnh đã cắt, nhưng trong trường hợp này, dữ liệu trung tâm – hoặc phần dữ liệu trung tâm vừa đủ – vẫn giữ nguyên.

Một lần, vào dịp sinh nhật tôi, một người bạn muốn tạo một con tem có hình tôi trên đó. Công ty cung cấp dịch vụ này, Stamps.com, có chính sách nghiêm ngặt chống lại việc sử dụng hình ảnh của những người từng bị kết án. Và hình ảnh của tôi đã bị từ chối. Có lẽ họ đã tìm kiếm hình ảnh trên mạng.

Thông tin về tôi, Kevin Mitnick, từng bị kết án tù đã có mặt trong một cơ sở dữ liệu ở đâu đó.

Năm sau đó, bạn tôi thử một bức ảnh chụp tôi thời trẻ, khi tôi còn chưa được nhiều người biết đến, với tên gọi khác. Cô cho rằng có lẽ bức ảnh này chưa được đăng tải trên mạng. Và bạn biết chuyện gì không? Mẹo này đã thành công: bức ảnh đã được chấp nhận! Điều này cho thấy những hạn chế của công nghệ tìm kiếm hình ảnh.

Tuy nhiên, nếu tìm thấy một bức ảnh nào của mình mà bạn không muốn xuất hiện trên mạng, bạn vẫn có một số phương án xử lý.

Trước tiên, hãy liên hệ với website đã đăng ảnh bạn. Hầu hết các website đều có địa chỉ email tiếp nhận các thông báo lạm dụng dạng "abuse@tentrangweb.com." Bạn cũng có thể liên hệ với quản trị viên của website tại địa chỉ "admin@tentrangweb.com." Hãy giải thích với họ rằng bạn là chủ sở hữu của hình ảnh đó và bạn không cho phép đăng tải nó. Trong phần lớn các trường hợp, quản trị viên sẽ gỡ bỏ hình ảnh mà không gây phiền hà gì. Tuy nhiên, nếu cần thiết, bạn có thể gửi yêu cầu thực thi Đạo luật Bản quyền Kỹ thuật số Thiên niên kỷ (Digital Millennium Copyright Act –DMCA)[78] tới email "DMCA@tentrangweb.com."

[78] DMCA: Đạo luật bản quyền của Mỹ, ra đời năm 1998, thực thi hai hiệp định của Tổ chức Sở hữu Trí tuệ Thế giới (WIPO) năm 1996. Đạo luật này nhằm bảo vệ bản quyền của các sản phẩm công nghệ trên mạng và ghép tội những hành vi xâm phạm bản quyền như xâm nhập trái pháp, cung cấp hoặc kinh doanh sản phẩm công nghệ trái phép.

Nhưng hãy cẩn thận. Bạn có thể gặp rắc rối nếu xuyên tạc nội dung yêu cầu DMCA, vì vậy, nếu sự việc nghiêm trọng đến cấp độ này, hãy xin tư vấn pháp lý. Nếu hình ảnh vẫn chưa được gỡ bỏ, hãy quay ngược lại liên hệ với nhà cung cấp dịch vụ Internet của website (Comcast, GoDaddy, hay một công ty khác). Hầu hết họ sẽ nghiêm túc xử lý một yêu cầu DMCA hợp lệ.

Ngoài hình ảnh, hồ sơ mạng xã hội của bạn còn có những gì? Không ai muốn chia sẻ tất cả thông tin về bản thân mình với một

hành khách lạ tình cờ ngồi chung một chuyến tàu. Cũng tương tự như thế, bạn không nên chia sẻ quá nhiều thông tin cá nhân trên các website vắng hình bóng con người. Bạn không thể biết ai đang xem hồ sơ của mình. Và một khi nó đã xuất hiện trên mạng, thì bạn không thể lấy lại. Hãy cân nhắc cẩn thận về những gì bạn đưa vào hồ sơ của mình – bạn không phải điền vào tất cả các trường trống, chẳng hạn như trường đã học (hay thời gian học). Thực ra, hãy cung cấp càng ít thông tin càng tốt.

Bạn có thể tạo một hồ sơ chuyên biệt trên mạng xã hội. Đừng nói dối, chỉ cần cung cấp sự thật mập mờ là được. Ví dụ, nếu bạn lớn lên ở Atlanta, hãy nói rằng bạn lớn lên ở "miền Đông Nam nước Mỹ," hoặc đơn giản là "Tôi đến từ miền Nam."

Bạn cũng có thể tạo một ngày sinh "an toàn" – tức không phải ngày sinh thực sự của bạn – để che giấu thông tin cá nhân hơn nữa. Nhưng hãy ghi nhớ những ngày sinh giả mạo này, vì đôi khi bạn sẽ cần đến chúng để xác minh danh tính khi cần hỗ trợ kỹ thuật hay cần đăng nhập lại một website.

Sau khi tạo hoặc chỉnh sửa hồ sơ trực tuyến, hãy dành vài phút để đọc các tùy chọn quyền riêng tư ở từng nơi. Ví dụ: với Facebook, bạn nên bật chế độ kiểm soát quyền riêng tư, bao gồm cả mục duyệt gắn thẻ. Hãy tắt tính năng "Suggest photos of me to friends" (Đề xuất ảnh của tôi cho bạn bè) và "Friends can check me into places" (Bạn bè có thể ký check-in tôi tại các địa điểm).

Nhưng có lẽ điều đáng lo ngại nhất là việc trẻ em sử dụng Facebook. Chúng thường điền thông tin vào mọi trường trống, kể cả mục tình trạng mối quan hệ. Hoặc chúng có thể ngây thơ tiết lộ tên trường, tên giáo viên, hay số tuyến xe bus đi học mỗi sáng. Tuy chúng không chỉ đích danh nơi ở, nhưng chừng đó thông tin cũng đủ để tiết lộ chúng sống ở đâu rồi. Các bậc phụ huynh cần kết bạn với con cái trên mạng xã hội, theo dõi những gì chúng đăng, và lý tưởng nhất là thống nhất trước với chúng về những nội dung có thể và và không thể đăng.

Ẩn danh không có nghĩa là bạn không thể chia sẻ những thông

tin cập nhật về cuộc sống cá nhân của mình một cách an toàn, nhưng nó đòi hỏi sự tỉnh táo, và bạn phải thường xuyên kiểm tra phần cài đặt bảo mật của các website mạng xã hội mà bạn sử dụng – vì chính sách bảo mật sẽ có sự thay đổi, và những thay đổi này không phải lúc nào cũng theo chiều hướng tốt hơn. Đừng hiển thị ngày sinh – kể cả ngày sinh giả – hay ít nhất là ẩn thông tin này đối với các "bạn bè" trên Facebook mà bạn không thực sự quen biết.

Ta hãy cùng xem xét một trường hợp sau đây. Một bài đăng trên mạng xã hội nói rằng cô Sanchez là một giáo viên tuyệt vời. Một bài đăng khác có thể viết về về hội chợ hàng thủ công tại Trường Tiểu học Alamo. Qua Google, chúng tôi có thể thấy rằng cô Sanchez dạy lớp 5 tại Trường Tiểu học Alamo – và qua đây, chúng tôi có thể đoán rằng chủ tài khoản đó khoảng mười tuổi.

Bất chấp những cảnh báo từ Consumer Reports[79] và các tổ chức khác, người ta vẫn tiếp tục chia sẻ mọi chuyện trên mạng. Hãy nhớ rằng một khi các thông tin trên được đăng tải công khai, các bên thứ ba hoàn toàn có thể thu thập chúng.

[79] Consumer Reports: Một tạp chí phục vụ người tiêu dùng của Mỹ.

Cũng nên nhớ rằng không ai ép buộc bạn phải đăng thông tin cá nhân. Bạn có thể đăng nhiều hoặc ít tùy thích. Trong một số trường hợp, bạn được yêu cầu điền vào một số thông tin. Ngoài ra, bạn được quyền quyết định mức độ thông tin muốn chia sẻ. Bạn phải xác định mức độ riêng tư cá nhân cho mình, và phải hiểu rằng mọi thông tin bạn cung cấp đều không thể rút lại được.

Để giúp bạn nắm bắt được tất cả các lựa chọn khả thi, tháng 5 năm 2015, Facebook ra mắt một công cụ kiểm tra quyền riêng tư mới. Mặc dù có các công cụ như thế, năm 2012, gần 13 triệu người dùng Facebook chia sẻ với tạp chí Consumer Reports rằng họ chưa từng cài đặt, hoặc không biết đến, các công cụ kiểm tra quyền riêng tư của Facebook. Và 28% trong số họ chia sẻ tất cả, hoặc gần như tất cả, các bài viết trên tường của họ với nhiều

người chứ không chỉ giới hạn ở danh sách bạn bè. Nhưng có một tin vui, 25% số người được Consumer Reports phỏng vấn cho biết họ đã giả mạo thông tin trong hồ sơ cá nhân để bảo vệ danh tính, và tỉ lệ này cao hơn so với mức 10% năm 2010. Ít nhất, chúng ta cũng đang rút ra được bài học cho mình.

Mặc dù bạn có quyền đăng thông tin không thực sự chính xác về bản thân, nhưng xin lưu ý rằng ở California, việc đăng bài trực tuyến với tư cách người khác là bất hợp pháp. Bạn không thể mạo danh một cá nhân khác đang sinh sống. Và Facebook cũng có chính sách không cho phép bạn tạo tài khoản bằng tên giả.

Chuyện này đã xảy ra với tôi. Tài khoản của tôi bị Facebook khóa vì cho rằng tôi mạo danh Kevin Mitnick. Vào thời điểm đó, có 12 Kevin Mitnick trên Facebook. Tình huống được giải quyết khiCNET đăng tải một bài báo về chuyện Kevin Mitnick "thật" bị khóa trên Facebook.

Tuy nhiên, có nhiều lý do để một người đăng bài dưới một cái tên khác. Nếu bạn cần phải làm thế, hãy tìm một dịch vụ mạng xã hội cho phép bạn đăng bài ẩn danh hoặc dưới một tên khác. Tuy nhiên, các website như vậy thường sẽ không thể so được với Facebook về mặt quy mô mạng lưới và mức độ tiếp cận độc giả.

Hãy cẩn thận với những người mà bạn kết bạn trên mạng xã hội. Nếu đó là người mà bạn đã gặp mặt trực tiếp thì tốt. Hoặc nếu đó là bạn của người quen thì cũng có thể chấp nhận được. Nhưng nếu bạn nhận được một yêu cầu kết bạn đường đột, hãy suy nghĩ cẩn thận. Tuy bạn có thể hủy kết bạn với người đó bất kỳ lúc nào, nhưng họ vẫn có cơ hội xem toàn bộ hồ sơ của bạn – và chỉ cần một vài giây là đủ để một kẻ có ý đồ xấu can thiệp vào cuộc sống của bạn rồi. Lời khuyên tốt nhất ở đây là hãy hạn chế mọi thông tin cá nhân mà bạn chia sẻ trên Facebook, bởi vì đã có những cuộc tấn công rất cá nhân, ngay cả giữa bạn bè, trên các website mạng xã hội. Và những dữ liệu mà bạn hiển thị cho bạn bè thấy vẫn có thể được họ đăng lại ở nơi khác mà không có sự đồng ý hoặc kiểm soát của bạn.

Tôi sẽ cho bạn một ví dụ. Có lần một anh chàng định thuê tôi vì anh ta là nạn nhân của một vụ tống tiền. Anh này quen một cô gái tuyệt vời, xinh đẹp trên Facebook, và gửi cho cô ta những bức ảnh khỏa thân của mình. Chuyện này tiếp diễn trong một thời gian. Rồi một ngày nọ, người phụ nữ này – nhưng có lẽ là một người đàn ông sống ở Nigeria dùng ảnh của một người phụ nữ để mạo danh – yêu cầu anh phải gửi 4.000 đô-la. Anh chàng làm theo, nhưng sau đó lại tiếp tục bị đòi 4.000 đô-la nữa, nếu không những bức ảnh khỏa thân kia sẽ được gửi đến tất cả bạn bè của anh trên Facebook, trong đó có cả bố mẹ anh. Vì quá bối rối trước tình huống này, anh liên hệ với tôi. Và tôi nói rằng giải pháp thực tế lúc này là nói sự thật với gia đình hoặc thi gan xem kẻ tống tiền định làm gì. Tôi khuyên anh đừng chuyển tiền nữa, vì nếu anh còn tiếp tục làm thế, kẻ tống tiền sẽ tiếp tục đòi hỏi.

Ngay cả các mạng xã hội hợp pháp cũng có thể bị xâm nhập: một người có thể kết bạn với bạn chỉ để tiếp cận với người mà bạn biết. Một nhân viên thuộc cơ quan thực thi pháp luật có thể đang tìm kiếm thông tin về một người và người đó tình cờ lại nằm trong danh sách bạn bè của bạn trên mạng xã hội. Chuyện này vẫn xảy ra thường xuyên.

Theo Tổ chức Biên giới Điện tử, các nhà điều tra liên bang đã sử dụng mạng xã hội làm công cụ giám sát thụ động suốt nhiều năm nay. Năm 2011, tổ chức này phát hành tài liệu tập huấn dày 38 trang cho các nhân viên của Sở Thuế vụ (được biên soạn từ Đạo luật Tự do Thông tin) để thực hiện các cuộc điều tra qua mạng xã hội. Mặc dù về mặt pháp lý, các đặc vụ liên bang không thể đóng giả làm người khác, nhưng họ hoàn toàn có thể gửi cho bạn yêu cầu kết bạn. Như vậy, họ có thể xem tất cả các bài đăng của bạn (tùy thuộc vào cài đặt bảo mật của bạn) cũng như của những người khác trong danh sách bạn bè của bạn. Hiện Tổ chức Biên giới Điện tử vẫn đang tiếp tục nghiên cứu các vấn đề quyền riêng tư liên quan đến hình thức giám sát thực thi pháp luật mới này.

Đôi khi các công ty theo dõi, hoặc ít nhất là giám sát bạn, nếu bạn

đăng tải một nội dung nào đó mà họ thấy là xúc phạm – một nội dung vô tội như nhận xét về một bài kiểm tra ở trường chẳng hạn. Đối với một học sinh mà tôi biết, một tweet như thế đã gây ra rất nhiều rắc rối.

Khi Elizabeth C. Jewett, người phụ trách của trường Trung học Watchung Hills ở Warren, New Jersey, nhận được thông báo từ công ty cung cấp cho trường của cô một bài thi áp dụng cho toàn tiểu bang, phản ứng của cô là bất ngờ thay vì lo lắng. Cô bất ngờ vì Pearson Education lại chủ động theo dõi tài khoản Twitter của học sinh, vốn là những đối tượng có sự riêng tư và tự do nhất định đối với những gì chúng đăng trên mạng xã hội. Nhưng học sinh – dù đang học cấp hai, cấp ba, hay đại học – đều phải nhận thức được rằng các hoạt động trực tuyến của chúng là công khai và bị theo dõi. Trong trường hợp này, một học sinh của Jewett bị cáo buộc là đã đăng tải nội dung trong một bài kiểm tra tiêu chuẩn lên Twitter.

Trên thực tế, học sinh này đã đăng một vài từ ngắn gọn để hỏi về một câu hỏi – chứ không phải ảnh chụp trang giấy thi – trong ngày cả bang New Jersey thực hiện bài kiểm tra Hợp tác Đánh giá Mức độ Sẵn sàng cho Đại học và Nghề nghiệp, gọi tắt là PARCC. Tweet đó được đăng vào khoảng 3 giờ chiều, khi bài thi kia đã kết thúc từ lâu. Sau khi Jewett trao đổi với phụ huynh, học sinh trên đã xóa tweet kia đi. Không có bằng chứng nào về gian lận cả. Nội dung tweet – không được tiết lộ cho công chúng – là một nhận xét chủ quan chứ không hẳn ngụ ý xin câu trả lời.

Nhưng những thông tin được tiết lộ về Pearson khiến công chúng bất bình. Trong một email gửi cho các đồng nghiệp, về sau được một nhà báo của bang công bố mà không xin phép, Jewett viết: “DOE [Sở Giáo dục] đã thông báo với chúng tôi rằng Pearson theo dõi trên tất cả các mạng xã hội trong thời gian thực hiện bài kiểm tra PARCC.” Cũng trong email này, Jewett xác nhận rằng ít nhất có thêm ba trường hợp nữa được Pearson xác định và chuyển cho DOE.

Tuy Pearson không phải là tổ chức duy nhất thực hiện theo dõi

trên các mạng xã hội để phát hiện hành vi trộm cắp tài sản trí tuệ, nhưng hành vi của họ đã làm dấy lên các câu hỏi. Chẳng hạn, làm thế nào công ty này lại biết danh tính của học sinh trên từ tên trên Twitter của học sinh đó? Trong một tuyên bố cung cấp cho tờ New York Times, Pearson nói: "Hành vi vi phạm bao gồm việc chia sẻ thông tin về một bài kiểm tra bên ngoài lớp học vào bất kỳ thời điểm nào – từ các cuộc trao đổi bình thường cho đến các bài đăng trên mạng xã hội. Một lần nữa, mục tiêu của chúng tôi là đảm bảo cho tất cả học sinh một kỳ thi công bằng. Mỗi học sinh đều xứng đáng có cơ hội tham gia kỳ thi trên sân chơi bình đẳng."

Tờ Times cho biết theo xác nhận từ các quan chức ở Massachusetts, những người cũng tham gia điều hành kỳ thi PARCC, Pearson có thực hiện tham chiếu chéo các tweet nói về bài kiểm tra tiêu chuẩn với danh sách các học sinh đã đăng ký dự thi. Nhưng Pearson từ chối bình luận về điều này.

Trong nhiều năm, tiểu bang California cũng tiến hành theo dõi các mạng xã hội trong thời gian diễn ra các kỳ thi Kiểm tra và Báo cáo Tiêu chuẩn (STAR) hằng năm. Năm 2013, năm cuối cùng kỳ thi này được áp dụng toàn tiểu bang, Sở Giáo dục California xác định được 242 trường có học sinh đăng tin lên mạng xã hội trong thời gian thi, trong đó chỉ có 16 trường hợp đăng tải các câu hỏi hoặc câu trả lời liên quan đến bài thi.

Elana Zeide, một nghiên cứu sinh về bảo mật tại Viện Luật Thông tin ở Đại học New York, cho biết: "Sự kiện này cho thấy mức độ giám sát mà các học sinh đang phải chịu, cả bên trong và bên ngoài môi trường học đường truyền thống. Mạng xã hội thường được xem là một không gian riêng, tách biệt khỏi trường học. Twitter có vẻ giống như những bài phát biểu 'ngoài khuôn viên học đường' hơn, vì thế hoạt động theo dõi của Pearson giống như hành vi do thám các cuộc trao đổi của học sinh trong những chiếc xe đi chung hơn là trong hành lang trường học."

Tuy nhiên, cô cũng nói, "Cuộc tranh luận của chúng ta cũng không nên chỉ dừng lại ở những lợi ích và mối nguy hại cho cá

nhân mà còn cần phải tính đến cả những hệ quả rộng lớn hơn của các hoạt động liên quan đến thông tin. Các trường học và đối tác của họ phải ngừng thái độ coi các bậc phụ huynh là những người cổ hủ, chống lại công nghệ chỉ bởi vì họ không thể nêu ra một cách cụ thể mối nguy hại nào cho con mình. Về phía phụ huynh, họ cũng cần phải hiểu rằng trường học không thể chiều theo tất cả các mong muốn về quyền riêng tư của họ vì còn có những lợi ích tập thể khác liên quan, tác động đến toàn bộ hệ thống giáo dục."

Twitter, với giới hạn 140 ký tự nổi tiếng, đã trở nên phổ biến và thu thập được rất nhiều những thông tin tưởng chừng như chỉ là chi tiết lặt vặt về cuộc sống hằng ngày của chúng ta. Chính sách bảo mật của Twitter thừa nhận rằng họ thu thập – và giữ lại – các thông tin cá nhân thông qua website, các ứng dụng, dịch vụ nhắn tin, API (giao diện lập trình ứng dụng), và các bên thứ ba khác. Khi sử dụng dịch vụ của Twitter, người dùng cũng đồng ý với việc thu thập, chuyển giao, lưu trữ, kiểm soát, tiết lộ, và các hình thức sử dụng khác đối với các thông tin này. Để tạo tài khoản Twitter, người ta phải cung cấp tên, tên đăng nhập, mật khẩu, và địa chỉ email.

Một địa chỉ email chỉ được dùng cho duy nhất một tài khoản Twitter.

Một vấn đề khác về quyền riêng tư trên Twitter là rỏ rỉ nội dung tweet – tức là các tweet riêng tư bị phát tán công khai. Điều này xảy ra khi một người có tài khoản Twitter riêng tư đăng bài, rồi bạn bè của người đó đăng lại, hoặc sao chép và dán, tweet đó lên một tài khoản công khai. Như vậy, nội dung riêng tư trên sẽ không thể rút lại được nữa.

Việc chia sẻ thông tin cá nhân qua Twitter vẫn có thể gây nguy hiểm, đặc biệt là khi các tweet được đặt ở chế độ công khai (mặc định). Tránh chia sẻ địa chỉ, số điện thoại, số thẻ tín dụng, và số An sinh xã hội trên Twitter. Trong trường hợp cần chia sẻ thông tin nhạy cảm, hãy sử dụng tính năng nhắn tin trực tiếp để liên hệ với một người cụ thể. Nhưng hãy lưu ý rằng ngay cả tin nhắn

riêng hoặc tin nhắn trực tiếp cũng có thể trở thành công khai.

Đối với giới trẻ ngày nay – được gọi là Thế hệ Z – Facebook và Twitter đã trở thành đồ cổ. Các hoạt động trên thiết bị di động của Thế hệ Z tập trung quanh WhatsApp (trớ trêu thay, WhatsApp hiện đã là một phần của Facebook), Snapchat (không phải Facebook), Instagram và Instagram Stories (cũng là của Facebook). Tất cả các ứng dụng này đều trực quan ở chỗ chúng cho phép bạn đăng ảnh/video, hoặc chủ yếu cung cấp ảnh/video do người khác chụp.

Instagram, một ứng dụng chia sẻ hình ảnh và video, chính là Facebook đối với giới trẻ. Nó cho phép các thành viên theo dõi, thích, và trò chuyện với nhau. Instagram có các điều khoản dịch vụ và có vẻ khá nhanh nhạy trong việc đáp ứng các yêu cầu gỡ xuống của các thành viên và chủ sở hữu bản quyền.

Snapchat có lẽ là mạng xã hội đáng sợ nhất trong nhóm này, có lẽ bởi vì nó không thuộc sở hữu của Facebook. Snapchat quảng cáo rằng họ có thể cho phép bạn gửi một bức ảnh tự hủy cho người khác. Bức ảnh chỉ tồn tại trong khoảng hai giây, vừa kịp để người nhận xem được. Thật không may, hai giây là đủ để một người chụp ảnh màn hình và lưu trữ lại.

Mùa đông năm 2013, hai nữ sinh trung học ở New Jersey tự chụp ảnh khỏa thân và gửi qua Snapchat cho một nam sinh cùng trường, đinh ninh rằng các bức ảnh sẽ bị xóa tự động hai giây sau đó. Ít nhất đó là những gì mà Snapchat đã hứa.

Tuy nhiên, nam sinh kia biết cách chụp ảnh màn hình tin nhắn Snapchat và sau đó tải ảnh lên ứng dụng Instagram. Instagram không xóa ảnh sau hai giây. Không cần phải nói chắc ai cũng hình dung được các bức ảnh này được lan truyền với tốc độ chóng mặt như thế nào, và giám thị nhà trường phải gửi thông báo về cho từng phụ huynh, yêu cầu họ buộc con em mình phải xóa ảnh khỏi điện thoại, nếu không họ có thể bị bắt vì tội khiêu dâm trẻ em. Vì vẫn đang trong độ tuổi vị thành niên nên ba học sinh ban đầu không bị kết án, nhưng cả ba đều bị xử lý kỷ luật

trong học khu.

Và không chỉ có các cô gái mới gửi ảnh khỏa thân cho các cậu con trai. Ở Anh, một cậu bé 14 tuổi đã gửi ảnh khỏa thân của mình cho một cô gái cùng trường qua Snapchat, và cũng đinh ninh rằng hình ảnh sẽ biến mất sau vài giây. Tuy nhiên, cô gái này đã chụp ảnh màn hình và... bạn biết phần còn lại của câu chuyện rồi đấy. Theo BBC, tuy chưa đến tuổi bị truy tố, nhưng tên của cả hai đều sẽ được đưa vào cơ sở dữ liệu về tội phạm tình dục của Anh.

Giống như WhatsApp, khả năng làm mờ hình ảnh của Snapchat là không ổn định, và ứng dụng này không thực sự xóa hình ảnh như đã hứa hẹn. Thực ra, năm 2014, Snapchat đã chấp nhận dàn xếp với Ủy ban Thương mại Liên bang về các cáo buộc rằng công ty này đã lừa dối người dùng về bản chất của kỹ thuật xóa tin nhắn; cơ quan này cho rằng các tin nhắn có thể được lưu lại hoặc truy xuất vào một thời điểm sau khi xóa. Trong chính sách bảo mật, Snapchat cũng tuyên bố họ không yêu cầu, theo dõi, hoặc truy cập bất kỳ thông tin nào liên quan đến địa điểm từ thiết bị của người dùng, nhưng Ủy ban Thương mại Liên bang cũng phát hiện ra rằng các tuyên bố đó là sai sự thật.

Yêu cầu bắt buộc đối với tất cả các dịch vụ trực tuyến là các cá nhân từ 13 tuổi trở lên mới được đăng ký. Đó là lý do tại sao các dịch vụ này lại yêu cầu bạn cung cấp ngày sinh. Tuy nhiên, bất kỳ ai cũng có thể nghiêm nghị cam đoan: "Tôi thề rằng tôi đã trên 13 tuổi" – hay 21, hay bất kỳ con số nào. Các bậc phụ huynh thấy con mình chưa đủ tuổi nhưng đã đăng ký sử dụng Snapchat hoặc Facebook có thể báo cáo để xóa tài khoản. Ngược lại, nếu muốn tạo tài khoản mạng xã hội cho con, họ có thể thay đổi ngày sinh trong hồ sơ cá nhân của trẻ. Vậy là con bạn từ 10 tuổi bỗng nhiên trở thành 14 tuổi, cũng tức là đứa bé có thể sẽ nhận được những nội dung quảng cáo trực tuyến dành cho trẻ lớn hơn. Cũng xin lưu ý rằng mọi địa chỉ email và ảnh mà con bạn chia sẻ qua dịch vụ này đều sẽ được ghi lại.

Ứng dụng Snapchat cũng truyền dữ liệu về vị trí được xác định dựa trên sóng Wi-Fi và di động từ thiết bị di động của người dùng

Android đến nhà cung cấp dịch vụ phân tích theo dõi của họ. Nếu bạn sử dụng iOS và nhập số điện thoại của mình để tìm bạn bè, Snapchat sẽ thu thập tên và số điện thoại của tất cả các liên hệ trong sổ địa chỉ lưu trên thiết bị di động mà không cần thông báo hay xin phép bạn, mặc dù khi lần đầu được yêu cầu cung cấp các dữ liệu trên, iOS sẽ hỏi bằng chứng về thẩm quyền của họ. Lời khuyên của tôi là nếu bạn muốn có sự riêng tư thực sự, hãy sử dụng ứng dụng khác.

Ở Bắc Carolina, một học sinh trung học và bạn gái bị kết tội sở hữu ảnh khỏa thân của trẻ vị thành niên, mặc dù đó là ảnh của họ, được chụp và chia sẻ trong sự đồng thuận giữa hai bên. Người bạn gái phải đối mặt với hai tội danh liên quan đến lạm dụng tình dục trẻ vị thành niên: một là hành vi chụp ảnh, và một là hành vi sở hữu ảnh. Không bàn đến tin nhắn sex, điều đó có nghĩa là việc chụp hay sở hữu hình ảnh khỏa thân của chính mình là bất hợp pháp đối với các thiếu niên ở Bắc Carolina. Trong lệnh bắt giữ của cảnh sát, người bạn gái trên được đề cập tới trên cả hai cương vị nạn nhân và tội phạm.

Người bạn trai phải đối mặt với năm tội danh, trong đó có hai tội danh dành cho hai bức ảnh cậu tự chụp, và một tội danh dành cho việc sở hữu ảnh của người bạn gái. Nếu bị kết án, cậu có thể phải đối mặt với án tù mười năm, đồng thời phải chịu ghi danh là kẻ lạm dụng tình dục suốt đời. Tất cả chỉ vì tự chụp ảnh khỏa thân và giữ ảnh khỏa thân của bạn gái gửi cho.

Thời còn đi học, tôi chỉ cần đến mời một cô gái đi chơi. Ngày nay, bạn phải đăng tải một số thông tin trên mạng để mọi người có thể kiểm tra trước. Nhưng hãy cẩn thận.

Nếu bạn sử dụng một website hẹn hò và truy cập vào đó từ máy tính của người khác hay máy tính công cộng, hãy nhớ đăng xuất. Tôi nói nghiêm túc đấy. Bạn sẽ không muốn người khác nhấn nút “Back” (Quay lại trang trước) trên trình duyệt và xem, thậm chí thay đổi, thông tin hẹn hò của bạn đâu. Ngoài ra, hãy nhớ bỏ tích chọn ở ô có nội dung “Remember me” (Nhớ thông tin đăng nhập của tôi) trên màn hình đăng nhập. Không nên để thiết bị đó tự

động đăng nhập người khác vào tài khoản hẹn hò của bạn.

Giả sử bạn mới hẹn hò ngày đầu tiên hoặc ngày thứ hai. Người ta thường ít khi bộc lộ con người thực của mình vào lần hẹn đầu tiên hoặc thứ hai. Nhưng ngay sau khi bạn hẹn hò của bạn kết bạn với bạn trên Facebook hoặc theo dõi bạn trên Twitter hoặc trên bất kỳ mạng xã hội nào khác, họ sẽ nhìn thấy tất cả bạn bè, ảnh, sở thích của bạn… Và mọi chuyện có thể nhanh chóng trở nên rắc rối.

Chúng ta vừa nói về các dịch vụ trực tuyến. Vậy còn các ứng dụng dành cho thiết bị di động thì sao?

Ứng dụng hẹn hò có thể báo cáo vị trí của bạn, và một phần là theo chủ ý người dùng. Ví dụ, khi nhìn thấy chàng trai/cô gái mà bạn thích xuất hiện ở khu vực mình sinh sống, bạn có thể dùng ứng dụng này để tìm hiểu xem người đó có ở gần bạn không. Ứng dụng hẹn hò di động Grindr cung cấp thông tin về vị trí rất chính xác cho các thành viên của nó, có lẽ là chính xác quá mức cho phép.

Các nhà nghiên cứu Colby Moore và Patrick Wardle của công ty an ninh mạng Synack có thể làm giả yêu cầu gửi tới Grindr để theo dõi một số người sử dụng dịch vụ của Grindr khi họ di chuyển trong một thành phố. Họ cũng nhận thấy rằng nếu để ba tài khoản khác nhau cùng tìm kiếm một cá nhân, họ có thể lập thành lưới tam giác để định vị cá nhân kia chính xác hơn.

Có thể bạn không mặn mà với các ứng dụng hẹn hò, nhưng ngay cả việc đăng nhập vào dịch vụ tìm kiếm địa phương Yelp để tìm một nhà hàng ngon cũng có thể cung cấp cho các bên thứ 3 thông tin về giới tính, tuổi tác, và vị trí của bạn. Cài đặt mặc định trong ứng dụng này cho phép nó gửi thông tin về nhà hàng rằng, ví dụ, một phụ nữ 31 tuổi từ thành phố New York đang xem các đánh giá về nhà hàng. Tuy nhiên, bạn có thể đi tới phần cài đặt của mình và chọn “Basics” (Cơ bản) để ứng dụng chỉ hiển thị thành phố của bạn (tiếc là bạn không thể tắt hoàn toàn tính năng này). Có lẽ cách tốt nhất để tránh điều này là không đăng nhập và chỉ

sử dụng Yelp bằng tài khoản khách.

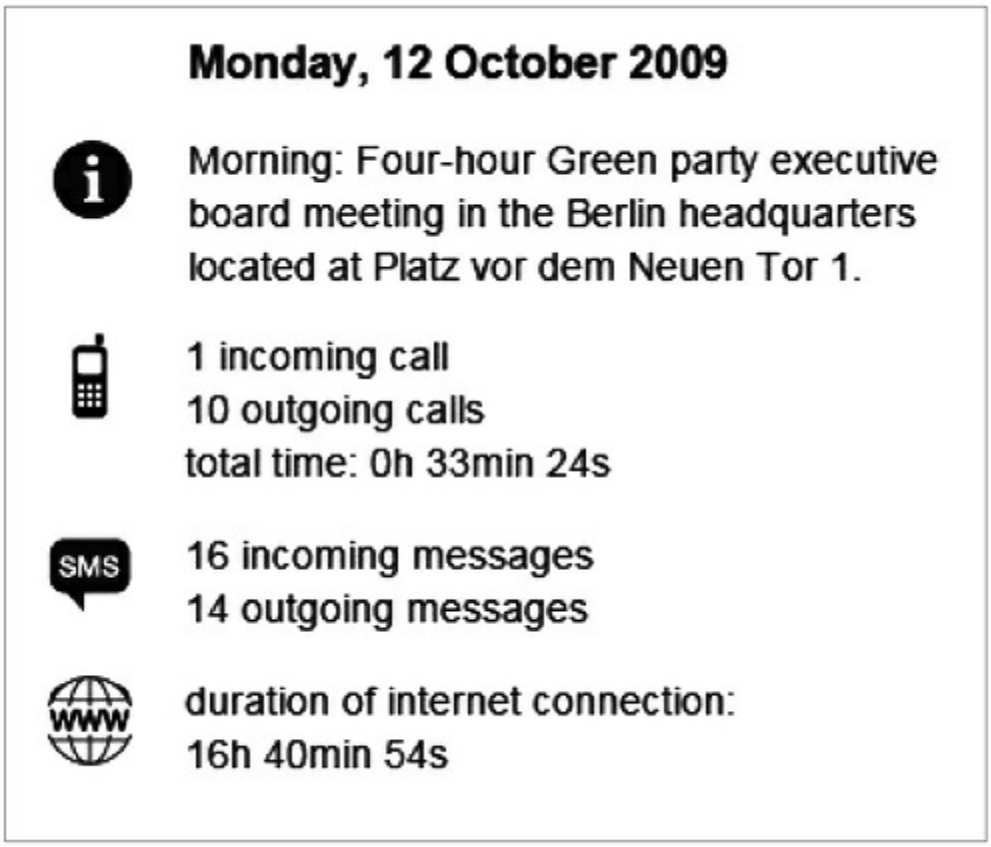
Về vị trí địa lý, bạn nên kiểm tra một lượt xem có ứng dụng di động nào đang dùng phát đi thông tin về vị trí của mình hay không. Trong hầu hết các trường hợp, bạn có thể tắt tính năng này, hoặc trong từng ứng dụng riêng hoặc toàn bộ.

Và trước khi tải xuống bất kỳ ứng dụng Android nào, hãy nhớ đọc phần cho phép. Bạn có thể đọc phần này trong Google Play bằng cách truy cập ứng dụng, sau đó cuộn xuống phần phía trên nội dung của Google Play có ghi “Permissions” (Cho phép). Nếu phần này khiến bạn cảm thấy không thoải mái, hoặc nếu bạn cho rằng nó mang lại cho nhà phát triển ứng dụng quá nhiều quyền kiểm soát, thì không nên tải ứng dụng xuống. Apple không cung cấp thông tin tương tự về các ứng dụng trong cửa hàng của hãng này, phần cho phép được hiển thị khi cần thiết để chạy ứng dụng. Thực ra, tôi thích sử dụng các thiết bị iOS hơn vì hệ điều hành luôn nhắc nhở trước khi tiết lộ các thông tin cá nhân như vị trí của tôi. iOS cũng an toàn hơn nhiều so với Android, nếu bạn không bẻ khóa iPhone hoặc iPad. Tất nhiên, kẻ xấu nhiều tiền có thể mua thông tin về lỗ hổng của bất kỳ hệ điều hành nào trên thị trường, nhưng lỗ hổng iOS khá tốn kém – chi phí lên đến trên 1 triệu đô-la.

Chương 10: BẠN CÓ THỂ CHẠY CHỨ KHÔNG THỂ TRỐN

Nếu cũng như hầu hết mọi người, bạn mang theo điện thoại di động suốt cả ngày, thì bạn không vô hình đâu. Bạn đang bị theo dõi đấy – ngay cả khi điện thoại bạn không bật tính năng theo dõi vị trí. Ví dụ, nếu bạn có iOS 8.2 trở xuống, Apple sẽ tắt GPS ở chế độ trên máy bay, nhưng nếu bạn sử dụng các thiết bị phiên bản mới hơn – mà hầu hết chúng ta đều như vậy – thì GPS vẫn hoạt động ở cả chế độ trên máy bay, trừ khi bạn thực hiện thêm một vài bước. Để tìm hiểu xem nhà mạng biết những gì về hoạt động hằng ngày của mình, Malte Spitz, một chính trị gia nổi tiếng người Đức, đã đệ đơn kiện họ, và tòa án Đức ra lệnh cho công ty này giao nộp các bản ghi. Chỉ riêng khối lượng các bản ghi này đã khiến người khác phải sửng sốt. Chỉ trong vòng sáu tháng, họ đã ghi lại 85.000 lần vị trí của ông, đồng thời theo dõi mọi cuộc gọi mà ông đã nghe và nhận, số điện thoại của người gọi, và thời lượng của từng cuộc. Nói cách khác, đây là siêu dữ liệu do điện thoại của Spitz tạo ra. Và nó không chỉ dành cho giao tiếp thoại mà còn cho cả tin nhắn văn bản nữa.

Spitz hợp tác với các tổ chức khác, yêu cầu họ định dạng dữ liệu và công bố cho công luận. Một tổ chức đã lập ra các tóm tắt hằng ngày như dưới đây. Vị trí tổ chức cuộc họp của Đảng Xanh vào buổi sáng hôm đó được xác định từ vĩ độ và kinh độ nêu trong các bản ghi của nhà mạng trên.



Thứ Hai ngày 12 tháng 10 năm 2009

Buổi sáng: Cuộc họp ban quản trị Đảng Xanh kéo dài 4 tiếng tại trụ sở ở Berlin, Platz Vor dem Neuen Tor 1.

1 cuộc gọi đến

10 cuộc gọi đi

Tổng thời lượng: 0 giờ 33 phút 24 giây

16 tin nhắn đến

14 tin nhắn đi

Thời lượng kết nối internet: 16 giờ 40 phút 54 giây

Hoạt động của Malte Spitz vào ngày 12 tháng 10 năm 2009

Cũng từ dữ liệu này, một tổ chức khác đã lập ra một bản đồ hoạt ảnh, biểu diễn các hoạt động của Spitz theo từng phút trên khắp nước Đức và hiển thị biểu tượng nhấp nháy mỗi lần ông nhận

hay thực hiện cuộc gọi. Đây là mức độ dữ liệu chi tiết đáng kinh ngạc được ghi lại chỉ trong vài ngày bình thường.

Tất nhiên, dữ liệu về Spitz không phải là trường hợp cá biệt, và tình trạng này cũng không chỉ có ở nước Đức. Nó chỉ đơn thuần là một ví dụ điển hình về dữ liệu mà nhà cung cấp dịch vụ di động lưu giữ. Và nó có thể được sử dụng trước tòa án.

Năm 2015, Tòa án Phúc thẩm Liên bang Khu vực 4 thụ lý một vụ án liên quan đến việc sử dụng các bản ghi điện thoại di động tương tự tại Mỹ, trong đó hai tên cướp bị tình nghi cướp một ngân hàng, một cửa hàng thuộc chuỗi tiện ích 7-Eleven, một số nhà hàng đồ ăn nhanh, và một cửa hàng trang sức ở Baltimore. Bằng cách yêu cầu nhà mạng Sprint bàn giao thông tin về vị trí điện thoại của các nghi phạm trong 221 ngày trước đó, cảnh sát đã chứng minh được vai trò của các nghi phạm trong một loạt vụ án, vừa dựa trên khoảng cách các vụ án vừa dựa trên khoảng cách giữa nghi phạm với hiện trường.

Một vụ án thứ hai, do Tòa án Quận Bắc California thụ lý, không cung cấp thông tin chi tiết nhưng cũng xoay quanh các "thông tin lịch sử về vị trí của điện thoại" lấy được từ Verizon và AT&T là hai nhà mạng mà các đối tượng sử dụng. Theo lời của Liên đoàn Tự do Dân sự Mỹ, tổ chức đã gửi một văn bản amicus curiae[80] trong vụ án trên, dữ liệu này "tạo ra một hồ sơ liên tục về vị trí và sự di chuyển của một cá nhân." Theo hồ sơ chính thức, khi một thẩm phán liên bang đề cập đến quyền riêng tư của điện thoại di động trong vụ án trên ở California, công tố viên liên bang nói rằng: "Nếu quan tâm đến sự riêng tư, người dùng điện thoại di động hoặc là không nên mang theo điện thoại bên người hoặc là tắt chúng đi."

[80] Amicus curiae: Từ Latin, nghĩa là "bạn của tòa án," chỉ một bên không liên quan đến một vụ án cung cấp thông tin/ý kiến cho tòa với mong muốn làm rõ một vài khía cạnh liên quan.

Điều này có vẻ vi phạm quyền được bảo vệ trước các hoạt động tìm kiếm bất hợp lý của chúng ta trong Tu Chính án thứ Tư. Hầu

hết mọi người không cho rằng việc mang theo điện thoại di động cũng đồng nghĩa với việc từ bỏ quyền không bị chính phủ theo dõi – nhưng ngày nay, đó là hệ quả đi kèm với việc mang theo điện thoại. Cả hai vụ án trên đều có một điểm chung là Verizon, AT&T, và Sprint không nêu rõ với khách hàng về phạm vi của hoạt động theo dõi vị trí trong phần chính sách bảo mật. Trong một bức thư gửi Quốc hội năm 2011, AT&T cho biết họ lưu trữ dữ liệu di động trong năm năm "để đề phòng phát sinh tranh chấp về thanh toán."

