Wi-Fi công cộng

Học viên sẽ tìm hiểu về các mạng Wi-Fi công cộng cũng như những lợi ích và rủi ro của loại mạng này. Cụ thể hơn, họ sẽ tìm hiểu cách nhận diện mạng Wi-Fi không bảo mật trên thực tế, hiểu được ưu nhược điểm vốn có trong việc sử dụng mạng Wi-Fi không bảo mật, cũng như đưa ra những quyết định sáng suốt về thời điểm nên kết nối và sử dụng mạng Wi-Fi không bảo mật.

Tài nguyên

Hình ảnh modem không dây
Phiếu bài tập về Mức độ an toàn của kết nối

Wi-Fi là gì?

Phần 1

Hỏi học viên

Chúng ta dùng các thiết bị nào để truy cập Internet?

Những thiết bị đó kết nối Internet bằng cách nào?

Tương tác với lớp học thông qua hình ảnh

Wi-Fi là một phương thức phổ biến để kết nối các thiết bị với Internet. Wi-Fi kết nối các thiết bị qua tín hiệu vô tuyến mà không cần đến dây hoặc kết nối vật lý nào khác.

Giả sử trong nhà có 3 máy tính xách tay cần kết nối Internet. Để kết nối, chúng ta cần có:

1. Điểm truy cập: Điểm truy cập (AP) là bất kỳ điểm nào truyền (hoặc phát?) tín hiệu Wi-Fi và cung cấp quyền truy cập Internet. Nếu muốn kết nối Internet, thiết bị của chúng ta phải bắt được những tín hiệu này. Đôi khi chúng ta phải được cho phép (ví dụ: tên người dùng và mật khẩu) thì mới có thể đăng nhập và sử dụng tín hiệu không dây mà một AP phát ra.

2. Bộ định tuyến: Bộ định tuyến là thiết bị tạo ra một mạng lưới kết nối tất cả các thiết bị (ví dụ: máy tính, máy tính bảng, điện thoại di động) ở một địa điểm nhất định (chẳng hạn như trường học, thư viện hoặc nhà riêng). Thông thường, bộ định tuyến có điểm truy cập được tích hợp bên trong (xem sơ đồ phía trên).

> Phạm vi hoạt động của các bộ định tuyến đều có giới hạn (thường ngắn). Đó là lý do thiết bị của chúng ta bắt tín hiệu Wi-Fi kém hoặc không bắt được Wi-Fi nếu ở quá xa bộ định tuyến. Ngoài ra, nếu có vật cản giữa chúng ta và bộ định tuyến (chẳng hạn như tòa nhà hoặc tường gạch) thì tín hiệu cũng yếu hơn.
>
> Mặc dù kết nối với bộ định tuyến thì chúng ta có quyền truy cập vào mạng, nhưng vẫn không có nghĩa là vào Internet. Để nhiều thiết bị trên một mạng có thể kết nối với Internet, bộ định tuyến phải được kết nối với modem.

3. Modem: Modem là thiết bị tạo và duy trì kết nối với Nhà cung cấp dịch vụ Internet (ISP) để chúng ta có thể truy cập Internet. Công dụng của modem là chuyển đổi các tín hiệu từ bên ngoài địa điểm cụ thể của chúng ta thành các tín hiệu mà máy tính và thiết bị kĩ thuật số đọc được.

> Thông thường thì AP và bộ định tuyến được lắp trong cùng một thiết bị và kết nối

vật lý với modem thông qua một dây cáp đặc biệt gọi là cáp Ethernet. Đây chính là lý do mọi người gọi kết nối Internet là kết nối "có dây".

Các thiết bị di động cũng có thể sử dụng kết nối mạng di động để vào Internet, nhất là khi những thiết bị này không kết nối với mạng tại trường học, thư viện hoặc tại nhà. Kết nối mạng di động là loại tín hiệu vô tuyến không dây có vùng phủ sóng rộng hơn nhiều so với bộ định tuyến. Kết nối mạng di động sử dụng bộ thu phát đặc biệt, được gọi là các tháp di động, để kết nối thiết bị di động của chúng ta với Internet.

Phần 2

Hỏi học viên

Wi-Fi có những lợi ích gì?

Đâu là một số nhược điểm của Wi-Fi?

Một số lo ngại về bảo mật khi sử dụng Wi-Fi so với kết nối Internet có dây là gì?

