HIEU NGO

NHỮNG THỦ THUẬT AN NINH MẠNG TỪ MỘT CỰU HACKER

LỜI NÓI ĐẦU

Cuối năm 2019, tôi đã được thả khỏi nhà tù liên bang Mỹ sau khi hoàn thành một phần của bản án 13 năm. Tôi - một cựu hacker - và là một kẻ đánh cắp thông tin cá nhân chuyên nghiệp. Năm 16 tuổi, tôi bị cuốn hút bởi máy tính và công nghệ thông tin, có thể là do gia đình tôi có một cửa hàng điện tử nhỏ ở Việt Nam. Thông qua Google và các tạp chí về công nghệ, tôi đã học về tấn công xâm nhập (hacking) và bảo mật (security). Lúc đầu, hacking với tôi chỉ là một sở thích và tôi chỉ hack cho vui. Nhưng sau đó, tôi thấy rằng mình có thể kiếm tiền một cách dễ dàng bằng cách hack các websites và đánh cắp thông tin cá nhân. Tôi cảm thấy đời mình thật tươi đẹp, tôi nghĩ rằng mình có thể phụ giúp cho gia đình. Nhưng không, càng nhiều tiền kiếm được đồng nghĩa với việc tôi phải ở trong tù và rời xa gia đình tôi lâu hơn.

Trong tù, tôi nhận ra mình đã làm hại cuộc sống của rất nhiều người và tôi đã được nỗi đau của họ. Đó là lý do lớn nhất khiến tôi viết tài liệu những hướng dẫn bảo mật an ninh mạng này. Tôi hy vọng nó sẽ giúp đỡ được thật nhiều người. Đây cũng là cơ hội để tôi nói lời xin lỗi với tất cả mọi người. Nhà tù là một nơi rất khắc nghiệt, nhưng nó cho tôi thời gian để suy nghĩ về cuộc đời và những lựa chọn của mình. Tôi cam kết với bản thân phải làm những điều có ích và sống tốt hơn mỗi ngày. Tôi hiểu rằng tiền chỉ là một phần của cuộc sống và tiền không phải là tất cả, nó không thể mang lại hạnh phúc đích thực cho bạn. Tôi hy vọng những tội phạm an ninh mạng ngoài kia có thể học được nhiều điều từ bài học kinh nghiệm của tôi. Tôi hy vọng họ sẽ dừng những việc mình đang làm, thay vào đó sử dụng kỹ năng của họ để giúp thế giới tốt đẹp hơn.

Hướng dẫn bảo mật này chỉ là bước mở đầu trong hành trình cống hiến những điều tốt đẹp cho xã hội của tôi. Tôi đã mất rất nhiều tháng để thực hiện dự án này với vô số lần chỉnh sửa, tôi viết và nghiên cứu bất kể ngày đêm. Trong tù, tôi phải đối mặt với rất nhiều thử thách: Không có Microsoft Word, không Google và không Internet. Giải pháp của tôi là viết bằng bút và giấy, sau đó nhập những nội dung đó vào hệ thống nhắn tin (online messaging system) mà chúng tôi được phép sử dụng. Đó là hệ thống cho phép chúng tôi giữ liên lạc với gia đình và bạn bè. Nó không phải là một trình soạn thảo văn bản, nhưng vẫn cảm ơn vì ít ra nó cũng có chức năng kiểm tra lỗi chính tả.

Tôi đã gửi bản thảo của tôi cho Jonathan Lusthaus để chuẩn bị cho việc công bố. Tôi rất biết ơn vì sự hỗ trợ và sự động viên anh ấy đã dành cho tôi. Tôi cũng cảm ơn sự hỗ trợ của gia đình, bà ngoại tôi và những người thân yêu khác. Tôi xin dành tặng tài liệu này cho những người đã mất: Bob và Roy. Tôi cũng cám ơn người yêu cũ của mình vì đã truyền cảm hứng để tôi có thể thực hiện dự án này.

Tôi rất hạnh phúc vì đã hoàn thành tài liệu này. Hy vọng bạn, những người dùng phổ thông trên mạng Internet sẽ cảm thấy nó hữu ích trong việc nâng cao sự an toàn cũng như bảo vệ quyền riêng tư của mình. Tôi viết tài liệu này với tư cách một hacker, người đã hưởng lợi rất

nhiều từ các lỗ hổng bảo mật nhung nhiều thủ thuật trong đây rất dễ sử dụng và phổ biến trong lĩnh vực an ninh mạng. Tôi hy vọng chúng sẽ được thật nhiều người áp dụng.

Tài liệu này được viết trong thời gian tôi ở trong tù, do đó không có đủ điều kiện để kiểm tra hoặc nghiên cứu kỹ mọi thứ. Nếu bạn là một người có nhiều kiến thức về công nghệ và tìm thấy những lỗi hoặc thông tin chưa chính xác thì tôi thành thật xin lỗi. Rất mong bạn hiểu và thông cảm cho sự cố gắng của tôi. Trong nhiều trường hợp, tôi chỉ có thể đưa ra ý kiến của mình về bảo mật và bảo vệ quyền riêng tư, mọi người cần cẩn trọng và chịu trách nhiệm về lựa chọn của mình. Tuy nhiên, đây là những vấn đề cần được xem xét một cách nghiêm túc, thế giới ngoài kia có rất nhiều kẻ xấu và luôn dõi theo từng bước đi của bạn - tôi đã từng là một người như thế.

GIỚI THIỆU

Tài liệu này sẽ hướng dẫn bạn những phương pháp thực tế để bảo vệ mình trên không gian mạng và những thủ thuật giúp bạn bảo vệ tốt hơn quyền riêng tư của mình. Mục tiêu chính là giúp những người dùng Internet phổ thông có thể giảm rủi ro về một mức độ có thể chấp nhận được, bởi vì bạn không thể loại bỏ hoàn toàn rủi ro khi sử dụng môi trường Internet. Trển thực tế, không có cách nào để đảm bảo an toàn một cách tuyệt đối. Mục tiêu của chúng ta là nâng chi phí phải đánh đổi khi thực hiện tấn công lên một mức không còn đáng giá so với lợi ích mà những hacker, tội phạm mạng và gián điệp mạng nhận lại được.