Và không chỉ các nhà mạng mới lưu trữ dữ liệu vị trí; nhà cung cấp các dịch vụ khác cũng vậy. Ví dụ, tài khoản Google sẽ lưu lại tất cả các dữ liệu vị trí địa lý trên thiết bị Android. Nếu bạn sử dụng iPhone, Apple cũng sẽ có lưu dữ liệu của bạn. Để ngăn người khác xem dữ liệu này trên thiết bị, đồng thời ngăn không cho nó bị sao lưu vào đám mây, bạn nên định kỳ xóa dữ liệu vị trí khỏi điện thoại thông minh. Trên thiết bị Android, đi đến Google Settings>Location>Delete location history (Cài đặt Google>Vị trí>Xóa lịch sử vị trí). Trên thiết bị iOS, bạn phải thao tác nhiều hơn; Apple muốn gây khó dễ cho người dùng một chút. Đi đến Settings>Privacy>Location Services (Cài đặt>Bảo mật>Dịch vụ vị trí), sau đó cuộn xuống "System Services"(Dịch vụ hệ thống), tới "Frequent Locations" (Vị trí thường xuyên), rồi "Clear Recent History" (Xóa lịch sử gần đây).

Trong trường hợp của Google, dữ liệu vị trí địa lý có sẵn trên mạng có thể được dùng để tái tạo lại các hoạt động di chuyển của bạn, trừ khi bạn tắt tính năng này. Ví dụ, bạn có thể dành phần lớn thời gian trong ngày tại một địa điểm, nhưng có thể phát sinh di chuyển, chẳng hạn như để gặp khách hàng hay tìm chỗ ăn. Đáng lo ngại hơn, nếu có người lấy được quyền truy cập vào tài khoản Google hoặc Apple của bạn, người đó cũng có thể xác định được nơi bạn sống hoặc bạn bè của bạn dựa vào nơi bạn dành phần lớn thời gian của mình. Ít nhất họ cũng có thể phát hiện ra thói quen hằng ngày của bạn.

Như vậy, chỉ một hoạt động đơn giản là đi bộ cũng mang đến vô

số cơ hội để người khác theo dõi hành vi của bạn. Sau khi biết điều này, giả sử bạn quyết định để điện thoại di động ở nhà. Vậy là vấn đề bị theo dõi đã được giải quyết rồi, đúng không? Ồ, điều đó còn tùy.

Bạn có đeo thiết bị theo dõi tập thể dục như Fitbit, vòng đeo tay UP của Jawbone hay Nike+FuelBand không? Nếu không, có thể bạn đeo đồng hồ thông minh của Apple, Sony, hoặc Samsung. Nếu sử dụng một hoặc cả hai loại này – vòng theo dõi tập thể dục và/hoặc đồng hồ thông minh – bạn vẫn có thể bị theo dõi đấy. Các thiết bị này và ứng dụng đi kèm được thiết kế để ghi lại các hoạt động của bạn, thường là với thông tin định vị toàn cầu GPS, nên bạn vẫn có thể bị theo dõi, dù dữ liệu được phát trực tiếp hay tải lên sau.

Từ sousveillance do nhà hoạt động vì quyền riêng tư Steve Mann tạo ra là cách chơi chữ của từsurveillance (giám sát). Trong tiếng Pháp, sur nghĩa là "ở trên," sous nghĩa là "ở dưới." Như vậy,sousveillance có nghĩa là thay vì bị theo dõi từ trên – chẳng hạn bị người khác hoặc camera an ninh theo dõi – chúng ta lại đang bị theo dõi từ "bên dưới" bởi các thiết bị mini mà chúng ta mang theo, thậm chí là đeo trên người.

Thiết bị theo dõi tập thể dục và đồng hồ thông minh ghi lại dữ liệu sinh trắc học như nhịp tim, số bước đi, kể cả thân nhiệt của bạn. Cửa hàng ứng dụng của Apple hỗ trợ nhiều ứng dụng được thiết kế độc lập để theo dõi sức khỏe và tình trạng thể chất trên điện thoại và đồng hồ của hãng này. Cửa hàng Google Play cũng vậy. Và bạn biết điều gì không? Các ứng dụng này đều được cài đặt để phát dữ liệu trở về công ty mẹ qua sóng vô tuyến, bề ngoài là nhằm thu thập dữ liệu để chủ sở hữu nghiên cứu trong tương lai, nhưng đồng thời cũng chia sẻ nó, đôi khi không qua sự đồng thuận của bạn.

Chẳng hạn, trong thời gian diễn ra giải đua xe đạp Amgen Tour 2015 của California, những người tham gia có thể xác định ai đã vượt qua họ và sau đó, khi vào mạng, có thể gửi tin nhắn trực tiếp cho những người đó. Điều này có thể khiến bạn giật mình khi có

người lạ bắt chuyện và nói về một động tác mà bạn thực hiện trong cuộc đua – một động tác mà bạn còn không nhớ là mình đã làm.

Tôi cũng từng gặp chuyện tương tự. Khi đang lái xe trên cao tốc từ Los Angeles đến Las Vegas, tôi bị một anh chàng lái xe BMW cắt ngang. Do mải nói chuyện điện thoại, anh ta đột ngột chuyển làn, chen lên trước, chỉ cách xe tôi vài xăng-ti-mét. Tôi được phen hú hồn, suýt nữa thì cả hai cùng đi đời.

Tôi vơ lấy điện thoại và giả làm người của cơ quan thực thi pháp luật gọi cho Cục Quản lý xe Cơ giới (DMV). Tôi yêu cầu DMV kiểm tra biển số xe, sau đó họ cung cấp cho tôi tên, địa chỉ, và số An sinh Xã hội của anh ta. Sau đó, tôi gọi tới hãng viễn thông AirTouch Cellular, mạo danh một nhân viên của hãng này và yêu cầu họ tìm kiếm số điện thoại dựa trên số An sinh Xã hội này. Nhờ vậy tôi đã lấy được số di động của anh ta.

Chỉ năm phút sau khi bị tạt đầu xe, tôi gọi điện thoại cho anh chàng kia. Với giọng vẫn còn run rẩy và giận dữ, tôi hét lên: “Này, đồ ngốc, tôi là người mà cậu vừa tạt đầu xe cách đây năm phút đấy, suýt nữa cậu giết cả hai chúng ta rồi. Tôi là người của DMV, và nếu diễn trò này thêm lần nữa, cậu sẽ bị tước bằng lái xe đấy!”

Có lẽ đến bây giờ, anh chàng kia vẫn băn khoăn không hiểu vì sao tôi lại có được số điện thoại của anh ta. Hy vọng rằng cuộc gọi đã khiến anh chàng sợ mà lái xe tử tế hơn. Nhưng có Chúa mới biết.

Nhưng gậy ông lại đập lưng ông. Tài khoản di động AT&T của tôi cũng có lần bị một đám hacker non tay tấn công bằng cách sử dụng kỹ thuật social engineering. Chúng giả danh là nhân viên ở một cửa hàng của AT&T và gọi tới một cửa hàng AT&T khác ở miền Trung Tây, thuyết phục nhân viên ở đó đặt lại địa chỉ email trên tài khoản AT&T của tôi để họ đặt lại mật khẩu trực tuyến và chiếm quyền truy cập vào dữ liệu chi tiết về tài khoản của tôi, bao gồm cả hồ sơ thanh toán!

Trong trường hợp ở Amgen Tour, các tay đua đã sử dụng tính năng Flyby của ứng dụng Strava để chia sẻ, theo chế độ cài đặt

mặc định, các dữ liệu cá nhân với những người dùng Strava khác. Trong một cuộc phỏng vấn cho tờ Forbes, Gareth Nettleton, giám đốc tiếp thị quốc tế của Strava, cho biết: “Về cơ bản, Strava về là một nền tảng mở nơi các vận động viên kết nối với một cộng đồng toàn cầu. Tuy nhiên, chúng tôi hết sức đề cao sự riêng tư của các vận động viên nên đã thực hiện các biện pháp để họ có thể quản lý quyền riêng tư của mình theo những cách đơn giản.”

Strava có chế độ cài đặt bảo mật nâng cao cho phép bạn kiểm soát những ai có thể xem dữ liệu về nhịp tim của mình. Bạn cũng có thể tạo vùng bảo mật của thiết bị để những người khác không thể nhìn thấy nơi bạn sinh sống hoặc làm việc. Tại Amgen Tour, khách hàng có thể chọn không tham gia tính năng Flyby, như vậy dữ liệu về các hoạt động của họ được đánh dấu là “riêng tư” tại thời điểm tải lên.

Các thiết bị và dịch vụ theo dõi tập thể dục khác cũng có chế độ bảo vệ quyền riêng tư tương tự. Có thể bạn cho rằng mình không phải là vận động viên đua xe chuyên nghiệp, cũng không mấy khi đi đường cao tốc, nên không cần đến những sự bảo vệ đó. Điều gì có thể gây hại ở đây chứ? Nhưng có những hoạt động khác mà bạn thực hiện, một số trong đó mang tính riêng tư, vẫn có thể được chia sẻ trên ứng dụng và trên mạng, và do đó tạo ra các vấn đề về quyền riêng tư.

Bản thân việc ghi lại các hoạt động như ngủ hoặc đi cầu thang bộ, đặc biệt là khi được thực hiện cho mục đích y tế, chẳng hạn như giảm phí bảo hiểm y tế, có thể không làm ảnh hưởng đến quyền riêng tư của bạn. Tuy nhiên, khi dữ liệu này được kết hợp với các dữ liệu khác, chúng có thể dần dựng lên một bức tranh toàn diện về bạn. Và chúng có thể tiết lộ nhiều thông tin hơn mức mà bạn cảm thấy thoải mái chia sẻ.

Khi xem dữ liệu trực tuyến, một người đeo thiết bị theo dõi sức khỏe phát hiện ra rằng nhịp tim của anh tăng đáng kể mỗi khi quan hệ tình dục. Thực ra, Fitbit từng đưa tình dục vào danh sách trực tuyến ghi lại các hoạt động thường nhật. Mặc dù ẩn danh, song dữ liệu trên vẫn có thể được tìm kiếm qua Google cho đến

khi nó bị tiết lộ công khai và Fitbit phải nhanh chóng gỡ bỏ nó.

Một số người có thể nghĩ: "Thế thì sao nào?" Đúng, bản thân dữ liệu không có gì thú vị cả. Nhưng giả sử kết hợp dữ liệu nhịp tim với dữ liệu định vị, rủi ro có thể phát sinh. Kashmir Hill, phóng viên tờ Fusion, đặt ra một trường hợp cực đoan đối với dữ liệu của Fitbit: "Điều gì sẽ xảy ra nếu các công ty bảo hiểm kết hợp dữ liệu hoạt động của bạn với dữ liệu vị trí GPS để xác định không những thời gian mà cả địa điểm bạn quan hệ tình dục? Liệu họ có đưa một khách hàng vào nhóm rủi ro y tế cao dựa trên dữ liệu cho thấy người này quan hệ tình dục ở nhiều địa điểm khác nhau trong một tuần không?"

Mặt khác, dữ liệu Fitbit cũng được sử dụng thành công trong các vụ án để chứng minh hoặc bác bỏ lời khai. Trong một trường hợp cá biệt, dữ liệu Fitbit được sử dụng để chứng minh rằng một người phụ nữ đã nói dối về một vụ hiếp dâm.

Trong thời gian đến thăm Lancaster, Pennsylvania, một phụ nữ báo với cảnh sát rằng vào nửa đêm, khi cô thức dậy, một kẻ lạ mặt đang đè lên người cô, và trong lúc vật lộn để thoát ra, cô đánh rơi chiếc Fitbit của mình. Khi cảnh sát tìm thấy chiếc Fitbit và được người phụ nữ đồng ý cho họ truy cập dữ liệu trong đó, thiết bị này đã kể một câu chuyện khác. Rõ ràng, cô đã thức và đi bộ suốt đêm. Theo đài truyền hình địa phương, người phụ nữ trên bị "buộc tội báo cáo sai sự thật, báo động giả về an toàn công cộng, cố tình làm lộn xộn đồ đạc và đặt một con dao tại hiện trường để làm giả hiện trường vụ hiếp dâm."

Các phương tiện theo dõi hoạt động cũng có thể được dùng để hỗ trợ các tuyên bố về tình trạng mất sức lao động. Một hãng luật Canada đã sử dụng dữ liệu theo dõi hoạt động để chứng minh những hậu quả nghiêm trọng của tai nạn lao động đối với một thân chủ của mình. Người này đã cung cấp dữ liệu Fitbit cho Vivametrica, công ty thu thập dữ liệu từ thiết bị đeo thông minh và so sánh nó với dữ liệu về hoạt động và sức khỏe của toàn dân chúng, để chứng minh rằng hoạt động của mình đã bị sụt giảm rõ rệt. Chia sẻ với Forbes, Simon Muller, thuộc Công ty Luật McLeod

ở Calgary, nói: “Đến nay, chúng ta vẫn luôn phải dựa vào các diễn giải lâm sàng. Bây giờ chúng ta có thể nắm được dữ liệu chắc chắn về những khoảng thời gian dài hơn.”

Dù bạn không sử dụng thiết bị theo dõi hoạt động, nhưng đồng hồ thông minh như Galaxy Gear của Samsung cũng có thể xâm phạm quyền riêng tư của bạn theo những cách tương tự. Nếu bạn nhận được các thông báo nhanh như tin nhắn, email, và cuộc gọi qua thiết bị đeo tay, thì người khác cũng có thể xem các nội dung đó.

Gần đây, ngày càng có nhiều người sử dụng GoPro, một camera mini gắn vào mũ bảo hiểm hoặc bảng điều khiển trên xe để có thể ghi lại các chuyển động của bạn. Nhưng điều gì sẽ xảy ra nếu bạn quên mật khẩu của ứng dụng này? Một nhà nghiên cứu người Israel mượn GoPro của bạn và ứng dụng di động liên kết với nó, nhưng anh ta không có mật khẩu. Giống như email, ứng dụng GoPro cho phép bạn đặt lại mật khẩu. Tuy nhiên, quy trình thay đổi mật khẩu có sơ hở (hiện đã được khắc phục). Để đặt lại mật khẩu, GoPro gửi một liên kết đến email của bạn, nhưng liên kết này thực ra lại dẫn đến một file nén ZIP để tải xuống và chèn vào thẻ SD của thiết bị. Khi nhà nghiên cứu trên mở file ZIP, anh thấy một file văn bản có tên “settings” (cài đặt) chứa thông tin đăng nhập không dây của người dùng – bao gồm SSID và mật khẩu mà GoPro sẽ sử dụng để truy cập Internet. Nhà nghiên cứu phát hiện ra rằng nếu thay đổi số trong liên kết – 8605145 – thành một số khác, giả dụ 8604144, anh có thể truy cập dữ liệu cấu hình GoPro của người khác, bao gồm mật khẩu không dây của họ.

Có lẽ hãng sản xuất thiết bị nhiếp ảnh Eastman Kodak là nơi đầu tiên nêu lên vấn đề về sự riêng tư ở Mỹ – hay ít nhất đã khiến chủ đề này trở nên thú vị – vào cuối những năm 1800. Trước đó, nhiếp ảnh là một môn nghệ thuật nghiêm túc, tốn thời gian, và bất tiện, đòi hỏi các thiết bị chuyên dụng (máy ảnh, đèn chiếu sáng, phòng tối) và thời gian người được chụp phải bất động để giữ nguyên tư thế khá lâu (thời đó, người ta vẫn phải chụp ảnh trong phòng kín). Sau đó, Kodak xuất hiện và giới thiệu một chiếc

máy ảnh xách tay với giá cả tương đối hợp lý. Dòng sản phẩm đầu tiên của hãng này được bán với giá 25 đô-la – tức khoảng 100 đô-la theo thời giá hiện nay. Kodak tiếp tục ra mắt dòng Brownie với giá vẻn vẹn 1 đô-la. Cả hai loại máy ảnh này đều được thiết kế để chụp ở ngoài nhà hay văn phòng. Có thể coi chúng là máy tính di động và điện thoại di động đương thời.

Đột nhiên, người ta phải đối phó với thực tế rằng một người nào đó trên bãi biển hoặc trong công viên công cộng có thể mang theo máy ảnh, và trong những bức ảnh mà họ chụp có thể có cả bạn. Vì thế, bạn trông phải đẹp. Bạn phải hành động có trách nhiệm. Brian Wallis, cựu giám tuyển tại Trung tâm Nhiếp ảnh Quốc tế, nói: "Điều đó không chỉ thay đổi thái độ của bạn đối với nhiếp ảnh, mà còn đối với bản thân những thứ mà bạn chụp vào ảnh. Vì vậy, bạn phải sửa sang bàn ăn, phải chuẩn bị tiệc sinh nhật thật cẩn thận."

Tôi tin rằng chúng ta thực sự sẽ hành xử khác đi khi đang bị theo dõi. Hầu hết chúng ta đều cố gắng cư xử tốt nhất khi biết đang có camera theo dõi, dù rằng vẫn có những người chẳng quan tâm gì.

Sự ra đời của nhiếp ảnh cũng ảnh hưởng đến suy nghĩ của mọi người về sự riêng tư. Đột nhiên, hành vi xấu của ai đó có thể bị ghi lại bằng hình ảnh. Thực ra, ngày nay các nhân viên thực thi pháp luật có máy quay và máy quay cơ thể, vì vậy sẽ có hồ sơ về hành vi của chúng ta khi chúng ta có chuyện dính líu tới luật pháp. Và hiện nay, với công nghệ nhận diện khuôn mặt, bạn có thể chụp ảnh một người để đối chiếu với hồ sơ Facebook của họ. Ngày nay, chúng ta có các bức ảnh tự sướng.

Nhưng vào năm 1888, khả năng lúc nào cũng có thể bị ghi lại như thế vẫn còn là một điều mới vẻ và đáng lo ngại. Tờ Hartford Courant cảnh báo: "Các công dân nghiêm túc không thể thoải mái cười đùa mà không có nguy cơ bị bắt tại trận và bức ảnh của anh ta sẽ bị đem cho đám trẻ con truyền tay nhau xem. Và chàng trai trẻ muốn tán tỉnh cô gái trong mộng lúc chèo thuyền xuôi dòng sông lúc nào cũng phải khư khư giương ô lên che chắn."

Một số người không thích sự thay đổi này. Vào những năm 1880, một nhóm phụ nữ ở Mỹ đã đập vỡ một chiếc máy ảnh trên tàu vì họ không muốn chủ nhân chiếc máy chụp ảnh họ. Ở Anh, một nhóm thanh niên lập hội để đi tuần tra trên bãi biển, dọa nạt những người định chụp ảnh những phụ nữ bước lên bờ sau khi bơi.

Vào những năm 1890, Samuel Warren và Louis Brandeis (về sau Louis Brandeis làm việc trong Tòa án tối cao) đã viết trong một bài báo rằng: "Các bức ảnh tức thời và báo chí đã xâm chiếm các khu vực thiêng liêng trong cuộc sống riêng tư và gia đình." Họ đề nghị luật pháp Mỹ nên chính thức thừa nhận quyền riêng tư và, để chống lại nạn chụp ảnh lén, áp đặt trách nhiệm pháp lý đối với bất kỳ xâm phạm nào. Các luật như vậy đã được thông qua ở một số tiểu bang.

Ngày nay, nhiều thế hệ đã trưởng thành trong sự đe dọa của những bức ảnh tức thời. Ảnh chụp lấy ngay, có ai chụp không nhỉ? Nhưng ngày nay chúng ta cũng hài lòng với sự phổ biến của nhiếp ảnh. Dù đi đâu, bạn cũng có thể xuất hiện trong một video hay bức ảnh nào đó – bất kể bạn có cho phép hay không. Và bất kỳ ai ở bất kỳ đâu trên thế giới cũng có thể xem được những hình ảnh đó.

Đối với sự riêng tư, chúng ta sống trong sự mâu thuẫn. Một mặt, chúng ta đề cao nó, coi nó như một quyền, và coi nó có liên hệ với sự tự do và độc lập của mình: Chẳng phải bất cứ điều gì chúng ta làm trên mảnh đất của mình, đằng sau cánh cửa đóng kín, vẫn là riêng tư hay sao? Mặt khác, con người là những sinh vật tò mò. Và bây giờ chúng ta có phương tiện để thỏa mãn tối đa sự tò mò đó theo những cách trước đây là không tưởng.

Bạn có bao giờ tự hỏi cái gì đằng sau hàng rào kia trên phố, trong sân sau nhà hàng xóm không? Công nghệ có thể trả lời câu hỏi đó cho hầu hết mọi người. Ngày nay, các công ty sản xuất máy bay không người lái như 3D Robotics và CyPhy giúp cho một người bình thường cũng có thể sở hữu máy bay dễ dàng (ví dụ, tôi có máy bay không người lái DJI Phantom 4). Đó là loại máy bay điều

khiển từ xa và tinh vi hơn nhiều so với trước đây. Hầu như tất cả đều được trang bị camera mini, giúp bạn nhìn thế giới theo một cách mới. Một số máy bay không người lái có thể được điều khiển từ điện thoại di động.

Về bản chất, máy bay không người lái cá nhân là những kẻ tọc mạch. Giờ đây, không nơi nào là quá xa xôi hẻo lánh, vì bạn có thể cho máy bay lượn vòng cách mặt đất vài trăm mét.

Ngày nay, ngành bảo hiểm sử dụng máy bay không người lái vì lý do kinh doanh. Hãy thử nghĩ mà xem. Nếu bạn là chuyên viên tính toán tổn thất và cần phải đánh giá về một khu đất sắp sửa ký hợp đồng bảo hiểm, bạn có thể đưa máy bay không người lái bay một vòng quanh đó, vừa để kiểm tra trực quan những nơi vốn trước đây bạn không thể tiếp cận, vừa để tạo bản ghi vĩnh viễn về những gì bạn tìm thấy. Bạn có thể đưa máy bay lên cao để có được góc nhìn từ trên xuống mà trước đây chỉ máy bay trực thăng mới làm được.

Bây giờ, chúng ta có thể dùng máy bay không người lái giờ để do thám hàng xóm – chỉ cần đưa máy bay bay trên mái nhà rồi nhìn xuống để thấy rằng nhà hàng xóm có bể bơi, hay họ thích khỏa thân tắm nắng. Mọi chuyện trở nên phức tạp: chúng ta mong giữ được sự riêng tư trong nhà riêng và trên bất động sản của mình, nhưng điều đó đang bị thách thức. Ví dụ, trên Google Street View và Google Earth, Google che giấu khuôn mặt, biển số xe, và thông tin cá nhân khác. Nhưng một người hàng xóm có máy bay không người lái sẽ không bảo đảm được chuyện đó – dù rằng bạn có thể lịch sự yêu cầu anh ta đừng cho máy bay bay qua sân nhà mình. Máy bay không người lái trang bị video sẽ mang đến những dữ liệu của cả Google Earth và Google Street View cộng lại.

Có một số quy định. Chẳng hạn, Cục Hàng không Liên bang quy định rằng máy bay không người lái không được rời khỏi tầm nhìn của người điều khiển, rằng nó không được bay trong một khoảng cách nhất định của sân bay, và rằng nó không được bay quá độ cao cho phép. Có một ứng dụng gọi là B4UFLY giúp bạn xác định nơi để thả máy bay không người lái. Và trước trào lưu sử dụng

máy bay không người lái thương mại, một số tiểu bang đã thông qua các luật hạn chế việc sử dụng chúng. Ở Texas, công dân bình thường không được phép sử dụng máy bay không người lái, nhưng vẫn có một số ngoại lệ, bao gồm ngoại lệ cho các nhân viên bất động sản. Colorado có lẽ là bang có quan điểm tự do nhất về máy bay không người lái; ở đây, công dân bình thường cũng có thể vận hành thiết bị này.

Ở mức tối thiểu, chính phủ Mỹ nên yêu cầu những người đam mê máy bay không người lái đăng ký cho thiết bị của mình. Ở Los Angeles, nơi tôi sống, có người đã đâm máy bay không người lái vào các đường dây điện ở West Hollywood, gần ngã tư đường Larrabee và Đại lộ Sunset. Nếu chiếc máy đó có đăng ký, các nhà chức trách có thể xác định được ai đã làm gián đoạn công việc của 700 người trong nhiều giờ đồng hồ trong khi hàng chục nhân viên của công ty điện lực phải làm việc tới tận đêm để khôi phục điện cho khu vực.

Các cửa hàng bán lẻ ngày càng muốn tìm hiểu kỹ hơn về khách hàng của mình. Một phương pháp hiệu quả là sử dụng bộ bắt sóng IMSI di động. Khi bạn bước vào một cửa hàng, máy bắt sóng IMSI lấy thông tin từ điện thoại di động và bằng cách nào đó tìm ra số điện thoại của bạn. Từ đó, hệ thống này có thể truy vấn hàng tấn cơ sở dữ liệu và xây dựng một hồ sơ về bạn. Các nhà bán lẻ truyền thống cũng bắt đầu sử dụng công nghệ nhận dạng khuôn mặt. Hãy nghĩ về nó như một người đứng chào ở cửa một đại siêu thị của Walmart.

Trong tương lai không xa, khi bước vào một cửa hàng chưa từng đặt chân đến, có thể tôi vẫn nhận được câu chào: “Xin chào Kevin.” Việc cá nhân hóa trải nghiệm bán lẻ là một hình thức giám sát khác, tuy rằng tinh tế hơn. Chúng ta không còn có thể mua sắm ẩn danh nữa.

Tháng Sáu năm 2015, chỉ hai tuần sau khi gây sức ép buộc Quốc hội thông qua Đạo luật Tự do Hoa Kỳ – một phiên bản sửa đổi của Đạo luật Patriot, có bổ sung một số điều khoản bảo vệ quyền riêng tư – chín nhóm hoạt động vì quyền riêng tư của người tiêu

dùng, trong số đó một vài nhóm đã mạnh tay vận động hành lang rất nhiều để ủng hộ Đạo luật Tự do, trở nên bất mãn với một số nhà bán lẻ lớn và rút khỏi các vòng đàm phán nhằm hạn chế việc sử dụng công nghệ nhận diện khuôn mặt.

Vấn đề gây tranh cãi là liệu nhà bán lẻ có cần xin phép người tiêu dùng trước khi quét dữ liệu của họ hay không. Nghe có vẻ hợp lý, nhưng các tổ chức bán lẻ lớn tham gia vào cuộc đàm phán trên không nhân nhượng điểm này. Theo họ, khi bước chân vào cửa hàng của họ, tất nhiên là thông tin nhận dạng của bạn sẽ bị quét.

Một số người có thể muốn được đón tiếp theo lối riêng tư như vậy khi bước vào cửa hàng, nhưng nhiều người trong chúng ta sẽ thấy điều này thực sự đáng lo ngại. Các cửa hàng lại có cách nhìn khác. Họ muốn bắt những kẻ trộm đã được biết mặt, nên không muốn trao cho người tiêu dùng quyền được rút lui. Nếu cửa hàng sử dụng công nghệ nhận diện khuôn mặt, ngay khi những kẻ trộm đã được biết mặt bước vào, chúng sẽ bị nhận diện tức thì.

Khách hàng nói gì? Ít nhất tại Anh, bảy trong số mười người được khảo sát cảm thấy việc sử dụng công nghệ nhận diện khuôn mặt trong cửa hàng là “quá đáng sợ.” Và một số tiểu bang của Mỹ, bao gồm Illinois, đã tự ra quy định về hoạt động thu thập và lưu trữ các dữ liệu sinh trắc học. Những quy định này đã dẫn đến nhiều vụ kiện tụng. Ví dụ, một người đàn ông ở Chicago hiện đang kiện Facebook vì anh ta chưa đồng ý cho phép hãng này sử dụng công nghệ nhận diện khuôn mặt để xác định anh ta trong ảnh của người khác.

Có thể sử dụng công nghệ nhận diện khuôn mặt để xác định một người hoàn toàn dựa trên hình ảnh của họ. Nhưng nếu bạn đã biết người đó là ai và bạn chỉ muốn chắc chắn rằng anh ta đang ở chỗ mà anh ta nên ở thì sao? Đây là một cách sử dụng tiềm năng khác của công nghệ nhận diện khuôn mặt.

Moshe Greenshpan là Giám đốc Điều hành của công ty cung cấp công nghệ nhận diện khuôn mặt Face-Six có trụ sở tại Israel và Las Vegas. Một trong những ứng dụng của phần mềm Churchix

của họ là kiểm tra những người tham dự các buổi lễ ở nhà thờ. Ý tưởng ở đây là để giúp các nhà thờ xác định được đâu là những giáo dân tham dự không thường xuyên, từ đó khích lệ họ năng đến nhà thờ hơn; đồng thời xác định những người tham dự thường xuyên để khích lệ họ đóng góp nhiều hơn.

Face-Six nói có ít nhất 30 nhà thờ trên thế giới đang sử dụng công nghệ của hãng này. Các nhà thờ chỉ cần tải lên hình ảnh chất lượng cao của các giáo dân, sau đó hệ thống sẽ tìm kiếm và giám sát họ trong các buổi lễ và hoạt động xã hội.

Khi được hỏi liệu các giáo hội có thông báo với giáo dân rằng họ đang bị theo dõi hay không, Greenshpan nói với Fusion: "Tôi không cho rằng các nhà thờ có thông báo việc đó. Chúng tôi có khuyến khích họ làm như vậy, nhưng tôi nghĩ họ sẽ làm theo."

Jonathan Zittrain, giám đốc Trung tâm Internet và Xã hội Berkman của trường Luật Harvard, đã đưa ra đề xuất rằng con người cần một thẻ "không theo dõi" giống như thẻ được sử dụng trên một số website. Điều này sẽ giúp những người không muốn tham gia không xuất hiện trong cơ sở dữ liệu nhận diện khuôn mặt. Để làm được điều này, Viện Tin học Quốc gia tại Nhật Bản đã tạo ra một "kính bảo hộ riêng tư" thương mại. Cặp kính này, được bán với giá khoảng 240 đô-la, tạo ra ánh sáng chỉ nhìn thấy được trên camera. Ánh sáng quang được phát ra xung quanh mắt để ngăn chặn các hệ thống nhận diện khuôn mặt. Theo những người thử nghiệm ban đầu, kính này phát huy hiệu quả lên tới 90%. Cảnh báo duy nhất ở đây là chúng không thích hợp khi lái xe hoặc đi xe đạp. Chúng cũng không có vẻ ngoài hợp thời trang, nhưng vẫn là giải pháp hoàn hảo để thực thi quyền riêng tư của bạn ở nơi công cộng.

Như vậy, bạn đã biết rằng sự riêng tư của mình có thể bị xâm phạm khi bạn ở ngoài trời, vậy có khi bạn sẽ cảm thấy an toàn hơn khi ở trong xe ô tô, nhà, thậm chí văn phòng. Thật không may, điều này không còn đúng nữa. Trong các chương tiếp theo, tôi sẽ giải thích tại sao.

Chương 11: ĐỪNG CHIA SẺ ĐỊA CHỈ CỦA TÔI

Các nhà nghiên cứu Charlie Miller và Chris Valasek không xa lạ gì với việc đột nhập vào các hệ thống ô tô. Trước đây, cả hai đã xâm nhập vào một chiếc Toyota Prius – nhưng là trong bối cảnh họ ngồi ngay ở ghế sau của xe. Sau đó, vào mùa hè năm 2015, Miller và Valasek đã thành công trong việc giành quyền điều khiển chính của chiếc Jeep Cherokee trong khi nó vẫn đang chạy ở tốc độ 110km/giờ trên một đường cao tốc ở St. Louis. Họ có thể điều khiển từ xa một chiếc xe mà không cần ở gần nó.

Thực ra, có tài xế ngồi trong chiếc Jeep nhắc đến ở trên – đó là phóng viên Andy Greenberg của tạp chí Wired. Các nhà nghiên cứu đã thông báo trước với Greenberg rằng dù có chuyện gì xảy ra cũng đừng hoảng sợ. Nhưng hóa ra đó lại là một nhiệm vụ khó khăn, ngay cả đối với một người đã biết trước rằng xe của mình sẽ bị xâm nhập.

Greenberg viết về trải nghiệm này như sau: “Chân ga ngừng hoạt động ngay lập tức. Khi tôi cuống cuồng nhấn bàn đạp và quan sát chỉ số RPM (tốc độ động cơ) tăng vọt, chiếc Jeep bị mất một nửa tốc độ, rồi chậm lại như rùa bò. Chuyện này xảy ra khi tôi vừa đi đến một đoạn cầu vượt dài, không có ai giúp đỡ. Thí nghiệm này bỗng mất đi sự thú vị của nó.”

Sau đó, các nhà nghiên cứu bị chỉ trích vì “liều lĩnh” và “nguy hiểm.” Chiếc xe Jeep của Greenberg đang đi trên đường công cộng, không phải trên đường chạy thử nghiệm, do đó, tại thời điểm tôi viết cuốn sách này, cơ quan thực thi pháp luật Missouri vẫn đang cân nhắc buộc tội Miller và Valasek – và có thể là cả Greenberg nữa.

Việc xâm nhập những chiếc xe được kết nối từ xa là đề tài được bàn đến trong nhiều năm nay, nhưng phải đến thí nghiệm của Miller và Valasek thì cả ngành công nghiệp ô tô mới chú ý. Cho dù

mục đích của nó là gì, thí nghiệm này cũng đã khiến các nhà sản xuất ô tô phải bắt đầu suy nghĩ nghiêm túc về an toàn mạng – và về việc Quốc hội có nên cấm hoạt động xâm nhập bất hợp pháp vào ô tô hay không.

Các nhà nghiên cứu khác đã chứng minh rằng họ có thể đảo ngược giao thức kiểm soát xe bằng cách chặn và phân tích lưu lượng GSM hoặc CDMA di chuyển từ máy tính trên xe tới hệ thống của nhà sản xuất ô tô. Các nhà nghiên cứu đã có thể giả mạo các hệ thống điều khiển ô tô bằng cách gửi tin nhắn SMS để khóa và mở khóa cửa xe. Một số người thậm chí còn chiếm đoạt các khả năng khởi động từ xa bằng cách sử dụng các phương thức tương tự. Nhưng Miller và Valasek là những người đầu tiên có thể giành kiểm soát hoàn toàn một chiếc xe từ xa. Theo họ, cũng với những phương thức tương tự, họ có thể chiếm được quyền kiểm soát xe ô tô ở các bang khác.

Có lẽ kết quả quan trọng nhất trong thí nghiệm Miller-Valasek là họ đã khiến hãng Chrysler thu hồi hơn 1,4 triệu chiếc xe vì vấn đề lập trình – đây cũng là lần đầu tiên ô tô bị thu hồi vì lý do này. Chrysler cũng tạm thời ngắt kết nối của những chiếc xe bị ảnh hưởng với mạng Sprint mà các xe sử dụng cho di động viễn thông, dữ liệu mà các xe thu thập và chia sẻ với nhà sản xuất theo thời gian thực. Tại hội nghị DEF CON 23, Miller và Valasek phát biểu rằng họ nhận ra mình có thể chiếm quyền điều khiển xe ở các bang khác, nhưng điều đó vi phạm các nguyên tắc đạo đức. Thay vào đó, họ thực hiện thí nghiệm với Greenberg ở quê nhà của Miller.

Trong chương này, tôi sẽ chỉ ra rằng những chiếc ô tô mà chúng ta lái, những chiếc tàu mà chúng ta đi, và những ứng dụng di động mà chúng ta sử dụng hằng ngày có thể bị sơ sở ra sao trước những cuộc tấn công trên mạng, chưa kể đến vô số những sự xâm phạm về quyền riêng tư mà xe kết nối có thể mang đến cho cuộc sống của chúng ta.

Khi Johana Bhuiyan, một phóng viên của BuzzFeed, đến văn phòng của Uber ở New York trong một chiếc xe của Uber, Josh

Mohrer, giám đốc quản lý của hãng này, đang ngồi đợi. “Cô đây rồi,” anh nói, và giơ chiếc iPhone lên. “Tôi đã theo dõi cô.” Đó không phải là một khởi đầu tốt đẹp cho cuộc phỏng vấn của họ, vốn liên quan đến vấn đề quyền riêng tư của người tiêu dùng.

Trước khi bài báo của Bhuiyan xuất hiện vào tháng 11 năm 2014, rất ít người bên ngoài Uber biết đến God View, một công cụ mà Uber dùng để theo dõi vị trí của hàng nghìn lái xe hợp đồng cũng như khách hàng của họ, tất cả đều theo thời gian thực.

Như tôi đã đề cập ở phần trước, các ứng dụng thường xin phép người dùng nhiều nội dung khác nhau, bao gồm quyền truy cập dữ liệu vị trí địa lý của họ. Ứng dụng Uber đi xa hơn: nó yêu cầu vị trí gần đúng (Wi-Fi) và chính xác (GPS), quyền truy cập danh bạ của bạn, và không cho phép thiết bị di động của bạn ở chế độ ngủ (để nó có thể giám sát nơi bạn ở).

Bhuiyan cho Mohrer biết rằng cô không cho phép công ty này theo dõi cô vào bất cứ lúc nào và ở bất cứ nơi đâu. Nhưng trên thực tế là cô đã làm như vậy, mặc dù có thể không rõ ràng. Nội dung cho phép này nằm trong thỏa thuận người dùng mà cô đã đồng ý khi tải dịch vụ xuống thiết bị di động của mình. Sau cuộc gặp, Mohrer đã gửi email cho Bhuiyan nhật ký một số chuyến đi Uber gần đây của cô.

Uber thu thập một hồ sơ cá nhân cho mỗi khách hàng, ghi lại từng chuyến đi mà họ thực hiện. Đó là một ý tưởng tồi nếu cơ sở dữ liệu không an toàn. Được biết đến trong lĩnh vực bảo mật như một “hũ mật ngọt,” cơ sở dữ liệu của Uber có thể thu hút mọi đối tượng rình mò, từ chính phủ Mỹ cho đến hacker Trung Quốc.

Năm 2015, Uber thay đổi một số chính sách bảo mật, một số thay đổi theo hướng gây thiệt hại cho người tiêu dùng. Uber hiện thu thập dữ liệu vị trí địa lý từ tất cả người dùng ở Mỹ – ngay cả khi ứng dụng này chỉ chạy ngầm. Uber cho biết họ sẽ sử dụng địa chỉ Wi-Fi và IP để theo dõi người dùng “ngoại tuyến.” Điều đó có nghĩa là ứng dụng Uber hoạt động như một gián điệp thầm lặng trên thiết bị di động của bạn. Tuy nhiên, công ty này không nói

tại sao họ lại cần khả năng này.

Uber cũng không giải thích đầy đủ lý do tại sao họ lại cần tới God View. Mặt khác, theo chính sách bảo mật của họ: "Uber có chính sách nghiêm ngặt nghiêm cấm tất cả nhân viên ở mọi cấp truy cập vào dữ liệu của người lái. Ngoại lệ duy nhất đối với chính sách này là dành cho một nhóm hạn chế các mục đích hoạt động hợp pháp." Hoạt động hợp pháp có thể bao gồm việc giám sát các tài khoản bị nghi ngờ là gian lận và giải quyết các vấn đề của lái xe (ví dụ: mất kết nối). Hoạt động hợp pháp có lẽ không bao gồm việc theo dõi những chuyến đi của một phóng viên.

Bạn có thể nghĩ rằng Uber sẽ cung cấp cho khách hàng quyền xóa thông tin theo dõi. Không. Và nếu sau khi đọc xong cuốn sách này, bạn xóa ứng dụng trên khỏi điện thoại của mình, hãy đoán xem điều gì sẽ xảy ra? Dữ liệu của bạn vẫn tồn tại trong Uber.

Theo chính sách bảo mật sửa đổi, Uber cũng thu thập cả thông tin sổ địa chỉ của bạn. Nếu có iPhone, bạn có thể vào phần cài đặt và thay đổi tùy chọn chia sẻ địa chỉ liên hệ. Nếu bạn sử dụng Android, thì đó không phải là một lựa chọn.

Các đại diện của Uber tuyên bố rằng họ hiện không thu thập loại dữ liệu khách hàng này. Tuy nhiên, bằng cách đưa vấn đề thu thập dữ liệu vào trong chính sách bảo mật – mà người dùng hiện tại đã đồng ý và người dùng mới bắt buộc phải đồng ý – công ty này có thể triển khai các tính năng trên bất kỳ lúc nào. Và người dùng sẽ không được nhận bất kỳ bồi thường nào.

Chế độ God View của Uber có lẽ cũng đủ để khiến bạn phải mong muốn quay trở lại những chiếc taxi cũ thông thường. Trước đây, bạn chỉ việc nhảy vào một chiếc taxi, nêu điểm đến rồi thanh toán tiền mặt cho chuyến đi. Nói cách khác, chuyến đi của bạn gần như là hoàn toàn ẩn danh.

Với sự ra đời và phổ biến toàn cầu của thẻ tín dụng trong đầu thế kỷ 21, rất nhiều giao dịch bình thường đã trở nên có thể bị theo dõi, vì vậy có lẽ sẽ có một bản ghi về chuyến xe taxi của bạn ở đâu đó – có thể nó không nằm trong tay tài xế hay công ty cung cấp

dịch vụ taxi, mà nằm ở hãng cung cấp thẻ tín dụng của bạn. Trở lại những năm 1990, khi còn là một thám tử tư, tôi có thể tìm ra hoạt động di chuyển của mục tiêu theo dõi bằng cách lấy thông tin các giao dịch bằng thẻ tín dụng của họ. Chỉ cần nhìn vào bản sao kê, người ta có thể biết rằng tuần trước bạn đã đi taxi ở thành phố New York và trả 54 đô-la cho chuyến đi đó.

