Các hướng dẫn sử dụng Wi-Fi công cộng an toàn

Những kẻ xấu có thể lợi dụng quý vị trên mạng. Hãy đọc bên dưới để biết một số hướng dẫn cần cân nhắc nếu quý vị phải sử dụng Wi-Fi công cộng.

Để ứng phó với sự bùng phát dịch Corona và sự đóng cửa các doanh nghiệp và thư viện, nhiều người trong số chúng ta đang dành nhiều thời gian hơn để lên mạng. Kết quả là, chúng ta có thể phải sử dụng Wi-Fi công cộng để kết nối Internet. Nếu quý vị cần dùng Wi-Fi công cộng, xin hãy xem xét những khuyến nghị sau đây đến từ Chief Privacy Officer tiểu bang để giúp bảo vệ dữ liệu của quý vị:

1. Xác nhận rằng quý vị có mạng chính xác.

Đảm bảo là quý vị đang kết nối vào đúng mạng. Kẻ xấu có thể tạo ra những mạng mà cái tên của chúng nhìn có vẻ vô hại nhưng thật ra đang định hướng quý vị kết nối với một thiết lập mạng để quan sát việc lên mạng của quý vị. Điều này có nghĩa là nếu quý vị nhập những thông tin đăng nhập hoặc mật khẩu vào các trang web, tin tặc sẽ có khả năng đánh cắp thông tin của quý vị. Để phòng tránh điều này, hãy đọc tên mạng thật cẩn thận và nếu có thể, hãy nhờ một nhân viên hoặc kiểm tra bảng chỉ dẫn của doanh nghiệp để đảm bảo đó là mạng hợp pháp.

Những mạng phổ biến, ví dụ như mạng của chuỗi cà phê quen thuộc, ít phải nghi ngờ hơn vì công ty đó đang vận hành mạng này dưới dạng dịch vụ đi kèm với công việc kinh doanh của họ. Những mạng mà quý vị đã nhận biết rồi thì thường an toàn hơn những mạng Wi-Fi miễn phí ngẫu nhiên có thể xuất hiện trên điện thoại của quý vị ở một nơi công cộng.

2. Tắt tính năng tự động kết nối.

Có nhiều thiết bị (điện thoại thông minh, máy tính xách tay và máy tính bảng) có các cài đặt kết nối tự động. Cài đặt này cho phép các thiết bị của quý vị kết nối thuận tiện với các mạng gần đó. Điều này được chấp nhận với các mạng đáng tin cậy, nhưng nó cũng có thể kết nối các thiết bị của quý vị với những mạng không an toàn. Quý vị có thể tắt tính năng này thông qua tính năng cài đặt trên thiết bị của mình. Đảm bảo những cài đặt này luôn được tắt đi, đặc biệt là khi quý vị đang đi du lịch đến những nơi xa lạ. Để phòng ngừa thêm, quý vị có thể chọn “quên mạng sau khi sử dụng Wi-Fi công cộng.

Quý vị cũng nên theo dõi Bluetooth của mình khi ở những nơi công cộng. Kết nối Bluetooth cho phép các thiết bị khác nhau giao tiếp với nhau và tin tặc có thể tìm kiếm các tín hiệu Bluetooth mở để có quyền truy cập vào thiết bị của quý vị. Đảm bảo chức năng này được tắt đi trên điện thoại và các thiết bị khác khi quý vị ở khu vực xa lạ.

3. Tắt chức năng chia sẻ tập tin.

Nhớ tắt tùy chọn chia sẻ tập tin trong khi bật Wi-Fi công cộng. Quý vị có thể tắt tùy chọn chia sẻ tập tin trong tùy chọn hệ thống hoặc bảng điều khiển, tùy thuộc vào hệ điều hành của quý vị. AirDrop là một ví dụ về tính năng chia sẻ tập tin mà quý vị nên tắt. Một số hệ điều hành như Windows/PC sẽ tắt tính năng chia sẻ tập tin cho quý vị bằng cách chọn tùy chọn "công khai" khi lần đầu tiên kết nối với một mạng công cộng mới.