Công nghệ không ngừng phát triển từng ngày, từ những máy chủ, máy tính bàn, máy tính xách tay đến các máy tính bảng. Hiện nay, mỗi người đều sở hữu cho mình một chiếc điện thoại thông minh - mà chính bản thân nó cũng được xem là một "máy tính". Trong quyển sách "Future Crimes" của mình, Marc Goodman đã đề cập "Bất cứ thứ gì khi được kết nối đều có thể bị tấn công" ("Everything is connected, everything is vulnerable"). Thực tế là vậy, Internet có thể giúp chúng ta ngồi tại chỗ và ngao du khắp thế giới, cho chúng ta rất nhiều ý tưởng và thông tin đánh giá. Internet giúp kết nối mọi người, cho phép bạn kết nối với những người bạn mới ở khắp nơi trên thế giới. Với Internet of Things (IoTs), thậm chí các thiết bị gia dụng cũng có thể sử dụng web để giúp cuộc sống của con người thuận tiện hơn.
Nhưng cũng không thiếu những tin tức về việc các cá nhân và tổ chức bị tấn công vẫn đang diễn ra hàng ngày trên khắp thế giới. Trong những năm gần đây, những kẻ xấu đã khai thác các thiết bị IoT ở những gia đình và văn phòng để tạo nên một mạng lưới botnet mạnh mẽ. Họ có thể dùng mạng lưới này để đánh sập một hệ thống máy chủ bằng cách tấn công từ chối dịch vụ (DOS). Họ cũng có thể dùng mạng bonet để gửi email rác (spam), email lừa đảo (phishing) hoặc đánh cắp các thông tin tài chính.
Sự thiếu kiến thức về bảo mật trên môi trường trực tuyến (online security) và quyền riêng tư (privacy) cần phải được nghiêm túc xem xét trong thời đại này. Chúng ta đang sống trong kỷ nguyên số, nơi mà mọi thứ đều được kết nối với nhau. Đây là lúc quan trọng hơn bao giờ hết để chúng ta dừng lại một chút và đặt câu hỏi xem liệu thiết bị chúng ta đang dùng hoặc các thông tin cá nhân của chúng ta có bị đánh cắp hay không. Thiệt hại gây ra có thể ảnh hưởng nặng nề đến cả mặt vật chất lẫn tinh thần của chúng ta. Cái gì cũng có hai mặt của nó, Internet cũng vậy: mặt lợi và mặt hại.

Những dịch vụ trực tuyến miễn phí như Google, Facebook, Twitter, Snapchat, Instagram "miễn phí" vì có lý do của nó. Cái giá mà bạn đang trả cho các dịch vụ miễn phí đó chính là quyền riêng tư của chính mình. Các công ty đó cung cấp cho chúng ta những lợi ích tuyệt vời, kết nối bạn với những người thân yêu, làm quen với những người bạn mới hoặc tìm giúp bạn kiếm thông tin mình cần. Nhưng trên thực tế, bạn đã từ bỏ nhiều quyền lợi của mình bằng cách chấp nhận các điều khoản sử dụng (TOS) dài dòng và nhàm chán của họ, thứ mà bạn không bao giờ đọc! Các công ty thu thập dữ liệu của bạn để phát triển sản phẩm, dịch vụ của họ, và họ cũng có thể bán dữ liệu của bạn cho các nhà quảng cáo, các tổ chức khác hoặc thậm chí là giao nộp chúng cho chính phủ.

Những dữ liệu nhạy cảm của bạn cũng đang phải đối mặt với các rủi ro. Khi dữ liệu được lưu trữ trên các máy chủ trên khắp thế giới, chúng trở thành mục tiêu của những hackers, tội phạm mạng và gián điệp mạng. Những kẻ xấu làm việc không ngừng nghỉ để tìm cách khai thác những dữ liệu đó. Họ có thể tìm ra những lỗ hổng trên máy hệ thống, hoặc dụ những nhân viên khiến họ vô tình download các phần mềm độc hại (malicious software).

Quyền riêng tư là một quyền vốn có của con người. Đây là cơ hội cho bạn học cách để bảo vệ quyền riêng tư của mình, cả trên môi trường trực tuyến và môi trường thực tế. Tin vui là các công nghệ bảo mật luôn được phát triển và cập nhật từng ngày để chống lại những kẻ xấu ăn cắp thông tin nhạy cảm của bạn. Tuy nhiên, bạn không thể dựa hoàn toàn vào chúng cũng như bộ phận IT. Một sự bảo mật tốt đòi hỏi phải có sự kết hợp giữa tổ chức và các người dùng cá nhân. Chẳng hạn, các cá nhân luôn là đối tượng nhạy cảm của kiểu tấn công "social engineering", bộ phận IT không thể ngăn cản khi người dùng bị những kẻ tấn công lừa để cung cấp thông tin cá nhân cho họ hoặc click vào các đường dẫn chứa mã độc.

Tài liệu này viết ra dành cho bạn - những người dùng Internet phổ thông. Cách tốt nhất để đương đầu với bảo mật trực tuyến (online security) và bảo vệ quyền riêng tư là phải hiểu rõ bạn đang đối mặt với ai. Người xưa đã từng nói "biết địch biết ta, trăm trận trăm thắng", với tư cách là một cựu hacker, tôi hy vọng mình sẽ cung cấp cho bạn một cái nhìn sâu hơn về những phương pháp đơn giản (và trung cấp) liên quan đến bảo mật và bảo vệ quyền riêng tư để giúp bạn an toàn hơn.