Khoảng năm 2010, taxi bắt đầu sử dụng dữ liệu định vị toàn cầu GPS. Lúc này, hãng taxi sẽ biết vị trí bạn bắt xe và xuống xe, tiền cước, và có lẽ số thẻ tín dụng liên quan đến chuyến đi của bạn nữa. Dữ liệu này được New York, San Francisco và các thành phố khác hỗ trợ phong trào dữ liệu mở trong chính phủ cung cấp cho các nhà nghiên cứu. Chỉ cần không công khai danh tính, thì việc công khai những dữ liệu ẩn danh đó có hại gì chứ?

Vào năm 2013, Anthony Tockar, khi đó là sinh viên cao học ở Đại học Northwestern đang thực tập cho một công ty tên là Neustar, xem xét siêu dữ liệu ẩn danh được Ủy ban Taxi và Limousine thành phố New York công bố. Tập dữ liệu này chứa hồ sơ về mọi chuyến đi của những chiếc xe trong đoàn xe taxi thuộc Ủy ban trong năm trước đó, bao gồm số xe taxi, thời gian đón và trả khách, địa điểm, giá vé và số tiền tip, và phiên bản ẩn danh (giá trị băm) của bằng lái và số hiệu của các lái xe taxi. Bản thân bộ dữ liệu này không phải là điều thú vị. Giá trị băm trong trường hợp này đáng tiếc là có thể dễ dàng truy ngược.

Tuy nhiên, khi kết hợp tập dữ liệu công khai với các tập dữ liệu khác, bạn bắt đầu có được bức tranh hoàn chỉnh về những gì đang diễn ra. Trong trường hợp này, Tockar đã có thể xác định nơi những người nổi tiếng như Bradley Cooper và Jessica Alba bắt taxi trong thành phố New York. Tockar đã làm thế nào để phát hiện được điều này?

Với dữ liệu vị trí, anh biết taxi đón và trả khách khi nào và ở đâu, nhưng còn nhiều việc phải làm để có thể xác định được người ngồi trong xe. Vì vậy, anh kết hợp siêu dữ liệu của Ủy ban Taxi và Limousine thành phố New York với hình ảnh trực tuyến từ các trang báo lá cải có sẵn trên mạng. Một cơ sở dữ liệu của các thợ

săn ảnh (paparazzi).

Hãy nghĩ về điều này. Các paparazzi thường xuyên chụp ảnh những người nổi tiếng khi họ vào và ra khỏi taxi ở Thành phố New York. Trong những trường hợp này, số hiệu của taxi thường hiển thị trong khung hình. Nó được in ở phía bên cạnh của mỗi chiếc taxi. Như vậy, số taxi bên hông xe được chụp vào ảnh cùng với một ngôi sao, chẳng hạn như Bradley Cooper, có thể được kết hợp với các dữ liệu công khai có liên quan đến các địa điểm đón và trả và giá vé cùng tiền tip.

May mắn thay, không phải ai trong chúng ta cũng bị paparazzi bám đuổi. Nhưng điều đó không có nghĩa là không có cách nào khác để theo dõi chuyến đi của chúng ta. Có thể bạn không đi taxi. Có cách nào khác để xác định vị trí của bạn không? Có. Ngay cả khi bạn sử dụng phương tiện công cộng.

Nếu đi làm bằng xe buýt, xe lửa, hoặc phà, bạn sẽ không còn vô hình giữa đám đông nữa. Hệ thống chuyển tuyến đang thử nghiệm cách sử dụng các ứng dụng dành cho thiết bị di động và giao tiếp trường gần (NFC) để gắn thẻ hành khách khi họ lên và xuống phương tiện công cộng. NFC là tín hiệu vô tuyến trường gần, thường yêu cầu sự liên hệ vật lý. Các hệ thống thanh toán như Apple Pay, Android Pay và Samsung Pay đều sử dụng NFC, giúp chúng ta không còn phải lúng túng khi thiếu tiền lẻ nữa.

Giả sử bạn có một chiếc điện thoại hỗ trợ NFC được cài đặt ứng dụng của hãng vận tải công cộng địa phương. Ứng dụng này sẽ muốn kết nối với tài khoản ngân hàng hoặc thẻ tín dụng của bạn để bạn luôn có thể lên xe mà không phải lo lắng về số dư trên tài khoản của mình. Kết nối đó kết hợp với số thẻ tín dụng của bạn có thể tiết lộ cho đơn vị chuyển tuyến biết bạn là ai. Thay thế số thẻ tín dụng của bạn bằng mã thông báo token là một tùy chọn mới mà Apple, Android và Samsung cung cấp. Bằng cách đó, người bán trong trường hợp này là cơ quan chuyển tuyến chỉ có mã thông báo chứ không phải số thẻ tín dụng thực của bạn. Sử dụng mã thông báo sẽ cắt giảm các vi phạm dữ liệu ảnh hưởng đến thẻ tín dụng trong tương lai gần vì sau đó, tội phạm sẽ cần

hai cơ sở dữ liệu: mã thông báo và số thẻ tín dụng thực sự đằng sau mã thông báo.

Nhưng giả sử bạn không sử dụng điện thoại hỗ trợ NFC. Thay vào đó bạn có thẻ đi lại, như thẻ CharlieCard ở Boston, thẻ SmarTrip ở thủ đô Washingtonvà thẻ Clipper ở San Francisco. Các thẻ này sử dụng mã thông báo để cảnh báo thiết bị nhận – cho dù là cửa quay hoặc hộp thu tiền vé rằng bạn có đủ số dư để đi xe hay không. Tuy nhiên, hệ thống vận tải công cộng không sử dụng mã thông báo ở phía máy chủ. Bản thân chiếc thẻ chỉ có một số tài khoản chứ không phải thông tin thẻ tín dụng của bạn trên chip từ của nó. Nhưng nếu cơ quan vận tải bị xâm nhập ở phía máy chủ, thì thẻ tín dụng hoặc thông tin ngân hàng của bạn cũng có thể bị lộ. Ngoài ra, một số hệ thống vận tải muốn bạn đăng ký thẻ trực tuyến để họ có thể gửi cho bạn email, có nghĩa là địa chỉ email của bạn cũng có thể bị lộ trong một cuộc tấn công về sau này. Dù bằng cách nào, khả năng đi xe vận tải công cộng ẩn danh gần như đã phá sản, trừ khi bạn thanh toán bằng tiền mặt thay vì thẻ tín dụng.

Sự phát triển này vô cùng hữu ích cho các cơ quan thực thi pháp luật. Bởi vì các công ty cung cấp thẻ vận tải này là các bên thứ ba thuộc sở hữu tư nhân, chứ không phải chính phủ, nên họ có thể đặt bất kỳ quy tắc nào họ muốn về chia sẻ dữ liệu. Họ có thể chia sẻ dữ liệu không chỉ với cơ quan thực thi pháp luật mà còn với các luật sư theo đuổi các vụ kiện dân sự – trong trường hợp người tình cũ muốn quấy rối bạn.

Vì vậy, khi nhìn vào nhật ký di chuyển, người ta có thể biết chính xác ai đã đi qua một ga tàu điện ngầm vào một thời điểm nào đó – nhưng họ có thể không biết mục tiêu của mình đã lên tuyến tàu nào, đặc biệt nếu nhà ga ấy là trung tâm của một vài tuyến. Điều gì sẽ xảy ra nếu thiết bị di động của bạn có thể giải quyết được câu hỏi về chuyến tàu nào bạn đi và do đó suy ra điểm đến của bạn?

Các nhà nghiên cứu tại Đại học Nam Kinh, Trung Quốc, đã quyết định trả lời câu hỏi trên bằng cách tập trung nghiên cứu gia tốc

kế bên trong điện thoại. Mỗi thiết bị di động đều có một gia tốc kế. Đó là một con chip nhỏ chịu trách nhiệm xác định hướng của thiết bị – để biết bạn đang cầm thiết bị ở chế độ xem ngang hay dọc. Những con chip này rất nhạy cảm nên các nhà nghiên cứu đã quyết định sử dụng dữ liệu gia tốc riêng trong các tính toán của mình. Và quả nhiên, họ có thể dự đoán chính xác tàu điện ngầm mà người dùng đang đi. Điều này là do hầu hết các tuyến tàu điện ngầm đều bao gồm các lượt rẽ ảnh hưởng đến gia tốc kế. Khoảng thời gian giữa các ga dừng cũng quan trọng – bạn chỉ cần xem bản đồ để thấy tại sao. Độ chính xác của các dự đoán của họ được cải thiện với mỗi ga mà một hành khách đã vượt qua. Các nhà nghiên cứu cho rằng phương pháp của họ có tỷ lệ chính xác 92%.

Giả sử bạn sở hữu một chiếc xe kiểu cũ và tự lái xe đi làm. Bạn có thể nghĩ rằng mình đang vô hình, chỉ là một trong số một triệu chiếc xe trên đường ngày hôm nay không? Có thể bạn đúng. Nhưng công nghệ mới – ngay cả khi nó không phải là một phần của chính chiếc xe – đang làm suy yếu khả năng ẩn danh của bạn. Nếu nỗ lực, người ta vẫn có thể xác định được bạn khi bạn đang di chuyển với tốc độ cao trên đường cao tốc.

Tại thành phố San Francisco, Cơ quan Giao thông Đô thị đã bắt đầu sử dụng hệ thống thu phí FasTrak, cho phép bạn đi qua bất kỳ cây cầu nào trong số tám cây cầu ở Vùng Vịnh một cách dễ dàng, để theo dõi chuyển động của những chiếc xe ô tô có bật FasTrak trên toàn thành phố. Sử dụng công nghệ tương tự như những cầu thu phí sử dụng để đọc thiết bị FasTrak (hoặc E-ZPass) trong xe hơi của bạn, thành phố đã bắt đầu tìm kiếm những thiết bị đó khi người dùng vòng quanh tìm chỗ đậu xe. Nhưng các quan chức không phải lúc nào cũng quan tâm đến hoạt động di chuyển của bạn – họ quan tâm đến chỗ đỗ xe, hầu hết trong số đó được trang bị đồng hồ đỗ xe điện tử. Các không gian được tìm kiếm cao có thể bị tính phí cao hơn. Thành phố có thể điều chỉnh giá mà không cần dùng dây mạng ở những mét cụ thể, bao gồm cả những mét gần một sự kiện phổ biến.

Ngoài ra, năm 2014, các quan chức đã quyết định không sử dụng người thu phí ở Cầu Cổng Vàng, vì vậy tất cả mọi người, ngay cả khách du lịch, đều phải trả tiền bằng phương thức điện tử hoặc nhận hóa đơn bằng thư. Làm thế nào để các nhà chức trách biết chỗ để gửi hóa đơn của bạn? Họ chụp ảnh biển số xe của bạn khi bạn đi qua trạm thu phí. Những hình ảnh tấm giấy phép này cũng được sử dụng để bắt những người vượt đèn đỏ tại các giao lộ nhiều vấn đề. Và càng ngày cảnh sát càng sử dụng nhiều chiến lược tương tự khi họ đi qua các bãi đậu xe và đường lái xe dân cư.

Các sở cảnh sát theo dõi thụ động chuyển động của xe bạn mỗi ngày bằng công nghệ nhận dạng biển số tự động (ALPR). Họ có thể chụp ảnh biển số xe của bạn và lưu trữ dữ liệu đó, đôi khi trong nhiều năm, tùy thuộc vào chính sách của sở cảnh sát. Các máy ảnh ALPR quét và đọc tất cả các biển số xe đã đi qua, cho dù chiếc xe có được đăng ký bởi một tội phạm hay không.

Bề ngoài, công nghệ ALPR được sử dụng chủ yếu để xác định vị trí xe ô tô bị đánh cắp, tội phạm truy nã, và hỗ trợ với Cảnh báo AMBER. Công nghệ này liên quan đến ba camera gắn trên nóc xe tuần tra được nối với một màn hình máy tính bên trong xe. Hệ thống này được liên kết với cơ sở dữ liệu của Bộ Tư pháp để theo dõi các biển số xe ô tô bị đánh cắp và các phương tiện liên quan đến tội phạm. Khi một nhà chức trách lái xe, công nghệ ALPR có thể quét lên đến 60 tấm mỗi giây. Nếu một tấm được quét phù hợp với một tấm trong cơ sở dữ liệu của Bộ Tư pháp, nhân viên cảnh sát sẽ nhận được một cảnh báo cả bằng hình ảnh và âm thanh.

Tạp chí Wall Street lần đầu viết về công nghệ nhận dạng biển số vào năm 2012. Vấn đề đối với những người phản đối hoặc nghi ngờ công nghệ ALPR không phải là bản thân hệ thống mà là dữ liệu được lưu giữ trong bao lâu và tại sao một số cơ quan thực thi pháp luật sẽ không phát hành nó, ngay cả cho chủ sở hữu của chiếc xe đang bị theo dõi. Đó là một công cụ đáng lo ngại mà cảnh sát có thể sử dụng để tìm ra nơi bạn đã đến.

Bennett Stein thuộc Dự án Lời nói, Quyền riêng tư và Công nghệ

của ACLU cho biết: “Các đầu đọc biển số cấp phép tự động là một cách tinh vi để theo dõi vị trí của người lái xe và khi dữ liệu được tổng hợp theo thời gian họ có thể vẽ hình ảnh chi tiết về cuộc sống của mọi người.”

Một người dân ở California đã nộp đơn yêu cầu hồ sơ công khai khi bị làm phiền bởi một loạt ảnh (hơn 100 chiếc) chụp biển số xe mà anh được cấp, phần lớn là tại các điểm giao cắt và các địa điểm công cộng khác. Tuy nhiên, một bức ảnh cho thấy anh và con gái ra khỏi xe của gia đình trong khi chiếc xe đã được đậu trong đường lái xe riêng của họ. Xin lưu ý, người này không bị nghi ngờ phạm tội gì. Các tài liệu thu được từ ACLU cho thấy rằng ngay cả văn phòng của tổng cố vấn của FBI cũng đã đặt câu hỏi về việc sử dụng ALPR trong trường hợp không có chính sách nhất quán của chính phủ.

Thật không may, bạn không phải gửi yêu cầu hồ sơ công khai để xem một số dữ liệu ALPR. Theo Tổ chức Biên giới Điện tử, các hình ảnh từ hơn 100 máy ảnh ALPR luôn có sẵn trên mạng cho bất kỳ ai. Tất cả những gì bạn cần là một trình duyệt. Trước khi công bố những phát hiện của mình, tổ chức này đã làm việc với cơ quan thực thi pháp luật để sửa lỗi rò rỉ dữ liệu. Tổ chức Biên giới Điện tử cho biết cấu hình sai này đã được tìm thấy trong hơn 100 trường hợp và kêu gọi các cơ quan thực thi pháp luật trên cả nước gỡ xuống hoặc giới hạn những gì được đăng trên Internet. Nhưng tại thời điểm viết cuốn sách này, vẫn có thể xem được những hình ảnh đó, nếu bạn gõ đúng truy vấn vào một cửa sổ tìm kiếm, để có được quyền truy cập vào hình ảnh biển số xe trong nhiều cộng đồng. Một nhà nghiên cứu đã tìm thấy hơn 64.000 tấm ảnh và các điểm dữ liệu vị trí tương ứng của chúng trong khoảng thời gian một tuần.

Có lẽ bạn không sở hữu xe và chỉ thỉnh thoảng thuê một chiếc để dùng. Tuy nhiên, bạn chắc chắn không phải là vô hình, vì khi làm thủ tục thuê, bạn phải cung cấp thông tin cá nhân và thẻ tín dụng. Hơn nữa, hầu hết các xe cho thuê ngày nay đều có GPS tích hợp. Tôi biết. Tôi phát hiện ra điều đó một cách khó khăn.

Khi bạn đưa xe đi bảo dưỡng và phải thuê xe dùng tạm, bạn thường đồng ý với hãng cho thuê là sẽ không đi xe qua các ranh giới của tiểu bang. Đại lý muốn giữ xe ở bang nơi nó được thuê. Quy tắc này chủ yếu liên quan đến bảo hiểm của họ chứ không phải của bạn.

Điều này đã xảy ra với tôi. Tôi mang xe của tôi vào một đại lý Lexus ở Las Vegas để bảo dưỡng, và họ cho tôi sử dụng một chiếc xe cho thuê. Vì đã khá muộn, tôi đã ký giấy tờ mà không đọc kỹ, chủ yếu là vì tôi đã bị nhân viên dịch vụ thúc giục. Sau đó, tôi lái xe đến Bắc California, đến Vùng Vịnh, vì một hợp đồng tư vấn. Khi nhân viên bảo dưỡng gọi cho tôi để xin ý kiến về việc sửa xe, anh ta hỏi, “Anh đang ở đâu?” Tôi nói, “San Ramon, California.” Anh ta nói, “Vâng, chúng tôi cũng thấy nó ở đấy.” Rồi anh ta đọc cho tôi điều khoản về việc lấy xe ra khỏi tiểu bang. Rõ ràng là thỏa thuận cho thuê tôi đã ký một cách nhanh chóng quy định rằng tôi không được đưa xe ra khỏi Nevada.

Ngày nay, khi thuê hoặc mượn xe, bạn thường muốn kết nối thiết bị không dây của mình với hệ thống giải trí ở xe. Tất nhiên, ở đây nổi lên một số vấn đề đáng lo ngại nhãn tiền về vấn đề riêng tư. Đây không phải là xe của bạn. Vậy điều gì sẽ xảy ra với dữ liệu thông tin giải trí của bạn sau khi bạn trả lại xe?

Trước khi bạn kết nối thiết bị với một chiếc xe không phải của bạn, hãy xem xét hệ thống giải trí. Có thể bằng cách nhấn vào cài đặt điện thoại di động, bạn sẽ thấy các thiết bị và/hoặc tên của người dùng trước đó được liệt kê trên màn hình Bluetooth. Hãy suy nghĩ về việc bạn có muốn tham gia danh sách đó hay không.

Nói cách khác, dữ liệu của bạn không tự biến mất khi bạn rời khỏi xe.

Bạn phải tự xóa nó.

Bạn có thể nghĩ, “Việc chia sẻ giai điệu yêu thích của tôi với những người khác thì có hại gì chứ?” Vấn đề ở đây là âm nhạc không phải là thứ duy nhất của bạn được chia sẻ. Khi hầu hết các thiết bị di động kết nối với hệ thống thông tin giải trí ô tô, chúng

sẽ tự động liên kết danh bạ của bạn với hệ thống của ô tô. Giả định là có thể bạn muốn thực hiện cuộc gọi rảnh tay trong khi lái xe, vì vậy việc liên hệ của bạn được lưu trữ trong xe khiến việc này trở nên dễ dàng hơn nhiều. Rắc rối là, nó không phải là chiếc xe của bạn.

“Khi tôi nhận được một chiếc xe cho thuê,” David Miller, giám đốc an ninh cho Covisint, nói, “điều cuối cùng tôi làm là kết nối điện thoại của tôi. Nó tải xuống tất cả địa chỉ liên hệ của tôi vì đó là những gì nó muốn làm. Trong hầu hết các xe cho thuê, bạn có thể vào, và nếu có ai đó đã kết nối với nó, bạn có thể xem các địa chỉ liên hệ của họ.”

Điều này cũng tương tự như khi bạn bán xe. Những chiếc xe hiện đại cung cấp cho bạn quyền truy cập vào thế giới kỹ thuật số khi đang trên đường. Bạn muốn kiểm tra Twitter? Bạn muốn đăng bài lên Facebook? Ô tô ngày nay ngày càng giống với máy tính cá nhân truyền thống và điện thoại di động: chúng chứa dữ liệu cá nhân mà bạn nên xóa trước khi bán máy hoặc thiết bị đi.

Làm việc trong ngành bảo mật sẽ giúp bạn có thói quen suy nghĩ trước, ngay cả về các giao dịch thông thường. “Tôi dành tất cả khoảng thời gian này kết nối chiếc xe của tôi với toàn bộ cuộc sống của tôi,” Miller nói, “và rồi năm năm sau tôi lại bán nó đi – làm sao tôi ngắt kết nối chiếc xe khỏi toàn bộ cuộc sống của mình được chứ? Tôi không muốn người mua có thể nhìn thấy bạn bè trên Facebook của tôi, vì vậy bạn phải gỡ bỏ quyền truy cập. Các chuyên gia bảo mật quan tâm đến các lỗ hổng bảo mật xung quanh việc gỡ bỏ quyền truy cập hơn việc cấp quyền truy cập.”

Và, cũng giống như việc bạn làm với thiết bị di động, bạn sẽ cần phải bảo vệ xe bằng mật khẩu. Ngoại trừ một điều rằng tại thời điểm viết cuốn sách này, không có cơ chế nào cho phép bạn khóa hệ thống thông tin giải trí bằng mật khẩu cả. Cũng không dễ dàng xóa tất cả các tài khoản bạn đã đưa vào ô tô của mình trong những năm qua – cách bạn thực hiện phụ thuộc từng nhà sản xuất, kiểu dáng và số hiệu xe. Có lẽ điều đó sẽ thay đổi – sẽ có người phát minh ra một nút bấm một lần để xóa toàn bộ hồ sơ

người dùng khỏi ô tô của bạn. Nhưng trong khi chờ đến lúc đó, sau khi bán xe, ít nhất bạn hãy lên mạng và thay đổi tất cả các mật khẩu mạng xã hội của mình.

Có lẽ ví dụ tốt nhất về hình ảnh máy tính có bánh là một chiếc Tesla, một chiếc xe hoàn toàn điện tử tân tiến nhất. Tháng Sáu năm 2015, Tesla đạt đến một mốc quan trọng: Tính tổng thể, các ô tô Tesla trên toàn thế giới đã được lái hơn một tỷ dặm.

Tôi cũng đi xe Tesla. Đó là những chiếc xe tuyệt vời, nhưng với các bảng điều khiển phức tạp và hoạt động giao tiếp di động liên tục, chúng đặt ra các câu hỏi về dữ liệu mà chúng thu thập được.

Khi bạn mua xe Tesla, họ sẽ đưa cho bạn một phiếu đồng thuận. Bạn có quyền kiểm soát việc Tesla ghi lại thông tin về chiếc xe của bạn qua hệ thống thông tin liên lạc không dây. Bạn có quyền bật hoặc tắt tính năng chia sẻ dữ liệu cá nhân với Tesla thông qua màn hình cảm ứng trên bảng điều khiển. Nhiều người chấp nhận lập luận rằng dữ liệu của họ sẽ giúp Tesla tạo ra một chiếc xe tốt hơn trong tương lai.

Theo chính sách bảo mật của Tesla, công ty này có thể thu thập số nhận dạng xe, thông tin tốc độ, số độ dài đường đi, thông tin sử dụng pin, lịch sử sạc pin, thông tin về chức năng hệ thống điện, thông tin phiên bản phần mềm, dữ liệu hệ thống thông tin giải trí và dữ liệu liên quan đến an toàn (bao gồm thông tin liên quan đến hệ thống SRS của xe, hệ thống phanh, an ninh và hệ thống phanh điện tử), cùng với nhiều thông tin khác, để hỗ trợ phân tích hiệu suất của xe. Tesla tuyên bố rằng họ có thể thu thập thông tin đó trực tiếp (ví dụ: trong cuộc hẹn bảo dưỡng) hoặc thông qua truy cập từ xa.

Đó là những gì họ nói trong bản in về chính sách của họ.

Trên thực tế, họ cũng có thể xác định vị trí và trạng thái của ô tô của bạn bất kỳ lúc nào. Đối với các phương tiện truyền thông, Tesla đã thận trọng về những dữ liệu mà hãng này thu thập theo thời gian thực và cách sử dụng dữ liệu. Giống như Uber, Tesla ở vị thế gần như Chúa trời, cho phép họ biết tất cả mọi thứ về mỗi

chiếc xe và vị trí của chiếc xe đó vào bất cứ lúc nào.

Nếu điều đó không cần thiết với bạn, bạn có thể liên hệ với Tesla và chọn không tham gia chương trình viễn thông của hãng. Tuy nhiên, nếu làm như vậy, bạn sẽ bỏ lỡ các bản cập nhật phần mềm tự động, bao gồm các bản sửa lỗi bảo mật và các tính năng mới.

Tất nhiên, cộng đồng an ninh quan tâm đến Tesla, và nhà nghiên cứu bảo mật độc lập Nitesh Dhanjani đã xác định một số vấn đề. Tuy đồng ý với tôi rằng Tesla Model S là một chiếc xe tuyệt vời, song Dhanjani phát hiện ra rằng Tesla sử dụng hệ thống xác thực một yếu tố khá yếu để truy cập vào hệ thống xe từ xa. Trang web và ứng dụng Tesla thiếu khả năng để hạn chế số lần đăng nhập vào tài khoản người dùng, điều đó có nghĩa là kẻ tấn công có thể sử dụng thuật toán vét cạn để bẻ khóa mật khẩu của người dùng. Điều đó có nghĩa là một bên thứ ba có thể (giả sử mật khẩu của bạn bị bẻ khóa) đăng nhập và sử dụng API Tesla để kiểm tra vị trí của chiếc xe của bạn. Người đó cũng có thể đăng nhập từ xa vào ứng dụng Tesla và điều khiển hệ thống của xe, điều hòa không khí, đèn... mặc dù xe đang đứng yên.

Tesla ghi nhận hầu hết các mối quan tâm của Dhanjani tại thời điểm viết cuốn sách này, nhưng tình trạng đó là một ví dụ về việc ngày nay các nhà sản xuất ô tô cần phải làm thêm bao nhiêu việc để bảo mật xe của họ. Chỉ cần cung cấp một ứng dụng để khởi động từ xa và kiểm tra trạng thái của chiếc xe của bạn là chưa đủ. Nó cũng phải được an toàn. Bản cập nhật mới nhất, một tính năng được gọi là Summon, cho phép bạn dùng lời nói để kéo chiếc xe ra khỏi nhà xe hoặc đỗ xe ở một nơi chật hẹp. Trong tương lai, Summon sẽ cho phép chiếc xe đón bạn từ bất kỳ địa điểm nào trên khắp đất nước. Khá giống như trong chương trình truyền hình cũ Knight Rider.

Trong việc bác bỏ một đánh giá tiêu cực trên tờ New York Times, Tesla thừa nhận sức mạnh của dữ liệu họ có trong tay. Phóng viên tờ Times John Broder nói rằng chiếc Tesla Model S của anh đã bị hỏng và khiến anh bị kẹt bên trong. Trong một bài viết trên blog, Tesla đã phản đối và chỉ ra một số điểm mà họ cho rằng họ

nghi ngờ đối với câu chuyện của Broder. Ví dụ, Tesla lưu ý rằng Broder lái xe ở các mức tốc độ khác nhau, 100km/h – 130km/h, với một môi trường nhiệt độ cabin bình quân 220C. Theo Forbes, "máy ghi dữ liệu trong Model S biết cài đặt nhiệt độ trong xe, mức pin trong suốt chuyến đi, tốc độ của xe theo từng phút, và tuyến đường chính xác được chọn – cho tới thực tế là người đánh giá xe đã lái xe vòng tròn trong bãi đậu xe khi pin của xe gần như cạn kiệt."

Khả năng viễn thông là một phần mở rộng hợp lý của các hộp đen bắt buộc trong tất cả các xe được sản xuất để bán tại Mỹ sau năm 2015. Nhưng hộp đen trong xe hơi không hoàn toàn mới mẻ. Chúng có từ những năm 1970, khi túi khí được ra mắt lần đầu tiên. Sau đó, trong các vụ va chạm, người dân đã gặp những thương tích đe dọa tính mạng từ túi khí, và một số người bị chết do sức ép của những chiếc túi va vào cơ thể. Trong một số trường hợp, nếu xe không được trang bị những chiếc túi đó, những người bên trong có thể còn sống sót. Để cải thiện tình trạng trên, các kỹ sư cần dữ liệu về việc sử dụng túi trong những khoảnh khắc trước và sau một vụ tai nạn, được thu thập bởi các mô-đun cảm biến và chẩn đoán của túi khí (SDM). Tuy nhiên, cho đến gần đây các chủ xe không được cho biết rằng các cảm biến trong xe hơi của họ ghi lại dữ liệu về việc lái xe của họ.

Được kích hoạt bởi những thay đổi trọng lực đột ngột, các hộp đen trong xe hơi, giống như các hộp đen trong máy bay, chỉ ghi lại chừng vài giây cuối xung quanh một sự kiện trọng lực, chẳng hạn như gia tốc đột ngột, mô-men xoắn và phanh cứng.

Nhưng rất dễ dàng để hình dung nhiều loại dữ liệu được thu thập trong các hộp đen và truyền theo thời gian thực thông qua các kết nối di động. Hãy tưởng tượng, trong tương lai, dữ liệu được thu thập trong khoảng thời gian ba đến năm ngày có thể được lưu trữ trên xe hoặc trên đám mây. Thay vì cố gắng để mô tả tiếng ồn khi xe của bạn đi 60km/h hoặc nhiều hơn, bạn chỉ cần cung cấp cho cỗ máy của mình quyền truy cập dữ liệu được ghi. Câu hỏi ở đây là ai khác nữa có quyền truy cập vào tất cả dữ liệu

này? Ngay cả Tesla cũng thừa nhận rằng dữ liệu thu thập được có thể được các bên thứ ba sử dụng.

Điều gì sẽ xảy ra nếu bên thứ ba là ngân hàng của bạn? Nếu có thỏa thuận với nhà sản xuất ô tô, họ có thể theo dõi khả năng lái xe của bạn và đánh giá điều kiện của bạn cho các khoản vay tự động trong tương lai cho phù hợp. Hoặc công ty bảo hiểm y tế có thể làm như vậy. Hoặc thậm chí là công ty bảo hiểm xe hơi của bạn. Chính phủ liên bang cần xem xét về những người sở hữu dữ liệu từ chiếc xe của bạn và những quyền bạn có để giữ dữ liệu đó là riêng tư.

Hiện nay bạn không thể làm gì nhiều về điều này, nhưng điều này rất đáng để chú ý trong tương lai.

Ngay cả khi bạn không sở hữu Tesla, nhà sản xuất ô tô cũng có thể cung cấp ứng dụng cho phép bạn mở cửa xe, khởi động động cơ hoặc thậm chí kiểm tra chẩn đoán nhất định trên xe của bạn. Một nhà nghiên cứu đã chỉ ra rằng những tín hiệu này – giữa xe, đám mây và ứng dụng – có thể bị tấn công và được sử dụng để theo dõi một chiếc xe mục tiêu, dễ dàng mở khóa, kích hoạt còi và báo động và thậm chí điều khiển động cơ của nó. Tin tặc có thể làm tất cả mọi thứ ngoại trừ gài số xe và lái nó đi. Điều ấy vẫn đòi hỏi chìa khóa của người lái xe. Mặc dù vậy, gần đây tôi đã tìm ra cách tắt khóa fob Tesla để Tesla hoàn toàn nằm bẹp. Bằng cách sử dụng một máy phát nhỏ ở 315 MHz bạn có thể tắt khóa fob để không thể được nhận dạng các khóa bỏ túi, do đó vô hiệu hóa chiếc xe.

Phát biểu tại DEF CON 23, Samy Kamkar, nhà nghiên cứu bảo mật nổi tiếng với việc phát triển sâu Samy trên mạng xã hội Myspace từ thời năm 2005, đã chứng minh rằng một thiết bị mà anh xây dựng được gọi là OwnStar, có thể mạo danh một hệ thống mạng xe đã biết. Ví dụ, với nó, anh có thể mở chiếc xe General Motors được kích hoạt OnStar. Bí quyết nằm ở chỗ đặt thiết bị lên hãm xung hoặc dưới gầm của một chiếc xe hơi hoặc xe tải mục tiêu. Thiết bị này giả mạo điểm truy cập không dây của ô tô, thứ tự động liên kết thiết bị di động không nghi ngờ của người

lái với điểm truy cập mới (giả sử trình điều khiển trước đây được liên kết với điểm truy cập ban đầu). Bất cứ khi nào người dùng khởi chạy ứng dụng trên thiết bị di động OnStar, trên iOS hoặc Android, mã OwnStar khai thác lỗ hổng trong ứng dụng để lấy cắp thông tin đăng nhập OnStar của trình điều khiển. “Ngay sau khi bạn đang ở trên mạng của tôi và bạn mở ứng dụng, tôi đã tiếp quản trình điều khiển đó,” Kamkar nói.

Sau khi có được thông tin đăng nhập của người dùng trên RemoteLink, phần mềm hỗ trợ OnStar và nghe âm thanh khóa hoặc mở khóa (bíp), kẻ tấn công có thể theo dõi một chiếc xe trong một bãi đậu xe đông đúc, mở cửa và ăn cắp bất cứ thứ gì có giá trị bên trong. Sau đó, những kẻ tấn công sẽ gỡ các thiết bị khỏi hãm xung. Đó là một cuộc tấn công rất gọn gàng, vì không có dấu hiệu của sự xâm nhập cưỡng ép, bỏ mặc chủ sở hữu và công ty bảo hiểm giải quyết những gì đã xảy ra.

Các nhà nghiên cứu đã phát hiện ra rằng các tiêu chuẩn kết nối xe được thiết kế để cải thiện lưu lượng giao thông cũng có thể bị theo dõi. Thông tin liên lạc từ phương tiện-đến-phương tiện (vehicle-to-vehicle, viết tắt là V2V) và từ phương tiện-đến-cơ sở hạ tầng (vehicle-to-infrastructure, viết tắt làV2I), được gọi chung là V2X, kêu gọi xe phát sóng tin nhắn 10 lần một giây, sử dụng một phần phủ sóng Wi-Fi ở mức 5.9 gigahertz được gọi là 802.11p.

Thật không may, dữ liệu này được gửi không được mã hóa – nó cần phải như thế. Khi xe đang chạy tốc độ cao trên xa lộ, một phần nghìn giây trễ cần thiết để giải mã tín hiệu có thể dẫn đến một vụ tai nạn nguy hiểm, do đó, các nhà thiết kế đã lựa chọn các liên lạc mở, không được mã hóa. Biết được điều này, họ nhấn mạnh rằng các thông tin liên lạc không chứa thông tin cá nhân, thậm chí không có số giấy phép biển xe. Tuy nhiên, để ngăn chặn giả mạo, các tin nhắn được ký điện tử. Đó là những chữ ký số giống như IMEI (số sê-ri điện thoại di động) được gửi từ điện thoại di động của chúng ta, có thể truy dấu ngược lại tới chủ sở hữu đã đăng ký của chiếc xe.

Jonathan Petit, một trong những nhà nghiên cứu trong nhóm trên, nói với Wired, “Chiếc xe đang nói ‘Tôi là Alice, đây là vị trí của tôi, đây là tốc độ và hướng đi của tôi.” Mọi người xung quanh bạn đều có thể nghe điều đó… Họ có thể nói, ‘Có Alice, cô ấy nói đang ở nhà, nhưng cô ấy lái xe đến cửa hàng thuốc, đi đến một phòng khám sản,’… Ai đó có thể phỏng đoán rất nhiều thông tin cá nhân về hành khách.”

Petit đã thiết kế một hệ thống với giá khoảng 1.000 đô-la có thể lắng nghe thông tin liên lạc V2X và anh cho biết một thị trấn nhỏ có thể chi ra 1 triệu đô-la để gắn các cảm biến này. Thay vì có một lực lượng cảnh sát lớn, thị trấn sẽ sử dụng các cảm biến để xác định các lái xe và, quan trọng hơn, thói quen của họ.

Một đề xuất từ Cơ quan Quản lý An toàn Giao thông Quốc gia và các chính quyền châu Âu là đặt tín hiệu 802.11p – “bút danh” của chiếc xe – thay đổi sau mỗi năm phút. Tuy nhiên, điều đó sẽ không ngăn được một kẻ tấn công chuyên nghiệp – hắn ta sẽ chỉ cài đặt thêm các cảm biến bên đường để xác định chiếc xe trước và sau khi nó thay đổi. Nói tóm lại, dường như có rất ít lựa chọn để tránh nhận dạng xe.

“Thay đổi bút danh không ngăn được theo dõi. Nó chỉ có thể giảm thiểu đòn tấn công này,” Petit nói. “Nhưng nó vẫn cần thiết để cải thiện sự riêng tư… Chúng tôi muốn chứng minh rằng trong bất kỳ cuộc triển khai nào, bạn vẫn phải có sự bảo vệ này, nếu không bạn sẽ bị theo dõi.”

Kết nối xe hơi với Internet thực sự tốt cho chủ sở hữu xe: nhà sản xuất có thể đẩy ra các bản sửa lỗi phần mềm ngay lập tức nếu chúng cần thiết. Tại thời điểm viết cuốn sách này, Volkswagen, Land Rover, và Chrysler đã trải nghiệm qua những lỗ hổng phần mềm nổi tiếng. Tuy nhiên, chỉ có một vài nhà sản xuất ô tô, chẳng hạn như Mercedes, Tesla và Ford, gửi các bản cập nhật từ xa cho tất cả các xe ô tô của họ. Phần còn lại của chúng ta vẫn phải đi vào cửa hàng để cập nhật phần mềm cho xe của mình.

Nếu bạn nghĩ cách mà Tesla và Uber đang theo dõi mọi chuyến đi

bạn thực hiện là đáng sợ, thì những chiếc xe tự lái sẽ còn đáng sợ hơn nữa. Giống như các thiết bị giám sát cá nhân mà chúng ta giữ trong túi của mình – những chiếc điện thoại – những chiếc xe tự lái của chúng ta sẽ cần phải theo dõi nơi chúng ta muốn đến và thậm chí có thể biết chúng ta đang ở đâu tại một thời điểm nhất định để luôn sẵn sàng. Kịch bản do Google và những đơn vị khác đề xuất là các thành phố sẽ không còn cần bãi đậu xe hoặc nhà để xe nữa – xe của bạn sẽ chạy xung quanh cho đến khi cần đến nó. Hoặc có lẽ các thành phố sẽ theo mô hình theo yêu cầu, trong đó quyền sở hữu tư nhân là một điều của quá khứ và mọi người chia sẻ bất kỳ chiếc xe nào ở gần đó.

Nếu như điện thoại di động giống với máy tính truyền thống hơn là giống điện thoại dây đồng, thì tương tự, những chiếc xe tự lái cũng sẽ là một dạng máy tính mới. Chúng sẽ là các thiết bị tính toán độc lập, có thể đưa ra quyết định tự trị từng giây trong khi lái xe trong trường hợp chúng bị cắt khỏi liên lạc mạng của chúng. Sử dụng kết nối di động, chúng sẽ có thể truy cập vào nhiều dịch vụ đám mây, cho phép chúng nhận thông tin giao thông theo thời gian thực, cập nhật xây sửa đường và thông tin thời tiết.

Các bản cập nhật này hiện có sẵn trên một số loại xe thông thường. Nhưng người ta dự đoán rằng đến năm 2025, phần lớn những chiếc xe trên đường sẽ được kết nối với những chiếc xe khác, đến các dịch vụ hỗ trợ dọc đường – và có khả năng là một tỷ lệ đáng kể trong số này sẽ tự lái. Hãy tưởng tượng một lỗi phần mềm trong một xe tự lái sẽ như thế nào.

Trong khi đó, mỗi chuyến đi của bạn sẽ được ghi lại ở đâu đó. Bạn sẽ cần một ứng dụng, giống như ứng dụng Uber, thứ này sẽ được đăng ký với bạn và thiết bị di động của bạn. Ứng dụng đó sẽ ghi lại các chuyến đi của bạn và có lẽ là các chi phí liên quan đến chuyến đi của bạn nếu chúng được tính vào thẻ tín dụng trong hồ sơ, thông tin này có thể bị thu hồi, nếu không phải từ Uber thì từ công ty phát hành thẻ tín dụng của bạn. Và rõ rằng một công ty tư nhân có nhiều khả năng sẽ tham gia thiết kế phần mềm

chạy những chiếc xe tự lái này, bạn sẽ phải lo lắng về những công ty đó và quyết định của họ về việc chia sẻ bất kỳ hoặc tất cả thông tin cá nhân của bạn với các cơ quan thực thi pháp luật.

Chào mừng bạn đến với tương lai.

Tôi hy vọng rằng vào thời điểm bạn đọc những điều này sẽ có những quy định nghiêm ngặt hơn hoặc ít nhất là gợi ý các quy định nghiêm ngặt hơn trong tương lai gần – liên quan đến việc sản xuất xe ô tô kết nối và giao thức truyền thông của chúng. Thay vì sử dụng các biện pháp bảo mật phần mềm và phần cứng được chấp nhận rộng rãi đã thành tiêu chuẩn ngày nay, ngành công nghiệp ô tô, giống như ngành công nghiệp thiết bị y tế và những ngành khác, đang cố gắng phát minh lại phương tiện vận tải như thể chúng ta chưa học được nhiều về an ninh mạng trong suốt 40 năm qua. Chúng ta đã học, và sẽ là tốt nhất nếu các ngành này bắt đầu theo các phương pháp hay nhất hiện có thay vì nhấn mạnh rằng những gì họ đang làm hoàn toàn khác với những gì đã được thực hiện trước đây. Không phải vậy. Thật không may, thất bại trong việc bảo mật mã trong xe hơi có hậu quả lớn hơn nhiều so với một vụ treo phần mềm đơn thuần, với màn hình xanh chết chóc. Trong xe hơi, thất bại đó có thể gây hại hoặc giết chết một con người. Tại thời điểm viết cuốn sách này, ít nhất một người đã chết trong khi một chiếc Tesla đang ở chế độ chạy tự động thử nghiệm phiên bản beta, mà kết quả là do phanh bị lỗi hay lỗi do phần mềm của xe phán đoán sai vẫn chưa được tìm ra.

Đọc điều này, bạn có thể không muốn ra khỏi nhà nữa. Trong chương tiếp theo, tôi sẽ bàn về việc các tiện ích trong nhà lắng nghe và ghi lại những gì chúng ta làm sau cánh cửa đóng kín. Trong trường hợp này, chính phủ không phải là điều chúng ta cần phải sợ.