Các bước để tắt tính năng chia sẻ tập tin

Trên PC:

1. Vào Trung tâm Mạng và Chia sẻ.
2. Sau đó Thay đổi cài đặt chia sẻ nâng cao.
3. Tắt tính năng chia sẻ tập tin và máy in.

Dành cho máy Mac:

1. Vào Tùy chọn Hệ thống.
2. Chọn Chia sẻ.
3. Bỏ chọn tất cả mọi thứ.
4. Tiếp theo trong mục Trình tìm kiếm, nhấn vào AirDrop và lựa chọn Cho phép việc tôi được phát hiện bởi: Không một ai.

Đối với iOS, chỉ cần tìm AirDrop trong Trung tâm Điều khiển và tắt nó đi.

4. Sử dụng VPN.

Cân nhắc việc cài đặt VPN (Mạng riêng ảo) trên thiết bị của quý vị. VPN là tùy chọn an toàn nhất để đảm bảo quyền riêng tư kỹ thuật số khi dùng Wi-Fi công cộng. Nó mã hóa dữ liệu của quý vị khi truyền đến và từ thiết bị của quý vị và hoạt động như một "đường hầm" bảo vệ, vì vậy dữ liệu của quý vị không hiển thị khi truyền qua mạng.

5. Cảnh báo của FBI về các trang web được mã hóa - HTTPS.

FBI đã cảnh báo về các trang web có địa chỉ bắt đầu bằng "https." Sự hiện diện của các "https." và biểu tượng khóa có ý nghĩa là cho biết lưu lượng truy cập web được mã hóa và người truy cập có thể chia sẻ dữ liệu một cách an toàn. Tuy nhiên, bọn tội phạm mạng hiện đang lợi dụng

sự tin tưởng của công chúng bằng cách dụ dỗ mọi người vào các trang web độc hại kết hợp https, chúng có vẻ an toàn nhưng chúng thật ra không an toàn.

Khuyến nghị của FBI:

- Đừng tin tưởng tên trên một email một cách đơn giản: hãy đặt câu hỏi về mục đích của nội dung email.
- Nếu quý vị nhận được email đáng ngờ với liên kết từ một người quen mà quý vị đã biết, hãy xác nhận tin nhắn đó là hợp pháp bằng cách gọi điện thoại hoặc gửi email cho người đó. Không trả lời trực tiếp một email đáng ngờ.
- Kiểm tra lỗi chính tả hoặc tên miền sai trong liên kết (ví dụ: nếu địa chỉ phải kết thúc bằng chữ ".gov" thì lại kết thúc bằng chữ ".com").
- Đừng tin tưởng một trang web chỉ vì nó có biểu tượng khóa hoặc có "https" trong thanh địa chỉ trình duyệt.

6. Truy cập thông tin nhạy cảm không được khuyến nghị.

Ngay cả khi quý vị có VPN, việc truy cập tài khoản ngân hàng cá nhân hoặc dữ liệu cá nhân nhạy cảm tương tự như vậy, ví dụ như số an sinh xã hội trên các mạng công cộng không bảo mật vẫn không được khuyến nghị. Ngay cả các mạng bảo mật công cộng cũng có thể có rủi ro. Hãy xem xét kỹ lưỡng nếu quý vị phải truy cập các tài khoản này trên Wi-Fi công cộng. Đối với các giao dịch tài chính, có thể việc sử dụng chức năng điểm truy cập trên điện thoại thông minh của quý vị là tốt hơn.

7. Bảo mật và không bảo mật.

Về cơ bản có hai loại mạng Wi-Fi công cộng: Bảo mật và không bảo mật.

Bất cứ khi nào có thể, hãy kết nối với các mạng công cộng được bảo mật. Mạng không bảo mật có thể được kết nối mà không cần bất kỳ loại tính năng bảo mật nào như mật khẩu hoặc thông tin đăng nhập. Mạng được bảo mật thường yêu cầu người dùng đồng ý với các điều khoản và điều kiện, đăng ký tài khoản hoặc nhập mật khẩu trước khi kết nối với mạng.