NHỮNG PHƯƠNG PHÁP BẢO MẬT VÀ BẢO VỆ QUYỀN RIÊNG TƯ

10 thủ thuật bảo mật căn bản

Tôi sẽ bắt đầu với 10 thủ thuật chung giúp bạn an toàn hơn trên không gian mạng:

1. Đừng bao giờ click vào những quảng cáo hay những liên kết (links) mà bạn không tìm kiếm. Nếu bạn tìm kiếm điều gì đó, đừng bao giờ cho rằng mọi website đều an toàn. (Chẳn hạn nhiều trang web liên kết đến những từ khóa phổ biến như "free" hoặc "lyrics" đều có thể ẩn chứa nguy hiểm). Chỉ nên truy cập những website nổi tiếng và lâu đời vì họ có một nền tảng bảo mật đáng tin cậy.
2. Bookmark lại những website bạn thường truy cập để tránh tình trạng gõ sai chính tả, việc này có thể dẫn bạn đến những trang web lừa đảo. Ví dụ: Thay vì đi đến website chính thức là www.facebook.com, bạn có thể vô tình trạng cập vào những website độc hại như www.faceboook.com hoặc www.facbook.com.

3. Nếu bạn nhận được những email đáng ngờ và có tài liệu đính kèm, hãy luôn xác nhận lại với người gửi bằng một kênh liên lạc khác trước khi mở tài liệu. Rất có thể email này không phải do chính họ gửi.
4. Không bao giờ tin vào những email hoặc tin nhắn nào nghe có vẻ "quá thật". Chúng có thể được gửi từ những kẻ xấu đang cố gắng cài mã độc vào máy tính của bạn và ăn cắp mật khẩu hoặc các thông tin nhạy cảm khác. (Đối với những người chuyên nghiệp, có thể download những file này bằng cách sử dụng máy ảo (Virtual Machine) để cô lập rủi ro - tuy nhiên đây cũng là một rủi ro lớn cho những ai không thực sự hiểu rõ điều mình đang làm).
5. Luôn sử dụng xác thực nhiều yếu tố (multi-factor authentication) bất cứ nơi nào có thể. Kiểm tra thêm các thông tin liên quan đến "hoạt động của tôi" (my activity) hoặc "hoạt động của tài khoản" (account activities) để theo dõi các rủi ro có thể xảy ra với tài khoản của bạn.
6. Không dùng chung mật khẩu cho các dịch vụ trực tuyến. Nếu kẻ xấu lấy được mật khẩu chung này của bạn, họ có thể truy cập vào các tài khoản khác. Mỗi dịch vụ quan trọng nên được sử dụng một khẩu riêng biệt (Chẳng hạn sử dụng phương pháp "Spider's Web" phía dưới)
7. Tránh sử dụng các mật khẩu đơn giản và dễ đoán như: những từ nằm trong từ điển - "password" - hoặc tên người dùng của bạn (username). "123456" và "qwerty" cũng là những mật khẩu không tốt. Tránh sử dụng các thông tin cá nhân làm mật khẩu vì chúng sẽ dễ bị đoán: Ví dụ như ngày sinh, tên một người thân, số điện thoại, tên thú cưng ... Đồng thời cũng nên tránh chia sẻ mật khẩu của bạn cho người khác.
8. Ghi chép lại mật khẩu có thể giúp bạn khỏi phải nhớ chúng, nhưng nó cũng mang lại rủi ro cho bạn. Lưu trữ những mật khẩu đó trong email hoặc trên thiết bị của bạn là một điều rất nguy hiểm. Nếu bạn thật sự muốn ghi chép lại mật khẩu của mình, hãy đảm bảo rằng bạn ghi lại bằng một cách mà chỉ có bạn mới có thể hiểu được (phòng hờ trường hợp thông tin này rơi vào tay người khác).
9. Tránh đăng các thông tin nhạy cảm lên các tài khoản mạng xã hội, kẻ xấu có thể lợi dụng thông tin này để tấn công bạn hoặc những mối quan hệ của bạn.
10. Thay đổi mật khẩu mặc định trên tất cả các thiết bị hoặc phần mềm của bạn thành mật khẩu mới với độ phức tạp cao. Những kẻ xấu luôn tìm những cách dễ dàng để tấn công bạn, trong đó bao gồm cách sử dụng danh sách mật khẩu mặc định của các nhà sản xuất (Ví dụ như mật khẩu mặc định của wifi router có thể là "password", "admin" hoặc "123456").

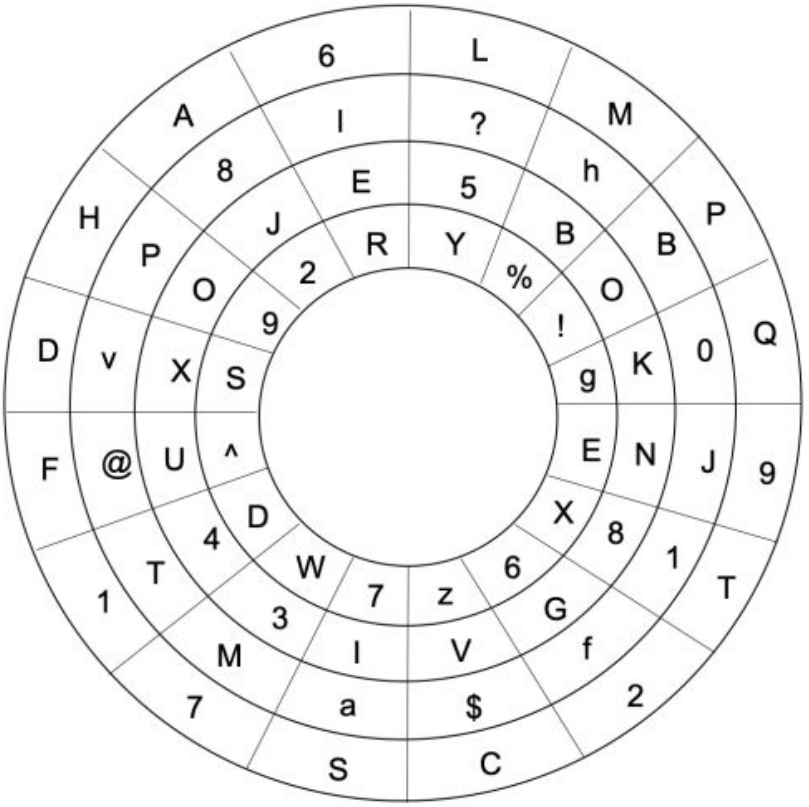
Ngoài những thủ thuật trên, dưới đây tôi sẽ chia sẻ thêm nhiều thông tin cụ thể để giúp bạn bảo mật tài khoản của mình, trình duyệt web (Browser), hệ điều hành (Operating Systems), dữ liệu (Data), các kết nối dữ liệu (Communications and Traffic).