Chương 12: INTERNET CỦA GIÁM SÁT

Vài năm trước đây, không ai quan tâm đến bộ điều nhiệt trong nhà. Đó là loại điều nhiệt đơn giản hoạt động thủ công, giúp duy trì nhiệt độ thoải mái cho ngôi nhà. Sau đó, nó được lập trình. Rồi một công ty tên là Nest quyết định rằng bạn nên có khả năng kiểm soát nó bằng một ứng dụng dựa trên nền tảng Internet. Bạn có thể cảm nhận được điều tôi sẽ nhắc đến, đúng không?

Trong một bài đánh giá sản phẩm với giọng đầy thù hằn về bộ điều nhiệt Wi-Fi Smart Touchscreen của Honeywell, một người tự gọi mình là General (Tướng) viết trên Amazon rằng người vợ cũ đã lấy ngôi nhà, con chó, và khoản tiền tiết kiệm khi về hưu, nhưng anh ta đã giữ lại được mật khẩu bộ điều nhiệt Honeywell. General nói khi người vợ cũ cùng bạn trai ra khỏi thị trấn, anh ta sẽ tăng nhiệt độ trong nhà lên, sau đó đưa trở về nhiệt độ bình thường trước khi họ quay lại. “Chỉ riêng việc nghĩ đến hóa đơn tiền điện của họ cũng khiến tôi mỉm cười.”

Các nhà nghiên cứu tại Hội nghị Bảo mật Black Hat tại Mỹ năm 2014 đã tiết lộ một số sơ hở trong phần mềm của bộ điều nhiệt Nest. Điều quan trọng cần lưu ý là nhiều sơ hở trong số này yêu cầu quyền truy cập vật lý vào thiết bị, nghĩa là có người sẽ phải vào trong nhà của bạn và cài đặt cổng USB trên bộ điều nhiệt. Daniel Buentello, một nhà nghiên cứu bảo mật độc lập, một trong bốn diễn giả đã nói về việc xâm nhập thiết bị này, nói: “Đây là một máy tính mà người dùng không thể cài phần mềm chống virus. Tệ hơn nữa, có một cánh cửa hậu bí mật mà kẻ xấu có thể sử dụng và ở đó mãi mãi. Nó cứ như là một con ruồi đậu trên tường vậy.”

Nhóm nghiên cứu trên công chiếu một video quay cảnh họ thay đổi giao diện bộ điều nhiệt Nest (họ làm cho nó trông giống như ống kính máy ảnh lặn HAL 9000) và tải lên nhiều tính năng mới khác. Điều thú vị là, họ không thể tắt tính năng báo cáo tự động

trong thiết bị, vì vậy họ đành tự tạo công cụ riêng để làm điều đó. Công cụ này sẽ cắt luồng dữ liệu chảy ngược trở lại Google, công ty mẹ của Nest.

Nhận xét về bài thuyết trình trên, Zoz Cuccias của Nest sau đó đã nói với VentureBeat: "Tất cả các thiết bị phần cứng – từ máy tính xách tay đến điện thoại thông minh – đều dễ bị bẻ khóa; đây không phải là vấn đề của riêng ai. Đây là một cách bẻ khóa vật lý yêu cầu truy cập vật lý vào Nest Learning Thermostat. Nếu có người vào được trong nhà của bạn và được tự do, rất có thể họ sẽ cài đặt thiết bị riêng, hoặc lấy đồ trang sức. Việc bẻ khóa này không ảnh hưởng đến an ninh của máy chủ hoặc các kết nối với máy chủ, và theo những gì chúng tôi biết, chưa có thiết bị nào được truy cập và xâm nhập từ xa. Bảo mật khách hàng là rất quan trọng đối với chúng tôi và ưu tiên cao nhất của chúng tôi là lỗ hổng từ xa. Một trong những biện pháp phòng thủ tốt nhất của bạn là mua Dropcam Pro để có thể giám sát nhà của mình khi vắng nhà."

Với sự ra đời của Internet Vạn Vật, các công ty như Google đang háo hức chiếm lĩnh từng khía cạnh trong đó để sở hữu các nền tảng mà các sản phẩm khác sẽ sử dụng. Nói cách khác, các công ty này muốn thiết bị do các công ty khác phát triển phải kết nối với dịch vụ của họ chứ không phải với dịch vụ của công ty khác. Google sở hữu cả Dropcam và Nest, nhưng họ muốn các thiết bị Internet Vạn Vật khác, chẳng hạn như bóng đèn thông minh và các thiết bị giám sát trẻ, kết nối với tài khoản Google của người dùng. Ưu điểm của điều này, ít nhất là với Google, là họ thu thập được nhiều dữ liệu thô hơn về thói quen cá nhân của bạn (và điều này áp dụng cho bất kỳ công ty lớn nào – Apple, Samsung, thậm chí cả Honeywell).

Khi nói về Internet Vạn Vật, chuyên gia bảo mật máy tính Bruce Schneier kết luận trong một cuộc phỏng vấn rằng: "Điều này rất giống với lĩnh vực máy tính trong những năm 1990. Không ai chú ý đến an ninh, không ai cập nhật, không ai biết bất cứ điều gì – tất cả đều thực sự, thực sự rất tệ và nó sẽ đổ sụp. Sẽ có những lỗ

hổng, chúng sẽ bị kẻ xấu khai thác, và không có cách nào để vá chúng."

Để chứng minh điều đó, mùa hè năm 2013, nhà báo Kashmir Hill đã tiến hành điều tra và tự thực hiện xâm nhập máy tính. Bằng cách sử dụng tìm kiếm của Google, cô tìm thấy một cụm từ đơn giản cho phép cô điều khiển một số thiết bị trung tâm (hub) Insteon cho nhà riêng. Hub là thiết bị trung tâm cung cấp quyền truy cập trực tiếp vào một ứng dụng di động hoặc Internet. Thông qua ứng dụng này, mọi người có thể kiểm soát ánh sáng trong phòng khách, khóa cửa ra vào, hoặc điều chỉnh nhiệt độ trong nhà. Thông qua Internet, chủ sở hữu có thể điều chỉnh những yếu tố này trong khi vắng nhà.

Như Hill đã chỉ ra, kẻ tấn công cũng có thể sử dụng Internet để liên lạc từ xa với hub. Để lấy bằng chứng, cô liên lạc với Thomas Hatley, một người lạ hoàn toàn, sống ở Oregon, và xin phép lấy nhà của anh để thử nghiệm.

Từ nhà cô ở San Francisco, Hill có thể bật và tắt đèn trong nhà Hatley cách đó 1.000km về phía bờ biển Thái Bình Dương. Cô cũng có thể điều khiển bồn tắm nước nóng, quạt, tivi, máy bơm nước, cửa garage, và máy quay video giám sát – nếu anh kết nối các thiết bị đó.

Vấn đề (hiện đã được khắc phục) là Insteon đã đưa tất cả các thông tin của Hatley lên Google. Tệ hơn, quyền truy cập thông tin này không được bảo vệ bằng mật khẩu vào thời điểm đó – bất kỳ ai gặp được thông tin này đều có thể kiểm soát bất kỳ hub Insteon nào tìm được trên mạng. Bộ định tuyến của Hatley có mật khẩu, nhưng có thể tránh dùng đến mật khẩu bằng cách tìm kiếm cổng được Insteon sử dụng – và Hill đã làm như vậy.

"Nhà của Thomas Hatley là một trong số tám nhà mà tôi đã truy cập được," Hill viết. "Thông tin nhạy cảm đã được tiết lộ – không chỉ những ứng dụng và thiết bị mà mọi người có, mà còn cả múi giờ (cùng với đó là thành phố lớn gần nhất với nhà của họ), địa chỉ IP và thậm chí cả tên của một đứa trẻ; rõ ràng, các bậc cha mẹ

muốn có thể cắm điện cho ti-vi từ xa. Trong ít nhất ba trường hợp, có đủ thông tin để tìm ra vị trí thực của các ngôi nhà trên Internet. Tên của hầu hết các hệ thống là chung chung, nhưng với một trong những trường hợp đó, dữ liệu bao gồm cả địa chỉ đường phố, giúp tôi có thể lần ra địa chỉ một ngôi nhà ở Connecticut."

Cùng lúc đó, Nitesh Dhanjani, một nhà nghiên cứu bảo mật, cũng phát hiện một vấn đề tương tự. Dhanjani tập trung nghiên cứu hệ thống chiếu sáng Philips Hue, cho phép chủ sở hữu điều chỉnh màu sắc và độ sáng của bóng đèn từ thiết bị di động. Bóng đèn có phổ màu gồm 16 triệu màu.

Dhanjani thấy rằng chỉ cần chèn một tập lệnh đơn giản vào một máy tính ở nhà trên mạng của gia đình là đủ để gây ra một cuộc tấn công từ chối dịch vụ – DDoS – trên hệ thống chiếu sáng. Nói cách khác, anh có thể khiến bóng đèn Hue ở bất kỳ phòng nào tắt đi theo ý muốn. Nội dung tập lệnh anh viết là một mã đơn giản để khi người dùng khởi động lại bóng đèn, nó sẽ nhanh chóng tắt đi và sẽ tiếp tục tắt khi mã chương trình còn hoạt động.

Dhanjani nói rằng điều này có thể gây ra rắc rối nghiêm trọng cho một tòa nhà văn phòng hoặc chung cư. Mã chương trình sẽ làm cho tất cả các đèn không hoạt động được, và những người bị ảnh hưởng sẽ gọi cho sở điện địa phương chỉ để phát hiện ra rằng khu vực của họ không bị cúp điện.

Trong khi các thiết bị gia dụng tự động hóa có thể truy cập Internet có thể là mục tiêu trực tiếp của các cuộc tấn công DDoS, nhưng đồng thời chúng cũng có thể bị xâm nhập và tham gia vào một botnet – một đội quân các thiết bị bị nhiễm độc phụ thuộc vào một bộ điều khiển có thể được sử dụng để khởi động các cuộc tấn công DDoS chống lại các hệ thống khác trên Internet. Tháng 10 năm 2016, một công ty tên là Dyn, chuyên xử lý các dịch vụ cơ sở hạ tầng DNS cho các thương hiệu Internet lớn như Twitter, Reddit và Spotify, đã phải hứng chịu một cuộc tấn công nặng nề kiểu này. Hàng triệu người dùng ở miền đông của Mỹ không thể truy cập nhiều website lớn vì trình duyệt của họ không thể tiếp

cận các dịch vụ DNS của Dyn.

Thủ phạm là một phần mềm độc hại gọi là Mirai, một chương trình độc hại sục sạo trên Internet để tìm kiếm các thiết bị Internet Vạn Vật không an toàn, như camera CCTV, bộ định tuyến, DVR, và thiết bị giám sát trẻ, để chiếm đoạt điều khiển và tận dụng cho các cuộc tấn công trong tương lai. Mirai cố gắng chiếm quyền kiểm soát thiết bị bằng cách đoán mật khẩu đơn giản. Nếu cuộc tấn công thành công, thiết bị sẽ được kết nối với một botnet trực sẵn ở đó. Giờ đây, với một dòng lệnh đơn giản, kẻ điều hành mạng botnet có thể chỉ dẫn mọi thiết bị – trong số đó có hàng trăm nghìn hoặc hàng triệu thiết bị – gửi dữ liệu đến một trang đích và đưa thông tin dồn dập vào để đánh sập trang đó.

Tuy không thể ngăn chặn hacker thực hiện các cuộc tấn công DDoS, bạn có thể trở thành vô hình trước các botnet của chúng. Mục đầu tiên khi triển khai thiết bị Internet Vạn Vật là thay đổi mật khẩu thành một thứ khó đoán. Nếu bạn đã triển khai một thiết bị, việc khởi động lại nó sẽ loại bỏ bất kỳ mã độc hại hiện có nào.

Các tập lệnh máy tính có thể ảnh hưởng đến các hệ thống nhà thông minh khác.

Nếu gia đình bạn có trẻ sơ sinh, bạn có thể sử dụng thiết bị giám sát trẻ. Thiết bị này, có thể là micro hoặc camera hoặc kết hợp cả hai, cho phép cha mẹ ra khỏi phòng nhưng vẫn theo dõi được trẻ. Thật không may, những thiết bị này cũng có thể mời gọi người khác theo dõi trẻ.

Thiết bị giám sát trẻ bằng kỹ thuật tương tự (analog) sử dụng tần số không dây trong dải tần 43-50 MHz. Những tần số này lần đầu tiên được sử dụng cho điện thoại không dây trong những năm 1990, và bất kỳ ai có máy quét vô tuyến giá rẻ đều có thể dễ dàng chặn các cuộc gọi không dây mà đối tượng không hay biết.

Thậm chí ngày nay, hacker có thể sử dụng một máy phân tích phổ để phát hiện tần số mà một thiết bị giám sát trẻ analog sử dụng, sau đó dùng các phương án phân giải mô hình hóa khác

nhau để chuyển đổi tín hiệu điện thành âm thanh. Cũng có thể dùng một máy quét cảnh sát mua ở một cửa hàng điện tử. Đã có rất nhiều vụ án pháp lý trong đó những người hàng xóm sử dụng thiết bị giám sát trẻ của cùng một thương hiệu, đặt cho cùng một kênh để nghe lén lẫn nhau. Năm 2009, Wes Denkov ở Chicago đã kiện các nhà sản xuất thiết bị giám sát trẻ Summer Infant Day & Night, tuyên bố rằng hàng xóm của anh có thể nghe những cuộc trò chuyện riêng được thực hiện tại nhà anh.

Để khắc phục tình trạng trên, bạn có thể sử dụng thiết bị giám sát trẻ bằng phương pháp kỹ thuật số. Những loại này vẫn dễ bị nghe trộm, nhưng chúng có an ninh tốt hơn và nhiều tùy chọn cấu hình hơn. Ví dụ, bạn có thể cập nhật phần mềm của thiết bị giám sát (phần mềm trên chip) ngay sau khi mua. Ngoài ra, hãy nhớ thay đổi tên người dùng và mật khẩu mặc định.

Ở đây, một lần nữa, thiết kế của thiết bị có thể nằm ngoài tầm kiểm soát của bạn. Nitesh Dhanjani phát hiện ra rằng thiết bị giám sát trẻ không dây Belkin WeMo sử dụng mã thông báo token trong một ứng dụng mà sau khi được cài đặt trên thiết bị di động và được sử dụng trên mạng gia đình, sẽ duy trì trạng thái hoạt động – từ bất cứ nơi đâu trên thế giới. Giả sử bạn đồng ý trông đứa cháu gái mới sinh và anh trai bạn nhờ bạn tải ứng dụng Belkin về điện thoại của bạn thông qua mạng gia đình nội bộ của anh ấy (với may mắn nào đó, mạng này được bảo vệ bằng mật khẩu WPA2). Giờ đây, bạn có quyền truy cập vào thiết bị giám sát trẻ của người anh trai từ khắp nơi trên đất nước, từ khắp nơi trên thế giới.

Dhanjani lưu ý rằng lỗ hổng thiết kế này xuất hiện trong nhiều thiết bị Internet Vạn Vật được kết nối với nhau. Về cơ bản, các thiết bị này giả định rằng mọi thứ trên mạng cục bộ đều đáng tin cậy. Nếu trong nhà của tất cả chúng ta đều có 20 hoặc 30 thiết bị như vậy, mô hình bảo mật sẽ phải thay đổi. Vì mọi thứ trên mạng lưới đều đáng tin cậy, khi đó một lỗ hổng trong bất kỳ thiết bị nào – thiết bị giám sát trẻ, bóng đèn, bộ điều nhiệt – có thể cho phép kẻ tấn công từ xa truy cập vào mạng gia đình thông minh của

bạn và cho hắn cơ hội tìm hiểu thêm về thói quen cá nhân của bạn.

Trước khi các ứng dụng di động ra đời, chúng ta có thiết bị điều khiển từ xa cầm tay. Hầu hết chúng ta khi đó đều còn quá trẻ để có thể nhớ về những ngày trước khi tivi có điều khiển từ xa – thời mà mọi người phải đứng dậy khỏi ghế và vặn núm để thay đổi kênh, hoặc để tăng âm lượng. Ngày nay, chúng ta có thể nằm trên ghế sofa và điều khiển tivi bằng giọng nói. Điều đó có thể rất thuận tiện, nhưng nó cũng có nghĩa là tivi đang lắng nghe, dù chỉ là lệnh để nó tự bật lên.

Trong những ngày đầu, điều khiển từ xa ti-vi đòi hỏi phải có đường ngắm trực tiếp và được vận hành bằng cách sử dụng loại ánh sáng đặc biệt, cụ thể là công nghệ hồng ngoại. Một điều khiển từ xa chạy bằng pin sẽ phát ra một chuỗi ánh sáng nhấp nháy hầu như không nhìn thấy được bằng mắt thường nhưng có thể nhìn thấy (xin nhắc lại là trong tầm mắt) bằng một cảm biến trên ti-vi. Chiếc ti-vi làm gì để biết bạn muốn bật nó lên? Đơn giản: cảm biến hồng ngoại nằm trong ti-vi luôn bật, ở chế độ nghỉ, chờ một chuỗi xung ánh sáng hồng ngoại đặc biệt từ điều khiển từ xa cầm tay để đánh thức nó.

Ti-vi điều khiển từ xa phát triển qua nhiều năm để tích hợp tín hiệu không dây, điều đó có nghĩa là bạn không phải đứng ngay trước ti-vi; bạn có thể đi sang một bên, đôi khi là đi sang một căn phòng khác. Lại một lần nữa, ti-vi luôn ở chế độ chờ tín hiệu thích hợp để đánh thức nó.

Chuyển tới thời của những chiếc ti-vi được kích hoạt bằng giọng nói. Chúng loại bỏ chiếc điều khiển từ xa. Thay vào đó, bạn chỉ cần nói một câu ngớ ngẩn như “Ti-vi bật” hoặc “Chào ti-vi” là nó tự động bật lên.

Mùa xuân năm 2015, các nhà nghiên cứu bảo mật Ken Munro và David Lodge muốn xem liệu ti-vi Samsung kích hoạt bằng giọng nói có lắng nghe các cuộc hội thoại trong phòng ngay cả khi không hoạt động hay không. Trong khi họ thấy rằng ti-vi kỹ

thuật số thực sự nghỉ khi chúng được tắt – điều này khiến chúng ta yên tâm – thì những chiếc ti-vi thế hệ mới này ghi lại mọi điều được nói ra sau khi bạn cấp cho chúng một lệnh đơn giản, chẳng hạn như "Chào ti-vi" (nghĩa là chúng ghi lại mọi thứ cho đến khi nhận được lệnh tắt một lần nữa). Có bao nhiêu người trong chúng ta sẽ nhớ giữ im lặng hoàn toàn trong khi tivi đang bật?

Chúng ta sẽ không nhớ điều đó, và để làm cho vấn đề còn trở nên đáng lo ngại hơn, những gì chúng ta nói (và những gì được ghi lại) sau lệnh "Chào ti-vi" không được mã hóa. Nếu truy cập được vào mạng gia đình của bạn, tôi có thể nghe lén bất kỳ cuộc trò chuyện nào bạn đang thực hiện trong nhà trong khi tivi được bật. Lập luận bảo vệ cho việc giữ tivi ở chế độ nghe là nó cần phải nghe các lệnh khác từ bạn, chẳng hạn như "Tăng âm lượng," "Thay đổi kênh" và "Tắt âm thanh." Điều đó có thể là tốt, ngoại trừ việc các lệnh thoại thu được sẽ được chuyển tới vệ tinh trước khi chúng quay trở lại. Và bởi vì toàn bộ chuỗi dữ liệu không được mã hóa, tôi có thể thực hiện một cuộc tấn công MITM trên ti-vi của bạn, chèn các lệnh của riêng tôi để thay đổi kênh của bạn, tăng âm lượng, hoặc đơn giản là tắt ti-vi bất cứ khi nào tôi muốn.

Hãy suy nghĩ một lát. Điều đó có nghĩa là nếu bạn đang ở trong phòng có ti-vi được kích hoạt bằng giọng nói, đang trò chuyện với ai đó và bạn quyết định bật ti-vi, sau đó nội dung cuộc trò chuyện có thể được chiếc ti-vi ghi lại. Hơn nữa, cuộc trò chuyện về đợt bán bánh nướng sắp tới tại trường tiểu học có thể được truyền đến một máy chủ ở đâu đó cách xa phòng khách của bạn. Trong thực tế, Samsung không chỉ truyền dữ liệu đó cho bản thân hãng này mà còn cho Nuance, một công ty phần mềm nhận dạng giọng nói. Đó là hai công ty có thông tin quan trọng về việc bán bánh nướng sắp tới.

Và chúng ta hãy cùng trung thực thừa nhận một thực tế rằng những cuộc nói chuyện trong phòng xem ti-vi có thể không liên quan đến việc bán bánh nướng. Có thể bạn đang nói về điều gì đó bất hợp pháp mà cơ quan thực thi pháp luật có thể muốn biết. Hoàn toàn có khả năng là các công ty này sẽ thông báo cho cơ

quan thực thi pháp luật, nhưng nếu chẳng hạn cơ quan thực thi pháp luật đã quan tâm đến bạn từ trước, thì các nhà chức trách có thể ra lệnh bắt buộc các công ty này cung cấp các bản gỡ băng hoàn chỉnh. “Xin lỗi, nhưng chính chiếc tivi thông minh của bạn đã tiết lộ bí mật của bạn…”

Để bảo vệ mình, Samsung tuyên bố rằng các tình huống nghe trộm như vậy đã được đề cập trong thỏa thuận riêng tư mà tất cả người dùng hoàn toàn đồng ý khi họ bật ti-vi. Nhưng lần cuối cùng bạn đọc thỏa thuận về quyền riêng tư trước khi bật một thiết bị lần đầu tiên là khi nào? Samsung cho biết trong tương lai gần, tất cả các thông tin liên lạc ti-vi của hãng này sẽ được mã hóa. Nhưng đến năm 2015, hầu hết các mẫu trên thị trường đều không được bảo vệ.

May mắn thay, có nhiều cách để vô hiệu hóa tính năng giống dòng HAL 9000 này trên chiếc Samsung và có lẽ là trên cả ti-vi của các nhà sản xuất khác. Với Samsung PN60F8500 và các sản phẩm tương tự, đi vào menu Settings (Cài đặt), chọn “Smart Features” (Tính năng thông minh), sau đó trong “Voice Recognition” (Nhận dạng giọng nói), chọn “Off” (Tắt). Nhưng nếu muốn ngăn ti-vi ghi lại các cuộc hội thoại nhạy cảm trong nhà, bạn sẽ phải từ bỏ việc ra lệnh cho nó bằng giọng nói. Với điều khiển từ xa, bạn vẫn có thể chọn nút micro và ra lệnh. Hoặc bạn có thể đứng dậy khỏi ghế và tự mình chuyển kênh. Tôi biết. Cuộc sống thật khó khăn.

Các luồng dữ liệu không được mã hóa không phải là độc quyền của riêng Samsung. Trong khi thử nghiệm ti-vi thông minh LG, một nhà nghiên cứu nhận thấy dữ liệu đang được gửi trở lại LG qua Internet mỗi khi người xem thay đổi kênh. Tivi cũng có tùy chọn cài đặt gọi là “Collection of watching info” (Bộ sưu tập thông tin đang xem), được bật theo mặc định. “Thông tin xem” bao gồm tên của các tệp được lưu trữ trên bất kỳ ổ đĩa USB nào mà bạn kết nối với chiếc tivi LG, giả dụ, một ổ có chứa ảnh chụp kỳ nghỉ gia đình của bạn. Các nhà nghiên cứu đã thực hiện một thí nghiệm khác, trong đó họ tạo ra một tệp video giả và tải nó

vào một ổ USB, sau đó cắm nó vào tivi. Khi phân tích lưu lượng mạng, họ thấy rằng tên tệp video được truyền đi không được mã hóa trong luồng http và được gửi đến địa chỉ GB.smartshare.lgtvsdp.com.

Sensory, một công ty cung cấp giải pháp nhận dạng giọng nói nhúng cho các sản phẩm thông minh, nghĩ rằng họ có thể làm nhiều hơn nữa. “Chúng tôi nghĩ rằng sự kỳ diệu bên trong [chiếc ti-vi thông minh] là hãy để nó ở chế độ luôn hoạt động và lắng nghe” Todd Mozer, Giám đốc Điều hành của Sensory cho biết. “Hiện nay, [việc nghe] tiêu thụ quá nhiều năng lượng. Samsung đã có giải pháp thông minh là tạo ra chế độ nghe. Chúng tôi muốn vượt xa điều đó và làm cho nó luôn luôn được bật, luôn luôn lắng nghe bất kể bạn đang ở đâu.”

Bây giờ bạn biết chiếc tivi kỹ thuật số của mình có khả năng làm được những gì, bạn có thể tự hỏi: Điện thoại di động có thể nghe trộm khi nó bị tắt hay không? Có ba đáp án. Có, không, và còn tùy.

Một số người trong cộng đồng các chuyên gia về bảo mật khẳng định rằng dẫu đã tắt điện thoại thông minh, bạn vẫn phải tháo pin ra khỏi thiết bị để chắc chắn rằng nó không lắng nghe bạn nữa. Dường như không có nhiều bằng chứng để ủng hộ điều này. Sau đó, có những người cam đoan rằng chỉ cần tắt điện thoại là đủ. Nhưng tôi nghĩ trong thực tế có những trường hợp, nói ví dụ, nếu phần mềm độc hại được thêm vào điện thoại thông minh, khi ấy nó không tắt hoàn toàn và vẫn có thể ghi lại các cuộc hội thoại ở gần đó. Vì vậy, nó phụ thuộc vào nhiều yếu tố.

Có một số điện thoại hoạt động khi bạn nói một câu lệnh, giống hệt loại ti-vi được kích hoạt bằng giọng nói. Điều này có nghĩa là điện thoại luôn luôn lắng nghe, chỉ chờ đợi câu lệnh kia phát ra. Điều này cũng ngụ ý rằng bằng cách nào đó, những phát ngôn đã được ghi lại hoặc truyền đi. Trong một số điện thoại bị nhiễm phần mềm độc hại thì điều này đúng: camera hoặc micro của điện thoại được kích hoạt khi không có cuộc gọi nào diễn ra. Tôi nghĩ rất hiếm có những trường hợp này.

Nhưng quay lại câu hỏi chính. Có một số người trong cộng đồng bảo mật cam đoan rằng bạn có thể kích hoạt một chiếc điện thoại khi nó bị tắt. Phần mềm độc hại có thể làm cho điện thoại có vẻ như bị tắt trong khi thực tế không phải như vậy. Tuy nhiên, khả năng một người nào đó có thể kích hoạt một điện thoại bị tắt (không có nguồn pin) đối với tôi là không thể. Về cơ bản, bất kỳ thiết bị nào có nguồn pin cho phép phần mềm ở trạng thái hoạt động đều có thể bị khai thác. Có thể sửa dụng một phần mềm chạy nền để khiến cho thiết bị trông giống như bị tắt trong khi nó không tắt. Nhưng một thiết bị không có điện thì không thể làm gì cả. Hoặc nó có thể chăng? Một số người vẫn tranh luận rằng NSA đã đặt chip vào điện thoại của chúng ta để cung cấp năng lượng cho thiết bị và cho phép hoạt động theo dõi diễn ra ngay cả khi điện thoại bị tắt nguồn (ngay cả khi pin bị tháo ra).

Cho dù điện thoại của bạn có khả năng nghe hay không, trình duyệt bạn sử dụng chắc chắn là có. Khoảng năm 2013, Google ra mắt hotwording, một tính năng cho phép bạn đưa ra một lệnh đơn giản để kích hoạt chế độ nghe trong Chrome. Các hãng khác cũng bắt chước, bao gồm Siri của Apple, Cortana của Microsoft, và Alexa của Amazon. Vì vậy, điện thoại, máy tính cá nhân truyền thống, và thiết bị độc lập trên bàn cà phê của bạn đều chứa các dịch vụ dựa trên nền tảng máy chủ, điện toán đám mây được thiết kế để đáp ứng các lệnh thoại như “Siri, ta còn cách trạm xăng gần nhất bao xa?” Có nghĩa là chúng đang lắng nghe. Và nếu điều đó không khiến bạn lo lắng, hãy biết rằng các hoạt động tìm kiếm của các dịch vụ này được ghi lại và lưu trữ vô thời hạn.

Vô thời hạn.

Vậy các thiết bị này nghe được bao nhiêu? Trên thực tế, chúng ta vẫn chưa rõ chúng làm gì trong khi không phải trả lời các câu hỏi của chủ nhân hoặc không phải bận rộn với việc tắt-mở. Ví dụ, khi sử dụng phiên bản máy tính cá nhân truyền thống của trình duyệt Chrome, các nhà nghiên cứu nhận thấy rằng có người nào đó – Google chăng? – đã phải luôn lắng nghe mọi lúc bằng cách

bật micro. Tính năng này đến với Chrome từ phần mềm nguồn mở tương ứng của nó, một trình duyệt được gọi là Chromium. Năm 2015, các nhà nghiên cứu phát hiện ra rằng có người nào đó – Google chăng? – có vẻ lắng nghe mọi lúc. Khi điều tra thêm, họ phát hiện ra điều này là do trình duyệt bật micro theo mặc định. Mặc dù được đưa vào trong phần mềm nguồn mở, mã này không có sẵn để kiểm tra.

Điều này tiềm ẩn một số vấn đề. Đầu tiên, "nguồn mở" có nghĩa là mọi người đều có thể kiểm tra mã, nhưng trong trường hợp này mã là một hộp đen, loại mã mà không ai được quyền xem. Thứ hai, mã này tự đi tới phiên bản phổ biến của trình duyệt thông qua bản cập nhật tự động từ Google, thứ mà người dùng không có cơ hội từ chối. Và đến năm 2015, Google vẫn không xóa nó. Họ đã đưa ra một phương tiện để mọi người chọn không tham gia, nhưng việc chọn không tham gia đó yêu cầu kỹ năng lập trình quá phức tạp đến mức người dùng bình thường không thể tự thực hiện.

Có những cách khác, công nghệ thấp hơn để giảm thiểu tính năng nghe trộm đáng sợ này trong Chrome và các chương trình khác. Đối với webcam, chỉ cần đặt một miếng băng dính lên trên. Đối với micro, một trong những biện pháp phòng thủ tốt nhất là cắm micro giả vào ổ cắm micro của máy tính cá nhân truyền thống. Để thực hiện việc này, hãy lấy một bộ tai nghe nhét lỗ hoặc bộ tai nghe có quai cũ bị hỏng và chỉ cần cắt dây gần giắc cắm micro. Bây giờ, cắm cuống của một giắc mic vào ổ cắm. Máy tính sẽ nghĩ rằng ở đó có micro trong khi thực tế là không có. Tất nhiên, nếu bạn muốn thực hiện cuộc gọi bằng Skype hoặc một số dịch vụ trực tuyến khác, thì trước tiên bạn phải tháo đầu cắm. Ngoài ra – và điều này rất quan trọng – hãy đảm bảo rằng hai dây trên cuống mic không chạm nhau để bạn không làm cháy cổng mic.

Một thiết bị kết nối khác sống trong nhà là Amazon Echo, một hub Internet cho phép người dùng đặt phim theo yêu cầu và các sản phẩm khác từ Amazon bằng giọng nói. Echo cũng luôn bật, ở

chế độ chờ, nghe từng từ, chờ đợi một câu lệnh để "đánh thức" nó. Bởi vì Amazon Echo thực hiện nhiều hơn một chiếc ti-vi thông minh, nó yêu cầu người dùng lần đầu nói lên đến 25 cụm từ cụ thể vào thiết bị trước khi đưa ra bất kỳ lệnh nào. Amazon có thể cho bạn biết thời tiết bên ngoài, cung cấp kết quả thể thao mới nhất và đặt hàng hoặc sắp xếp lại các mục từ bộ sưu tập của nó nếu bạn yêu cầu điều này. Do tính chất chung của một số cụm từ mà Amazon nhận ra – ví dụ: "Trời có mưa vào ngày mai không?" – điều này có nghĩa là Echo có thể nghe nhiều hơn ti-vi thông minh.

May mắn thay, Amazon cung cấp các cách để xóa dữ liệu giọng nói khỏi Echo. Nếu muốn xóa mọi thứ (ví dụ trong trường hợp bạn định bán Echo), bạn cần truy cập trực tuyến để xóa.

Trong khi tất cả các thiết bị kích hoạt bằng giọng nói này đều yêu cầu một cụm từ lệnh để thức dậy, chúng ta vẫn chưa biết chúng làm gì trong thời gian ngủ – thời gian chúng không bị ra lệnh làm gì. Khi có thể, hãy tắt tính năng kích hoạt bằng giọng nói trong cài đặt cấu hình. Bạn luôn có thể bật lại khi cần.

Ngoài ti-vi và bộ điều nhiệt, tủ lạnh cũng gia nhập cùng Amazon Echo trong Internet Vạn Vật.

Tủ lạnh?

Samsung mới công bố một mô hình tủ lạnh kết nối với lịch Google để hiển thị các sự kiện sắp tới trên màn hình phẳng được gắn vào cửa của thiết bị, một dạng giống như cái bảng trắng mà chúng ta vẫn đặt ở đó. Bây giờ tủ lạnh sẽ được kết nối với Internet thông qua tài khoản Google của bạn.

Samsung đã làm một vài điều đúng đắn trong việc thiết kế tủ lạnh thông minh này, chẳng hạn như một kết nối SSL/https để mã hóa luồng dữ liệu giữa tủ lạnh và máy chủ chứa lịch Google. Và họ đã gửi một chiếc tủ lạnh tương lai đến thử nghiệm tại DEF CON 23 – một trong những hội nghị hacker lớn nhất thế giới.

Tuy nhiên, theo các nhà nghiên cứu bảo mật Ken Munro và David

Lodge, những người đã xâm nhập vào dòng giao tiếp của các ti-vi kỹ thuật số, Samsung không kiểm tra chứng chỉ cho phép thực hiện giao tiếp với các máy chủ của Google và lấy thông tin lịch Gmail. Chứng chỉ xác thực rằng thông tin liên lạc giữa tủ lạnh và các máy chủ Google là bảo mật. Nhưng nếu không có nó, kẻ xấu có thể tạo chứng chỉ riêng để nghe trộm kết nối giữa tủ lạnh và Google.

Vậy thì sao?

Trong trường hợp này, khi xâm nhập được vào mạng gia đình của bạn, kẻ xấu không chỉ có thể truy cập vào tủ lạnh và làm hỏng sữa và trứng nhà bạn mà còn có thể truy cập vào thông tin tài khoản Google của bạn bằng cách thực hiện một cuộc tấn công MITM ở phần mềm lịch trong tủ lạnh và ăn cắp thông tin đăng nhập Google của bạn để đọc lén email, thậm chí có thể gây thiệt hại lớn hơn.

Tủ lạnh thông minh vẫn chưa phổ biến. Nhưng rõ ràng, khi chúng ta kết nối nhiều thiết bị hơn với Internet, và thậm chí với mạng gia đình, sẽ có sự mất an toàn. Điều này thật đáng sợ, nhất là khi thứ bị xâm phạm là thứ thực sự quý giá và riêng tư, như gia đình bạn chẳng hạn.

Các công ty Internet Vạn Vật đang nghiên cứu các ứng dụng có thể biến bất kỳ thiết bị nào thành một hệ thống an ninh gia đình. Ví dụ, một ngày nào đó chiếc ti-vi của bạn có thể chứa camera. Trong trường hợp đó, một ứng dụng trên điện thoại thông minh hoặc máy tính bảng có thể cho phép bạn xem bất kỳ phòng nào trong nhà hoặc văn phòng từ bất kỳ vị trí nào ở xa. Đèn cũng có thể bật lên khi có chuyển động bên trong hoặc bên ngoài ngôi nhà.

Chúng ta hãy cùng hình dung một ví dụ sau đây. Khi bạn lái xe về nhà, ứng dụng hệ thống báo động trên điện thoại hoặc trong ô tô sử dụng khả năng định vị địa lý được tích hợp sẵn để cảm nhận sự xuất hiện của bạn. Khi bạn cách nhà 15 mét, ứng dụng sẽ báo hiệu cho hệ thống báo động tại nhà để mở khóa cửa trước hoặc

cửa garage (ứng dụng trên điện thoại đã được kết nối với ngôi nhà và xác thực). Hệ thống báo động tiếp tục liên hệ với hệ thống chiếu sáng trong nhà, yêu cầu nó chiếu sáng cổng vòm, lối vào, và có thể là phòng khách hoặc nhà bếp. Ngoài ra, bạn cũng có thể bước vào nhà trong tiếng nhạc dìu dặt phát trên dàn âm thanh nổi từ một dịch vụ như Spotify. Và dĩ nhiên, khi bạn trở về, nhiệt độ của ngôi nhà sẽ ấm lên hoặc mát đi tùy theo mùa và sở thích của bạn.

Hệ thống báo động tại nhà trở nên phổ biến trong thời điểm đầu thế kỷ 21. Khi đó, để lắp đặt hệ thống này, kỹ thuật viên phải gắn các cảm biến có dây ở cửa ra vào và cửa sổ của ngôi nhà. Các cảm biến có dây này được kết nối với một trung tâm sử dụng điện thoại cố định có dây để gửi và nhận tin nhắn từ dịch vụ giám sát. Bạn sẽ đặt báo động và nếu có ai xâm phạm cửa ra vào và cửa sổ đã được bảo vệ, dịch vụ giám sát sẽ liên lạc với bạn, thường là qua điện thoại. Hệ thống được trang bị pin để đề phòng trường hợp mất điện. Xin lưu ý, điện thoại cố định thường không bao giờ mất điện trừ khi dây dẫn đến nhà bị cắt.

Khi mọi người chuyển từ điện thoại cố định dùng dây đồng sang các dịch vụ thông tin di động, các công ty giám sát báo động cũng bắt đầu cung cấp các kết nối dựa trên mạng di động. Gần đây, họ chuyển sang dịch vụ ứng dụng dựa trên Internet.

Hiện nay, các cảm biến cảnh báo trên cửa ra vào và cửa sổ chính đều là không dây. Dĩ nhiên, việc lắp đặt chúng không đòi hỏi phải khoan đục tường hay những sợi dây cáp xấu xí nữa, nhưng cũng có nhiều rủi ro hơn. Các nhà nghiên cứu đã nhiều lần phát hiện ra rằng tín hiệu từ các cảm biến không dây này không được mã hóa. Kẻ tấn công có thể chỉ cần nghe lén thông tin liên lạc giữa các thiết bị để xâm nhập chúng. Ví dụ, nếu xâm nhập được vào mạng cục bộ của bạn, tôi có thể nghe lén thông tin liên lạc giữa các máy chủ của công ty báo động với thiết bị trong nhà bạn (giả sử nó trên cùng một mạng cục bộ và không được mã hóa), và bằng cách thao túng các liên lạc đó, tôi có thể chiếm quyền kiểm soát ngôi nhà thông minh của bạn, giả mạo các lệnh để điều khiển hệ

thống.

Các công ty hiện cung cấp nhiều dịch vụ giám sát tại nhà "tự lắp đặt." Nếu có cảm biến nào bị xâm nhập, điện thoại di động của bạn sẽ nhận được tin nhắn thông báo. Hoặc ứng dụng có thể cung cấp hình ảnh webcam từ trong nhà. Dù bằng cách nào, bạn cũng nắm được quyền kiểm soát và tự mình theo dõi ngôi nhà. Điều đó thật tuyệt vời, cho đến khi Internet trong nhà bạn bị ngắt kết nối.

Ngay cả khi Internet đang hoạt động, kẻ xấu vẫn có thể phá hoại các hệ thống báo động không dây tự lắp đặt này. Ví dụ, kẻ tấn công có thể kích hoạt báo động giả (một số thành phố quy định chủ nhà sẽ phải trả tiền phạt trong trường hợp này). Có thể kích hoạt thiết bị tạo báo động giả từ ngoài đường, trước cửa nhà bạn hoặc cách đó 200 mét. Quá nhiều báo động giả sẽ khiến hệ thống trở nên thiếu tin cậy (và chủ nhà sẽ điêu đứng vì những khoản tiền phạt).

Hoặc kẻ tấn công có thể gây nhiễu tín hiệu cảm biến không dây tự lắp đặt bằng cách gửi nhiễu vô tuyến để ngăn luồng thông tin liên lạc quay lại hub hoặc bảng điều khiển chính. Điều này khiến còi báo động không phát ra tiếng được, từ đó vô hiệu hóa cơ chế bảo vệ và cho phép các tội phạm đột nhập thẳng vào nhà.

Rất nhiều người đã cài đặt webcam trong nhà – có thể để bảo mật, giám sát người giúp việc, hay theo dõi người thân bị ốm. Thật không may, webcam qua Internet thường dễ bị tấn công từ xa.

Một công cụ tìm kiếm công khai tên là Shodan hiển thị thông tin về các thiết bị phi truyền thống được cấu hình để kết nối với Internet. Shodan không chỉ hiển thị kết quả từ các thiết bị Internet Vạn Vật của bạn ở nhà mà còn từ các mạng tiện ích nội bộ và các hệ thống điều khiển công nghiệp đã bị cấu hình sai để kết nối máy chủ của chúng với mạng công cộng. Nó cũng hiển thị các luồng dữ liệu từ vô số các webcam thương mại bị cấu hình sai trên toàn thế giới. Người ta ước tính rằng trong một ngày có đến 100.000 webcam không được bảo mật hoặc bảo mật hạn chế tham gia truyền dữ liệu qua Internet.

Trong số này có các camera Internet không có xác thực mặc định của một công ty tên là D-Link, có thể được sử dụng để theo dõi mọi người trong những hoạt động riêng tư (tùy thuộc vào nội dung quay được thiết lập trong camera). Kẻ tấn công có thể sử dụng bộ lọc Google để tìm kiếm "Camera Internet D-Link," sau đó tìm kiếm các model không có xác thực theo mặc định, rồi truy cập vào một website như Shodan, nhấp vào một liên kết, và xem luồng video mong muốn.

