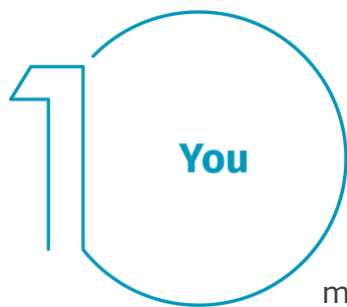


5 bước hàng đầu để làm việc an toàn tại nhà

Chúng tôi biết làm việc tại nhà có thể làm điều mới mẻ với một vài người, có lẽ quý vị thấy quá tải khi phải điều chỉnh theo môi trường mới. Một trong các mục tiêu của chúng tôi là giúp quý vị làm việc tại nhà bảo mật nhất có thể. Bên dưới là năm bước đơn giản để làm việc một cách bảo mật. Lợi ích lớn nhất là các bước này không chỉ giúp quý vị làm việc bảo mật, mà còn giúp quý vị và gia đình của quý vị an toàn hơn rất nhiều khi quý vị tạo ra ngôi nhà bảo mật mạng.



Quý vị: Trước hết, một mình công nghệ không thể bảo vệ toàn bộ cho quý vị. Chính quý vị là tuyến phòng thủ hiệu quả nhất. Những kẻ tấn công biết được rằng cách dễ nhất để đạt được mục tiêu là nhắm vào quý vị, thay vì nhắm vào máy tính hay thiết bị khác của quý vị. Nếu chúng muốn lấy mật khẩu, dữ liệu công việc hay kiểm soát máy tính của quý vị, chúng sẽ cố lừa quý vị tự trao cho chúng, thường là bằng cách tạo cảm giác cấp bách. Ví dụ: chúng có thể gọi điện cho quý vị, giả vờ là bộ phận hỗ trợ kỹ thuật của Microsoft và tuyên bố rằng máy tính của quý vị đã bị nhiễm mã độc. Hoặc là chúng sẽ gửi cho quý vị một email để cảnh báo rằng không thể gửi một gói bưu kiện để lừa quý vị nhấn vào một liên kết độc hại. Các dấu hiệu phổ biến nhất của một cuộc tấn công kỹ thuật xã hội bao gồm:

- Ai đó đang tạo cảm giác vô cùng khẩn cấp, thường là thông qua sự sợ hãi, hăm dọa, một cuộc khủng hoảng hoặc một hạn chót quan trọng. Những kẻ tấn công mạng rất giỏi tạo ra tin nhắn có tính thuyết phục, trông giống như được gửi bởi các tổ chức đáng tin cậy như ngân hàng, tổ chức chính phủ hoặc tổ chức quốc tế.
- Gây áp lực để bỏ qua hoặc làm ngơ các chính sách hoặc quy trình bảo mật, hoặc một lời đề nghị quá hấp dẫn so với thường lệ (đừng tin là mình trúng vé số nhé!)
- Thư được gửi từ một người bạn hoặc đồng nghiệp có chữ ký, giọng điệu hoặc văn phong nghe không giống họ viết.

Sau cùng, lớp phòng thủ tốt nhất chống lại các cuộc tấn công này chính là quý vị.

2 Home Network

Mạng gia đình: Hầu hết các mạng gia đình đều sử dụng mạng không dây (thường được gọi là mạng Wi-Fi). Đây là mạng cho phép toàn bộ các thiết bị của quý vị kết nối với mạng Internet. Hầu hết các mạng không dây được kiểm soát bởi bộ định tuyến Internet hoặc điểm truy cập không dây riêng, chuyên dụng. Cả hai loại đều hoạt động giống nhau: bằng cách phát sóng không dây để các thiết bị gia đình kết nối. Điều này có nghĩa là việc bảo mật cho mạng không dây của quý vị là phần chủ chốt trong việc bảo vệ cho nhà của quý vị. Chúng tôi khuyến nghị quý vị thực hiện các bước sau để bảo mật cho mạng:

- Thay đổi mật khẩu quản trị viên mặc định của thiết bị kiểm soát mạng không dây của quý vị. Tài khoản quản trị viên là tài khoản cho phép quý vị cấu hình cài đặt của mạng không dây.
- Đảm bảo rằng chỉ những người quý vị tin tưởng mới có thể kết nối vào mạng không dây của quý vị. Thực hiện điều này bằng cách bật phương thức bảo mật mạnh. Khi đó, cần phải có mật khẩu để người khác có thể kết nối vào mạng không dây của quý vị, và khi đã kết nối, hoạt động trực tuyến của họ sẽ được mã hóa.
- Đảm bảo rằng mật khẩu mà mọi người sử dụng để kết nối với mạng không dây của quý vị là mật khẩu mạnh và khác với mật khẩu quản trị viên. Hãy nhớ rằng quý vị chỉ cần nhập mật khẩu một lần cho mỗi thiết bị, vì chúng sẽ lưu trữ và nhớ mật khẩu đó.