BẢO MẬT TÀI KHOẢN

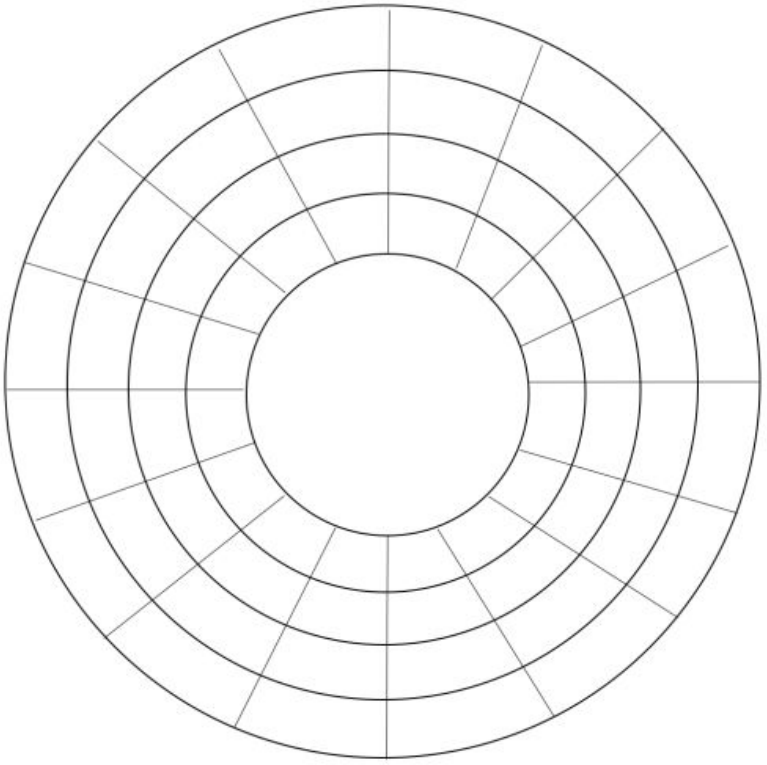
Mật khẩu là thứ quan trọng nhất bạn cần phải đặc biệt chú ý, mọi thứ sẽ trở nên rất tồi tệ nếu thông tin đăng nhập của bạn rơi vào tay những kẻ xấu. Đây cũng là cách phổ biến nhất để bảo vệ tài khoản của bạn. Trong phần này, bạn sẽ học cách để tạo ra một mật khẩu tốt và mạnh - tốt nhất là dài hơn 8 - 10 ký tự - để tránh các kẻ xấu đoán hoặc bẻ khóa được mật khẩu của bạn. Bạn cũng sẽ học về các phần mềm quản lý mật khẩu, ứng dụng xác thực nhiều yếu tố (multi-factor authentication app) và những thủ thuật khác để bảo vệ các tài khoản trực tuyến của bạn: email, tài khoản mạng xã hội, cloud storage …

Khái niệm Spider's Web Password Generator

Tôi đã nghĩ ra một phương pháp tạo mật khẩu rất đơn giản, an toàn, tiện lợi và hoàn toàn miễn phí có tên gọi "Spider's Web". Không cần phải cài đặt ứng dụng, không cần phải đăng nhập vào website để sử dụng, tất cả những gì bạn cần chỉ là giấy và bút (hoặc cũng có thể sử dụng Microsoft Word).
Cách sử dụng:



Hình 1: Một ví dụ về "Spider's Web"



Hình 2: Một bản "Spider's Web" trống

Ở hình 1, chúng ta có 4 vòng tròn, mỗi vòng tròn có 16 ô và mỗi ô chứa một cứ tự ngẫu nhiên (viết hoa hoặc viết thường, số hoặc ký tự đặc biệt).
Đi từ ngoài vào trong, vòng tròn thứ 1 và vòng tròn thứ 3 chứa các ký tự viết hoa và số. Những vòng tròn này chứa mật khẩu gốc (master password), đây là mật khẩu đơn giản mà bạn cần phải nhớ. Lưu ý: ở vòng tròn số 1 và số 3 này, các ký tự và chữ số phải khác nhau, không được trùng lặp. Bạn không cần phải sử dụng ký tự đặc biệt ở vòng tròn số 1 và số 3 vì điều này sẽ khiến cho mật khẩu gốc trở nên khó nhớ.

Vòng tròn thứ 2 và thứ 4 chứa chữ, số, và ký tự đặc biệt, các ký tự này không được in đậm. Đây chính là phần để tạo ra các mật khẩu dành cho máy tính của bạn hoặc các tài khoản trực tuyến như email, tài khoản mạng xã hội. Bằng cách sử dụng phương pháp này, bạn có thể tạo ra các mật khẩu phức tạp mà không cần phải nhớ chúng.