Để ngăn chặn điều này, hãy tắt webcam Internet khi không dùng đến. Hành động ngắt kết nối vật lý là nhằm bảo đảm chắc chắn rằng webcam đã được tắt. Khi sử dụng chúng, hãy đảm bảo rằng chúng có xác thực phù hợp và có mật khẩu mạnh, chứ không phải mật khẩu mặc định.

Nếu bạn nghĩ ngôi nhà của mình như vậy đã là một thảm họa về sự riêng tư, vậy hãy chờ tới khi bạn đến nơi làm việc. Tôi sẽ bàn đến vấn đề này ở chương tiếp theo.

Chương 13: NHỮNG ĐIỀU SẾP KHÔNG MUỐN BẠN BIẾT

Nếu bạn đã đọc tới đây, rõ ràng bạn có quan tâm đến quyền riêng tư, nhưng đối với hầu hết chúng ta, vấn đề không nằm ở việc che giấu thông tin trước chính phủ liên bang. Thực ra, chúng ta biết rằng ở nơi làm việc, công ty có thể thấy chính xác những gì mà chúng ta đang làm trên mạng của họ (ví dụ: mua sắm, chơi trò chơi, giải trí). Rất nhiều người chỉ muốn che giấu những chuyện đó mà thôi!

Nhưng điều này càng ngày càng khó thực hiện hơn, một phần do những chiếc điện thoại di động mà chúng ta mang theo người. Bất cứ khi nào Jane Rodgers, quản lý tài chính của một công ty dịch vụ cảnh quan ở Chicago, muốn biết liệu các nhân viên thực địa có mặt ở đúng nơi cần thiết không, cô chỉ việc mở máy tính xách tay ra là biết vị trí chính xác của họ. Giống như nhiều nhà quản lý và chủ doanh nghiệp khác, cô đang chuyển sang sử dụng phần mềm theo dõi trên thiết bị điện thoại thông minh và xe tải dịch vụ do công ty sở hữu, được cá nhân hóa (COPE) có trang bị thiết bị định vị GPS để giám sát nhân viên. Một hôm, một khách hàng hỏi Jane xem nhân viên của cô có ra ngoài làm việc cho họ hay không. Sau khi gõ một vài phím, Jane xác nhận được ngay rằng từ 10 – 10:30 giờ sáng, nhân viên của cô có đến đó làm việc.

Dịch vụ di động viễn thông mà Rodgers sử dụng cung cấp nhiều khả năng hơn cả công nghệ định vị. Ví dụ, trên chín chiếc điện thoại thuộc sở hữu của công ty, cô còn có thể xem ảnh, tin nhắn, và email mà nhân viên của mình gửi đi. Cô cũng có quyền truy cập vào nhật ký cuộc gọi và lượt truy cập website của những chiếc điện thoại đó. Nhưng Rodgers nói rằng cô chỉ sử dụng tính năng GPS.

Từ lâu ngành dịch vụ đã sử dụng công nghệ theo dõi GPS. Hãng chuyển phát hàng hóa United Parcel Service (UPS) đã kết hợp công nghệ này với thuật toán lựa chọn tuyến đường do họ tự xây

dựng là ORION để cắt giảm chi phí gas bằng cách theo dõi và đề xuất các tuyến đường tối ưu cho các lái xe của công ty. Họ cũng có thể phát hiện và có biện pháp xử lý những tài xế lười biếng. Bằng những cách này, UPS đã tăng khối lượng hàng hóa vận chuyển thêm 1,4 triệu gói hàng mỗi ngày, trong khi số lượng tài xế giảm đi hơn 1.000 người.

Tất cả những điều này mang lại lợi ích cho các nhà tuyển dụng, bởi họ vẫn nói rằng bằng cách ép để thu về mức lợi nhuận cao hơn, họ sẽ có khả năng nâng cao mức lương cho người lao động. Nhưng nhân viên cảm thấy thế nào? Hoạt động giám sát này có một nhược điểm. Trong một phân tích, tạp chí Harper's giới thiệu về một tài xế được theo dõi bằng các công cụ điện tử trong khi làm việc. Người này cho biết phần mềm xác định thời gian giao hàng của anh theo từng giây và thông báo bất cứ khi nào anh chậm hoặc nhanh hơn thời gian tối ưu. Thông thường, mỗi ngày anh làm quá thời gian tối ưu tới bốn giờ.

Chểnh mảng chăng? Lái xe đã chỉ ra rằng một điểm dừng có thể bao gồm nhiều gói hàng – phần mềm ORION không phải lúc nào cũng tính đến việc này. Anh kể về những đồng nghiệp ở trung tâm phân phối New York cũng đang phải chiến đấu với cơn đau mãn tính ở lưng và đầu gối khi cố gắng mang theo quá nhiều hàng trong một chuyến đi mặc dù liên tục bị công ty nhắc nhở về việc xử lý quá tải, để có thể đạt hạn mức ứng với phần mềm. Như vậy, việc giám sát nhân viên này làm phát sinh chi phí về con người.

Dịch vụ thực phẩm cũng là một ngành thường xuyên sử dụng công nghệ giám sát. Từ các camera trên trần nhà của các nhà hàng cho đến các hộp thiết bị nhỏ đặt trên mặt bàn, nhân viên phục vụ có thể bị theo dõi và đánh giá bởi các hệ thống phần mềm khác nhau. Một nghiên cứu năm 2013 của các nhà nghiên cứu thuộc Đại học Washington, Đại học Brigham Young, và MIT đã phát hiện ra rằng phần mềm theo dõi hành vi trộm cắp được sử dụng trong 392 nhà hàng đã làm giảm 22% hành vi trộm cắp từ phía nhân viên phục vụ. Như tôi đã đề cập, việc chủ động giám

sát mọi người làm thay đổi hành vi của họ.

Hiện tại ở Mỹ không có đạo luật liên bang nào cấm các công ty theo dõi nhân viên của họ. Chỉ có tiểu bang Delaware và Connecticut yêu cầu người sử dụng lao động phải thông báo với nhân viên trong trường hợp họ đang bị theo dõi. Ở hầu hết các bang, nhân viên không biết họ có đang bị theo dõi tại nơi làm việc hay không.

Vậy còn về các nhân viên trong văn phòng thì sao? Hiệp hội Quản lý Mỹ nhận thấy 66% người sử dụng lao động theo dõi việc sử dụng Internet của nhân viên, 45% theo dõi hoạt động gõ bàn phím, và 43% theo dõi nội dung email. Một số công ty theo dõi các mục nhập lịch Outlook, tiêu đề email, và nhật ký tin nhắn của nhân viên. Bề ngoài, dữ liệu được dùng để giúp các công ty tìm hiểu cách thức sử dụng thời gian của nhân viên – từ việc nhân viên bán hàng sử dụng bao nhiêu thời gian với khách hàng, các bộ phận nào của công ty đang giữ liên lạc bằng email, cho đến việc nhân viên sử dụng bao nhiêu thời gian cho các buổi họp hành hoặc rời khỏi bàn làm việc.

Tất nhiên, ở đây có điểm tích cực: với những số liệu như vậy, các công ty có thể tăng cường hiệu quả lên lịch họp hoặc khuyến khích các nhóm giao tiếp với nhau nhiều hơn. Nhưng điều quan trọng là có người đang thu thập tất cả các dữ liệu doanh nghiệp này. Và một ngày nào đó, dữ liệu trên có thể bị chuyển sang cơ quan thực thi pháp luật hoặc ít nhất được sử dụng để chống lại bạn trong một đợt đánh giá kết quả làm việc.

Bạn không vô hình ở nơi làm việc. Bất cứ điều gì đi qua mạng cục bộ của công ty đều thuộc về công ty, chứ không phải của bạn. Ngay cả khi bạn kiểm tra tài khoản email cá nhân, đơn đặt hàng gần đây với Amazon, hoặc lập kế hoạch cho kỳ nghỉ, thì vẫn có thể bạn thực hiện những thao tác đó trên thiết bị hoặc mạng VPN do công ty trang bị cho; do đó, hãy yên tâm là có người đang theo dõi mọi thứ bạn làm.

Dưới đây là một cách dễ dàng để tránh việc quản lý, thậm chí cả

đồng nghiệp, rình mò bạn: khi rời bàn làm việc để đi họp hoặc vào nhà vệ sinh, hãy khóa màn hình máy tính lại. Tôi nói nghiêm túc đấy. Đừng hớ hênh để ngỏ email hoặc các chi tiết về dự án bạn đã vất vả làm hàng tuần nay. Hãy khóa máy tính cho đến khi bạn quay lại. Phải mất thêm vài giây nữa, nhưng nó sẽ khiến bạn tránh được rất nhiều rắc rối. Đặt bộ hẹn giờ trong hệ điều hành để khóa màn hình sau một số giây nhất định. Hoặc sử dụng các ứng dụng Bluetooth để tự động khóa màn hình nếu điện thoại di động của bạn không ở gần máy tính. Tuy nhiên, có một kiểu tấn công mới sử dụng thiết bị USB chuyên biệt để phá hoại các thiết bị mà nó cắm vào. Rất nhiều văn phòng niêm phong các cổng USB trên máy tính xách tay và máy tính để bàn, nhưng nếu máy của bạn không bị niêm phong, một thiết bị USB như vậy khi được cắm vào vẫn có thể mở khóa máy tính mà không cần mật khẩu.

Ngoài các bí mật của công ty, còn có một số lượng email cá nhân tương đối lớn đi qua máy tính của chúng ta trong ngày làm việc, và đôi khi chúng ta còn in nội dung ra giấy. Nếu bạn quan tâm đến sự riêng tư, đừng làm bất cứ điều gì cá nhân trong khi làm việc. Hãy duy trì ranh giới nghiêm ngặt giữa cuộc sống công việc và cuộc sống gia đình. Hoặc nếu bạn cần phải làm một số công việc cá nhân trong giờ nghỉ ở công ty, hãy mang theo thiết bị cá nhân như máy tính xách tay hoặc iPad từ nhà đi. Và nếu thiết bị di động của bạn đã bật, đừng bao giờ sử dụng Wi-Fi của công ty và hơn nữa, hãy tắt chế độ phát SSID nếu bạn đang sử dụng điểm phát sóng di động. Chỉ sử dụng dữ liệu di động khi thực hiện những công việc cá nhân tại nơi làm việc.

Khi đến văn phòng, hãy làm việc ở văn phòng. Cũng giống như việc bạn không nên chia sẻ những chuyện quá riêng tư với đồng nghiệp, bạn cũng cần phải giữ cho các hoạt động cá nhân của mình nằm ngoài các hệ thống máy tính của công ty (đặc biệt là khi bạn đang tìm kiếm các chủ đề liên quan đến sức khỏe hoặc tìm kiếm một công việc mới).

Nói thì dễ hơn làm. Vì thứ nhất, chúng ta đã quen với sự phổ biến của thông tin và Internet. Nhưng nếu muốn làm chủ nghệ thuật

tàng hình, bạn phải tự kiềm chế để bản thân không làm những điều riêng tư nơi công cộng.

Giả sử mọi thứ bạn nhập vào máy tính văn phòng đều ở chế độ công khai. Điều đó không có nghĩa là bộ phận IT đang chủ động theo dõi thiết bị của bạn hoặc sẽ có hành động phản ứng khi thấy bạn dùng chiếc máy in đắt tiền ở tầng năm để in tài liệu học cho con (mặc dù họ có thể làm điều đó). Vấn đề là, có một bản ghi cho thấy bạn đã làm những việc này, và nếu trong tương lai có phát sinh sự cố gì đó khiến bạn bị nghi ngờ, họ có thể truy cập các bản ghi về tất cả mọi thứ bạn đã làm trên máy đó. Đó là máy của họ, không phải của bạn. Và đó là mạng của họ. Điều đó có nghĩa là họ đang quét nội dung lưu chuyển trong công ty.

Hãy xem xét trường hợp của Adam, người đã tải xuống báo cáo tín dụng miễn phí trên máy tính ở nơi làm việc. Anh dùng máy và mạng của công ty để đăng nhập vào website của Cục Tín dụng. Giả sử bạn cũng tải xuống báo cáo tín dụng tại nơi làm việc. Bạn sẽ muốn in nó ra, phải không? Vậy tại sao không in nhờ máy của công ty chứ? Bởi vì nếu bạn làm như vậy, sẽ có một bản sao của tập tin PDF chứa lịch sử tín dụng của bạn nằm trên ổ đĩa cứng của máy in. Bạn không kiểm soát máy in đó. Và sau khi máy in hết hạn sử dụng và thanh lý khỏi văn phòng, bạn không có quyền kiểm soát cách ổ đĩa cứng. Một số máy in hiện đang mã hóa các ổ đĩa, nhưng bạn đã chắc chắn rằng máy in trong văn phòng của mình đã được mã hóa không? Bạn không thể.

Đó chưa phải là tất cả. Mọi tài liệu Word hoặc Excel mà bạn tạo bằng Microsoft Office đều bao gồm siêu dữ liệu mô tả tài liệu. Thông thường, siêu dữ liệu này bao gồm tên của tác giả, ngày tạo, số lần sửa đổi và kích thước tệp cũng như tùy chọn thêm chi tiết khác. Điều này không được Microsoft kích hoạt mặc định; bạn phải thực hiện một số thao tác để xem được nó. Tuy nhiên, Microsoft đã bao gồm một công cụ Document Inspector có thể loại bỏ các chi tiết này trước khi bạn xuất tài liệu ở nơi khác.

Một nghiên cứu năm 2012 do Xerox và McAfee tài trợ cho thấy 54% nhân viên nói rằng không phải lúc nào họ cũng tuân theo

chính sách bảo mật IT của công ty, và 51% nhân viên ở nơi làm việc có máy in, máy photocopy hoặc máy in đa chức năng nói rằng họ đã sao chép, quét hoặc in thông tin bí mật của cá nhân tại nơi làm việc. Và điều này diễn ra không chỉ ở văn phòng: tương tự với các máy in tại cửa hàng photocopy và thư viện địa phương. Tất cả các máy này đều chứa ổ cứng ghi nhớ mọi thứ chúng đã in trong suốt thời gian hoạt động. Nếu cần in một tài liệu cá nhân, có lẽ bạn nên chờ tới khi về nhà để in trên thiết bị và mạng mà bạn có quyền kiểm soát.

Hoạt động do thám, ngay cả là do thám nhân viên, đã trở nên rất sáng tạo. Một số công ty sử dụng cả các thiết bị văn phòng phi truyền thống mà chúng ta vẫn bỏ qua, chưa bao giờ tưởng tượng rằng chúng có thể được sử dụng để theo dõi chúng ta. Hãy xem xét câu chuyện của một sinh viên cao học thuộc Đại học Columbia tên là Ang Cui. Để xem mình có thể đột nhập vào một văn phòng và ăn cắp dữ liệu nhạy cảm thông qua các phương tiện phi truyền thống hay không, Cui quyết định tấn công máy in laser, một thiết bị cần thiết trong hầu hết các văn phòng ngày nay.

Cui nhận thấy rằng các máy in lạc hậu rất xa so với thời đại. Trong một số cuộc kiểm định an ninh, tôi cũng đã quan sát thấy điều này. Tôi đã có thể tận dụng máy in để có quyền truy cập sâu hơn vào mạng cục bộ của công ty. Sở dĩ tôi làm được thế là do nhân viên hiếm khi thay đổi mật khẩu quản trị trên các máy in nội bộ.

Phần mềm sử dụng trong máy in, đặc biệt là máy in thương mại cho văn phòng, chứa rất nhiều lỗi bảo mật cơ bản. Vấn đề là, rất ít người cho rằng máy in văn phòng là đối tượng dễ bị tấn công. Họ đinh ninh rằng mình đang được hưởng cái gọi là "an ninh qua sự mù mờ"[81] – nếu không ai nhận thấy lỗ hổng, thì bạn được an toàn.

[81] An ninh qua sự mù mờ: Chỉ việc bảo đảm an ninh cho một hệ thống bằng cách dựa vào tính bí mật của thiết kế hay sự triển khai hệ thống.

Nhưng như tôi đã nói, tùy thuộc vào kiểu máy, máy in và máy photo thường có một điều quan trọng chung – cả hai đều có thể chứa ổ đĩa cứng. Và trừ khi ổ đĩa cứng đó được mã hóa (nhưng trên thực tế, rất nhiều máy không được mã hóa), việc truy cập các hoạt động in ấn trên máy là hoàn toàn khả thi. Tất cả những điều này đã được biết đến trong nhiều năm. Điều mà Cui băn khoăn là liệu anh có thể khiến máy in của công ty chống lại chủ nhân của nó và giải mã bất cứ thứ gì đã được in ra hay không.

Để làm cho mọi việc trở nên thú vị hơn, Cui muốn tấn công mã phần mềm của máy in, đây là chương trình được nhúng trong một con chip bên trong máy in. Không giống như các máy tính cá nhân và thiết bị di động truyền thống, ti-vi kỹ thuật số và các thiết bị điện tử "thông minh" khác không có sức mạnh hoặc tài nguyên xử lý để chạy hệ điều hành đầy đủ như Android, Windows, và iOS. Thay vào đó, các thiết bị này sử dụng những gì được gọi là hệ điều hành thời gian thực (RTOS), được lưu trữ trên các chip riêng lẻ bên trong thiết bị (thường được gọi là fireware). Những chip này chỉ lưu trữ các lệnh cần thiết để vận hành hệ thống và không cần nhiều thứ khác. Thỉnh thoảng, ngay cả những lệnh đơn giản này cũng cần được nhà sản xuất hoặc nhà cung cấp cập nhật bằng cách di chuyển hoặc thay thế các chip. Do điều này được thực hiện rất không thường xuyên, rõ ràng là nhiều nhà sản xuất chỉ đơn giản là không xây dựng trong các biện pháp an ninh thích hợp. Việc thiếu cập nhật là hướng mà Cui quyết định theo đuổi cho cuộc tấn công của mình.

Cui muốn xem điều gì sẽ xảy ra nếu anh tấn công định dạng tệp mà HP sử dụng để cập nhật phần mềm, và anh phát hiện ra rằng HP không kiểm tra tính hợp lệ của từng bản cập nhật. Vì vậy, anh đã tạo ra phần mềm máy in riêng và chiếc máy in chấp nhận nó. Mọi chuyện chỉ đơn giản có vậy. Không có xác thực nào ở phía máy in rằng bản cập nhật đến từ HP. Máy in chỉ quan tâm rằng mã chương trình có định dạng mong muốn.

Bây giờ Cui đã được tự do khám phá.

Trong một thí nghiệm nổi tiếng, Cui cho biết anh có thể bật

thanh nhiệt áp, một phần của máy in làm nóng giấy sau khi mực đã được in, và cứ để nó ở chế độ bật – điều này có thể khiến máy in bắt lửa. Nhà cung cấp, không phải là HP, ngay lập tức đáp lại rằng có một lỗi an toàn nhiệt trong thanh nhiệt áp, có nghĩa là máy in không thể quá nóng. Tuy nhiên, đó là điểm Cui nhắm tới – anh đã tắt được tính năng an toàn nhiệt để máy có thể bắt lửa.

Theo kết quả của những thí nghiệm này, Cui và cố vấn của anh, Salvatore Stolfo, lập luận rằng máy in là những liên kết yếu trong bất kỳ tổ chức hay ngôi nhà nào. Ví dụ, bộ phận nhân sự của một doanh nghiệp lớn có thể nhận được một file lý lịch được mã hóa độc qua Internet. Trong thời gian người quản lý tuyển dụng in tài liệu đó, máy in mà nó đi qua có thể bị xâm nhập hoàn toàn bằng cách cài đặt phiên bản phần mềm độc hại.

Để ngăn người khác lấy tài liệu của bạn khỏi máy in, thì công nghệ in an toàn[82], còn được gọi là in kéo, đảm bảo rằng tài liệu chỉ được phát hành khi xác thực người dùng tại máy in (thông thường, phải nhập mật khẩu thì máy mới thực hiện lệnh in). Điều này có thể được thực hiện bằng cách sử dụng mã PIN, thẻ thông minh, hoặc vân tay sinh trắc học. In kéo cũng loại bỏ tài liệu chưa được xác nhận, ngăn ngừa tình trạng thông tin nhạy cảm bị để hớ hênh.

[82] In an toàn (secure print): Thuật ngữ chỉ các tác vụ in ấn đáp ứng tiêu chuẩn bảo mật nhằm ngăn chặn việc sử dụng trái phép các thông tin được in ra.

Từ các cuộc tấn công máy in, Cui bắt đầu để mắt tới các vật dụng phổ biến khác trong văn phòng có khả năng sơ hở, và anh chọn điện thoại Truyền giọng nói qua giao thức Internet (VoIP). Cũng như với máy in, không ai đánh giá cao giá trị tiềm ẩn của các thiết bị này trong việc thu thập thông tin. Và như với một máy in, bạn có thể giả mạo một bản cập nhật cho hệ thống và được điện thoại VoIP chấp nhận.

Hầu hết các điện thoại VoIP đều có tùy chọn hands-free (không cần cầm tay) để bạn có thể nói chuyện qua loa ngoài. Điều đó có

nghĩa là không chỉ có một chiếc loa mà còn có một micro ở bên ngoài điện thoại. Ngoài ra còn có một công tắc "nhấc máy," giúp cho điện thoại nhận biết khi có người đã nhấc ống nghe và muốn thực hiện hay nghe cuộc gọi, hay biết khi nào ống nghe được đặt xuống và loa ngoài được bật lên. Cui nhận ra rằng nếu thao túng được công tắc "nhấc máy," anh có thể khiến cho điện thoại lắng nghe cuộc trò chuyện gần đó thông qua micro của loa ngoài, ngay cả khi ống nghe đang úp xuống!

Một cảnh báo: không giống như máy in, vốn có thể nhận mã độc qua Internet, điện thoại VoIP cần phải được "cập nhật" riêng lẻ từng lần bằng cách thủ công. Như vậy, phải truyền mã bằng ổ USB. Cui cho rằng anh có thể dễ dàng xử lý vấn đề này. Anh hối lộ một người lau dọn ban đêm để nhờ họ tranh thủ dùng USB cài đặt mã vào từng chiếc điện thoại.

Cui đã trình bày nghiên cứu này tại một số hội nghị, mỗi lần lại sử dụng các điện thoại VoIP khác nhau. Và mỗi lần như vậy, anh đều thông báo trước cho nhà cung cấp, họ lại đưa ra một bản sửa lỗi. Nhưng Cui đã chỉ ra rằng việc tồn tại bản vá lỗi không có nghĩa là bản vá được áp dụng. Ngay lúc này, một số điện thoại chưa được vá lỗi có thể vẫn đang hoạt động trong các văn phòng, khách sạn, và bệnh viện.

Vậy Cui đã lấy dữ liệu khỏi điện thoại bằng cách nào? Vì các mạng máy tính văn phòng được theo dõi để phát hiện các hoạt động bất thường, nên anh cần một phương tiện khác để trích xuất dữ liệu. Anh quyết định không sử dụng mạng mà dùng sóng vô tuyến.

Trước đây, các nhà nghiên cứu tại Đại học Stanford và Israel đã phát hiện ra rằng việc để điện thoại di động bên cạnh máy tính có thể cho phép một bên thứ ba từ xa nghe lén các cuộc hội thoại của bạn. Để làm được điều này, kẻ xấu phải cài phần mềm độc hại vào thiết bị di động của bạn. Nhưng với các ứng dụng mã hóa độc có thể tải xuống từ các cửa hàng ứng dụng có ý đồ xấu, điều đó thật dễ dàng, phải không?

Khi phần mềm độc hại được cài vào điện thoại di động của bạn,

con quay chuyển hướng trong điện thoại đã đủ nhạy cảm để nhận các rung động nhẹ. Phần mềm độc hại trong trường hợp này, theo các nhà nghiên cứu cho biết, cũng có thể nhận được những rung động trong không khí, bao gồm cả những rung động được tạo ra bởi lời nói của con người. Hệ điều hành Android của Google cho phép chuyển động từ các cảm biến được đọc ở mức 200 Hz hoặc 200 chu kỳ mỗi giây. Hầu hết giọng nói của con người nằm trong khoảng từ 80 đến 250 Hz. Điều đó có nghĩa là cảm biến có thể nhận được một phần đáng kể những tiếng nói đó. Thậm chí các nhà nghiên cứu còn xây dựng một chương trình nhận dạng giọng nói tùy chỉnh để biên dịch tín hiệu 80-250 Hz tốt hơn.

Cui nhận thấy một điều tương tự nhau trong điện thoại VoIP và máy in. Anh phát hiện ra rằng các chân tóc dính vào mọi microchip trong bất kỳ thiết bị nhúng ngày nay đều có thể bị điều khiển để dao động theo trình tự duy nhất và do đó thẩm thấu dữ liệu trên tần số vô tuyến (RF). Anh gọi đây là funtenna, và nó là một sân chơi ảo cho những người muốn trở thành hacker. Nhà nghiên cứu bảo mật Michael Ossmann, người được Cui cho là chủ nhân của ý tưởng trên, nhận định: “Funtenna là một ăng-ten mà nhà thiết kế hệ thống không chủ định sử dụng làm ăng-ten, đặc biệt khi được kẻ tấn công sử dụng làm ăng-ten.”

Ngoài funtenna, người ta có thể do thám những việc bạn làm ở nơi làm việc bằng cách nào?

Các nhà nghiên cứu ở Israel đã phát hiện ra rằng khi bị cài phần mềm độc hại, điện thoại di động thông thường có thể nhận dữ liệu nhị phân từ máy tính. Và trước đây, các nhà nghiên cứu của Stanford từng phát hiện ra rằng các cảm biến điện thoại di động có thể chặn để thu thập âm thanh của phát xạ điện tử từ bàn phím không dây. Điều này được xây dựng dựa trên các nghiên cứu tương tự được thực hiện bởi các nhà khoa học tại MIT và Georgia Tech. Như vậy có thể khẳng định rằng mọi thứ bạn gõ hoặc xem trong văn phòng đều có thể bị một bên thứ ba nghe từ xa theo cách này hay cách khác.

Ví dụ, giả sử bạn sử dụng bàn phím không dây. Tín hiệu vô tuyến được gửi từ bàn phím đến máy tính xách tay hoặc máy tính để bàn có thể bị chặn. Nhà nghiên cứu bảo mật Samy Kamkar đã thiết kế ra KeySweeper để làm điều đó: một thiết bị sạc USB giả trang với nhiệm vụ tìm kiếm, giải mã, ghi lại, và báo cáo (qua GSM) tất cả các phím bấm từ bất kỳ bàn phím không dây nào của Microsoft trong khu vực lân cận.

Chúng ta đã nói về nguy cơ khi sử dụng các điểm phát sóng ma tại các quán cà phê và sân bay. Điều này cũng có thể đúng trong văn phòng. Ai đó trong văn phòng của bạn có thể thiết lập điểm phát sóng không dây và thiết bị của bạn có thể tự động kết nối với nó. Các phòng IT thường quét các thiết bị như vậy, nhưng đôi khi họ không làm như thế.

Một cách tương ứng với việc mang bộ phát sóng cá nhân đến văn phòng là mang kết nối di động của riêng bạn. Femtocell là các thiết bị mini được các nhà mạng cung cấp. Chúng được thiết kế để tăng cường kết nối di động trong nhà hoặc văn phòng nơi tín hiệu có thể yếu. Chúng không phải là không có các rủi ro về riêng tư.

Trước hết, bởi vì femtocell là các trạm cơ sở cho hoạt động giao tiếp qua di động, nên thiết bị di động của bạn thường sẽ kết nối với chúng mà không thông báo cho bạn. Hãy nghĩ về điều đó.

Tại Mỹ, cơ quan thực thi pháp luật sử dụng StingRay, còn được gọi là máy bắt IMSI, một máy mô phỏng trạm cơ sở. Ngoài ra còn có TriggerFish, Wolfpack, Gossamer, và swamp box. Mặc dù công nghệ khác nhau, nhưng các thiết bị này về cơ bản đều hoạt động giống như một femtocell không có kết nối di động. Chúng được thiết kế để thu thập danh tính người đăng ký di động quốc tế hoặc IMSI từ điện thoại di động. Cho đến nay, việc sử dụng các thiết bị này tại Mỹ phổ biến chỉ sau châu Âu. Những máy bắt IMSI được sử dụng trong các cuộc biểu tình lớn, ví dụ, để giúp cơ quan thực thi pháp luật xác định những ai tham gia biểu tình – dựa trên giả định rằng các nhà tổ chức sẽ điều phối sự kiện này qua điện thoại di động.

Sau một trận chiến pháp lý kéo dài, Liên đoàn Tự do Dân sự Mỹ thuộc Bắc California đã thu thập các tài liệu từ chính phủ nêu chi tiết cách thức sử dụng StingRay. Ví dụ, các nhân viên thực thi pháp luật phải xin lệnh sử dụng các thiết bị pen register hoặc trap-and-trace của tòa án. Các thiết bị pen register được sử dụng để lấy số điện thoại, một bản ghi các số được quay trên điện thoại. Công nghệ trap-and-trace được sử dụng để thu thập thông tin về các cuộc gọi đã nhận. Ngoài ra, bằng một yêu cầu, cơ quan thực thi pháp luật có thể được phép ghi âm cuộc gọi điện thoại hoặc nội dung của một email. Theo tờ Wired, các tài liệu mà ACLU nhận được mô tả rằng các thiết bị "có thể có khả năng chặn bắt nội dung liên lạc và do đó, các thiết bị này phải được cấu hình để vô hiệu hóa chức năng chặn bắt, trừ các trường hợp việc chặn bắt được cho phép theo Mục III của yêu cầu cho phép thực hiện chặn bắt liên lạc theo thời gian thực.

Giả sử bạn không bị cơ quan thực thi pháp luật giám sát. Giả sử bạn đang ở trong một văn phòng có độ ổn định cao, ví dụ, tại một cơ sở tiện ích công cộng. Một người có thể cài đặt femtocell để cho phép thực hiện các hoạt động liên lạc cá nhân ở bên ngoài hệ thống ghi nhật ký cuộc gọi thông thường của cơ sở tiện ích này. Mối nguy hiểm ở đây là đồng nghiệp với chiếc femtocell đã sửa đổi ở bàn mình có thể thực hiện một cuộc tấn công MITM, và anh ta cũng có thể lắng nghe các cuộc gọi của bạn hoặc chặn bắt các tin nhắn của bạn.

Trong một buổi thuyết trình tại Black Hat USA 2013, các nhà nghiên cứu cho thấy họ có thể bắt được các cuộc gọi thoại, tin nhắn, và thậm chí cả lưu lượng truy cập web từ các tình nguyện viên trong số khán giả trên femtocell Verizon của họ. Lỗ hổng trong femtocell do Verizon phát hành đã được vá, nhưng các nhà nghiên cứu muốn cho các công ty này thấy rằng dù sao thì họ cũng nên tránh sử dụng chúng.

Một số phiên bản Android sẽ thông báo khi bạn chuyển mạng di động; iPhone thì không. "Điện thoại của bạn sẽ liên kết với một femtocell mà bạn không biết," nhà nghiên cứu Doug DePerry giải

thích. “Điều này không giống như Wi-Fi; bạn không có lựa chọn nào cả.”

Hãng Pwnie Express đã sản xuất một thiết bị gọi là Pwn Pulse để xác định các femtocell và thậm chí cả các máy bắt IMSI như StingRay. Thiết bị này giúp các công ty có thể giám sát các mạng điện thoại di động xung quanh. Các công cụ phát hiện mối đe dọa tiềm ẩn đối với mạng điện thoại như thế này trước kia chủ yếu do các chính phủ mua – nhưng tình hình hiện nay đã khác.

Tuy là một phần mềm thân thiện với người dùng, nhưng Skype lại không phải là phần mềm thân thiện nhất khi nói đến quyền riêng tư. Theo Edward Snowden, người đã công bố các tài liệu mật lần đầu tiên trên tờ Guardian, Microsoft đã làm việc với NSA để đảm bảo rằng các cuộc trao đổi trên Skype có thể bị chặn bắt và theo dõi. Một tài liệu tiết lộ rằng một chương trình của NSA là Prism thực hiện giám sát video Skype và các dịch vụ truyền thông khác. “Phần âm thanh của các cuộc trao đổi này đã được xử lý chính xác, nhưng không có video đi kèm. Giờ đây, các nhà phân tích sẽ có được ‘bức tranh’ hoàn chỉnh,” tờ Guardian viết.

Tháng 3 năm 2013, một sinh viên cao học chuyên ngành khoa học máy tính tại Đại học New Mexico đã phát hiện ra rằng TOM-Skype, một phiên bản Skype của Trung Quốc được tạo ra thông qua sự hợp tác giữa Microsoft và TOM Group, tải lên danh sách từ khóa cho mọi máy của người dùng Skype – bởi vì ở Trung Quốc có những từ và cụm từ mà bạn không được phép tìm kiếm trực tuyến (bao gồm cả “Quảng trường Thiên An Môn”). TOM-Skype cũng gửi cho chính phủ Trung Quốc tên người dùng của chủ tài khoản, thời gian và ngày truyền tải, và thông tin về việc liệu người dùng có gửi hoặc nhận tin nhắn hay không.

Các nhà nghiên cứu đã phát hiện ra rằng ngay cả các hệ thống hội nghị truyền hình cấp cao – loại đắt tiền, không phải Skype – cũng có thể sơ hở trước các cuộc tấn công MITM. Điều đó có nghĩa là tín hiệu được định tuyến đi qua người khác trước khi nó tới điểm đến là bạn. Điều này cũng đúng với các hội nghị thoại. Trừ khi người điều hành có danh sách các số đã gọi đến, và trừ khi anh ta đã yêu

cầu xác minh bất kỳ số nào đáng nghi, giả dụ mã vùng bên ngoài Mỹ, thì không có cách nào để chứng minh hoặc xác định liệu một bên không được mời có tham gia hay không. Người điều hành hội nghị nên gọi cho những người tham dự mới, và nếu họ không xác minh được, hãy gác máy và sử dụng số điện thoại hội nghị dự phòng.

Giả dụ công ty bạn đã đầu tư lớn để mua một hệ thống hội nghị truyền hình đắt giá, nhờ vậy mà bạn đinh ninh rằng nó sẽ an toàn hơn các hệ thống bán đại trà. Nhưng có thể bạn đã sai đấy.

Khi nhìn vào những hệ thống cao cấp này, nhà nghiên cứu H. D. Moore nhận thấy rằng hầu như tất cả đều mặc định tự động trả lời các cuộc gọi video đến. Điều này cũng hợp lý. Bạn đặt cuộc họp vào lúc 10:00 sáng và bạn muốn những người tham gia gọi đến. Tuy nhiên, điều đó cũng có nghĩa là vào một thời điểm khác trong ngày, bất kỳ ai biết số đó cũng có thể gọi đến và liếc trộm vào văn phòng của bạn.

“Sự phổ biến của các hệ thống hội nghị truyền hình trong các lĩnh vực đầu tư vốn mạo hiểm và tài chính tạo ra một nhóm nhỏ các mục tiêu có giá trị cao cho bất kỳ ai muốn thực hiện hoạt động gián điệp công nghệ hoặc có ý định chiếm lợi thế kinh doanh không công bằng.”

Việc tìm ra các hệ thống này có khó không? Hệ thống hội nghị sử dụng một giao thức riêng biệt là H.323. Vì vậy, Moore tìm trong một phần Internet và xác định được ra 250.000 hệ thống sử dụng giao thức đó. Từ con số trên, anh ước tính rằng trong số này, dưới 5.000 hệ thống đã được cấu hình để tự động trả lời, một tỉ lệ nhỏ trong tổng thể, nhưng bản thân nó vẫn là một con số rất lớn. Và đó là chưa tính đến phần còn lại của Internet.

Kẻ tấn công có thể lấy được gì từ việc xâm nhập một hệ thống như vậy? Camera hệ thống hội nghị nằm dưới sự kiểm soát của người dùng, vì vậy kẻ tấn công từ xa có thể điều chỉnh vị trí của nó theo chiều ngang, dọc, trái, hay phải. Trong hầu hết các trường hợp, camera không có đèn đỏ để báo hiệu nó đang ở chế

độ bật, vì vậy nếu không nhìn vào máy, bạn sẽ không biết được rằng có người đã di chuyển nó. Camera này cũng có thể phóng to. Moore cho biết nhóm nghiên cứu của anh đã có thể đọc một mật khẩu gồm sáu chữ số được đăng trên tường cách máy ảnh 20 mét. Họ cũng có thể đọc email trên một màn hình của người dùng trong phòng.

Lần tới khi bạn ở văn phòng, hãy xem xét những gì có thể được nhìn thấy từ máy quay hội nghị truyền hình. Có lẽ là sơ đồ tổ chức của bộ phận nằm trên tường. Có lẽ màn hình máy tính để bàn của bạn đối diện với phòng hội nghị. Có lẽ hình ảnh của gia đình bạn cũng nằm trong tầm nhìn. Đó là những gì một kẻ tấn công từ xa có thể nhìn thấy và có thể sử dụng chống lại công ty của bạn hoặc thậm chí là cá nhân bạn.

Một số nhà cung cấp hệ thống nhận thức được vấn đề này. Ví dụ, Polycom cung cấp một sách hướng dẫn tăng cường an ninh, và thậm chí hạn chế việc định vị lại máy ảnh. Tuy nhiên, đội IT thường không có thời gian để làm theo các hướng dẫn như thế, và họ thường không coi an ninh là một mối quan tâm. Có hàng nghìn hệ thống hội nghị trên Internet sử dụng cài đặt mặc định.

Các nhà nghiên cứu cũng phát hiện ra rằng các tường lửa của công ty không biết cách xử lý giao thức H.323. Họ đề xuất cho thiết bị này một địa chỉ Internet công cộng và thiết lập một quy tắc cho nó trong tường lửa của công ty.

Rủi ro lớn nhất là nhiều bảng điều khiển quản trị cho các hệ thống hội nghị này không được tích hợp chế độ bảo mật hoặc bảo mật kém. Trong một ví dụ, Moore và nhóm của anh đã có thể truy cập vào hệ thống của một công ty luật, trong đó có sổ địa chỉ, có thông tin phòng họp của một ngân hàng đầu tư nổi tiếng. Các nhà nghiên cứu đã mua một thiết bị hội nghị truyền hình đã qua sử dụng từ eBay, và khi được giao đến, trong ổ cứng của nó vẫn có dữ liệu cũ, bao gồm sổ địa chỉ trên, liệt kê hàng chục số máy cá nhân, trong đó nhiều số được cấu hình để tự động trả lời cuộc gọi đến từ Internet. Như với máy in cũ và máy photo, nếu nó có ổ đĩa cứng, bạn cần xóa dữ liệu khỏi thiết bị trước khi bán hoặc tặng

nó.

Trong công việc, đôi khi chúng ta được phân công phối hợp với một đồng nghiệp ở cách mình nửa vòng trái đất. Các file dữ liệu có thể được chia sẻ qua lại qua email của công ty, nhưng đôi khi các file quá lớn nên email không xử lý được. Vì thế, ngày càng có nhiều người sử dụng các dịch vụ chia sẻ file để gửi và nhận các file lớn.

Các dịch vụ dựa trên đám mây này an toàn đến mức nào? Tùy từng trường hợp.

Bốn hãng lớn – iCloud của Apple, Google Drive, OneDrive của Microsoft (trước đây là SkyDrive) và Dropbox – tất cả đều có cơ chế xác thực hai yếu tố. Điều đó có nghĩa là bạn sẽ nhận được một văn bản ngoài dải trên thiết bị di động có chứa mã truy cập để xác nhận danh tính của bạn. Và mặc dù tất cả bốn dịch vụ trên mã hóa dữ liệu trong khi file đang chuyển tiếp, nếu không muốn công ty hoặc NSA đọc được dữ liệu của mình, bạn vẫn phải mã hóa dữ liệu trước khi gửi dữ liệu.

Sự tương đồng chỉ dừng lại ở đó.

Xác thực hai yếu tố (2FA) là quan trọng, nhưng tôi vẫn có thể bỏ qua điều này bằng cách chiếm đoạt các tài khoản không sử dụng. Ví dụ, trong một dự án kiểm định an ninh gần đây, khách hàng của tôi đã thêm 2FA của Google vào website VPN của họ bằng các công cụ có sẵn công khai. Tôi có thể vào đó bằng cách lấy thông tin đăng nhập thư mục hoạt động cho người dùng không đăng ký sử dụng cổng VPN. Vì là người đầu tiên đăng nhập vào dịch vụ VPN, tôi đã được nhắc thiết lập 2FA bằng Google Authenticator. Nếu nhân viên này chưa bao giờ tự mình truy cập dịch vụ, thì kẻ tấn công lẽ ra còn sẽ tiếp tục truy cập vào đó.

Đối với dữ liệu ở trạng thái nghỉ, Dropbox sử dụng mã hóa AES 256 bit (loại mã hóa khá mạnh). Tuy nhiên, Dropbox giữ lại các khóa, vốn có thể cho phép thực hiện truy cập trái phép từ Dropbox hoặc từ cơ quan thực thi pháp luật. Google Drive và iCloud sử dụng mã hóa 128 bit yếu hơn nhiều cho dữ liệu nghỉ.

Mối quan tâm ở đây là dữ liệu có thể được giải mã bằng công suất tính toán mạnh. Microsoft OneDrive không bận tâm đến việc mã hóa, khiến người ta không khỏi nghi ngờ rằng đây là một quyết định có chủ ý, có thể là do áp lực từ một số chính phủ.

Google Drive mới công bố tính năng mới là quản lý quyền thông tin (information rights management – IRM). Ngoài các tài liệu, bảng tính, và bản trình bày được tạo trong Google Documents, Google Drive hiện cũng chấp nhận định dạng file PDF và các định dạng file khác. Các tính năng hữu ích bao gồm vô hiệu hóa khả năng tải xuống, in và sao chép cho người nhận xét và người xem. Bạn cũng có thể ngăn mọi người thêm người khác vào file được chia sẻ. Tất nhiên, các tính năng quản lý này chỉ có sẵn cho các chủ sở hữu file. Điều đó có nghĩa là nếu ai đó mời bạn chia sẻ file, người đó phải đặt ra các giới hạn về quyền riêng tư chứ không phải bạn.