Quý vị không rõ cách thực hiện các bước này? Hãy hỏi Nhà cung cấp dịch vụ Internet của quý vị, kiểm tra trang mạng của họ, kiểm tra tài liệu đi kèm điểm truy cập không dây của quý vị hoặc tham khảo trang mạng của nhà cung cấp thiết bị.

3 Passwords

Mật khẩu: Khi một trang mạng yêu cầu quý vị tạo mật khẩu: hãy tạo mật khẩu mạnh, càng có nhiều ký tự thì càng mạnh. Dùng một cụm từ mật khẩu là một trong những cách đơn giản nhất để đảm bảo quý vị có một mật khẩu mạnh. Một cụm từ mật khẩu chính là một mật khẩu được tạo từ nhiều từ, ví dụ như "*bee honey bourbon.*" Sử dụng một cụm từ mật khẩu duy nhất có nghĩa là sử dụng một cụm từ mật khẩu khác nhau cho mỗi thiết bị hoặc tài khoản trực tuyến. Bằng cách này, nếu một cụm từ mật khẩu bị xâm nhập, thì các tài khoản và thiết bị khác của quý vị vẫn an toàn. Quý vị không thể nhớ hết được tất cả các cụm từ mật khẩu đó?

Hãy sử dụng một trình quản lý mật khẩu, là một chương trình chuyên dụng, lưu trữ bảo mật toàn bộ các cụm từ mật khẩu của quý vị theo định dạng được mã hóa (và chúng còn có rất nhiều tính năng tuyệt vời khác!). Cuối cùng, hãy bật xác minh hai bước (còn được gọi là xác thực hai yếu tố hoặc xác thực đa yếu tố) bất cứ khi nào có thể. Tính năng này sử dụng mật khẩu của quý vị nhưng cũng thêm một bước thứ hai, ví dụ như mã được gửi đến điện thoại thông minh của quý vị hoặc ứng dụng tạo mã cho quý vị. Có lẽ xác minh hai bước là bước quan trọng nhất mà quý vị có thể áp dụng để bảo vệ các tài khoản trực tuyến của quý vị và tính năng này không hề khó sử dụng như quý vị tưởng.



Bản cập nhật: Đảm bảo rằng mỗi máy tính, thiết bị di động, chương trình và ứng dụng của quý vị đang chạy phiên bản phần mềm mới nhất. Những kẻ tấn công mạng liên tục tìm kiếm các lỗ hổng bảo mật mới trong phần mềm và thiết bị của quý vị sử dụng. Khi chúng phát hiện ra các lỗ hổng bảo mật, chúng sẽ sử dụng các chương trình đặc biệt để khai thác và đột nhập vào thiết bị mà quý vị đang sử dụng. Đồng thời, các công ty phát triển phần mềm cho những thiết bị đó đang nỗ lực vá lỗ hổng bằng cách phát hành các bản cập nhật. Bằng cách đảm bảo rằng máy tính và thiết bị di động của quý vị cài đặt ngay các bản cập nhật này, quý vị sẽ khiến những kẻ tấn công khó hack hơn rất nhiều. Để được cập nhật, chỉ cần bật tính năng tự động cập nhật bất cứ khi nào có thể. Quy tắc này áp dụng cho hầu hết công nghệ được kết nối với mạng, bao gồm nhưng không chỉ có các thiết bị của quý vị mà các với TV kết nối Internet, thiết bị giám sát trẻ, camera an ninh, bộ định tuyến gia đình, máy chơi trò chơi hay thậm chí là xe hơi của quý vị.



Trẻ nhỏ / Khách: Tại văn phòng công ty, điều mà quý vị gần như không phải lo lắng về đó là trẻ nhỏ và khách ghé thăm hay các thành viên trong gia đình sử dụng máy tính xách tay công vụ hay các thiết bị khách dành cho công việc. Hãy đảm bảo gia đình và bạn bè của quý vị hiểu rằng họ không thể sử dụng các thiết bị dành cho công việc của quý vị vì họ có thể vô tình xóa hoặc thay đổi thông tin, hay tệ hơn là vô tình làm lây nhiễm thiết bị.