Ví dụ: bạn có thể sử dụng tên viết tắt của dịch vụ trực tuyến bạn cần sử dụng cộng với mật khẩu gốc của bạn để tạo ra mật khẩu riêng biệt cho mỗi tài khoản. Nếu bạn đang tạo một tài khoản Youtube mới, bạn có thể kết hợp cụm từ viết tắt của Youtube như là "utube" kết hợp với mật khẩu gốc của bạn, ví dụ như "vietnam". Kết quả, bạn sẽ tạo ra một cụm từ mới là "UTUBEVIETNAM", sau đó, bạn sử dụng vòng tròn thứ 2 và thứ 4 ở hình 1 để tìm ra mật khẩu "Spider's Web" của bạn. Nếu bạn tìm ký tự "U" ở vòng tròn thứ 3, bạn sẽ thấy nó tương ứng với ký tự "^" ở vòng tròn thứ 4. Ký tự "T" ở vòng tròn thứ 1 khớp với ký tự "1" ở vòng tròn thứ 2. Cứ tiếp như vậy, kết quả cuối cùng bạn có được từ mật khẩu gốc "UTUBEVIETNAM" tương ứng với "^1^%Rz7R1E8h". Đây chính là mật khẩu bạn sử dụng cho tài khoản Youtube của mình.

Hình phía trên chỉ là ví dụ để hướng dẫn cách sử dụng. Các bạn cần phải tạo cho mình một "Spider's Web" từ hình trống (hình 2) tôi cung cấp ở trên. Chỉ cần đảm bảo rằng vòng tròn thứ 1 và thứ 3 chứa tất cả các ký tự mà bạn dự định sử dụng để tạo ra các mật khẩu gốc của mình. Bạn có thể tạo ra phiên bản của riêng mình một cách thủ công hoặc sử dụng Microsoft Word, công cụ cho phép thiết kế một "Spider's Web" với số lượng ô linh hoạt, có thể thay đổi theo ý thích của bạn. Dù sử dụng cách nào đi nữa, sau khi hoàn tất, hãy nhớ lưu lại những bản sao - bạn có thể cất ở nhà, bỏ vào bóp, lưu trữ và điện thoại ... (tuy nhiên cần đảm bảo giữ gìn chúng cẩn thận đừng để thất lạc hoặc bị lộ ra ngoài).

Bạn cũng có thể sáng tạo thêm nhiều cách khác để tạo mật khẩu từ "Spider's Web".Chẳng hạn, vẫn sử dụng hướng tiếp cận căn bản như ở bước trên, mật khẩu gốc cho Facebook có thể là: FBVIETNAM. Thay vì sử dụng phương pháp ở bước trên, bạn có thể nhảy về phía trước hoặc lùi về phía sau với các ô ở vòng tròn thứ 2 và thứ 4. Ví dụ, trong hình 1, mật khẩu gốc bằng đầu bằng ký tự "F" ở vòng tròn đầu tiên, thay vì sử dụng ký tự "@", bạn có thể tiến về phía trước 1 ô và sử dụng ký tự "v" ở vòng trong thứ 2. Cứ tiếp tục như vậy, kết quả cuối cùng nhận được sẽ là "v!7WYfXlB".

Một cách khác là "jumping the circle". Nếu mật khẩu cho Gmail của bạn là GMVIETNAM, bạn sẽ bắt đầu bằng ký tự "G" ở vòng tròn thứ 3. Thay vì sử dụng ký tự "6" ở vòng tròn thứ 4, bạn có thể nhảy về vòng tròn thứ 2 và sử dụng ký tự "f". Tiếp tục như vậy, cuối cùng bạn sẽ có kết quả: "f%2aY$alXJ2%"

Có vô số cách để sử dụng "Spider's Web", cách dùng càng phức tạp thì càng giúp bạn bảo mật hơn. Nhưng phải đảm bảo rằng bạn phải nhớ được các quy luật để tạo ra mật khẩu đấy. Bạn có thể dùng cách này để nâng cao sự an toàn cho các câu hỏi bảo mật thường được dùng trong quá trình khôi phục mật khẩu. Các câu hỏi trong phần khôi phục mật khẩu thường dễ bị đoán hoặc bẻ khóa, bằng cách sử dụng "Spider's Web" bạn có thể tạo ra câu trả lời mang tính ngẫu nhiên, khó đoán nhưng bạn lại rất dễ nhớ.

Phần mềm quản lý mật khẩu

Ngoài cách sử dụng Spider's Web, có rất nhiều chương trình khác hỗ trợ lưu trữ và quản lý mật khẩu tập trung như: LastPass, KeePass, Bitwarden, 1Password, DashLane Password Safe, Password Gorilla và Roboform. Một vài trong số chúng là những ứng dụng cloud-based và có thể sử dụng trên nhiều thiết bị khác nhau, một số ứng dụng thì chỉ có thể được sử dụng trên thiết bị đã được cài đặt. Những ai không tin tưởng vào các phần mềm quản lý mật khẩu dạng cloud-based có thể sử dụng các phần mềm offline như Diceware. Bên cạnh việc cung cấp cho chúng ta những thủ thuật để tạo một mật khẩu mạnh, các phần mềm quản lý còn giúp ta mã hóa mật khẩu. Bạn chỉ cần nhớ một mật khẩu duy nhất đó là mật khẩu chính (master password) và đừng bao giờ quên nó.

Multi-factor Authentication Options

Chứng thực nhiều lớp (Multi-factor Authentication) giúp nâng cao tính bảo mật cho tài khoản của bạn, hãy sử dụng tính năng này trên bất kỳ nền tảng nào có hỗ trợ (Gmail, Facebook ...). Bạn có thể dùng tính năng này cho các tài khoản trực tuyến của mình bằng cách sử dụng các dịch vụ chứng thực hai lớp như Google Authenticator hoặc Duo Security. Khi bạn

đăng nhập vào tài khoản, những công cụ này sẽ tự động gửi cho bạn một mã chứng thực thông qua SMS hoặc thông qua những ứng dụng của họ.

Một vài công ty cũng đang phát triển các cách chứng thực sử dụng sinh trắc học như vân tay, võng mạc, giọng nói hoặc nhận diện khuôn mặt. Chúng có thể dùng để truy cập vào thiết bị của bạn hoặc xác nhận thanh toán như Alibaba hoặc Apple. Nếu bạn không muốn sử dụng tùy chọn chứng thực bằng sinh trắc học thì lựa chọn tốt nhất vẫn là mật khẩu.