Microsoft cũng giới thiệu một tính năng mã hóa theo từng file riêng biệt, tương tự như tính năng mã hóa từng file riêng lẻ bằng khóa riêng của chính file đó. Nếu một khóa bị xâm nhập, chỉ có file đó bị ảnh hưởng chứ không phải toàn bộ dữ liệu lưu trữ. Nhưng tính năng này không phải là mặc định, vì vậy người dùng sẽ phải tạo thói quen tự mã hóa từng file.

Điều này có vẻ như một đề nghị tốt xét về mặt tổng thể. Các nhân viên và người dùng nói chung nên quen với việc mã hóa dữ liệu trước khi gửi lên đám mây. Bằng cách đó, bạn giữ quyền kiểm soát các khóa. Nếu một cơ quan chính phủ đến gõ cửa Apple, Google, Dropbox hoặc Microsoft, các công ty này sẽ không thể giúp đỡ họ được, vì bạn sở hữu các khóa riêng lẻ.

Bạn cũng có thể sử dụng SpiderOak,một nhà cung cấp dịch vụ đám mây khác hẳn các dịch vụ còn lại. SpiderOak là nơi cung cấp đầy đủ các lợi ích của khả năng lưu trữ đám mây và tính năng đồng bộ hóa cùng với 100% sự riêng tư về dữ liệu. SpiderOak bảo vệ dữ liệu người dùng nhạy cảm thông qua xác thực mật khẩu hai yếu tố và mã hóa AES 256 bit để các file và mật khẩu luôn ở chế độ riêng tư. Người dùng có thể lưu trữ và đồng bộ hóa thông tin

nhạy cảm với sự riêng tư hoàn toàn, bởi vì dịch vụ đám mây này không biết mật khẩu và dữ liệu.

Nhưng hầu hết người dùng đều sẽ tiếp tục sử dụng các dịch vụ khác mặc cho những rủi ro mà họ phải gánh chịu. Chúng ta thích cái thuận tiện và dễ dàng của việc lấy dữ liệu từ đám mây, và các cơ quan thực thi pháp luật cũng vậy. Một mối quan tâm lớn về việc sử dụng đám mây là dữ liệu của bạn không có được sự bảo vệ từ Tu Chính án thứ Tư như đối với dữ liệu được lưu trữ trong ngăn kéo bàn hoặc thậm chí trên máy tính để bàn. Các cơ quan thực thi pháp luật ngày càng yêu cầu nhận được nhiều hơn các dữ liệu dựa trên đám mây (đây là điều đáng lo ngại). Và họ có thể dễ dàng lấy được quyền truy cập, vì mọi thứ bạn tải lên mạng – dù là dịch vụ webmail, Google Drive, hay Shutterfly – đều đi đến máy chủ thuộc về nhà cung cấp dịch vụ đám mây, không phải thuộc quyền sở hữu của bạn. Sự bảo vệ thực sự ở đây là phải hiểu rằng bất cứ thứ gì bạn đưa lên đám mây đều có thể bị người khác truy cập, theo đó bạn phải có biện pháp khắc phục là mã hóa tất cả trước khi tải lên.

Chương 14: ẨN DANH LÀ MỘT VIỆC KHÓ

Cách đây vài năm, trên chuyến đi từ Bogota, Colombia trở về Mỹ, và khi đến Atlanta, tôi đã được hai viên chức hải quan lặng lẽ hộ tống vào một căn phòng riêng. Vì đã từng bị bắt, cũng từng trải qua thời gian ngồi tù, nên tôi không có gì hốt hoảng lắm. Tuy vậy, điều này vẫn đáng lo ngại. Tôi không làm gì sai cả. Và tôi ở trong căn phòng đó suốt bốn tiếng, trong khi thời hạn giữ người mà không có lệnh bắt giữ là chín tiếng.

Sự cố bắt đầu khi một nhân viên Hải quan quét hộ chiếu của tôi rồi nhìn chằm chằm vào màn hình. "Kevin," anh này vừa cười toét miệng vừa nói. "Đoán xem có chuyện gì nào? Một số người ở tầng dưới muốn nói chuyện với anh. Nhưng đừng lo lắng. Mọi thứ sẽ ổn thôi."

Trước đó, tôi tới Bogota để thuyết trình theo nguồn tài trợ của tờ El Tiempo, đồng thời cũng ghé thăm bạn gái. Trong lúc ngồi chờ trong căn phòng ở tầng dưới, tôi gọi cho cô bạn gái lúc này đang ở Bogota và được biết cảnh sát ở Colombia đã gọi và yêu cầu khám xét một gói hàng mà tôi đã đặt vào trong một thùng chuyển phát nhanh của FedEx để gửi đến Mỹ. "Họ tìm thấy dấu vết của cocaine," cô ấy nói. Tôi đã biết là không phải như vậy.

Gói hàng chứa một chiếc ổ cứng gắn trong cỡ 4 xăng-ti-mét. Rõ ràng là các nhà chức trách Colombia, hoặc có thể Mỹ, muốn kiểm tra nội dung của ổ đĩa, vốn đã được mã hóa. Cocaine là một cái cớ để họ mở gói hàng. Tôi không bao giờ lấy lại được chiếc ổ cứng của mình.

Sau đó tôi biết được rằng cảnh sát đã xé rách hộp, tháo thiết bị điện tử ra từng mảnh, sau đó phá hủy ổ cứng của tôi trong lúc loay hoay mở thiết bị đó bằng cách khoan một lỗ để dò tìm cocaine. Lẽ ra họ nên dùng loại tuốc-nơ-vít chuyên dụng để mở ổ đĩa. Họ không tìm thấy bất kỳ loại ma túy nào.

Trong khi đó, tại Atlanta, các quan chức đã mở hành lý của tôi và tìm thấy chiếc MacBook Pro, một chiếc máy tính xách tay Dell XPS M1210, một chiếc máy tính xách tay Asus 900, ba hoặc bốn ổ cứng, nhiều thiết bị lưu trữ USB, một số thiết bị Bluetooth, ba chiếc iPhone và bốn chiếc điện thoại di động Nokia (mỗi chiếc có thẻ SIM riêng, vì vậy tôi có thể tránh được phí chuyển vùng trong khi gọi ở các quốc gia khác nhau). Đây là những công cụ tiêu chuẩn trong nghề của tôi.

Cũng trong hành lý của tôi còn có bộ đồ phá khóa và một thiết bị nhân bản có thể đọc và phát lại bất kỳ thẻ HID lân cận nào. Thiết bị nhân bản có thể được sử dụng để lấy thông tin đăng nhập lưu trữ trên thẻ truy cập bằng cách đặt nó ở gần chúng. Ví dụ, tôi có thể giả mạo thông tin thẻ của một người để truy cập các hệ thống mà không phải tạo thẻ giả. Tôi có những thứ này bởi vì tôi đã thực hiện một bài thuyết trình quan trọng về an ninh ở Bogota. Đương nhiên, mắt của các nhân viên hải quan sáng rực lên khi họ nhìn thấy chúng, họ nghĩ tôi có ý đồ gì – ví dụ như quét trộm thẻ tín dụng chẳng hạn, chỉ có điều các thiết bị này không thể làm được việc đó.

Cuối cùng, các nhân viên của Cục Di Trú và Hải quan Mỹ (ICE) xuất hiện và hỏi tại sao tôi ở Atlanta. Tôi đến đó để điều hành một hội đồng tại một hội nghị an ninh do Hiệp hội An ninh Công nghiệp Mỹ (ASIS) bảo trợ. Sau đó, một đặc vụ FBI thuộc hội đồng trên đứng ra xác nhận lý do cho chuyến đi của tôi.

Mọi chuyện dường như trở nên tồi tệ hơn khi tôi mở máy tính xách tay và đăng nhập để cho họ thấy email xác nhận tôi sẽ tham gia vào hội đồng.

Trình duyệt của tôi được đặt ở chế độ tự động xóa lịch sử khi máy khởi động, vì vậy khi máy bật lên, tôi được nhắc xóa lịch sử. Thấy tôi xác nhận và nhấp vào nút OK, các đặc vụ không giấu nổi sự hoảng hốt. Nhưng sau đó, tôi chỉ nhấn nút nguồn để tắt MacBook, vì vậy ổ đĩa của tôi không thể truy cập được nếu không có cụm mật khẩu PGP.

Tôi không phải giao mật khẩu của mình, trừ khi bị bắt – nhưng tất cả đều trấn an tôi rằng trường hợp này sẽ không xảy ra. Ngay cả khi bị bắt, theo luật pháp Mỹ, tôi cũng không phải giao mật khẩu của mình, nhưng liệu quyền đó có được bảo vệ hay không phụ thuộc vào thái độ sẵn sàng tranh đấu của chúng ta. Và các quốc gia khác nhau có quy định khác nhau về điều này. Ví dụ, ở Anh và Canada, các nhà chức trách có thể buộc bạn phải tiết lộ mật khẩu của mình.

Sau bốn giờ, cả ICE và các nhân viên hải quan đều cho tôi đi. Tuy nhiên, nếu tôi bị một cơ quan như NSA nhắm vào, khả năng cao là họ sẽ tìm hiểu được nội dung trong ổ cứng của tôi. Các cơ quan chính phủ có thể xâm nhập phần mềm trong máy tính hoặc điện thoại di động của bạn, làm hư hại mạng bạn sử dụng để kết nối với Internet, và khai thác nhiều lỗ hổng khác nhau được tìm thấy trong các thiết bị của bạn.

Tôi có thể đi tới các nước có quy định thậm chí còn nghiêm ngặt hơn và không gặp phải các vấn đề như đã gặp ở Mỹ vì ở đây tôi có tiền án tiền sự. Vậy bạn có thể mang dữ liệu nhạy cảm ra nước ngoài bằng cách nào? Và bạn có thể đi tới những quốc gia kém thân thiện như Trung Quốc?

Nếu không muốn ổ cứng có bất kỳ dữ liệu nhạy cảm nào, bạn có các phương án sau:

1. Dọn sạch mọi dữ liệu nhạy cảm trước khi đi và thực hiện sao lưu đầy đủ.

2. Để dữ liệu ở đó nhưng mã hóa bằng một khóa mạnh (nhưng một số quốc gia có thể buộc bạn tiết lộ khóa hoặc mật khẩu). Đừng giữ cụm từ mật khẩu bên người; bạn có thể cung cấp một nửa cụm từ mật khẩu cho một người bạn ở ngoài lãnh thổ Mỹ, người không thể bị buộc phải giao nộp mật khẩu đó.

3. Tải dữ liệu mã hóa lên dịch vụ đám mây, sau đó tải xuống và tải lên khi cần.

4. Sử dụng một sản phẩm miễn phí như VeraCrypt để tạo thư

mục file mã hóa ẩn trên ổ cứng. Một lần nữa, nếu một chính phủ nước ngoài tìm thấy thư mục file ẩn, họ có thể buộc bạn phải tiết lộ mật khẩu.

5. Bất cứ khi nào nhập mật khẩu vào thiết bị, hãy dùng áo khoác hoặc thứ quần áo nào đó để ngăn chặn sự giám sát của camera.

6. Niêm phong máy tính xách tay và các thiết bị khác trong FedEx hoặc phong bì Tyvek khác và ký tên vào đó, sau đó đặt nó trong két an toàn của phòng khách sạn. Nếu phong bì bị lục lọi, bạn sẽ nhận ra điều đó. Cũng xin lưu ý rằng két an toàn của khách sạn không thực sự an toàn. Bạn nên cân nhắc việc mua một thiết bị camera đặt bên trong két để chụp ảnh người mở két và gửi ảnh qua di động theo thời gian thực.

7. Tốt nhất là đừng chuốc lấy bất kỳ rủi ro nào. Hãy luôn mang theo thiết bị của bạn mọi lúc và đừng để nó ra khỏi tầm nhìn của bạn.

Theo các tài liệu do Liên đoàn Tự do Dân sự Mỹ lấy được thông qua Đạo luật Tự do Thông tin trong thời gian từ tháng 10 năm 2008 đến tháng 6 năm 2010, hơn 6.500 khách du lịch đến và đi khỏi Mỹ bị kiểm tra thiết bị điện tử ở biên giới. Đây là mức trung bình trong hơn 300 lần kiểm tra thiết bị điện tử ở biên giới mỗi tháng. Và gần một nửa số khách du lịch đó là công dân Mỹ.

Thực tế ít được biết đến: Thiết bị điện tử của tất cả mọi người đều có thể bị kiểm tra mà không cần lệnh của tòa án hay có nghi ngờ hợp lý trong vòng 100 km theo đường chim bay tính từ biên giới Mỹ, trong đó có khả năng bao gồm San Diego. Như vậy, vượt ra khỏi đường biên giới không có nghĩa là bạn đã được an toàn!

Hai cơ quan chịu trách nhiệm chính trong việc kiểm tra khách du lịch và các mặt hàng vào Mỹ là Cục Hải quan và Bảo vệ Biên giới (CBP) và Cục Di Trú và Hải quan (ICE) của Bộ An ninh Nội địa. Trong năm 2008, Bộ An ninh Nội địa đã thông báo rằng họ có thể kiểm tra bất kỳ thiết bị điện tử nào vào Mỹ. Cơ quan này cũng sử dụng Hệ thống Nhắm mục tiêu Tự động (ATS) độc quyền để tạo ra hồ sơ cá nhân tức thời rất chi tiết về bạn bất cứ khi nào bạn di

chuyển trong phạm vi quốc tế. Các nhân viên CBP sử dụng file ATS của bạn để quyết định xem có nên thực hiện kiểm tra tăng cường đối với bạn khi bạn quay lại Mỹ hay không.

Chính phủ Mỹ có thể thu giữ thiết bị điện tử, kiểm tra tất cả các file, và giữ nó để xem xét kỹ lưỡng hơn mà không có bằng chứng nào cho thấy bạn làm điều gì sai. Nhân viên CBP có thể kiểm tra thiết bị của bạn, sao chép nội dung trong đó, phục hồi hình ảnh và video.

Vì vậy, tôi đã đối phó như sau.

Để bảo vệ quyền riêng tư của mình và cho khách hàng, tôi mã hóa dữ liệu bí mật trên các máy tính xách tay của mình. Khi ở nước ngoài, tôi truyền các tệp được mã hóa qua Internet để lưu trữ trên các máy chủ bảo mật ở bất cứ đâu trên thế giới. Sau đó, trước khi về Mỹ, tôi tẩy chúng khỏi máy tính, đề phòng trường hợp các quan chức chính phủ muốn kiểm tra hoặc tịch thu thiết bị của mình.

Tẩy dữ liệu khác với xóa dữ liệu. Xóa dữ liệu chỉ thay đổi mục nhập bản ghi khởi động chính cho một file (chỉ mục được sử dụng để tìm các phần của file trên ổ cứng); các file (hoặc một số phần của nó) vẫn còn trên ổ cứng cho đến khi dữ liệu mới được ghi trên phần đó của ổ cứng. Đây là cách các chuyên gia pháp y số có thể tái tạo dữ liệu đã bị xóa.

Ngược lại, tẩy là ghi đè dữ liệu trong file một cách an toàn bằng dữ liệu ngẫu nhiên. Trên ổ cứng, việc tẩy rất khó khăn, vì vậy tôi mang theo một chiếc máy tính xách tay có ổ cứng thông thường và tẩy ít nhất 35 lần. Phần mềm băm file thực hiện điều này bằng cách ghi đè dữ liệu ngẫu nhiên hàng trăm lần trong mỗi lần ghi đè một file đã xóa, khiến cho việc phục hồi dữ liệu đó trở nên khó khăn đối với bất cứ ai.

Tôi thường tạo một bản sao lưu hình ảnh đầy đủ các thiết bị của mình vào một ổ cứng gắn ngoài và mã hóa nó. Sau đó, tôi sẽ gửi ổ đĩa dự phòng về Mỹ. Cho đến khi đồng nghiệp xác nhận đã nhận được ổ cứng trong tình trạng đọc được, tôi mới thực hiện tẩy dữ

liệu ở máy của mình. Sau đó, tôi sẽ tẩy sạch tất cả các file cá nhân và file khách một cách an toàn. Tôi không định dạng toàn bộ ổ đĩa và sẽ để nguyên hệ điều hành. Bằng cách đó, nếu tôi bị lục soát, việc khôi phục lại các file từ xa sẽ dễ dàng hơn mà không cần phải cài đặt lại toàn bộ hệ điều hành.

Kể từ sự cố ở Atlanta, tôi đã thay đổi giao thức của mình một chút. Tôi để một "bản sao" cập nhật của tất cả các máy tính du lịch của mình ở chỗ một đồng nghiệp. Sau đó, nếu cần, anh này chỉ việc gửi các hệ thống nhân bản cho tôi ở bất cứ đâu tại Mỹ.

iPhone là một vấn đề khác. Nếu bạn kết nối iPhone với máy tính xách tay của bạn để sạc, và bạn nhấp vào nút "Trust" (Tin tưởng) khi thiết bị hiển thị câu hỏi "Trust This Computer" (Tin tưởng máy tính này), một chứng chỉ theo cặp sẽ được lưu trữ trên máy tính, cho phép máy tính truy cập toàn bộ nội dung của iPhone mà không cần phải biết mật khẩu. Chứng chỉ theo cặp sẽ được sử dụng bất cứ khi nào chiếc iPhone trên được kết nối với máy tính đó.

Ví dụ, nếu bạn cắm iPhone vào máy tính của người khác và chọn "tin tưởng" nó, một mối quan hệ đáng tin cậy sẽ được thiết lập giữa máy tính và thiết bị iOS này, cho phép máy tính truy cập ảnh, video, tin nhắn SMS, nhật ký cuộc gọi, tin nhắn WhatsApp, và hầu hết những thứ khác mà không cần mật khẩu. Thậm chí đáng ngại hơn, người đó chỉ cần tạo bản sao lưu iTunes cho toàn bộ điện thoại của bạn, trừ khi trước đó bạn đã đặt mật khẩu cho các bản sao lưu iTunes mã hóa (đây là một ý tưởng hay). Nếu bạn không đặt mật khẩu, kẻ tấn công có thể đặt mật khẩu cho bạn và dễ dàng sao lưu thiết bị di động của bạn vào máy tính của hắn mà bạn không biết.

Điều đó có nghĩa là nếu cơ quan thực thi pháp luật muốn xem những gì có trên chiếc iPhone được bảo vệ bằng mật khẩu của bạn, họ có thể thực hiện việc này dễ dàng bằng cách kết nối nó với máy tính xách tay của bạn, vì nó có nhiều khả năng có chứng chỉ theo cặp hợp lệ với điện thoại đó. Quy tắc là: không bao giờ "Tin tưởng máy tính này" trừ khi đó là hệ thống cá nhân của bạn.

Điều gì sẽ xảy ra nếu bạn muốn thu hồi toàn bộ các chứng chỉ theo cặp trên các thiết bị Apple? Tin vui là bạn có thể đặt lại chứng chỉ theo cặp. Nếu cần chia sẻ file và bạn đang sử dụng một sản phẩm Apple, hãy dùng AirDrop. Và nếu bạn cần sạc điện thoại, hãy sử dụng cáp sét cắm vào hệ thống của bạn hoặc ổ cắm điện, chứ không phải vào máy tính của người khác. Hoặc bạn có thể mua bao cao su USB trên syncstop.com để có thể yên tâm cắm vào bất kỳ bộ sạc USB hoặc máy tính nào.

Nếu như trong quá trình di chuyển, bạn chỉ mang theo iPhone chứ không có máy tính thì sao?

Tôi đã bật chế độ Touch ID trên iPhone để nó nhận dạng vân tay của tôi. Tôi chỉ cần khởi động lại iPhone trước khi đến gần trạm kiểm soát nhập cư ở bất kỳ quốc gia nào. Và khi bật thiết bị lên, tôi cố tình không nhập mật khẩu. Mặc dù tôi đã bật Touch ID, nhưng tính năng đó được tắt theo mặc định cho đến khi tôi nhập mật khẩu lần đầu tiên. Các tòa án ở Mỹ nêu rõ rằng các cơ quan thực thi pháp luật không được phép yêu cầu bạn cung cấp mật khẩu. Theo truyền thống, ở Mỹ, bạn không bị ép phải đưa ra bằng chứng chứng thực; tuy nhiên, bạn có thể bị buộc phải giao nộp khóa vật lý của một két an toàn. Như vậy, tòa án có thể buộc bạn phải cung cấp vân tay để mở khóa thiết bị. Giải pháp đơn giản: khởi động lại điện thoại. Bằng cách đó, vân tay của bạn sẽ không được kích hoạt và bạn sẽ không phải giao mật khẩu.

Tuy nhiên, ở Canada, đó là luật; nếu là công dân Canada, bạn phải cung cấp mật khẩu khi được yêu cầu. Điều này xảy ra với Alain Philippon, một người ở Sainte-Anne-des-Plaines, Quebec. Khi từ Puerto Plata, Cộng hòa Dominica trở về, anh từ chối cung cấp cho các nhà chức trách biên giới ở Nova Scotia mật khẩu của điện thoại di động. Anh bị buộc tội theo mục 153.1 (b) của Đạo luật Hải quan Canada vì cản trở hoặc ngăn cản các nhà chức trách biên giới thực hiện vai trò của họ. Hình phạt nếu bạn bị kết tội là 1.000 đô-la, với mức phạt tối đa là 25.000 đô-la và khả năng bị tù một năm.

Đích thân tôi đã được trải nghiệm về luật mật khẩu của Canada.

Năm 2015, tôi thuê một dịch vụ xe hơi như Uber để đi từ Chicago đến Toronto, và khi ngang qua biên giới từ Michigan vào Canada, chúng tôi bị gửi đến một địa điểm kiểm tra phụ. Có lẽ đó là vì lái xe là người Trung Đông chỉ có một chiếc thẻ xanh. Ngay sau khi đến địa điểm kia, chúng tôi bị kiểm tra hệt như trong phim tình báo.

Một nhóm nhân viên hải quan giám sát để bảm đảm rằng chúng tôi đã để mọi hành lý trong xe, bao gồm cả điện thoại di động, và ra khỏi xe người không. Chúng tôi bị tách ra. Một nhân viên đi đến phía ghế tài xế trong chiếc xe và rút điện thoại di động của anh ra khỏi giá. Nhân viên này hỏi mật khẩu rồi kiểm tra chiếc điện thoại.

Trước đó, tôi đã tự nhủ rằng sẽ không bao giờ tiết lộ mật khẩu của mình. Lúc này, tôi phải đứng trước sự lựa chọn giữa việc cung cấp mật khẩu và việc được phép nhập cảnh vào Canada để thực hiện buổi thuyết trình. Vì vậy, tôi quyết định sử dụng một chút kỹ thuật social engineering.

Tôi gọi to nhân viên hải quan đang kiểm tra trên điện thoại của người lái xe. “Này – cô sẽ không tìm trong vali của tôi, đúng không? Nó bị khóa rồi nên cô không thể làm gì được đâu.” Điều này ngay lập tức thu hút sự chú ý của cô ta. Cô ta nói họ có quyền lục soát vali của tôi.

Tôi trả lời, “Tôi khóa rồi, các vị không động vào nó được đâu.”

Hai nhân viên bước ngay đến chỗ tôi và yêu cầu chìa khóa. Tôi vặn vẹo hỏi lý do, và một lần nữa, họ nói họ có quyền kiểm tra mọi thứ. Tôi rút ví ra và đưa cho nhân viên chìa khóa mở vali.

Thế là đủ. Họ hoàn toàn quên mất hai chiếc điện thoại di động và tập trung vào vali của tôi. Nhiệm vụ được hoàn thành thông qua mẹo đánh lạc hướng. Tôi đã được cho đi và, may mắn thay, không bị hỏi mật khẩu điện thoại.

Trong tâm trạng rối bời khi bị lục soát, bạn sẽ rất dễ bị phân tâm. Nhưng đừng để bản thân trở thành nạn nhân của hoàn cảnh. Khi

đi qua bất kỳ chốt an ninh nào, hãy làm sao để máy tính xách tay và thiết bị điện tử của bạn là các thiết bị cuối cùng trên băng chuyền tải đồ đạc. Không ai muốn máy tính xách tay của mình nằm ở đầu bên kia trong khi phía trước đang có người chắn đường cả. Ngoài ra, nếu bạn phải bước ra khỏi hàng, hãy mang theo cả máy tính xách tay và thiết bị điện tử.

Những sự bảo vệ quyền riêng tư mà chúng ta có được ở nhà không chắc sẽ áp dụng cho các du khách ở biên giới Mỹ. Đối với giới bác sĩ, luật sư và chuyên gia kinh doanh, hoạt động kiểm tra quá mức ở biên giới có thể làm tổn hại đến sự bảo mật của các thông tin nghề nghiệp nhạy cảm, bao gồm các bí mật thương mại, thông tin liên lạc giữa luật sư với thân chủ và bác sĩ với bệnh nhân, các tài liệu nghiên cứu và chiến lược kinh doanh, trong đó có một số thông tin mà du khách có nghĩa vụ phải bảo vệ đến cùng theo quy định của pháp luật hoặc theo các quy định trong hợp đồng mà họ đã ký.

Đối với phần còn lại trong chúng ta, hoạt động lục soát trên ổ cứng và thiết bị di động có thể tiết lộ email, thông tin sức khỏe, và thậm chí cả hồ sơ tài chính. Nếu gần đây bạn đã đi đến một số quốc gia được coi là không thân thiện với lợi ích của Mỹ, hãy lưu ý rằng điều này có thể khiến hải quan thực hiện các biện pháp kiểm tra tăng cường.

Các chính phủ chuyên chế đưa ra một thách thức khác. Họ có thể một mực yêu cầu phải lục soát cho bằng được các thiết bị điện tử của bạn – đọc email và kiểm tra thư mục tải về của bạn. Ngoài ra, còn có khả năng, đặc biệt là trong trường hợp họ lấy máy tính xách tay của bạn, họ có thể cài đặt phần mềm theo dõi trên đó.

Nhiều công ty cung cấp điện thoại ẩn danh và thuê máy tính cho nhân viên đi công tác nước ngoài. Các thiết bị này sẽ bị vứt bỏ hoặc tẩy sạch khi nhân viên trở về Mỹ. Nhưng đối với hầu hết chúng ta, việc tải các file mã hóa lên đám mây hoặc mua một thiết bị mới rồi vứt đi khi trở về không phải là các lựa chọn thực tế.

Nhìn chung, đừng mang theo các thiết bị điện tử lưu trữ thông tin nhạy cảm trừ khi thực sự cần. Nếu buộc phải làm thế, chỉ mang ở mức tối thiểu nhất. Và nếu cần tới điện thoại di động, hãy cân nhắc việc sử dụng điện thoại ẩn danh. Đặc biệt là khi cước chuyển vùng thoại và dữ liệu quá cao. Tốt hơn là mang theo một chiếc điện thoại ẩn danh đã mở khóa và mua thẻ SIM ở quốc gia bạn đang ghé đến.

Bạn có thể nghĩ rằng việc đi qua cửa hải quan là phần ác mộng nhất trong bất kỳ chuyến đi nào. Nhưng có thể không phải như vậy. Phòng khách sạn của bạn cũng có thể bị lục soát.

Năm 2008, tôi có một số chuyến đi đến Colombia. Vào một trong những chuyến đi dịp cuối năm đó, một vài điều kỳ lạ đã xảy ra trong phòng khách sạn của tôi ở Bogota. Và đây không phải là một khách sạn đáng ngờ, vì nó vốn thường xuyên được các quan chức Colombia ở lại.

Có lẽ đó là vấn đề.

Sau khi cùng bạn gái đi ăn tối về, tôi cắm chìa khóa phòng vào cửa thì khóa hiển thị màu vàng. Không phải màu xanh. Không phải màu đỏ. Màu vàng thường có nghĩa là cửa bị khóa từ bên trong.

Tôi đi xuống quầy lễ tân nhờ họ cấp cho một thẻ chìa khóa mới. Một lần nữa, khóa hiển thị màu vàng. Tôi thử lại lần nữa. Vẫn thế. Sau lần thứ ba, tôi nhờ khách sạn cho người tới giúp. Cánh cửa mở ra.

Bên trong không có gì bất thường. Thực ra lúc đó, tôi đã phấn khởi vì vấn đề hóa ra chỉ là do khóa hỏng. Phải đến khi trở về Mỹ, tôi mới nhận thức được điều gì đã xảy ra.

Trước khi rời Mỹ, tôi gọi cho cô bạn gái cũ Darci Wood, từng là kỹ thuật viên trưởng tại TechTV, nhờ cô ấy đến nhà để thay ổ đĩa cứng trong chiếc máy tính xách tay MacBook Pro. Thời đó, các ổ đĩa cứng MacBook Pro không hề dễ tháo, nhưng cô ấy vẫn làm được. Cô đặt vào đó một ổ đĩa mới mà tôi phải định dạng và cài

đặt hệ điều hành OSX.

Vài tuần sau, khi từ Colombia trở về, tôi nhờ Darci đến nhà tôi ở Las Vegas để đổi lại ổ đĩa.

Ngay lập tức, cô ấy nhận thấy có điều gì đó khác thường. Darci nói có người đã siết các vít ổ cứng chặt hơn cô ấy siết. Rõ ràng một người nào đó ở Bogota đã tháo ổ đĩa, có lẽ để tạo ra một bản sao hình ảnh của nó trong lúc tôi không có trong phòng.

Gần đây hơn, chuyện này cũng xảy ra với Stefan Esser, một nhà nghiên cứu nổi tiếng về việc bẻ khóa các sản phẩm iOS. Anh đã đăng tải trên Twitter hình ảnh chiếc ổ đĩa cứng được gắn lại một cách sơ sài.

Ngay cả một ổ đĩa với rất ít dữ liệu cũng có một số dữ liệu trên đó. May thay, tôi đã sử dụng tính năng mã hóa toàn bộ ổ đĩa PGP của Symantec. (Bạn cũng có thể sử dụng WinMagic cho Windows hoặc FileVault 2 cho OSX). Vì vậy, bản sao ổ đĩa cứng của tôi sẽ là vô giá trị trừ khi kẻ trộm có thể lấy được chìa khóa để mở. Chính vì những gì tôi nghĩ đã xảy ra ở Bogota mà giờ đây đi đâu tôi cũng mang theo máy tính xách tay, kể cả lúc ăn tối. Nếu buộc phải để lại, thì tôi không bao giờ để nó ở chế độ ngủ đông mà tắt hẳn đi. Nếu không, kẻ tấn công có thể kết xuất bộ nhớ và lấy khóa mã hóa PGP.

Ở phần đầu sách, tôi đã nói về nhiều biện pháp phòng ngừa mà Edward Snowden đã thực hiện để liên lạc an toàn với Laura Poitras. Tuy nhiên, khi bộ nhớ đệm dữ liệu bí mật của Snowden đã sẵn sàng được phát hành ra công chúng, anh và Poitras cần một nơi để lưu trữ nó. Các hệ điều hành phổ biến nhất – Windows, iOS, Android và thậm chí cả Linux – đều có những lỗ hổng. Tất cả các phần mềm đều có lỗ hổng. Vì vậy, họ cần một hệ điều hành an toàn, một hệ điều hành được mã hóa từ ngày đầu tiên và yêu cầu một chìa khóa để mở khóa nó.

Việc mã hóa ổ cứng hoạt động như sau: khi khởi động máy tính, bạn nhập mật khẩu an toàn hoặc cụm từ mật khẩu như “Chúng tôi không cần giáo dục” (trong bài hát nổi tiếng của Pink Floyd).

Sau đó, hệ điều hành khởi động và bạn có thể truy cập file và thực hiện các tác vụ mà không nhận thấy bất kỳ sự chậm trễ nào do trình điều khiển thực hiện các tác vụ mã hóa một cách minh bạch và nhanh chóng. Tuy nhiên, điều này tạo ra khả năng là nếu bạn đứng dậy và rời khỏi thiết bị, dù là trong giây lát, ai đó có thể truy cập các file của bạn (vì chúng được mở khóa). Điều quan trọng cần nhớ là trong khi ổ cứng mã hóa được mở, bạn cần phải thận trọng để giữ cho nó an toàn. Ngay sau khi bạn tắt, khóa mã hóa không còn khả dụng với hệ điều hành: nghĩa là, nó đã gỡ khóa khỏi bộ nhớ để dữ liệu trên ổ đĩa không còn truy cập được.

Tails là một hệ điều hành có thể được khởi động trên bất kỳ máy tính hiện đại nào nhằm tránh để lại các dữ liệu có thể phục hồi trên ổ đĩa cứng, đặc biệt là ổ cứng chống ghi. Tải Tails lên đĩa DVD hoặc ổ USB, sau đó đặt phần mềm BIOS hoặc trình tự khởi động ban đầu EFI (OSX) cho DVD hoặc USB để khởi động phiên bản Tails. Khi bạn khởi động, Tails sẽ khởi động hệ điều hành với một số công cụ bảo mật, bao gồm cả trình duyệt Tor. Các công cụ bảo mật cho phép bạn mã hóa email bằng PGP, mã hóa USB và ổ đĩa cứng, đồng thời bảo mật email bằng OTR.

Nếu bạn muốn mã hóa các file riêng lẻ thay vì toàn bộ ổ cứng của mình, có một số lựa chọn. TrueCrypt, một phương án miễn phí, vẫn tồn tại nhưng không còn được duy trì và không cung cấp mã hóa toàn bộ đĩa. Bởi vì nó không còn được duy trì, các lỗ hổng mới sẽ không được giải quyết. Nếu bạn tiếp tục sử dụng TrueCrypt, hãy lưu ý những rủi ro. Một tùy chọn thay thế cho TrueCrypt 7.1a là VeraCrypt, đó là sự tiếp nối của dự án TrueCrypt.

Cũng có một số chương trình mất phí. Một trong những chương trình nổi bật là Windows BitLocker, thường không được bao gồm trong các phiên bản home của hệ điều hành Windows. Nếu được cài đặt BitLocker, để kích hoạt chương trình này, hãy mở File Explorer, nhấp chuột phải vào ổ C và cuộn xuống tùy chọn “Turn on BitLocker” (Bật BitLocker). BitLocker tận dụng lợi thế của một chip đặc biệt trên bo mạch chủ của bạn được biết đến như một mô-đun nền tảng đáng tin cậy, gọi tắt là TPM. Nó được thiết kế để

mở khóa mã hóa chỉ sau khi xác nhận rằng chương trình bộ nạp khởi động của bạn chưa bị sửa đổi. Đây là một sự bảo vệ hoàn hảo chống lại những cuộc tấn công ác ý (tôi sẽ mô tả ngắn gọn về nó ở phần sau). Bạn có thể đặt BitLocker để mở khóa khi bật hoặc chỉ khi có mã PIN hoặc USB đặc biệt mà bạn cung cấp. Các lựa chọn mã PIN hoặc USB an toàn hơn nhiều. Bạn cũng có tùy chọn lưu khóa vào tài khoản Microsoft. Đừng làm điều đó, bởi vì nếu bạn làm như vậy, ít hay nhiều bạn sẽ giao cho Microsoft các chìa khóa của bạn (như bạn sẽ thấy, điều này có thể xảy ra).

Có một số vấn đề với BitLocker. Đầu tiên, nó sử dụng một bộ tạo chuỗi số giả ngẫu nhiên (pseudorandomnumber generator – PRNG) gọi là Dual_EC_DRBG, viết tắt của bộ tạo bit tất định ngẫu nhiên đường cong elíp kép, điều này có thể chứa một cánh cửa hậu cho NSA. Nó cũng thuộc sở hữu tư nhân, nghĩa là bạn chỉ có thể tin vào lời hứa của Microsoft rằng nó hoạt động và nó không có bất kỳ cửa hậu nào cho NSA – điều này sẽ không xảy ra với những phần mềm nguồn mở. Một vấn đề khác với BitLocker là bạn phải chia sẻ khóa với Microsoft trừ khi bạn mua với giá 250 đô-la. Nếu không, cơ quan thực thi pháp luật có thể đòi khóa từ Microsoft.

Bất chấp các hạn chế này, Tổ chức Biên giới Điện tử vẫn khuyên những người tiêu dùng bình thường nên sử dụng BitLocker nếu họ muốn bảo vệ dữ liệu. Tuy nhiên, hãy lưu ý rằng cũng có một cách để bỏ qua BitLocker.

Một phương án thương mại khác là PGP Whole Disk Encryption (mã hóa toàn bộ ổ đĩa) của Symantec. Rất nhiều trường đại học cũng như doanh nghiệp sử dụng sản phẩm này. Tôi cũng từng sử dụng nó. PGP Whole Disk Encryption do Phil Zimmermann tạo ra, đây cũng là người đã tạo PGP cho email. Giống như BitLocker, PGP có thể hỗ trợ chip TPM để cung cấp xác thực bổ sung khi bạn bật máy tính cá nhân của mình. Một bản quyền vĩnh viễn được bán với giá khoảng 200 đô-la.

Ngoài ra còn có WinMagic, một trong số ít phương thức yêu cầu xác thực hai yếu tố thay vì chỉ một mật khẩu. WinMagic cũng

không dựa vào mật khẩu chủ. Thay vào đó, các tệp được mã hóa được nhóm lại và mỗi nhóm có một mật khẩu. Điều này có thể khiến cho việc khôi phục mật khẩu trở nên khó hơn, vì vậy nó có thể không phù hợp với mọi người.

Và đối với Apple có FileVault 2. Sau khi cài đặt, bạn có thể kích hoạt FileVault 2 bằng cách mở System Preferences (Tùy chọn Hệ thống), nhấp vào biểu tượng "Security and Privacy" (Bảo mật & Riêng tư) và chuyển sang tab FileVault. Một lần nữa, đừng lưu khóa mã hóa vào tài khoản Apple. Điều này có thể cung cấp cho Apple quyền truy cập vào nó, mà họ theo đó có thể cung cấp cho bên thực thi pháp luật. Thay vào đó, hãy chọn "Create a recovery key and do not use my iCloud account" (Tạo chìa khóa khôi phục và không sử dụng tài khoản iCloud của tôi), sau đó in ra hoặc chép lại chìa khóa 24 ký tự này. Hãy bảo vệ khóa này, vì bất kỳ ai tìm thấy nó đều có thể mở khóa ổ cứng của bạn.

Nếu bạn có iOS 8 hoặc phiên bản mới hơn của hệ điều hành trên iPhone hoặc iPad, nội dung của nó sẽ được mã hóa tự động. Đi một bước xa hơn, Apple đã nói rằng chìa khóa tồn tại trên thiết bị, bên người dùng. Điều đó có nghĩa là chính phủ Mỹ không thể hỏi Apple về chìa khóa: nó là duy nhất cho từng và mọi thiết bị. Giám đốc FBI James Comey tuyên bố rằng rốt cuộc, mã hóa không thể phá vỡ không phải là một điều tốt. Trong một bài phát biểu, ông nói, "Những tên tội phạm tinh vi sẽ tìm đến để dựa vào những phương tiện tránh bị phát hiện. Và câu hỏi của tôi là, sẽ phải trả giá thế nào?" Điều đáng lo ngại ở đây là những thứ xấu xa sẽ bị bưng bít trong sự che chở của mã hóa.

Nỗi lo sợ tương tự đã trì hoãn vụ việc của tôi trong nhiều tháng khi tôi kiệt sức trong tù vào những năm 1990. Nhóm luật sư biện hộ của tôi muốn truy cập vào những phát hiện mà chính phủ dự định sử dụng để chống lại tôi trong phiên tòa. Chính phủ từ chối giao trả bất kỳ file mã hóa nào trừ khi tôi cung cấp khóa giải mã. Tôi đã từ chối. Đến lượt mình, tòa án đã từ chối yêu cầu chính phủ cung cấp thông tin bởi vì tôi không đưa cho họ chìa khóa.

Các thiết bị Android bắt đầu từ phiên bản 3.0 (Honeycomb) cũng

có thể được mã hóa. Hầu hết chúng ta chọn không làm như vậy. Từ Android 5.0 (Lollipop), ổ đĩa mã hóa là mặc định trên dòng Nexus của điện thoại Android nhưng là tùy chọn trên điện thoại của các nhà sản xuất khác, chẳng hạn như LG, Samsung, và các hãng khác. Nếu bạn chọn mã hóa điện thoại Android, hãy lưu ý rằng có thể mất tối đa một giờ để làm như vậy và thiết bị của bạn sẽ cần cắm sạc trong quá trình này. Được biết, mã hóa thiết bị di động không gây cản trở đáng kể hiệu suất, nhưng khi đã quyết định mã hóa, bạn không thể hoàn tác nó.

Trong bất kỳ chương trình mã hóa toàn bộ ổ lưu trữ nào, luôn tồn tại khả năng có cửa hậu. Tôi đã từng được một công ty thuê để kiểm tra sản phẩm USB cho phép người dùng lưu trữ các file trong vùng chứa được mã hóa. Trong quá trình phân tích mã, chúng tôi thấy rằng nhà phát triển đã đặt vào một cánh cửa hậu bí mật, chìa khóa để mở khóa hộp chứa mã hóa được chôn giấu ở một vị trí ngẫu nhiên trên ổ USB. Điều đó có nghĩa là bất cứ ai có kiến thức về vị trí của khóa có thể mở khóa dữ liệu được đã mã hóa bởi người dùng.

Tệ hơn nữa, các công ty không phải lúc nào cũng biết phải làm gì với thông tin này. Khi tôi hoàn thành phân tích bảo mật của mình về thiết bị USB được mã hóa, vị CEO của công ty trên đã gọi cho tôi và hỏi liệu ông ấy có nên để cửa hậu tồn tại hay không. Ông lo ngại rằng cơ quan thực thi pháp luật hoặc NSA có thể cần truy cập dữ liệu của người dùng. Thực tế điều ông cần phải hỏi đã nói lên nhiều điều.

Trong báo cáo nghe trộm năm 2014, chính phủ Mỹ cho hay rằng chỉ gặp 25 ổ cứng mã hóa trong tổng số 3.554 thiết bị mà cơ quan thực thi pháp luật đã kiểm tra để tìm bằng chứng. Và họ vẫn có thể giải mã 21/25 ổ đó. Vì vậy, mặc dù việc có mã hóa thường chỉ đủ để tránh một tên trộm thông thường truy cập dữ liệu của bạn, đối với một chính phủ chuyên nghiệp, điều này có thể không đặt ra nhiều thách thức.