8. Đảm bảo tường lửa của quý vị luôn được kích hoạt.

Nếu quý vị đang sử dụng máy tính xách tay, hãy đảm bảo tường lửa của quý vị luôn được kích hoạt khi đang sử dụng Wi-Fi công cộng. Tường lửa hoạt động như một rào cản bảo vệ thiết bị của quý vị khỏi các mối đe dọa phần mềm độc hại. Người dùng có thể vô hiệu hóa tường lửa Windows vì có các cửa sổ bật lên và các thông báo nhưng rồi sau đó họ quên đi. Nếu quý vị muốn khởi động lại tường lửa trên PC, hãy truy cập Bảng điều khiển, "Hệ thống và Bảo mật" và chọn "Tường lửa Windows". Nếu quý vị là người dùng Mac, hãy vào "Tùy chọn Hệ thống", sau đó vào "Bảo mật & Quyền riêng tư", sau đó chọn mục "Tường lửa" để bật tính năng này.

9. Sử dụng phần mềm chống vi-rút.

Đồng thời, hãy nhớ cài đặt phiên bản mới nhất của chương trình chống vi-rút trên máy tính xách tay của quý vị. Các chương trình chống vi-rút có thể giúp bảo vệ quý vị trong khi sử dụng Wi-Fi công cộng bằng cách phát hiện phần mềm độc hại có thể xâm nhập vào hệ thống của quý vị trong khi sử dụng mạng chia sẻ. Một cảnh báo sẽ báo cho quý vị nếu các virus đã được biết đến được tải vào thiết bị của quý vị hoặc nếu có bất kỳ hoạt động đáng ngờ, sự tấn công hoặc nếu có phần mềm độc hại xâm nhập vào hệ thống của quý vị.

10. Sử dụng xác thực hai yếu tố hoặc đa yếu tố.

Sử dụng xác thực đa yếu tố (MFA) khi đăng nhập vào trang web bằng thông tin cá nhân của quý vị. Điều này có nghĩa là quý vị có mã xác minh thứ hai (được nhắn tin tới điện thoại của quý vị hoặc được cung cấp bởi một ứng dụng hoặc khóa vật lý) để tăng cường bảo vệ quý vị. Vì vậy, ngay cả khi tin tặc có được tên người dùng và mật khẩu của quý vị, họ vẫn không thể truy cập vào tài khoản của quý vị mà không có mã xác thực.

11. Theo dõi các thiết bị cá nhân của quý vị.

Đừng để máy tính xách tay, máy tính bảng hoặc điện thoại thông minh của quý vị ở nơi công cộng hoặc phương tiện đi lại mà không có sự trông coi. Ngay cả khi quý vị đang thực hiện các biện pháp phòng ngừa trên mạng Wi-Fi, việc đó sẽ không đảm bảo là không ai lấy tài sản của quý vị hoặc lén xem thông tin của quý vị. Hãy nhận biết môi trường xung quanh quý vị và để ý đến những người xung quanh quý vị.

12. Các hướng dẫn an toàn trực tuyến khác.

Dưới đây là một số hướng dẫn để giữ an toàn trực tuyến, đặc biệt là khi quý vị sử dụng kết nối Wi-Fi công cộng:

- Sử dụng mật khẩu mạnh.
- Mã hóa các thiết bị của quý vị.
- Cảnh giác với các email lừa đảo.
- Hãy cẩn thận với những gì quý vị đăng trên mạng xã hội. Việc quý vị đăng quá nhiều chi tiết cá nhân có thể giúp tin tặc đoán mật khẩu.
- Xóa thông tin cũ mà quý vị không cần nữa.
- Nếu một mạng yêu cầu quý vị cài đặt bất kỳ phần mềm bổ sung hoặc phần mở rộng trình duyệt nào thì đừng kết nối.
- Đảm bảo các bản vá và cập nhật phần mềm mới nhất được cài đặt trên thiết bị của quý vị để bảo vệ khỏi các sự cố đã biết.