Dành cho những ai muốn khám phá nhiều hơn về vấn đề này, có nhiều thiết bị phần cứng hỗ trợ cho việc chứng thực nhiều yếu tố như: USB chứng thực hai bước của MobiKey, NitroKey và Yubikey U2F. Các thiết bị này tạo một kết nối bảo mật với thiết bị của bạn không qua một máy ảo. Ngoài ra, còn có các loại thẻ với các loại chip bảo mật đặc biệt như qwertycards.com

BẢO MẬT TRÌNH DUYỆT WEB

Các trình duyệt bảo mật chuyên biệt

Có rất nhiều loại trình duyệt web bảo mật chuyên biệt trên thị trường hiện tại như Brave, Comodo Dragon, Epic Browser, TOR Browser hoặc các loại phổ biến như Firefox Quantum, Microsoft Edge và Google Chromium. Hầu hết các trình duyệt web đều cung cấp các tùy chọn về bảo mật và bảo vệ sự riêng tư, như là che giấu địa chỉ IP thực, hoặc phát hiện các file cookies đáng ngờ đang theo dõi các hoạt động trực tuyến của bạn. Nhưng vấn đề nằm ở chỗ, khi lựa chọn một trình duyệt, nếu trình duyệt đó càng phổ biến thì đó càng là mục tiêu chính của các hackers, tội phạm mạng và gián điệp để tìm kiếm lỗ hổng và chèn các mã độc vào thiết bị của bạn.

Các add-ons của trình duyệt

HTTPS Everywhere là một addon tuyệt vời cho các trình duyệt web như Firefox, Chromium và Opera. Nó đảm bảo rằng kết nối giữa bạn và website được bảo mật bằng cách mã hóa kết nối sử dụng giao thức Transport Layer Socket (TLS) hoặc Secure Socket Layer (SSL). Điều này giúp ngăn chặn người khác nghe lén kết nối của bạn. Đây là giải pháp tốt nhất hiện tại nhưng cũng không thể ngăn chặn hoàn toàn việc nghe lén. Các hacker có thể sử dụng một kỹ thuật tấn công gọi là "man-in-the-middle", với việc đánh cắp hoặc giả mạo chứng chỉ TLS/SSL sẽ cho phép họ can thiệp vào kết nối giữa bạn và website bạn đang kết nối.

Có một số add-ons cũng rất hữu dụng trong việc ngăn chặn quảng cáo, cookies ... như là Ublock Origin, Adblock Browser, FlashBlock, Disconnect, Privacy Badger, Ghostery và NoScript. Chúng có thể ngăn chặn việc theo dõi các hoạt động trực tuyến, hoặc việc dụ dỗ bạn truy cập vào các website nguy hại.

BẢO MẬT HỆ ĐIỀU HÀNH (OS)

Cũng như trình duyệt, không có hệ điều hành nào là hoàn hảo. Mỗi hệ điều hành đều có những điểm mạnh và điểm yếu riêng. Chẳng hạn, hệ điều hành Microsoft Windows có rất nhiều tính năng bảo vệ mạnh mẽ, nhưng bởi vì nó quá phổ biến và có lượng người dùng khổng lồ, đây luôn là mục tiêu chính bị nhắm đến với những kẻ xấu. Ngoài ra còn có các hệ điều hành khách như Whonix, Qubes, TAILS, Ubuntu, RedHat, Mac OS, Google Chrome

OS và Gallium OS. Hệ điều hành cho thiết bị di động có thể kể đến Google Android, Apple iOS. Hệ điều hành cho thiết bị di động đang trở thành mục tiêu hấp dẫn cho các hacker vì ngày nay mọi người đều sở hữu điện thoại thông minh. Mấu chốt giúp bạn có thể thoát khỏi tầm ngắm của các hacker là thường xuyên cập nhật phiên bản mới của hệ điều hành và các phần mềm khác.
Bên cạnh việc lựa chọn đúng OS cũng có rất nhiều phần mềm giúp bảo vệ chúng ta. Bao gồm các giải pháp giúp mã hóa dữ liệu hoặc mã hóa toàn bộ ổ cứng như Viivo, Veracrypt, BitLocker, FileVault, WinMagic, và Whole Disk Encryption. Phổ biến nhất là các phần mềm diệt virus, các tên tuổi nổi tiếng có thể kể đến: Cylance, Kaspersky, Norton, AVG, BitDefender, Malwarebytes, McAfee ... Chúng giúp phát hiện, cô lập, loại bỏ virus và các loại mã độc khác. Tuy nhiên, chỉ dựa vào phần mềm thôi là chưa đủ. Điều quan trọng là cần tắt tính năng "auto-run" trên thiết bị của bạn để đảm bảo virus hoặc các loại mã độc khác không được thực thi một cách tự động hoặc chạy từ các thiết bị như USB. Nguyên tắc vàng là luôn luôn scan các thiết bị xách tay như USB, đĩa CDs ... bằng các phần mềm diệt virus.

Một số thủ thuật hữu ích khác:
1. Để hạn chế các nguy cơ, hãy thường xuyên cập nhật các tất cả các phần mềm. Nếu phần mềm nào bạn không sử dụng, hãy gỡ bỏ chúng.
2. Bật tính năng "auto-update" trên thiết bị của bạn để giúp hệ điều hành tự động cập nhật các bản vá mới nhất giúp chống lại các rủi ro về bảo mật.
3. Trừ khi bạn hiểu thật rõ mình đang làm gì, nếu không thì đừng "jail break" thiết bị của bạn.
4. Luôn luôn tải phần mềm từ các website uy tín và tin cậy. Nếu bạn không có ý định tìm kiếm 1 phần mềm nào đó, hãy cẩn thận đừng để bị lừa cài đặt các phần diệt virus giả mạo.
5. Hãy luôn sử dụng tường lửa (firewall). Đây thường là tính năng có sẵn trên các hệ điều hành, nó sẽ giúp ngăn chặn các kết nối không hợp lệ đến thiết bị của bạn. Cũng có rất nhiều phần mềm của bên thứ ba đáp ứng nhu cầu này.