Nhiều năm trước, nhà nghiên cứu Joanna Rutkowska đã viết về cuộc tấn công mà cô gọi là “evil mail attack” (cuộc tấn công của

người giúp việc tai ác). Giả sử có người để lại trong phòng khách sạn một máy tính xách tay đã tắt, có ổ đĩa cứng được mã hóa bằng mã hóa TrueCrypt hoặc PGP Whole Disk Encryption. (Tôi đã sử dụng PGP Whole Disk Encryption ở Bogota; tôi cũng tắt máy tính.) Kẻ xấu lẻn vào phòng và chèn một chiếc USB chứa bộ nạp khởi động độc hại. Sau đó, máy tính xách tay mục tiêu phải được khởi động từ USB để cài đặt bộ tải khởi động độc hại đánh cắp cụm mật khẩu của người dùng. Bây giờ, cái bẫy đã được đặt ra.

Một người dọn phòng, vốn có thể thường xuyên lui tới phòng khách sạn mà không bị nghi ngờ, sẽ là ứng cử viên tốt nhất để làm điều này – vì vậy là kiểu tấn công trên mới có tên là "người giúp việc tai ác." Một người giúp việc có thể trở lại hầu như bất kỳ phòng khách sạn nào vào ngày hôm sau và nhập vào một tổ hợp khóa bí mật để trích xuất cụm mật khẩu được lưu trữ bí mật trên đĩa. Bây giờ kẻ tấn công có thể nhập cụm từ mật khẩu và truy cập vào tất cả các file của bạn.

Tôi không biết liệu có ai làm thế với máy tính của mình ở Bogota hay không. Bản thân ổ đĩa cứng đã bị tháo ra và sau đó được thay thế bằng các vít vặn quá chặt. Dù bằng cách nào, may mắn thay, ổ đĩa không chứa thông tin thực sự.

Việc để thiết bị điện tử của bạn vào một két an toàn ở khách sạn thì sao? Nó có tốt hơn là để chúng bên ngoài hoặc giữ chúng trong vali hay không? Có, nhưng không tốt hơn nhiều. Khi tham dự một hội nghị Black Hat gần đây, tôi ở trong khách sạn Four Seasons ở Las Vegas. Tôi đã đặt 4.000 đô-la tiền mặt trong két an toàn với nhiều loại thẻ tín dụng và séc khác nhau. Một vài ngày sau, tôi rời đi và cố mở két an toàn nhưng không thành công. Tôi gọi cho an ninh và họ mở nó ra. Tôi ngay lập tức nhận thấy rằng tập các đồng tiền 100 đô-la đó đã mỏng hơn nhiều. Chỉ còn lại 2.000 đô-la. Vậy 2.000 đô-la khác đã đi đâu? An ninh khách sạn cũng chẳng biết gì. Một người bạn của tôi là chuyên gia kiểm định an ninh vật lý đã thử bẻ khóa két an toàn nhưng không được. Hôm nay, điều này vẫn là một bí ẩn. Trớ trêu thay, két an toàn lại được gọi là an toàn.

G DATA, một công ty chống virus của Đức, phát hiện ra rằng trong các phòng khách sạn nơi nhân viên nghiên cứu của họ ở lại, két an toàn thường được đặt mật khẩu mặc định là 0000. Trong trường hợp như vậy, bất kể bạn chọn mật khẩu cá nhân nào, bất kỳ ai biết mật khẩu mặc định cũng có thể tiếp cận đồ đạc giá trị của bạn bên trong. G DATA nói rằng những trường hợp thế này không được phát hiện hàng loạt, nhưng xảy ra rải rác trong nhiều năm.

Nếu kẻ tấn công không biết mật khẩu mặc định của két an toàn trong phòng khách sạn, hắn có thể thực hiện phương pháp vét cạn. Mặc dù người quản lý khách sạn được tin tưởng giao một thiết bị điện tử khẩn cấp cắm vào cổng USB và mở khóa két an toàn, kẻ trộm hiểu biết có thể chỉ cần tháo tấm trên mặt trước két an toàn và sử dụng thiết bị kỹ thuật số để mở khóa bên dưới. Hoặc hắn có thể ngắt mạch an toàn và thiết lập lại cài đặt ban đầu, sau đó nhập mã mới.

Nếu điều đó không khiến bạn quan tâm, hãy xem xét điều này. G DATA cũng thấy rằng các đầu đọc thẻ tín dụng trên két có thể bị bên thứ ba đọc được để quét trộm dữ liệu thẻ tín dụng và sau đó sử dụng hoặc bán thông tin đó trên Internet.

Ngày nay, các khách sạn sử dụng thẻ quét NFC hoặc thậm chí thẻ băng từ để khóa và mở khóa phòng. Ưu điểm là khách sạn có thể thay đổi các mã truy cập này nhanh chóng và dễ dàng từ quầy lễ tân. Nếu bị mất thẻ, bạn có thể yêu cầu thẻ mới. Một mã đơn giản được gửi cho khóa và ngay lập tức khi bạn đến phòng của mình, thẻ khóa mới sẽ hoạt động. Công cụ MagSpoof của Samy Kamkar có thể được sử dụng để giả mạo các trình tự chính xác và mở khóa một phòng khách sạn bằng cách sử dụng thẻ băng từ. Công cụ này được đã sử dụng trong một tập của chương trình truyền hình Mr. Robot.

Sự hiện diện của dải từ hoặc chip NFC đã làm nảy sinh ý tưởng rằng thông tin cá nhân có thể được lưu trữ trên thẻ khóa của khách sạn. Không phải vậy. Nhưng người ta vẫn rỉ tai nhau truyền thuyết này. Thậm chí còn có một câu chuyện nổi tiếng có

nguồn gốc từ Quận San Diego. Giả sử một phó cảnh sát trưởng ở đó đưa ra cảnh báo rằng họ tìm thấy trên chìa khóa của khách sạn thông tin về tên, địa chỉ nhà và thẻ tín dụng của khách. Có lẽ bạn đã nhìn thấy email đó. Nó trông giống như thế này:

Gần đây các chuyên gia thực thi pháp luật Nam California được giao nhiệm vụ phát hiện các mối đe dọa mới đối với các vấn đề bảo mật cá nhân đã phát hiện những loại thông tin nhúng trong các khóa phòng khách sạn vốn đang được toàn ngành này sử dụng.

Mặc dù chìa khóa phòng của các khách sạn là khác nhau, nhưng một chìa khóa thông thường sẽ chứa các thông tin sau:

• Tên khách hàng

• Địa chỉ nhà riêng của khách hàng

• Số phòng khách sạn

• Ngày nhận phòng và ngày trả phòng

• Số thẻ tín dụng của khách hàng và ngày hết hạn!

Khi bạn trả chúng về quầy lễ tân, bất kỳ ai cũng có thể lấy được thông tin cá nhân của bằng cách quét thẻ trong máy quét của khách sạn. Một nhân viên có thể lấy một số ít thẻ về nhà và với một thiết bị quét, anh ta có thể truy cập vào thông tin trên một máy tính xách tay và đi mua sắm bằng tiền của bạn.

Nói một cách đơn giản, khách sạn không xóa các thẻ này cho đến khi một nhân viên phát thẻ cho khách lưu trú tiếp theo. Nó thường được lưu giữ trong một ngăn kéo ở quầy lễ tân với THÔNG TIN CỦA BẠN TRÊN ĐÓ!!!!

Điểm mấu chốt là, hãy giữ thẻ hoặc tiêu hủy chúng! KHÔNG BAO GIỜ bỏ chúng lại và KHÔNG BAO GIỜ trả chúng về quầy lễ tân khi bạn trả phòng. Họ sẽ không bắt bạn đền tiền thẻ đâu.

Người ta tranh cãi nhiều về tính xác thực của email này. Thành thật mà nói, theo tôi, nó có vẻ rất nhảm nhí.

Các thông tin liệt kê ở trên chắc chắn có thể được lưu trữ trên một thẻ chìa khóa, nhưng điều đó có vẻ cực đoan, ngay cả với tôi. Khách sạn sử dụng những gì có thể được coi là một mã thông báo token, một số giữ chỗ, cho mỗi khách. Chỉ với quyền truy cập vào các máy tính phía máy chủ sau thực hiện thanh toán, mã token mới có thể được kết nối với thông tin cá nhân.

Tôi không nghĩ rằng bạn cần phải thu thập và tiêu hủy các thẻ khóa cũ của bạn, nhưng này, bạn có thể muốn làm như vậy vì thế tất cả cũng giống nhau thôi.

Một câu hỏi phổ biến khác liên quan đến việc đi lại và dữ liệu: Có gì trong mã vạch ở dưới cùng trên vé máy bay của bạn? Mã vạch này có thể tiết lộ điều gì, nếu có? Trong thực tế, nó có thể tiết lộ tương đối ít thông tin cá nhân, trừ khi bạn có mã số hành khách thường xuyên.

Bắt đầu từ năm 2005, Hiệp hội Vận tải Hàng không Quốc tế (IATA) đã quyết định sử dụng thẻ lên máy bay có mã vạch vì lý do đơn giản là thẻ từ tốn nhiều chi phí duy trì hơn. Khoản tiết kiệm được ước tính là khoảng 1,5 tỷ đô-la. Hơn nữa, sử dụng mã vạch trên vé máy bay cho phép hành khách tải xuống vé từ Internet và in chúng tại nhà, hoặc thay vào đó họ có thể sử dụng điện thoại di động tại cổng.

Dĩ nhiên, sự thay đổi thủ tục này đòi hỏi một số tiêu chuẩn nhất định. Theo nhà nghiên cứu Shaun Ewing, mã vạch lên máy bay điển hình chứa các thông tin hầu như vô hại như tên hành khách, tên hãng hàng không, số chỗ ngồi, sân bay khởi hành, sân bay đến và số hiệu chuyến bay. Tuy nhiên, phần nhạy cảm nhất của mã vạch là mã số khách hàng bay thường xuyên của bạn. Tất cả các trang web của các hãng hàng không hiện đang bảo vệ tài khoản khách hàng bằng mật khẩu cá nhân. Cung cấp mã số hành khách thường xuyên không giống như việc cung cấp số An sinh Xã hội, nhưng nó vẫn là một mối lo ngại về quyền riêng tư.

Mối lo ngại về quyền riêng tư lớn hơn là thẻ khách hàng thân thiết được cung cấp tại các siêu thị, hiệu thuốc, trạm xăng và các

doanh nghiệp khác. Không giống như vé máy bay yêu cầu tên hợp pháp, thẻ khách hàng thân thiết có thể được đăng ký dưới tên giả, địa chỉ và số điện thoại (số giả bạn có thể nhớ), vì vậy thói quen mua hàng của bạn không thể liên kết ngược lại với bạn.

Khi bạn nhận phòng khách sạn và khởi động máy tính, bạn có thể thấy danh sách các mạng Wi-Fi có sẵn, chẳng hạn như "Khách của khách sạn", "tmobile123", "iPhone của Kimberley", "attwifi", "Android của Steve" và "Điểm phát nóng của Chuck." Bạn nên kết nối với mạng nào? Tôi hy vọng đến đây bạn đã biết câu trả lời!

Hầu hết Wi-Fi của khách sạn không sử dụng mã hóa nhưng yêu cầu xác thực bằng họ và số phòng của khách. Tất nhiên, có những thủ thuật để đi vòng tránh được hàng rào thanh toán.

Một mẹo để truy cập Internet miễn phí tại bất kỳ khách sạn nào là gọi sang cho bất kỳ phòng nào khác – có thể là phòng đối diện – đóng giả làm nhân viên dọn phòng. Nếu khách sạn sử dụng ID người gọi, bạn chỉ cần sử dụng điện thoại ở sảnh đợi. Hãy thông báo với người nhấc máy là đồ ăn đang trên đường tới. Khi người này nói rằng cô ấy không gọi đồ, hãy nhã nhặn hỏi xin họ của cô này để điều chỉnh lại. Như vậy, bây giờ bạn đã có cả số phòng (bạn gọi tới phòng đó) và họ của khách trong phòng – đó là tất cả những gì cần thiết để xác thực bạn (một khách không trả tiền) như một khách hợp pháp tại khách sạn đó.

Giả sử bạn đang ở tại một khách sạn năm sao có Internet, miễn phí hoặc trả phí. Khi đăng nhập, có lẽ bạn thấy một thông báo cho bạn biết rằng Adobe (hoặc một số nhà sản xuất phần mềm khác) có bản cập nhật có sẵn. Là một cư dân mạng ngoan ngoãn, có thể bạn sẽ tuân lệnh và tải xuống bản cập nhật. Ngoại trừ một việc là mạng của khách sạn vẫn cần được coi là không thân thiện, ngay cả khi nó có mật khẩu. Đây không phải là mạng gia đình của bạn, vì vậy bản cập nhật có thể không phải là thực, và nếu tiếp tục tải xuống, bạn có thể vô tình cài đặt mã độc trên máy tính.

Nếu bạn thường xuyên đi lại, việc xem xét để cập nhật hay không là một quyết định khó khăn. Bạn chỉ có một lựa chọn là xác minh

rằng mình đã có bản cập nhật. Vấn đề là, nếu sử dụng Internet của khách sạn để tải xuống bản cập nhật đó, bạn có thể bị chuyển hướng đến một website giả mạo cung cấp bản "cập nhật" độc hại. Nếu có thể, hãy sử dụng thiết bị di động để xác nhận sự tồn tại của bản cập nhật từ website của nhà cung cấp và nếu nó không quan trọng, hãy đợi cho đến khi bạn trở lại trong một môi trường an toàn, chẳng hạn như văn phòng công ty hoặc ở nhà, để tải xuống.

Các nhà nghiên cứu tại Kaspersky Lab, một công ty phần mềm bảo mật, đã phát hiện ra một nhóm hacker tội phạm mà họ gọi là DarkHotel (còn gọi là Tapaoux), những kẻ sử dụng kỹ thuật này. Chúng hoạt động bằng cách xác định lãnh đạo các công ty có thể đang ở tại một khách sạn sang trọng, sau đó dự đoán ngày họ đến bằng cách đặt phần mềm độc hại trên máy chủ của khách sạn. Khi các các vị lãnh đạo này nhận phòng và kết nối với Wi-Fi của khách sạn, phần mềm độc hại được tải xuống và thực thi trên thiết bị của họ. Sau khi hoàn tất quá trình lây nhiễm, phần mềm độc hại sẽ bị xóa khỏi máy chủ. Các nhà nghiên cứu lưu ý rằng hoạt động này đã diễn ra trong gần một thập kỷ.

Mặc dù nó chủ yếu ảnh hưởng đến lãnh đạo ở các khách sạn sang trọng ở châu Á, nhưng nó có thể cũng phổ biến ở nơi khác. Nhìn chung, nhóm DarkHotel thường tiến hành tấn công spear phishing cấp thấp cho các đối tượng hàng loạt, còn những cuộc tấn công ở khách sạn là nhắm đến những mục tiêu cao cấp, chẳng hạn lãnh đạo trong các lĩnh vực năng lượng hạt nhân và quốc phòng.

Một phân tích ban đầu cho rằng DarkHotel xuất phát từ Hàn Quốc. Một keylogger – tức phần mềm độc hại dùng để ghi lại các thao tác gõ phím trên thiết bị mà nó tấn công – dùng trong các cuộc tấn công có chứa các ký tự tiếng Hàn bên trong mã. Và zero-day – lỗ hổng trong phần mềm mà những người muốn vá nó không biết đến – là những lỗi rất tiên tiến mà trước đây chưa được biết tới. Hơn nữa, người ta đã truy ra rằng một tên Hàn Quốc được xác định trong keylogger bắt nguồn từ các keylogger

tinh vi khác được người Hàn Quốc sử dụng trước đây.

Tuy nhiên, cần lưu ý rằng điều này là không đủ để xác nhận kết luận trên. Phần mềm có thể được cắt và dán từ nhiều nguồn khác nhau. Ngoài ra, có thể thiết kế để phần mềm được tạo ra ở quốc gia A lại trông có vẻ như đến từ quốc gia B.

Để cài được phần mềm độc hại trên máy tính xách tay, DarkHotel sử dụng các chứng chỉ giả mạo trông có vẻ được phát hành từ chính phủ Malaysia và Deutsche Telekom. Nếu bạn nhớ những nội dung đã nhắc đến trong Chương 5, chứng chỉ được sử dụng để xác minh nguồn gốc của phần mềm hoặc máy chủ Web. Để tiếp tục che giấu kỹ hơn công việc của mình, các hacker đã sắp xếp để phần mềm độc hại nằm im trong tối đa sáu tháng trước khi phát tác. Điều này là để ngăn đội ngũ IT có thể nghi ngờ một truy cập là một vụ lây nhiễm.

Kaspersky chỉ biết đến vụ tấn công này khi một nhóm khách hàng của họ bị lây nhiễm sau lần lưu trú tại một số khách sạn sang trọng ở châu Á. Các nhà nghiên cứu đã chuyển sang một máy chủ Wi-Fi của bên thứ ba chung cho cả hai, và máy chủ Wi-Fi hợp tác với công ty chống virus để tìm hiểu những gì đang xảy ra trên mạng của họ. Mặc dù các file được sử dụng để lây nhiễm cho các khách hàng đã biến mất từ lâu, nhưng bản ghi về việc xóa file còn lại tương ứng với ngày lưu trú của khách.

Cách dễ nhất để tự vệ trước loại tấn công này là kết nối với dịch vụ VPN ngay khi bạn kết nối với Internet tại khách sạn. Dịch vụ VPN tôi sử dụng khá rẻ – chỉ 6 đô-la mỗi tháng. Tuy nhiên, đó không phải là lựa chọn tốt nếu bạn muốn tàng hình vì nó sẽ không cho phép thiết lập ẩn danh.

Nếu bạn muốn ẩn danh, đừng tin tưởng đưa cho nhà cung cấp VPN thông tin thực của bạn. Để làm được điều này, bạn phải thiết lập từ trước một địa chỉ email giả và sử dụng một mạng không dây mở. Khi đã có địa chỉ email giả, hãy sử dụng Tor để thiết lập ví Bitcoin, tìm một máy ATM Bitcoin để nạp tiền cho ví, và sau đó sử dụng một máy trộn để rửa Bitcoin nhằm ngăn người khác truy

ngược lại bạn trên blockchain. Quá trình rửa tiền này đòi hỏi phải thiết lập hai ví Bitcoin sử dụng các mạch Tor khác nhau. Ví tiền đầu tiên được sử dụng để gửi Bitcoin cho dịch vụ rửa, và ví thứ hai được thiết lập để nhận Bitcoin sau khi rửa.

Sau khi đã đạt được trạng thái ẩn danh thực sự bằng cách sử dụng Wi-Fi mở nằm ngoài tầm ngắm của các camera cộng với Tor, hãy tìm một dịch vụ VPN chấp nhận thanh toán bằng Bitcoin. Hãy thanh toán bằng Bitcoin đã rửa. Một số nhà cung cấp VPN như WiTopia chặn Tor, vì vậy bạn cần tìm một nhà cung cấp dịch vụ VPN không làm điều đó – tốt nhất là sử dụng nhà cung cấp VPN không lưu lịch sử kết nối.

Trong trường hợp này, chúng ta không "tin tưởng" nhà cung cấp VPN có địa chỉ IP hoặc tên thật của chúng ta. Tuy nhiên, khi sử dụng VPN mới thiết lập, bạn phải cẩn thận không sử dụng bất kỳ dịch vụ nào được kết nối với tên thật của bạn và không kết nối với VPN từ địa chỉ IP có thể được gắn với bạn. Bạn có thể xem xét việc chia sẻ kết nối với một điện thoại dùng một lần ẩn danh, xem tại đây.

Trong trường hợp này, chúng ta không giao cho nhà cung cấp VPN địa chỉ IP hoặc tên thật của mình. Tuy nhiên, khi sử dụng VPN mới thiết lập, bạn phải cẩn thận không sử dụng bất kỳ dịch vụ nào được kết nối với tên thật của bạn và không kết nối với VPN từ địa chỉ IP có thể được gắn với bạn. Bạn có thể cân nhắc việc sử dụng điện thoại ẩn danh.

Tốt nhất bạn nên mua một thiết bị phát sóng di động (nhớ là mua theo cách khó xác định được bạn). Ví dụ, bạn có thể thuê người mua hộ để bạn không xuất hiện trong camera của cửa hàng bán thiết bị. Trong khi đang sử dụng điểm phát sóng ẩn danh, bạn nên tắt bất kỳ thiết bị cá nhân nào sử dụng tín hiệu di động để tránh việc thiết bị cá nhân của bạn đăng ký ở cùng một nơi với thiết bị ẩn danh.

Tóm lại, đây là những gì bạn cần làm để sử dụng Internet một cách riêng tư khi đi lại:

1. Mua thẻ quà tặng trả trước ẩn danh. Ở châu Âu, bạn có thể mua thẻ tín dụng trả trước ẩn danh tại viabuy.com.

2. Sử dụng Wi-Fi mở sau khi thay đổi địa chỉ MAC.

3. Tìm một nhà cung cấp email cho phép đăng ký mà không cần xác thực qua tin nhắn. Hoặc bạn có thể đăng ký số Skype-in bằng cách sử dụng Tor và thẻ quà tặng trả trước. Với Skype-in, bạn có thể nhận cuộc gọi thoại để xác minh danh tính. Hãy đảm bảo bạn không nằm trong tầm quan sát của camera (nghĩa là, không phải trong quán cà phê Starbucks hoặc bất kỳ nơi nào khác có giám sát bằng camera). Sử dụng Tor để che dấu vị trí khi bạn đăng ký dịch vụ email này.

4. Sử dụng địa chỉ email ẩn danh mới để đăng nhập vào một website như paxful.com qua Tor, sau đó đăng ký ví Bitcoin và mua Bitcoin. Thanh toán cho họ bằng thẻ quà tặng trả trước.

5. Thiết lập địa chỉ email ẩn danh thứ hai và ví Bitcoin thứ hai mới sau khi đóng và thiết lập một mạch Tor mới để ngăn chặn bất kỳ liên kết nào với tài khoản email và ví tiền đầu tiên.

6. Sử dụng dịch vụ rửa tiền Bitcoin như bitlaunder.com để khó có thể theo dõi nguồn gốc của đồng tiền. Gửi Bitcoin đã rửa đến ví thứ hai.

7. Đăng ký một dịch vụ VPN loại không ghi lịch sử luồng truy cập hoặc IP các kết nối bằng cách sử dụng Bitcoin được rửa. Bạn có thể tìm hiểu những gì được ghi lại lịch sử bằng cách xem chính sách bảo mật của nhà cung cấp VPN (ví dụ: TorGuard).

8. Thuê người dùng tiền mặt mua thiết bị phát sóng di động ẩn danh.

9. Để truy cập Internet, hãy sử dụng thiết bị phát sóng ẩn danh ở xa nhà, nơi làm việc và các thiết bị di động khác của bạn.

10. Sau khi bật nguồn, hãy kết nối VPN thông qua thiết bị phát sóng di động ẩn danh đó.

11. Sử dụng Tor để duyệt Internet.

Chương 15: FBI LUÔN BẮT ĐƯỢC NGƯỜI

Trong khu vực tiểu thuyết khoa học viễn tưởng tại Thư viện Công cộng San Francisco, chi nhánh Glen Park, cách không xa căn hộ của mình, Ross William Ulbricht đang tham gia vào một cuộc trò chuyện hỗ trợ khách hàng trực tuyến cho công ty mà anh sở hữu. Khi đó – tháng 10 năm 2013 – người trao đổi với anh trên mạng đang đinh ninh rằng tiếp chuyện mình là quản trị viên của website với biệt danh Dread Pirate Roberts, một cái tên lấy từ bộ phim The Princess Bride. Roberts, còn được gọi là DPR, trên thực tế là Ross Ulbricht, không chỉ là quản trị viên mà còn là chủ sở hữu của Silk Road, một trung tâm buôn bán ma túy trực tuyến lớn, và do đó là đối tượng của cơ quan săn lùng tội phạm liên bang. Ulbricht thường xuyên sử dụng các địa điểm Wi-Fi công cộng như thư viện để làm việc – có lẽ quyết định này xuất phát từ một hiểu nhầm rằng nếu phát hiện ra anh chính là DPR thì FBI cũng không bao giờ tổ chức đột kích ở nơi công cộng cả. Tuy nhiên, vào ngày hôm đó, người mà Ulbricht đang tiếp chuyện thực ra lại là một mật vụ FBI.

Điều hành một trung tâm thương mại ma túy trực tuyến – trong đó khách hàng có thể đặt mua cocaine và heroin và các loại ma túy tổng hợp một cách nặc danh – đòi hỏi một tinh thần thép. Website của Silk Road được đặt trên Dark Web và chỉ có thể truy cập thông qua Tor. Website nhận thanh toán bằng Bitcoin. Và nhà sáng lập Silk Road đã cẩn thận, nhưng vẫn chưa đủ cẩn thận.

Vài tháng trước đó, FBI đã khoanh vùng được Ulbricht, sau khi một người bất ngờ liên lạc với cơ quan này để cung cấp bằng chứng cho thấy Ulbricht chính là DPR. Người này, một nhân viên của Cục Thuế vụ (IRS) tên là Gary Alford, đã đọc về Silk Road và nguồn gốc của nó, và vào các buổi tối anh ta thường thực hiện thêm các tìm kiếm nâng cao trên Google. Anh ta phát hiện ra rằng Silk Road được nhắc đến lần đầu từ năm 2011, khi một

người có biệt danh “altoid” nhắc tới nó trong một nhóm trò chuyện. Do lúc đó Silk Road vẫn chưa ra đời, nên Alford cho rằng altoid nắm được thông tin nội bộ về hoạt động này. Một cách tự nhiên, Alford bắt đầu tìm kiếm các thông tin tham khảo khác.

Anh ta đã đào trúng hố vàng.

Altoid đã đăng câu hỏi lên một nhóm trò chuyện khác, nhưng xóa tin nhắn gốc. Alford tìm ra một câu trả lời cho câu hỏi gốc lúc này đã bị xóa đi, trong đó altoid cho biết nếu ai trả lời được câu hỏi của mình, người đó có thể liên lạc với anh ta tại địa chỉ email là rossulbricht@gmail.com.

Đó không phải là lần lộ thông tin duy nhất. Một số câu hỏi khác cũng được đăng lên, trong đó có một câu được đăng lên một website tên là Stack Overflow: câu hỏi ban đầu được gửi từ rossulbricht@gmail.com, nhưng sau đó tên người gửi được đổi thành DPR.

Quy tắc số 1 về việc tàng hình: không bao giờ được liên kết con người trực tuyến ẩn danh với con người trong thế giới thực. Không bao giờ được làm điều đó.

Sau đó là những đầu mối liên kết khác. Ulbricht, giống như DPR, tán dương các triết lý thị trường tự do của nhà tự do chủ nghĩa Ron Paul. Và có lúc, Ulbricht thậm chí còn đặt mua một số giấy phép lái xe giả với những tên gọi khác nhau từ các tiểu bang khác nhau – việc này trở thành vết lông ngỗng dẫn các đặc vụ liên bang đến trước cửa nhà anh ta ở San Francisco vào tháng 7 năm 2013, nhưng tại thời điểm đó, chính quyền không hề biết họ đang nói chuyện với DPR.

Các bằng chứng càng lúc càng trở nên thuyết phục hơn, và cuối cùng, vào một buổi sáng tháng 10 năm 2013, ngay khi cuộc trò chuyện hỗ trợ khách hàng của DPR bắt đầu, các đặc vụ liên bang cũng lặng lẽ tiến vào thư viện Glen Park. Sau đó, trong một cuộc tấn công bất ngờ, họ bắt giữ Ulbricht trước khi anh ta có thể tắt máy tính xách tay của mình. Nếu anh ta tắt máy, một số bằng chứng quan trọng có thể sẽ bị tiêu hủy. Ít giây sau vụ bắt giữ, họ

có thể chụp ảnh màn hình quản trị hệ thống cho website Silk Road, từ đó thiết lập một liên kết cụ thể giữa Ulbricht, Dread Pirate Roberts và Silk Road.

Vào sáng tháng 10 hôm đó ở Glen Park, Ulbricht đăng nhập vào Silk Road với tư cách quản trị viên. Và FBI biết điều đó bởi vì họ quan sát máy tính của anh ta đăng nhập vào Internet. Nhưng nếu anh ta có thể giả mạo vị trí của mình thì sao? Điều gì sẽ xảy ra nếu anh ta không ở trong thư viện mà sử dụng một máy chủ proxy?

Mùa hè năm 2015, nhà nghiên cứu Ben Caudill của Rhino Security thông báo rằng tại Hội nghị DEF CON 23, ông sẽ không chỉ thuyết trình giới thiệu thiết bị mới của mình là ProxyHam mà còn có ý định bán nó với giá gốc – khoảng 200 đô-la – trong phòng của các nhà phân phối tại hội nghị trên. Khoảng một tuần sau đó, Caudill thông báo rằng bài thuyết trình của ông đã bị hoãn, và tất cả các thiết bị ProxyHam hiện có sẽ bị tiêu hủy. Ông không đưa ra lời giải thích nào thêm.

Các bài thuyết trình tại các hội nghị an ninh lớn bị hoãn vì nhiều lý do khác nhau. Hoặc là các công ty có sản phẩm mới đang bị đưa ra tranh cãi, hoặc chính phủ liên bang gây áp lực lên các nhà nghiên cứu để buộc họ không công bố sản phẩm. Trong trường hợp này, Caudill không chỉ ra một lỗ hổng cụ thể nào mà thiết kế một thứ mới.

Điều thú vị về Internet là khi một ý tưởng xuất hiện ở đó, nó vẫn tồn tại ở đó. Vì vậy, ngay cả khi các đặc vụ FBI hoặc người khác nói với Caudill rằng bài thuyết trình của ông không phục vụ lợi ích của an ninh quốc gia, thì người khác vẫn sẽ tạo ra một thiết bị mới. Và đó chính xác là những gì đã xảy ra.

ProxyHam là một điểm truy cập từ rất xa, giống như bạn đặt máy phát Wi-Fi tại nhà hoặc văn phòng, nhưng điểm khác là phạm vi kiểm soát ProxyHam có thể lên tới 2km. Máy phát Wi-Fi sử dụng sóng vô tuyến tần số 900 MHz để kết nối với thiết bị điều chỉnh ăng-ten trên máy tính ở cách đó tới 4km. Như vậy, trong trường

hợp của Ross Ulbricht, FBI có thể tập trung bên ngoài thư viện Glen Park trong khi anh ta đang lúi húi dọn dẹp ở tầng hầm của ai đó cách đó vài dãy nhà.

Các thiết bị như vậy rõ ràng là cần thiết nếu bạn sống ở một quốc gia có chính quyền áp bức. Liên hệ với thế giới bên ngoài thông qua Tor là một nguy cơ được nhiều người chọn. Loại thiết bị này sẽ thêm một lớp bảo mật khác bằng cách che giấu vị trí của người dùng.

Ngoại trừ trường hợp có người không muốn Caudill trình bày về thiết bị mới này tại DEF CON.

Trong các cuộc phỏng vấn, Caudill phủ nhận rằng Ủy ban Truyền thông Liên bang đã gây áp lực. Tờ Wired phỏng đoán rằng việc bí mật đặt ProxyHam trên mạng của người khác có thể được diễn giải là hành vi truy cập trái phép theo Đạo luật Gian lận và Lạm dụng máy tính vốn có nhiều điểm chưa rõ ràng của Mỹ. Caudill từ chối bình luận về bất kỳ suy đoán nào.

Như tôi đã nói, khi một ý tưởng xuất hiện, bất cứ ai cũng có thể triển khai nó. Vì vậy, nhà nghiên cứu an ninh Samy Kamkar đã tạo ra ProxyGambit, một thiết bị về cơ bản có thể thay thế ProxyHam. Điểm khác biệt ở đây là ProxyGambit sử dụng mạng điện thoại di động đảo chiều, nghĩa là thay vì phải ở cách nó vài ki-lô-mét, bạn có thể đứng cách nửa vòng trái đất mà vẫn có thể dùng được thiết bị này. Quá tuyệt vời!

ProxyGambit và các thiết bị tương tự dĩ nhiên khiến các cơ quan thực thi pháp luật phải đau đầu khi bọn tội phạm sử dụng chúng.

Silk Road của Ulbricht là một siêu thị ma túy trực tuyến. Đó không phải là thứ bạn có thể tìm kiếm trên Google; nó không được gọi là web nổi (Surface Web), có thể được lập chỉ mục và tìm kiếm dễ dàng. Web nổi, chứa các website quen thuộc như Amazon và YouTube, chỉ chiếm 5% toàn bộ Internet. Tất cả những website mà hầu hết mọi người đã truy cập hoặc từng nghe đến tên chỉ chiếm một phần rất nhỏ so với số lượng website thực tế. Phần lớn số lượng website trên Internet đều bị ẩn khỏi các

công cụ tìm kiếm.

Xếp sau web nổi là web chìm (Deep Web), được ẩn đằng sau mật khẩu truy cập – ví dụ, nội dung của danh mục thẻ cho chi nhánh Glen Park của Thư viện Công cộng San Francisco. Web chìm cũng chứa phần lớn là các website chỉ dành cho người đăng ký và website mạng nội bộ của các công ty. Netflix. Pandora. Bạn có thể tưởng tượng ra rồi đấy.

Cuối cùng, Internet còn có một phần nhỏ hơn nhiều, gọi là web tối (Dark Web), không thể truy cập bằng trình duyệt thông thường, cũng không thể tìm kiếm trên các trang như Google, Bing, và Yahoo.

Web tối là nơi hoạt động của Silk Road, cùng với các website để bạn có thể rao tin thuê sát thủ hay mua các nội dung khiêu dâm trẻ em. Các website này hoạt động trên web tối vì nó hầu như ẩn danh. Tôi nói "hầu như" bởi vì không có gì là thực sự cả.

Chỉ có thể truy cập vào web tối thông qua trình duyệt Tor. Trên thực tế, các trang web tối, với các đường dẫn URL gồm các chữ và số phức tạp, đều kết thúc bằng đuôi .onion. Như tôi đã đề cập trước đó, bộ định tuyến Onion do Phòng thí nghiệm Nghiên cứu Hải quân Mỹ tạo ra để cung cấp cho những người bị áp bức một cách thức để liên lạc với nhau cũng như thế giới bên ngoài. Tôi cũng đã giải thích rằng Tor không kết nối trực tiếp trình duyệt của bạn với một website; thay vào đó, nó thiết lập liên kết đến một máy chủ khác, sau đó liên kết đó được gắn với một máy chủ khác để cuối cùng đến được trang đích. Nhiều bước nhảy như vậy khiến việc theo dõi trở nên khó khăn hơn. Và các website như Silk Road là sản phẩm của các dịch vụ ẩn trong mạng Tor. URL của chúng được tạo ra từ một thuật toán và danh sách các trang trên web tối thay đổi thường xuyên. Tor có thể truy cập cả web nổi và web tối. Một trình duyệt web tối khác, I2P, cũng có thể truy cập cả web nổi và web tối.

Ngay cả trước khi đánh sập Silk Road, người ta đã suy đoán rằng NSA hoặc những tổ chức khác đã có cách để xác định người dùng

trên web tối. Ví dụ, trồng và kiểm soát các nút thoát, tức các điểm mà tại đó một yêu cầu Internet được chuyển đến một trong các dịch vụ ẩn này, dù rằng như thế vẫn chưa đủ để nhận dạng người yêu cầu ban đầu.

Để làm được điều đó, chuyên gia quan sát của chính phủ sẽ phải thấy rằng một yêu cầu truy cập vào website X vừa được gửi đi, và rằng vài giây trước đó, một người nào đó ở New Hampshire đã khởi động trình duyệt Tor. Người quan sát có thể nghi ngờ rằng hai sự kiện trên có liên quan với nhau. Dần dần, việc truy cập vào website trên và hoạt động truy cập thường xuyên vào Tor cùng thời điểm có thể chỉ ra một đường mòn. Để tránh tạo đường mòn đó, bạn có thể giữ cho trình duyệt Tor luôn ở chế độ kết nối.

Trong trường hợp của Ulbricht, sai sót nằm ở sự cẩu thả. Rõ ràng là Ulbricht không có kế hoạch từ sớm. Trong những trao đổi ban đầu của anh ta về Silk Road, Ulbricht sử dụng lẫn địa chỉ email thực sự và biệt danh.

Như bạn có thể thấy, ngày nay rất khó hoạt động trên Internet mà không để lại dấu vết về danh tính thực sự của bạn. Nhưng như tôi đã nói ngay từ đầu, với một chút cẩn thận, bạn cũng có thể làm chủ nghệ thuật ẩn mình. Trong các trang sau, tôi sẽ chỉ cho bạn cách làm điều đó.

Chương 16: LÀM CHỦ NGHỆ THUẬT ẨN MÌNH

Đọc đến đây, có lẽ bạn đang suy nghĩ về mức độ trải nghiệm của bản thân và khả năng biến mất của mình trên mạng. Hoặc cũng có thể bạn băn khoăn không biết mình nên thực hiện bảo mật ở mức nào, hay nội dung nào trong cuốn sách này là dành cho bạn. Suy cho cùng, bạn đâu có giữ bí mật nhà nước nào chứ! Tuy nhiên, có thể bạn đang trong một cuộc tranh chấp pháp lý với vợ/chồng cũ. Hoặc có thể bạn đang có sự bất đồng với sếp. Hoặc có thể bạn đang liên lạc với một người bạn vẫn còn dính dáng tới một thành viên trong gia đình vốn trước đây hay ngược đãi bạn. Hoặc có thể bạn muốn giữ kín một số hoạt động riêng tư, không bị luật sư theo dõi. Có nhiều lý do chính đáng để bạn phải duy trì sự ẩn danh khi giao tiếp trên mạng, sử dụng website hay các công nghệ khác. Vì thế…

Bạn thực sự cần thực hiện những bước nào để làm được những điều đó? Mất bao lâu để làm như vậy? Và tốn kém ra sao?

Nếu hiện tại những điều này không quá rõ ràng, thì để ẩn danh trên mạng, ít nhiều bạn cần phải tạo ra một nhận dạng riêng, hoàn toàn không liên quan đến bạn. Đó là ý nghĩa của việc ẩn danh. Khi không ẩn danh, bạn cũng phải tách biệt rõ ràng cuộc sống thực của mình với danh tính ẩn đó. Điều tôi muốn nói ở đây là bạn cần mua một vài thiết bị riêng biệt, chỉ sử dụng khi ẩn danh. Và điều này có thể tốn kém.

Ví dụ, bạn có thể sử dụng máy tính xách tay hiện tại và tạo một máy ảo (VM) trên máy tính để bàn. Máy ảo là máy tính bằng phần mềm, được chứa trong một ứng dụng máy ảo, như VMware Fusion. Bạn có thể tải một bản sao Windows 10 có bản quyền bên trong máy ảo và cho biết bạn muốn bao nhiêu RAM, dung lượng đĩa bạn cần… Đối với người đang lén quan sát bạn, họ sẽ thấy bạn đang sử dụng máy tính Windows 10 trong khi trên thực tế bạn lại dùng máy Mac.

Các nhà nghiên cứu bảo mật chuyên nghiệp sử dụng máy ảo mọi lúc, họ có thể tạo và phá hủy chúng dễ dàng. Nhưng ngay cả trong số các chuyên gia vẫn có tồn tại khả năng rò rỉ. Ví dụ, có thể bạn đang sử dụng máy ảo phiên bản Windows 10, và vì lý do nào đó, bạn đăng nhập vào tài khoản email cá nhân. Lúc này, máy ảo đó có thể được liên kết với bạn.

Vì vậy, bước đầu tiên của việc ẩn danh là mua một máy tính xách tay riêng, chỉ dùng cho các hoạt động trực tuyến ẩn danh. Như chúng ta đã thấy, trong nano giây mà bạn lơ đễnh và kiểm tra tài khoản email cá nhân trên máy đó, trò chơi ẩn danh đã kết thúc. Vì vậy, tôi khuyên bạn dùng một máy tính xách tay Windows giá rẻ (Linux thì tốt hơn, nếu bạn biết cách sử dụng nó). Lý do tôi không đề xuất MacBook Pro là vì nó đắt hơn nhiều so với máy Windows.

Tôi đã khuyên bạn nên mua một chiếc máy tính xách tay thứ hai, cụ thể là Chromebook, chỉ sử dụng cho ngân hàng trực tuyến. Một lựa chọn khác cho ngân hàng trực tuyến là sử dụng iPad. Bạn phải đăng ký Apple ID bằng địa chỉ email và thẻ tín dụng hoặc bằng cách mua thẻ quà tặng iTunes. Nhưng do thiết bị này chỉ được sử dụng cho an toàn ngân hàng cá nhân của bạn, tàng hình không phải là mục tiêu.

Nhưng nếu mục tiêu của bạn ở đây là ẩn danh, thì Chromebook không phải là giải pháp tốt nhất vì bạn không có sự linh hoạt như với máy tính xách tay có cài Windows hoặc hệ điều hành dựa trên Linux như Ubuntu. Windows 10 sẽ ổn khi bạn bỏ qua tùy chọn yêu cầu bạn đăng ký tài khoản Microsoft. Đừng tạo bất kỳ liên kết nào từ máy tính của bạn tới Microsoft.