BẢO MẬT DỮ LIỆU VÀ KẾT NỐI
Ngày nay, các hacker, tội phạm mạng và gián điệp có các công cụ để theo dõi và ghi âm cuộc gọi, tin nhắn, hình ảnh và email của bạn. Sẽ rất hữu ích nếu bạn được trang bị đầy đủ kiến thức để chống lại các rủi ro trên. Thật may mắn, các dịch vụ mã hóa kết nối ngày càng phổ biến, được áp dụng rộng rãi và sử dụng dễ dàng. Chúng có thể giúp mã hóa tin nhắn, cuộc gọi, email và các file được chia sẻ. Một vài nền tảng nổi tiếng: Signal, Wickr, Redphone, Telegram, ProtonMail, PGP (Pretty Good Privacy), và còn rất nhiều nữa. Tuy nhiên, dịch vụ mã hóa kết nối đầu cuối (end-to-end encryption communication) chỉ hoạt động khi hai người (hoặc nhiều hơn) cùng đồng ý và sử dụng cùng một dịch vụ. Bạn cũng cần luôn đảm bảo rằng người bạn nghĩ rằng mình đang trao đổi đúng chính xác là người mà bạn muốn trao đổi. Cẩn thận hơn, hãy sử dụng cryptophones, loại điện thoại có tính năng mã hóa được tích hợp sẵn.
Sao lưu dữ liệu (backup data) cũng là một biện pháp an ninh quan trọng nhưng cần được thực hiện một cách an toàn.Trong những năm gần đây, lưu trữ đám mây đã trở nên phổ biến. Những nhà cung cấp phổ biến bao gồm: Dropbox, Google Drive, Amazon AWS. Lợi ích của việc backup là bảo vệ trước các rủi ro như hỏng ổ cứng, nhiễm virus hoặc bị mất cắp thiết bị. Một vài dịch vụ có hỗ trợ mã hóa dữ liệu cho bạn, nhưng bạn nên tự mã hóa dữ liệu của mình trước khi upload chúng. Những người yêu cầu tính riêng tư cao hơn có thể tự xây dựng giải pháp lưu trữ cho họ bằng cách dùng máy chủ riêng (private server) hoặc máy

chủ ảo (VPS - Virtual Private Server) và các nền tảng như Docker Hub, NextCloud, OwnCloud.
Với những ai không tin tưởng vào dịch vụ điện toán đám mây, hoặc muốn có thêm những lớp bảo vệ, backup khác có thể lưu trữ những dữ liệu quan trọng của mình vào một ổ cứng hoặc thiết bị nào đó có mã hóa. Với các tài liệu cực kỳ quan trọng, bạn cũng có thể in nó ra thành một bản cứng và lưu trữ cẩn thận.

Một vài thủ thuật hữu ích:
1. Bằng cách đọc Điều khoản sử dụng (TOS - Term of services) của một dịch vụ trực tuyến, bạn sẽ biết được mình đang đối mặt với điều gì. Trên đời này không có gì là miễn phí, mọi thứ đều có những chi phí ngầm của nó, và tùy thuộc vào bạn có quyết định sử dụng nó hay không. Tất cả những gì bạn cần là phải thật cẩn thận.
2. Trước khi mua một thiết bị "thông minh", trước tiên hãy xem xét xem liệu nó có an toàn khi khi sử dụng cho gia đình của mình hay không. Thông thường, bạn có thể điều chỉnh những tính năng liên quan đến sự riêng riêng tư. Những thiết bị như Amazon Echo hay Google Home sẽ liên tục ghi âm, bạn không nên nói những gì quá nhạy cảm vì chúng sẽ được lưu giữ bởi các công ty chủ quản hoặc chuyển sang cho đơn vị khác.
3. Che webcam hoặc camera của bạn lại với một mảnh giấy màu đen khi bạn không sử dụng chúng. Điều này giúp ngăn chặn kẻ khác theo dõi bạn.
4. Bảo mật wifi cũng rất quan trọng giúp ngăn chặn việc nghe lén dữ liệu truy cập Internet của bạn. Những lưu ý quan trọng: sử dụng mật khẩu mạnh, luôn cập nhật phiên bản mới nhất của firmware, tắt tính năng Wifi Protected Setup (WPS) và sử dụng router Wifi có tính năng bảo mật mới nhất (ví dụ như mã hóa). Những dữ liệu nhạy cảm cũng có thể được phục hồi từ các ổ cứng cũ. Để đảm bảo chúng không rơi vào tay người khác, hãy sử dụng những phần mềm như WipeInfo.

BẢO MẬT KẾT NỐI INTERNET
Những tùy chọn bên dưới giúp bạn bảo vệ truy cập Internet của mình. Chúng có thể bảo vệ bạn danh tính và bảo vệ bạn khỏi các sự dòm ngó. Có thể bạn nghĩ rằng chúng sẽ rất khó để áp dụng, nhưng thực tế, đây là những giải pháp hết sức đơn giản giúp bảo vệ quyền riêng tư của bạn

Virtual Private Network (VPN)
VPNs thường được dùng bởi các doanh nghiệp khi họ muốn cho phép nhân viên của mình truy cập vào máy chủ của công ty thông qua một đường truyền bảo mật. Nhân viên có thể làm việc một cách an toàn khi họ ở ngoài văn phòng. VPN cũng là một cách đơn giản nhất để bảo mật khi sử dụng Wifi - bất kể bạn ở đâu và bất kể mạng Wifi bạn đang sử dụng có kém an toàn như thế nào. VPN có rất nhiều tính năng: giúp bạn bảo vệ IP thực, mã hóa dữ liệu kết nối Internet, điều này sẽ gây rối loạn cho những kẻ thực hiện nghe lén hoặc những người quản trị kết nối ở các Wifi công cộng mà bạn kết nối (ví dụ cafe, airport lounge ...)
Một vài nhà cung cấp dịch vụ VPN uy tín: F-Secure Freedome, NordVPN, ProtonVPN và Sprint Secure Wifi. Sau khi bạn mua dịch vụ VPN, các nhà cung cấp dịch vụ sẽ cung cấp cho bạn hướng dẫn sử dụng và thông tin đăng nhập.