Bạn nên mua máy tính xách tay mới bằng tiền mặt, không nên mua trực tuyến, như vậy sẽ không có mối liên hệ nào giữa cuộc mua bán trên với bạn cả. Hãy nhớ rằng, máy tính xách tay mới có một card mạng không dây với một địa chỉ MAC duy nhất. Đừng để bất cứ ai có thể theo dấu thiết bị ấy để lần tới bạn – trong trường hợp địa chỉ MAC của bạn bị rò rỉ. Ví dụ, nếu bạn đang ở Starbucks và bật máy tính xách tay, hệ thống sẽ dò tìm bất kỳ

mạng không dây nào “đã kết nối” trước đó. Nếu có thiết bị giám sát trong khu vực lưu bản ghi các yêu cầu thăm dò đó, nó có thể tiết lộ địa chỉ MAC thực của bạn. Một mối quan tâm ở đây là chính phủ có thể có cách truy tìm tung tích của việc mua máy tính xách tay nếu có bất kỳ liên kết nào tồn tại giữa địa chỉ MAC của card mạng và số sê-ri ở máy tính. Nếu vậy, đặc vụ FBI sẽ chỉ cần tìm người đã mua máy tính để nhận dạng bạn, điều này có lẽ không quá khó.

Bạn nên cài đặt cả Tails và Tor và sử dụng chúng thay vì hệ điều hành và trình duyệt gốc.

Không đăng nhập vào bất kỳ website hoặc ứng dụng nào bằng danh tính thực. Bạn đã biết đến những rủi ro dựa trên việc theo dõi con người và máy tính trên Internet. Như chúng ta đã thảo luận, việc sử dụng website hoặc tài khoản theo nhận dạng thực của bạn là ý tưởng rất tồi – các ngân hàng và các website khác thường sử dụng thiết bị nhận dạng dấu vân tay để giảm thiểu gian lận, và điều này để lại một dấu chân khổng lồ, có thể xác định máy tính của bạn nếu bạn truy cập ẩn danh cũng vào website đó.

Tốt nhất là hãy tắt bộ định tuyến không dây trước khi khởi động máy tính xách tay ẩn danh ở nhà. Nhà cung cấp dịch vụ có thể biết địa chỉ MAC của máy tính xách tay ẩn danh nếu bạn kết nối với bộ định tuyến (giả sử nhà cung cấp sở hữu và quản lý bộ định tuyến trong nhà của bạn). Tốt nhất, bạn nên mua bộ định tuyến mà bạn có toàn quyền kiểm soát, do đó nhà cung cấp dịch vụ không thể lấy được địa chỉ MAC ở máy tính trên mạng cục bộ của bạn. Như vậy, nhà cung cấp dịch vụ sẽ chỉ thấy địa chỉ MAC của bộ định tuyến, điều này không có rủi ro đối với bạn.

Điều bạn muốn là khả năng ngăn chặn hợp lý. Bạn có thể ủy quyền các kết nối thông qua nhiều lớp để cho việc tìm ra mối liên kết giữa chúng với một người – chưa nói đến cá nhân bạn – sẽ trở nên vô cùng khó khăn. Tôi đã phạm một sai lầm trong khi đang chạy trốn FBI. Tôi liên tục gọi đến modem ở nhà cung cấp dịch vụ Netcom bằng cách sử dụng modem điện thoại di động để che

giấu vị trí thực của mình. Vì tôi đang ở một vị trí cố định nên việc sử dụng các kỹ thuật tìm hướng phát thanh để tìm tôi khi họ biết tháp di động mà điện thoại của tôi đang sử dụng trở nên dễ như trò trẻ con. Điều này cho phép đối thủ của tôi (Tsutomu Shimomura) khoanh vùng được tôi và chuyển thông tin này cho FBI.

Điều này có nghĩa là bạn không được phép sử dụng máy tính xách tay ẩn danh tại nhà riêng hoặc cơ quan. Không bao giờ. Vậy đó, hãy mua một máy tính xách tay và nghiêm ngặt tuân thủ cam kết là không sử dụng nó để kiểm tra email cá nhân, Facebook, hoặc thậm chí thời tiết địa phương.

Một cách khác để lần dấu bạn là thông qua phương pháp cổ điển: theo dõi dòng tiền. Bạn sẽ phải trả tiền cho một vài thứ, vì vậy, trước khi mở máy tính ẩn danh và tìm kiếm một mạng không dây mở, bước đầu tiên là hãy mua – một cách ẩn danh – một số thẻ quà tặng. Vì các cửa hàng bán thẻ quà tặng có thể gắn camera giám sát tại quầy hàng hoặc quầy thanh toán, nên bạn phải hết sức thận trọng. Không nên tự mua những thứ này. Hãy thuê một người lạ ngoài phố để họ cầm tiền mặt vào cửa hàng mua, còn bạn đứng chờ ở một khoảng cách an toàn.

Nhưng làm như vậy bằng cách nào? Cách của tôi là tìm một người đang đứng ở bãi để xe, rồi phân trần rằng vợ cũ của tôi đang làm việc ở cửa hàng kia nên tôi không muốn chạm mặt – hay tìm ra lý do nào nghe hợp lý. Có thể bổ sung thêm rằng người vợ/chồng cũ đã xin lệnh cách ly bạn chẳng hạn. Với khoản thù lao 100 đô-la, một người lạ hoàn toàn có thể đồng ý đi mua đồ hộ bạn.

Nên mua loại thẻ nào? Tôi khuyên bạn nên mua một số thẻ trả trước trị giá 100 đô-la. Không mua thẻ tín dụng có thể nạp lại vì khi kích hoạt, bạn phải cung cấp danh tính thực của mình theo Đạo luật Patriot, bao gồm tên thật, địa chỉ, ngày sinh, và số An sinh Xã hội khớp với thông tin về bạn trong hồ sơ của cơ quan tín dụng. Cung cấp tên giả mạo hoặc số An sinh Xã hội của người khác là trái pháp luật và có lẽ không đáng để mạo hiểm.

Chúng ta đang cố gắng ẩn danh trên mạng, chứ không vi phạm pháp luật.

Tôi khuyên bạn nên mua thẻ quà tặng Vanilla Visa hoặc Vanilla MasterCard trị giá 100 đô-la từ các cửa hiệu tạp hóa, 7-Eleven, Walmart, hoặc các cửa hàng lớn. Chúng thường được dùng làm quà tặng và có thể được sử dụng như thẻ tín dụng thông thường. Với những thứ này, bạn không phải cung cấp bất kỳ thông tin nhận dạng nào. Và bạn có thể mua chúng ẩn danh, bằng tiền mặt. Nếu sống ở châu Âu, bạn nên đặt hàng ẩn danh một thẻ tín dụng vật lý qua trang viabuy.com. Ở châu Âu, họ có thể gửi các thẻ đến bưu điện, không yêu cầu bạn phải mang theo giấy tờ tùy thân để nhận. Với hiểu biết của tôi thì họ sẽ gửi cho bạn mã PIN để mở hộp đồ (trong trường hợp không có camera).

Vậy bạn có thể sử dụng máy tính xách tay mới và thẻ trả trước được mua ẩn danh ở đâu?

Với sự ra đời của các thiết bị lưu trữ quang học giá rẻ, các doanh nghiệp cung cấp dịch vụ truy cập không dây miễn phí có thể lưu trữ cảnh quay camera giám sát trong nhiều năm. Đối với một điều tra viên, việc có được cảnh quay đó và tìm kiếm các nghi phạm tiềm năng là tương đối dễ dàng. Trong thời gian truy cập của bạn, điều tra viên có thể phân tích nhật ký tìm kiếm địa chỉ MAC được xác thực trên mạng không dây khớp với địa chỉ MAC của bạn. Đó là lý do tại sao điều quan trọng là thay đổi địa chỉ MAC của bạn mỗi lần bạn kết nối với mạng không dây miễn phí. Vì vậy, bạn cần phải tìm một vị trí gần hoặc liền kề với một địa điểm cung cấp Wi-Fi miễn phí. Ví dụ: có thể có một nhà hàng Trung Quốc bên cạnh Starbucks hoặc cơ sở khác cung cấp truy cập không dây miễn phí. Hãy ngồi ở chiếc bàn gần bức tường liền kề với nhà cung cấp dịch vụ. Tốc độ kết nối chậm hơn một chút, nhưng bạn sẽ có được sự ẩn danh tương đối (ít nhất là cho đến khi điều tra viên bắt đầu nhìn vào tất cả các cảnh quay giám sát từ khu vực xung quanh).

Địa chỉ MAC của bạn có thể sẽ được ghi lại và lưu trữ khi bạn xác thực trên mạng không dây miễn phí. Bạn có nhớ câu chuyện

người tình của Tướng David Petraeus không? Bạn có nhớ rằng thời gian và ngày đăng ký khách sạn của cô ta khớp với thời gian và ngày xuất hiện địa chỉ MAC của cô ta trên mạng của khách sạn không? Đừng để những sai lầm đơn giản như thế này ảnh hưởng đến sự ẩn danh của bạn. Vì vậy, hãy nhớ thay đổi địa chỉ MAC của bạn mỗi khi bạn truy cập Wi-Fi công cộng.

Cho đến lúc này, mọi việc có vẻ vẫn khá đơn giản: Bạn mua một máy tính xách tay riêng cho các hoạt động ẩn danh, mua thẻ quà tặng, tìm một mạng Wi-Fi có thể truy cập từ một điểm gần hoặc kế cận để tránh bị quan sát trên camera, và thay đổi địa chỉ MAC mỗi khi kết nối với mạng không dây miễn phí.

Tất nhiên còn nhiều hơn nữa. Nhiều hơn nữa. Chúng ta chỉ mới bắt đầu thôi.

Bạn cũng nên thuê một người nữa, lần này là để thực hiện một đơn mua hàng quan trọng hơn: bộ phát sóng cá nhân. Như tôi đã đề cập trước đó, FBI bắt được tôi vì tôi đã gọi tới các hệ thống trên khắp thế giới bằng điện thoại và modem di động, và dần dần, vị trí của tôi bị rò rỉ vì điện thoại di động được kết nối với cùng một tháp di động. Vào thời điểm đó, có thể dễ dàng tìm kiếm bằng sóng vô tuyến để định vị bộ thu phát (điện thoại di động của tôi). Bạn có thể tránh điều đó bằng cách thuê một người vào một cửa hàng Verizon (hoặc AT&T hay T-Mobile) và mua một thiết bị phát sóng cá nhân cho phép bạn kết nối với Internet bằng dữ liệu di động. Điều đó có nghĩa là bạn có quyền truy cập Internet riêng, do đó không phải đi qua mạng Wi-Fi công cộng. Quan trọng nhất, không nên sử dụng bộ phát sóng cá nhân ở một vị trí cố định quá lâu.

Lý tưởng nhất là đừng để người bạn thuê nhìn thấy biển số xe của bạn hoặc có bất kỳ cách nào để nhận dạng bạn. Hãy đưa tiền mặt cho người đó: 200 đô-la cho bộ phát sóng và 100 đô-la nữa khi người đó quay lại với bộ phát sóng. Các nhà mạng sẽ bán bộ phát sóng cá nhân không mang thông tin nhận dạng. Và trong khi bạn đang ở đó, tại sao không mua một vài thẻ nạp tiền để thêm nhiều dữ liệu hơn? Hy vọng rằng người kia sẽ không mang tiền của bạn

bỏ trốn, nhưng rủi ro này cũng đáng để chấp nhận nếu bạn muốn duy trì tính ẩn danh của mình. Sau đó, bạn có thể nạp lại tiền cho điện thoại ẩn danh bằng Bitcoin.

Sau khi bạn đã mua bộ phát sóng di động một cách ẩn danh, giống như với máy tính xách tay, điều rất quan trọng là bạn không bao giờ, không bao giờ, không bao giờ được bật thiết bị đó ở nhà. Mỗi khi điểm phát sóng được bật, nó sẽ đăng ký với tháp mạng di động gần nhất. Bạn sẽ không muốn nhà riêng hoặc văn phòng của mình hoặc bất kỳ nơi nào bạn thường xuyên lui tới bị hiển thị trong các file nhật ký của nhà mạng di động.

Và đừng bao giờ bật điện thoại cá nhân hoặc máy tính xách tay cá nhân của bạn ở cùng vị trí nơi bạn bật máy tính xách tay hoặc điện thoại ẩn danh hay bộ phát sóng ẩn danh. Sự tách biệt thực sự rất quan trọng. Bất kỳ bản ghi nào liên kết bạn với danh tính ẩn danh của bạn sẽ làm hỏng toàn bộ kế hoạch này.

Bây giờ, sau khi đã có thẻ quà tặng trả trước và bộ phát sóng cá nhân với gói dữ liệu trả trước – cả hai đều được mua ẩn danh nhờ hai người khác nhau, những người sẽ không có bất kỳ thông tin nào về bạn để nhận diện bạn – chúng ta sắp hoàn thành công việc rồi. Gần như thế.

Từ thời điểm này, hãy luôn sử dụng trình duyệt Tor để tạo và truy cập tất cả các tài khoản trực tuyến vì nó giúp thay đổi địa chỉ IP của bạn liên tục.

Một trong những bước đầu tiên là thiết lập một vài tài khoản email ẩn danh bằng cách sử dụng Tor. Đây là điều mà Ross Ulbricht bỏ qua không làm. Như chúng ta đã thấy trong chương trước, anh ta đã sử dụng tài khoản email cá nhân nhiều lần trong khi điều hành hoạt động của Silk Road trên web tối. Những sợi dây liên kết vô chủ ý từ Dread Pirate Roberts đến Ross Ulbricht và ngược lại giúp các nhà điều tra xác nhận rằng hai cái tên đó liên quan đến cùng một người.

Để ngăn chặn hoạt động xâm phạm, hầu hết các nhà cung cấp email như Gmail, Hotmail, Outlook, và Yahoo đều yêu cầu xác

thực trên điện thoại di động. Điều đó có nghĩa là bạn phải cung cấp số điện thoại di động của mình và ngay lập tức trong quá trình đăng ký, tin nhắn văn bản được gửi đến thiết bị đó để xác nhận danh tính của bạn.

Nếu sử dụng điện thoại ẩn danh, bạn vẫn có thể sử dụng các dịch vụ thương mại như đã đề cập ở trên. Tuy nhiên, điện thoại ẩn danh và tất cả các thẻ nạp tiền đều phải được lấy một cách an toàn, chẳng hạn do một người lạ không biết bạn dùng tiền mặt để mua. Ngoài ra, khi có điện thoại ẩn danh, bạn cũng không thể sử dụng nó khi ở gần bất kỳ thiết bị di động nào khác mà bạn sở hữu. Một lần nữa, hãy để điện thoại cá nhân ở nhà.

Để mua Bitcoin trực tuyến, bạn sẽ cần ít nhất hai địa chỉ email ẩn danh và ví Bitcoin. Vậy làm cách nào để bạn tạo các địa chỉ email ẩn danh như những địa chỉ được tạo bởi Edward Snowden và Laura Poitras?

Trong nghiên cứu của mình, tôi thấy rằng tôi có thể tạo một tài khoản email trên protonmail.com và một trên tutanota.com bằng cách sử dụng Tor, cả hai đều không có bất kỳ yêu cầu nào về việc xác minh danh tính. Bạn có thể tự tìm hiểu bằng cách tìm kiếm nhà cung cấp email và kiểm tra xem họ có yêu cầu số điện thoại di động trong quá trình đăng ký hay không. Bạn cũng có thể xem họ cần bao nhiêu thông tin để tạo tài khoản mới. Một phương án email khác là fastmail.com, loại này không có nhiều tính năng phong phú như Gmail, nhưng vì là dịch vụ trả phí, nó không khai thác dữ liệu người dùng hoặc hiển thị quảng cáo.

Vậy là giờ đây chúng ta có một máy tính xách tay, với Tor và Tails đã được tải sẵn, một điện thoại ẩn danh, một số ít các thẻ quà trả trước ẩn danh, và một bộ phát sóng ẩn danh với một gói dữ liệu đã mua ẩn danh. Chúng ta vẫn chưa sẵn sàng đâu. Để duy trì tính ẩn danh này, chúng ta cần chuyển đổi thẻ quà tặng trả trước sang Bitcoin.

Trong Chương 6, tôi đã nói về tiền ảo Bitcoin. Bản thân Bitcoin không ẩn danh. Có thể truy tìm trở lại nguồn gốc của giao dịch

mua thông qua cái gọi là blockchain; tương tự, tất cả các lần mua hàng tiếp theo cũng có thể được truy tìm. Vì vậy, bản thân Bitcoin sẽ không giấu danh tính của bạn. Chúng ta sẽ phải đưa ngân sách thông qua một cơ chế ẩn danh hóa: chuyển đổi thẻ quà tặng trả trước thành Bitcoin, sau đó đưa Bitcoin chạy qua một dịch vụ rửa tiền. Quá trình này sẽ cho kết quả là Bitcoin được ẩn danh có thể sử dụng cho các khoản thanh toán trong tương lai. Ví dụ, chúng ta sẽ cần Bitcoin đã được rửa để thanh toán cho dịch vụ VPN và mọi giao dịch mua dữ liệu trong tương lai trên bộ phát sóng di động hoặc điện thoại ẩn danh.

Bạn có thể dùng Tor để thiết lập một ví Bitcoin ban đầu tại paxful.com hoặc các website ví Bitcoin khác. Một số website môi giới giao dịch mà ở đó bạn có thể mua Bitcoin với thẻ quà tặng trả trước, chẳng hạn như các thẻ quà tặng Vanilla Visa và Vanilla MasterCard mà tôi đã đề cập trước đó. Nhược điểm là bạn sẽ phải trả một khoản phí bảo hiểm rất lớn cho dịch vụ này, ít nhất là 50%.

Paxful.com giống một trang đấu giá của eBay nơi bạn tìm thấy những người bán Bitcoin – website này chỉ kết nối bạn với người mua và người bán.

Rõ ràng, để ẩn danh được, bạn phải trả một khoản phí cao. Để cung cấp càng ít thông tin nhận dạng trong giao dịch, bạn càng phải trả nhiều tiền hơn. Điều đó cũng hợp lý: những người bán Bitcoin đang mạo hiểm bằng cách không xác minh danh tính của bạn. Tôi đã có lần mua Bitcoin để đổi lấy thẻ quà tặng Vanilla Visa với mức phí 1,70 đô-la cho mỗi đô-la, tỉ lệ này hơi thái quá nhưng cần thiết để đảm bảo tính ẩn danh.

Tôi đã nói rằng Bitcoin không phải là vô danh. Ví dụ, có một bản ghi rằng tôi đã trao đổi một số thẻ quà tặng trả trước lấy Bitcoin. Một điều tra viên có thể theo dấu Bitcoin của tôi ngược về các thẻ quà tặng.

Nhưng có nhiều cách để rửa Bitcoin, che khuất mọi liên kết ngược về tôi.

Rửa tiền là điều mà giới tội phạm thường xuyên thực hiện. Nó thường được sử dụng trong buôn bán ma túy, nhưng nó cũng đóng một vai trò trong tội phạm tài chính. Rửa tiền có nghĩa là bạn ngụy trang người sở hữu ban đầu, thường bằng cách gửi tiền ra khỏi đất nước, cho nhiều ngân hàng ở những quốc gia có luật riêng tư nghiêm ngặt. Bạn cũng có thể làm điều tương tự với tiền ảo.

Có các dịch vụ trộn tiền, lấy Bitcoin từ nhiều nguồn khác nhau và kết hợp lại – hay gọi là trộn – để ra kết quả là Bitcoin giữ nguyên giá trị của nó nhưng mang dấu vết của rất nhiều chủ sở hữu. Điều này khiến người khác sau này khó nói được chủ sở hữu nào đã thực hiện một giao dịch mua nào đó. Nhưng bạn phải cực kỳ cẩn thận, bởi vì có hàng tỉ trò gian lận ngoài kia.

Tôi đã làm như vậy. Tôi tìm thấy một dịch vụ rửa tiền trực tuyến và họ đã lấy một khoản phí ngoài giao dịch. Tôi thực sự đã nhận được giá trị Bitcoin mong muốn. Nhưng hãy nghĩ về điều này: dịch vụ rửa tiền lúc này đã có một trong những địa chỉ email ẩn danh của tôi và cả hai địa chỉ Bitcoin được sử dụng trong giao dịch. Vì vậy, để tung thêm hỏa mù, tôi đã giao Bitcoin cho một ví Bitcoin thứ hai được thiết lập bằng cách mở một mạch Tor mới, thiết lập các bước nhảy mới giữa tôi và website cần truy cập. Bây giờ giao dịch được làm xáo trộn triệt để, khiến cho việc sau này một người muốn lần ra dấu vết rằng hai địa chỉ Bitcoin được sở hữu bởi cùng một người là rất khó khăn. Tất nhiên, dịch vụ rửa Bitcoin có thể hợp tác với các bên thứ ba bằng cách cung cấp cả hai địa chỉ Bitcoin. Đó là lý do tại sao việc mua thẻ quà tặng trả trước một cách an toàn là rất quan trọng.

Sau khi sử dụng thẻ quà tặng để mua Bitcoin, hãy nhớ loại bỏ các thẻ nhựa một cách an toàn (đừng vứt trong thùng rác ở nhà). Tôi khuyên bạn nên sử dụng máy hủy cắt ngang dùng được cho thẻ nhựa, sau đó xử lý các mảnh vụn trong một thùng rác ngẫu nhiên cách xa nhà hoặc văn phòng của bạn. Khi nhận về Bitcoin đã được rửa, bạn có thể đăng ký một dịch vụ VPN làm ưu tiên riêng tư của bạn. Chính sách tốt nhất khi bạn đang cố gắng ẩn

danh đơn giản là không tin tưởng bất kỳ nhà cung cấp VPN nào, đặc biệt là những người tuyên bố không giữ lại bất kỳ nhật ký nào. Rất có thể họ sẽ vẫn tiết lộ ra các chi tiết của bạn nếu bị cơ quan thực thi pháp luật hoặc NSA liên lạc.

Ví dụ, chắc chắn các nhà cung cấp VPN phải có khả năng khắc phục sự cố trong mạng riêng của mình. Và việc này đòi hỏi họ phải có nhật ký, chẳng hạn nhật ký kết nối để khớp khách hàng với địa chỉ IP ban đầu của họ.

Như vậy, bởi vì ngay cả những nhà cung cấp tốt nhất cũng không thể tin tưởng được, nên chúng ta hãy mua dịch vụ VPN bằng Bitcoin đã được rửa thông qua trình duyệt Tor. Tôi khuyên bạn nên xem lại các điều khoản dịch vụ và chính sách bảo mật của nhà cung cấp VPN và tìm ra nhà cung cấp có vẻ tốt nhất trong nhóm. Bạn sẽ không tìm thấy một sự phù hợp hoàn hảo, chỉ là một sự phù hợp vừa đủ tốt thôi. Hãy nhớ rằng bạn không thể tin tưởng bất kỳ nhà cung cấp nào để duy trì tính ẩn danh. Bạn phải tự mình làm điều đó với hiểu biết rằng chỉ cần một lỗi cũng có thể tiết lộ danh tính thực sự của bạn.

Bây giờ, với một máy tính xách tay riêng chạy Tor hoặc Tails, sử dụng một mạng VPN mua bằng Bitcoin đã được rửa, qua một bộ phát sóng ẩn danh, bạn đã hoàn thành xong phần dễ dàng: thiết lập sự ẩn danh. Điều này sẽ tốn một vài trăm đô-la, có thể là 500, nhưng tất cả các mảnh ghép đã được phân tách ngẫu nhiên để chúng không thể dễ dàng bị kết nối ngược về bạn. Bây giờ đến phần việc khó: duy trì sự ẩn danh đó.

Tất cả các thiết lập và quy trình mà chúng ta vừa trải qua đều có thể bị tiêu hủy trong giây lát nếu bạn sử dụng điểm phát sóng ẩn danh ở nhà hoặc bật điện thoại di động, máy tính bảng, hay bất kỳ thiết bị di động nào khác được liên kết với danh tính thực của bạn tại vị trí thực tế nơi bạn đang sử dụng nhận dạng ẩn danh. Chỉ cần một lần sảy chân, điều tra viên có thể phát hiện ra mối tương quan giữa sự hiện diện của bạn với một vị trí bằng cách phân tích nhật ký của nhà cung cấp dịch vụ di động. Nếu xuất hiện một đường mòn giữa hoạt động truy cập ẩn danh với việc

thiết bị di động của bạn đăng ký vào cùng một trạm phát sóng di động, danh tính thực của bạn có thể bị lộ.

Tôi đã đưa ra một số ví dụ về điều này.

Bây giờ, nếu tính ẩn danh của bạn bị xâm phạm và bạn quyết định tham gia vào một hoạt động ẩn danh khác, bạn sẽ phải thực hiện lại quy trình này một lần nữa – xóa và cài đặt lại hệ điều hành trên máy tính xách tay ẩn danh, tạo một bộ tài khoản email và ví Bitcoin ẩn danh khác, và mua một bộ phát sóng ẩn danh khác. Hãy nhớ rằng Edward Snowden và Laura Poitras tuy đều đã có tài khoản email ẩn danh nhưng vẫn thiết lập thêm tài khoản email ẩn danh để họ có thể giao tiếp riêng với nhau. Bạn chỉ nên làm điều này nếu nghi ngờ rằng sự ẩn danh mà bạn thiết lập đã bị xâm phạm. Nếu không, bạn có thể sử dụng trình duyệt Tor (sau khi thiết lập một mạch Tor mới) thông qua bộ phát sóng và VPN ẩn danh để truy cập Internet bằng một nhận dạng khác.

Tất nhiên, bạn là người quyết định nên làm theo bao nhiêu trong số những gợi ý của tôi.

Ngay cả khi bạn làm theo những lời khuyên của tôi, người khác vẫn có thể nhận ra bạn. Bằng cách nào? Bằng cách bạn gõ máy tính.

Rất nhiều nghiên cứu đi sâu tìm hiểu cách mọi người chọn từ khi viết email và bình luận trên mạng xã hội. Qua đó, các nhà nghiên cứu thường có thể xác định được giới tính và sắc tộc, nhưng họ không thể biết các thông tin chi tiết hơn.

Hay là họ có thể?

Trong Thế chiến II, chính phủ Anh đã thành lập một số trạm nghe trên cả nước để chặn bắt các tín hiệu từ quân đội Đức. Kết quả sau đó là Đồng minh giải mã các thông điệp này – tại Trang viên Bletchley, địa điểm đặt trường Mật mã và Tín hiệu Chính phủ, nơi mã Enigma của Đức bị phá vỡ. Ban đầu, những người ở Trang viên Bletchley thực hiện chặn bắt các điện báo của Đức có thể xác định một số đặc điểm độc đáo của người gửi dựa trên

khoảng cách giữa các dấu chấm và dấu gạch ngang. Ví dụ, họ có thể biết khi nào phía Đức có nhân viên trực tổng đài mới, họ thậm chí còn đặt tên cho những người này.

Dấu chấm và dấu gạch ngang tiết lộ những người đứng đằng sau chúng bằng cách nào?

Có thể đo được khoảng thời gian giữa các lần gõ bàn phím của người gửi. Phương pháp phân biệt này về sau được gọi là Fist of the Sender (Nắm tay của người gửi). Có thể xác định các tổng đài viên vận hành khóa mã Morse bằng những "nắm tay" rất riêng của họ. Công nghệ điện báo không được thiết kế để thực hiện những việc đó (ai quan tâm đến chuyện ai gửi điện báo, nội dung điện báo có gì chứ!), nhưng trong trường hợp này, đây là một sản phẩm phái sinh thú vị.

Ngày nay, với những tiến bộ trong công nghệ kỹ thuật số, các thiết bị điện tử có thể đo sự khác biệt ở mức nano giây cách gõ bàn phím của mỗi người – không chỉ là thời gian giữ phím mà còn cả tốc độ chuyển sang phím tiếp theo. Nó có thể cho biết sự khác biệt giữa một người bình thường và một người sục sạo tìm kiếm lén lút bên bàn phím. Điều đó, cùng với cách lựa chọn ngôn từ, có thể tiết lộ rất nhiều về một giao tiếp ẩn danh.

Đây là vấn đề nếu bạn gặp phải sự cố khi ẩn danh địa chỉ IP của mình. Các website vẫn có thể nhận ra bạn – không phải vì lý do kỹ thuật mà vì một điều gì đó liên quan đến con người. Đây được gọi là phân tích hành vi.

Giả sử một website ẩn danh trên Tor quyết định theo dõi hồ sơ về hoạt động gõ phím của bạn. Có thể những người đứng đằng sau đó có ý đồ xấu và muốn biết thêm về bạn. Hoặc có thể họ làm việc với cơ quan thực thi pháp luật.

Nhiều tổ chức tài chính đã sử dụng phân tích gõ phím để xác thực sâu hơn chủ tài khoản. Như vậy, dù có người lấy được tên người dùng và mật khẩu của bạn, họ vẫn không thể giả mạo nhịp điệu đánh máy của bạn được. Đó là một lợi ích khi xác thực trực tuyến. Nhưng nếu như bạn không muốn làm thế thì sao?

Bởi vì phân tích tổ hợp phím rất dễ triển khai, các nhà nghiên cứu Per Thorsheim và Paul Moore đã tạo một plugin trêm trình duyệt Chrome có tên là Keyboard Privacy (Bảo mật bàn phím). Plugin lưu trữ các lần nhấn phím cá nhân của bạn và sau đó phát chúng ra theo các khoảng thời gian khác nhau. Mục đích ở đây là để tạo ra sự ngẫu nhiên trong nhịp điệu gõ phím bình thường của bạn để đạt được ẩn danh trực tuyến. Plugin này có thể che giấu thêm các hoạt động Internet ẩn danh của bạn.

Như chúng ta đã thấy, duy trì sự tách biệt giữa cuộc sống thực và cuộc sống ẩn danh trực tuyến là có thể, nhưng nó đòi hỏi sự cảnh giác liên tục. Trong các chương trước, tôi đã nói về một số thất bại ngoạn mục khi đang tàng hình. Đã có những nỗ lực thành công nhưng không lâu bền trong việc tàng hình.

Trong trường hợp của Ross Ulbricht, anh ta không thực sự có kế hoạch thay đổi nhận dạng bản thân một cách cẩn thận, thỉnh thoảng sử dụng địa chỉ email thực thay vì một địa chỉ ẩn danh, đặc biệt khi mới bắt đầu. Thông qua việc sử dụng tìm kiếm nâng cao của Google, một nhà điều tra đã có thể ghép lại đủ thông tin để tiết lộ chủ sở hữu bí ẩn của Silk Road.

Vậy còn Edward Snowden và những người khác quan tâm đến việc bị các cơ quan chính phủ giám sát? Chẳng hạn Snowden có một tài khoản Twitter. Nhiều người quan tâm quyền riêng tư khác cũng vậy – tôi có cách nào khác để thu hút mọi người tham gia vào một cuộc trao đổi sôi nổi trực tuyến chứ? Có một vài khả năng để giải thích cách những người này vẫn còn “vô hình.”

Họ không bị giám sát tích cực. Có lẽ một cơ quan chính phủ biết chính xác mục tiêu của mình nhưng không quan tâm. Trong trường hợp đó, nếu các mục tiêu không vi phạm luật, ai có thể nói chắc rằng họ không mất cảnh giác tại một thời điểm nào đó? Họ có thể tuyên bố chỉ sử dụng Tor cho các email ẩn danh, nhưng biết đâu họ cũng dùng tài khoản đó để mua các sản phẩm của Netflix.

Họ bị giám sát, nhưng không thể bị bắt. Tôi nghĩ rằng điều này

rất đúng với trường hợp của Snowden. Có thể anh đã sơ ý để mất sự ẩn danh của mình và hiện tại anh đang bị theo dõi tích cực bất cứ nơi nào anh đi qua, ngoại trừ một việc là anh đang sống ở Nga. Nga không có lý do thực sự nào để bắt giữ và dẫn độ anh trở về Mỹ.

Chắc bạn cũng vừa kịp để ý thấy tôi dùng từ "sơ ý": Việc sống hai cuộc sống thực sự là rất khó khăn, trừ khi bạn chú ý đến từng chi tiết. Tôi biết. Tôi đã làm thế rồi. Tôi đã lơ là phòng vệ khi sử dụng vị trí cố định để truy cập máy tính thông qua mạng điện thoại di động.

Một sự thật đương nhiên trong công tác an ninh là một kẻ tấn công dai dẳng sẽ thành công nếu có đủ thời gian và nguồn lực. Tôi luôn thành công khi kiểm tra các điều khiển bảo mật của khách hàng. Tất cả những gì bạn đang làm để ẩn danh là quăng ra những chướng ngại vật để kẻ tấn công phải nản lòng mà bỏ cuộc và chuyển sang mục tiêu khác.

Hầu hết chúng ta chỉ phải ẩn mình trong một lúc. Để tránh sếp tìm ra cớ hòng sa thải chúng ta. Để tránh luật sư của vợ/chồng cũ tìm ra manh mối nào đó chống lại bạn. Để tránh kẻ rình rập đáng sợ đã nhìn thấy hình ảnh của bạn trên Facebook và rắp tâm quấy rối bạn. Dù bạn muốn vô hình vì bất cứ lý do gì, các bước tôi đã chỉ ra ở trên sẽ có tác dụng đủ lâu để giúp bạn thoát khỏi tình trạng xấu.

Việc ẩn danh trong thế giới kỹ thuật số ngày nay đòi hỏi rất nhiều nỗ lực và sự cảnh giác liên tục. Nhu cầu ẩn danh của mỗi người mỗi khác – bạn có cần bảo vệ mật khẩu và giữ kín tài liệu tránh các đồng nghiệp không? Bạn có cần phải ẩn khỏi một người hâm mộ đang rình rập không? Bạn có cần trốn tránh cơ quan thực thi pháp luật vì bạn là người tố giác không?

Nhu cầu cá nhân là yếu tố quyết định các bước cần thiết để duy trì mức độ ẩn danh mong muốn của bạn – từ việc thiết lập các mật khẩu mạnh và nhận ra rằng máy in văn phòng của bạn đang gây hại đủ thứ cho bạn tới việc thực hiện các bước mô tả chi tiết

tại đây để làm cho việc một nhà điều tra pháp lý khám phá danh tính thật của bạn thực sự khó khăn.

Tuy nhiên, nhìn chung, tất cả chúng ta đều có thể học chút gì đó về cách giảm thiểu các dấu vân tay của mình trong thế giới kỹ thuật số. Chúng ta có thể suy nghĩ trước khi đăng bức ảnh có địa chỉ nhà có thể nhìn thấy ở hậu cảnh. Hoặc trước khi cung cấp ngày sinh thật và thông tin cá nhân khác trên hồ sơ mạng xã hội. Hoặc trước khi duyệt Internet mà không cần sử dụng phần mở rộng HTTPS Everywhere. Hoặc trước khi thực hiện cuộc gọi bí mật hoặc gửi văn bản mà không cần sử dụng công cụ mã hóa đầu cuối như Signal. Hoặc trước khi nhắn tin cho bác sĩ thông qua AOL, MSN Messenger hoặc Google Talk mà không cần OTR. Hoặc trước khi gửi một email bí mật mà không cần sử dụng PGP hoặc GPG.

Chúng ta có thể chủ động suy nghĩ về các thông tin của mình và nhận ra rằng ngay cả khi cách sử dụng các thông tin đó có vẻ như vô hại – chia sẻ ảnh, quên thay đổi tên đăng nhập và mật khẩu mặc định, sử dụng điện thoại công việc cho tin nhắn cá nhân hoặc thiết lập tài khoản Facebook cho con cái chúng ta – song thực ra chúng ta đang đưa ra các quyết định có thể có những hệ quả lâu dài. Vì vậy, chúng ta cần phải hành động.

Trọng tâm của cuốn sách này là hướng dẫn bạn cách hoạt động trên mạng mà vẫn giữ được quyền riêng tư quý báu của mình. Tất cả mọi người – từ những người không am hiểu công nghệ cho đến các chuyên gia bảo mật chuyên nghiệp – đều cần nghiêm túc trau dồi thứ nghệ thuật này, vốn đang ngày càng trở nên thiết yếu hơn: nghệ thuật ẩn mình.

LỜI CẢM ƠN

Cuốn sách này dành tặng cho người mẹ yêu quý của tôi Shelly Jaffe và bà tôi Reba Vartanian, những người đã hi sinh rất nhiều cho tôi trong suốt cuộc đời tôi. Bất kể tôi rơi vào hoàn cảnh nào, mẹ và bà luôn ở bên tôi, đặc biệt là những khi tôi cần. Cuốn sách này sẽ không thể ra đời nếu không có gia đình tuyệt vời của tôi, nhưng người đã dành cho tôi tình yêu và sự hỗ trợ vô điều kiện trong suốt cuộc đời tôi.

Vào ngày 15 tháng 4 năm 2013, mẹ tôi qua đời sau cuộc chiến đấu dai dẳng với căn bệnh ung thư. Sự việc xảy ra sau nhiều năm khó khăn và đấu tranh để chống chịu với những ảnh hưởng của hóa trị. Mẹ tôi đã có được một vài ngày tốt lành sau những phương pháp điều trị khủng khiếp được sử dụng trong y học hiện đại để chống lại những loại ung thư này. Thông thường bệnh nhân có thời gian rất ngắn – thường là chỉ vài tháng trước khi họ không chịu nổi căn bệnh này. Tôi cảm thấy rất may mắn vì thời gian tôi có thể ở bên bà trong khi bà đang chiến đấu với trận chiến khủng khiếp này. Tôi rất biết ơn vì đã được nuôi dưỡng bởi một người mẹ yêu thương và tận tụy như vậy, người mà tôi cũng xem là người bạn tốt nhất của tôi. Mẹ tôi là một người tuyệt vời và tôi rất nhớ bà.

Vào ngày 7 tháng 3 năm 2012, bà tôi qua đời đột ngột trong khi được điều trị tại Bệnh viện Sunrise ở Las Vegas. Gia đình chúng tôi đã mong bà trở về nhà, nhưng điều đó không bao giờ xảy ra. Trong nhiều năm trước khi bà ngoại của tôi qua đời, trái tim bà luôn buồn bã vì cuộc chiến chống ung thư của mẹ tôi. Tôi rất nhớ bà và tôi ước bà có ở đây để tận hưởng thành tựu này.

Tôi hy vọng cuốn sách này sẽ mang lại nhiều hạnh phúc cho trái tim của mẹ và bà tôi, khiến cho họ tự hào rằng tôi đang giúp bảo vệ quyền riêng tư của con người.

Tôi hi vọng bố tôi, Alan Mitnick, và anh trai tôi, Adam Mitnick, có ở đây để kỷ niệm việc xuất bản cuốn sách quan trọng về trở nên

vô hình này khi tình trạng gián điệp và giám sát giờ đây đã trở thành chuẩn tắc.

Tôi đã có may mắn được hợp tác với chuyên gia bảo mật và quyền riêng tư Robert Vamosi để viết cuốn sách này. Kiến thức giá trị của Rob về an ninh và kỹ năng với tư cách là nhà văn bao gồm khả năng tìm kiếm những câu chuyện hấp dẫn, nghiên cứu các chủ đề này và lấy thông tin do tôi cung cấp rồi viết nó theo cách thức và văn phong mà bất kỳ một độc giả nào không phải chuyên gia kỹ thuật cũng có thể hiểu được. Tôi phải ngả mũ kính trọng Rob, người đã làm một khối lượng lớn công việc khó khăn cho dự án này. Thành thật mà nói, tôi không thể hoàn thành cuốn sách nếu không có anh ấy.

Tôi háo hức cảm ơn những người đại diện cho nghề nghiệp chuyên môn của tôi và có những cống hiến theo những cách phi thường. Người đại diện của tôi, David Fugate của LaunchBooks, đã đàm phán hợp đồng sách và đóng vai trò liên lạc với nhà xuất bản Little, Brown. Khái niệm về Nghệ thuật tàng hình do John Rafuse của 121 Minds đưa ra, ông là người đại diện của tôi để nói về các cam kết và chứng nhận, và ông cũng thực hiện phát triển kinh doanh chiến lược cho công ty của tôi. Hoàn toàn từ sáng kiến của riêng mình, John đã cho tôi một đề nghị về một cuốn sách hấp dẫn, cùng với một mô hình bìa. Ông đặc biệt khuyến khích tôi viết cuốn sách này để giúp giáo dục người dân trên thế giới về cách bảo vệ quyền riêng tư cá nhân của họ, tránh bị theo dõi, đặc biệt là trong kỷ nguyên Dữ liệu lớn hiện nay. John thật tuyệt vời.

Tôi rất biết ơn vì đã có cơ hội làm việc với Little, Brown về việc phát triển dự án thú vị này. Tôi muốn cảm ơn biên tập viên của tôi, John Parsley, vì tất cả công việc vất vả và lời khuyên tuyệt vời của anh ấy đối với dự án này. Cảm ơn, John.

Tôi muốn cảm ơn người bạn Mikko Hypponen, giám đốc nghiên cứu của F-Secure, vì đã dành thời gian quý giá để viết lời tựa cho cuốn sách này. Mikko là một chuyên gia về bảo mật và riêng tư có uy tín cao, người đã tập trung vào nghiên cứu phần mềm độc hại

trong hơn 25 năm.

Tôi cũng xin cảm ơn Tomi Tuominen của F-Secure vì đã dành thời gian trong lịch làm việc bận rộn của mình để thực hiện đánh giá kỹ thuật bản thảo và giúp phát hiện bất kỳ lỗi nào và nắm bắt bất cứ thứ gì bị bỏ qua.

VỀ TÁC GIẢ

KEVIN MITNICK là cái tên xuất hiện trong vô số tài liệu được công bố và phát sóng trên toàn thế giới. Nhóm kiểm định khả năng xâm nhập hàng đầu của Mitnick được các công ty và chính phủ lớn trên thế giới đánh giá cao và mời hợp tác. Mitnick Security Consulting LLC, công ty do ông thành lập, có nhiều khách hàng là các công ty lớn xuất hiện trong danh sách Fortune 500 và các chính phủ trên toàn thế giới. Mitnick cũng là tác giả của các cuốn sách ăn khách Ghost in the Wires (Bóng ma trên mạng), The Art of Intrusion (Nghệ thuật xâm nhập), và The Art of Deception (Nghệ thuật lừa dối). Ông sống ở Las Vegas và là một diễn giả hàng đầu trên khắp thế giới về an ninh mạng.

mitnicksecurity.comtwitter.com/kevinmitnick