Proxies

Proxies là một cách khá đơn giản để bảo vệ sự riêng tư của bạn, nhưng chúng lại có chất lượng kết nối không được tốt và thường tiện dụng cho các tác vụ cá nhân hoặc các hoạt động mang tính chất tạm thời. Các dịch vụ proxies thường là miễn phí, trong khi đó cũng có nhiều dịch vụ proxies có thu phí định kỳ (subscription-based).

The Onion Router (TOR)
TOR là một sự thay thế tuyệt vời dành cho proxies. Đây là một dự án công nghệ độc lập của Bộ Quốc Phòng Mỹ (United States Department Of Defense - DOD), và được hỗ trợ từ nhiều nhóm khác. TOR giúp bảo vệ kết nối Internet của bạn bằng cách sử dụng thuật toán của nó để giấu địa chỉ IP thực sự của bạn. TOR không phải là một công nghệ bảo mật tuyệt đối, FBI đã chứng minh điều này bằng cách "tắt điện" hệ thống Silk Road và bắt giữ admin của nó. Nhưng nếu bạn là những công dân "sống và làm việc theo pháp luật" và chỉ muốn bảo vệ kết nối Internet của mình trước con mắt của những kẻ tò mò thì có thể dùng TOR một cách thoải mái. Thậm chí, bạn còn có thể đóng góp vào sự phát triển chung của TOR, chỉ đơn giản bằng cách sử dụng nó. Càng nhiều người tham gia vào mạng lưới thì nó càng an toàn hơn.

Máy ảo (Virtual Machine - VM)
Một cách khác để bảo vệ truy cập của bạn là thiết lập một máy ảo trên máy tính của bạn. Điều này cho phép giả lập một hệ thống máy tính khác, có hệ điều hành và có các phần mềm khác như bình thường, trên cùng hệ thống phần cứng của bạn. Một ưu điểm của việc này là không cần tốn chi phí để mua một máy tính mới. Nhưng lợi ích chính của nó là giúp cô lập hệ thống thực sự của bạn và tránh bị lộ thông tin như địa chỉ MAC và Serial Number ổ cứng. Nó tạo ra một môi trường thoải mái hơn dành cho bạn, đặc biệt là khi bạn muốn thực hiện bảo vệ máy thật của mình khỏi bị dòm ngó hoặc lây nhiễm mã độc.
Bạn có thể thiết lập một máy ảo bằng cách sử dụng các phần mềm như Oracle VM Virtual Box, VMware, hoặc QEMU.org. Ví dụ, nếu bạn sử dụng dịch vụ miễn phí của Oracle, bạn có thể chọn thiết lập máy ảo sử dụng Linux OS, Windows OS hoặc Mac OS. Có rất nhiều thông tin trên mạng hướng dẫn chi tiết hơn về máy ảo và cách thiết lập chúng. Nếu bạn có nhiều ổ cứng, bạn có thể tạo nhiều máy ảo để dùng cho nhiều mục đích khác nhau. Bạn thậm chí còn có thể thiết lập một phiên bản máy ảo y hệt máy thật mà bạn đang sử dụng trên một thiết bị lưu động như USB, hoặc thiết lập một máy ảo trên Internet và có thể đăng nhập vào chúng bằng cách sử dụng điện thoại thông minh.

Máy chủ ảo (Virtual Private Server - VPS)
Máy chủ ảo (VPS) giống với máy ảo (VM), nó không đòi hỏi bạn phải thiết lập một máy chủ thật để có thể bảo vệ kết nối của mình. Thiết lập một máy chủ vật lý có thể rất nhiều thời gian và tiền bạc, trong khi đó, VPS có thể mua với giá rất rẻ từ những nhà cung cấp dịch vụ lưu trữ (Hosting). Một vài nhà cung cấp dịch vụ hosting phổ biến: Amazon AWS, SAP, Heroku, Rackspace, DigitalOcean và Dreamhost. Một VPS giúp cung cấp thêm một lớp bảo mật, tương tự như cái cách mà VM hỗ trợ. Nó giúp bạn tránh bị lộ thông tin thực sự của máy tính của bạn như MAC address, Serial ổ cứng, và địa chỉ IP.

Kết hợp các lựa chọn
Tùy thuộc vào mức độ bảo mật và riêng bạn muốn, bạn có thể kết hợp nhiều phương pháp lại bằng nhiều cách khác nhau. Tuy nhiên, càng nhiều lớp bảo vệ, tốc độ Internet của bạn sẽ

càng chậm, bạn cần cân nhắc và cân bằng với nhu cầu của mình. Nhiều người đã sử dụng mô hình này:

Thiết bị của bạn → VPN → Internet

Nhưng bạn hoàn toàn có thể sáng tạo và thêm vào nhiều lớp bảo mật nữa. Hai mô hình khác mà tôi đề xuất gồm:

Thiết bị của bạn → VPN → TOR → Internet

Thiết bị của bạn → VPS → VPN → Internet

Những ai cần sự riêng tư cao hơn, thậm chí có thể sử dụng mô hình

Thiết bị của bạn → VM → VPS → VPN → TOR → Internet

Có vô số mô hình bạn có thể chọn, hãy sáng tạo. Không mô hình nào trong số đó là hoàn hảo, nhưng ít ra chúng sẽ gây nhiều khó khăn hơn cho những kẻ xấu.

Dịch: Hưng Nguyễn aka Bo [at] Quản Trị Linux