Tại sao khi chúng ta rời khỏi một tòa nhà thì điện thoại lại mất quyền truy cập Wi-Fi?

Chọn mạng Wi-Fi

Phần 1

Hỏi học viên

Có phải tất cả các mạng Wi-Fi đều an toàn không? Tại sao có/tại sao không?

Nói với học viên

Sẽ có những lúc chúng ta được quyền chọn mạng Wi-Fi mà mình muốn dùng. Tuy nhiên, cần lưu ý rằng chúng ta sẽ đối mặt với các rủi ro nghiêm trọng nếu kết nối nhầm mạng. Ví dụ: mạng Wi-Fi không an toàn là những mạng không yêu cầu mật khẩu đăng nhập. Nếu chúng ta sử dụng mạng không an toàn, thì những người khác trên cùng mạng đó có thể xem thông tin của chúng ta. Họ có thể lấy cắp thông tin mà chúng ta gửi qua mạng hoặc giám sát những gì chúng ta làm.

Mặt khác, các mạng Wi-Fi an toàn và đáng tin cậy là những mạng yêu cầu mật khẩu, đã bật mã hóa. Đây cũng là những mạng mà chúng ta chắc chắn rằng mạng mình đang đăng nhập chính là mạng có tên hiển thị. Ví dụ: việc đăng nhập vào một mạng giả mạo tên mạng của trường chúng ta có thể làm lộ thông tin tài khoản. Do đó, các mạng an toàn và đáng tin cậy là những mạng cung cấp mức độ bảo vệ cao nhất.

Chúng ta cũng nên xem xét đến bối cảnh hoặc vị trí của mạng Wi-Fi. Ví dụ: nếu chúng ta đang ở rạp chiếu phim mà lại nhìn thấy tên mạng của trường mình trên điện thoại khi tìm kiếm kết nối Wi-Fi, thì có khả năng là mạng đó đang cố bắt chước hoặc "giả mạo" mạng của trường chúng ta nhằm thu thập mật khẩu của những học sinh thiếu cảnh giác.

Khi thiết lập một mạng Wi-Fi được bảo vệ bằng mật khẩu, chủ sở hữu mạng phải bật giao thức mã hóa của bộ định tuyến. Các giao thức mã hóa phổ biến là Wired Equivalent Privacy (WEP - Bảo mật tương đương mạng đi dây), Wi-Fi Protected Access (WPA - Truy cập Wi-Fi được bảo vệ) hoặc WPA2. Mục đích của những giao thức này là nhằm đảm bảo thông tin mà chúng ta gửi qua mạng không dây sẽ được mã hóa (hoặc "xáo trộn").

Khi có mã hóa, tin tặc sẽ khó xem được nội dung chúng ta gửi hơn. Tuy nhiên, tất cả những giao thức này (WEP, WPA và WPA2) vẫn có nguy cơ bị hack bởi tin tặc. Do đó, việc sử dụng các kết nối web an toàn khi truyền thông tin online cũng đóng vai trò rất quan trọng.

HTTPS là tiêu chuẩn mà các trang web sử dụng để mã hóa dữ liệu truyền qua mạng Internet. Quá trình mã hóa có thể khiến bên thứ ba khó lòng mà xem được dữ liệu từ kết nối của chúng ta. Nó cung cấp thêm một lớp bảo mật và có thể dùng được trên mọi trình duyệt bằng cách thêm "https://" vào trước URL mà chúng ta sử dụng (ví dụ: https://www.mysite.com). Tuy nhiên, không phải mọi trang web đều hỗ trợ HTTPS.

1. Chúng ta chỉ nên nhập thông tin nhạy cảm (chẳng hạn như mật khẩu, thông tin thẻ tín dụng) trên trang web có tiền tố HTTPS://.

2. Hầu hết các trình duyệt lớn đều có các chỉ báo bảo mật trông giống như hình ổ khóa, ở gần thanh địa chỉ để chỉ ra các kết nối HTTPS.

3. Tuy nhiên, rất tiếc là HTTPS không đảm bảo được an toàn cho chúng ta vì một số trang web độc hại cũng có thể hỗ trợ HTTPS. HTTPS bảo mật kết nối nhưng không đảm bảo trang web đó là một trang web hợp pháp.

Nói với học viên

Giao thức SSL/TLS là tên của công nghệ đảm bảo tính an toàn của HTTPS. SSL/TLS sử dụng các khóa mã hóa kỹ thuật số (có vai trò y như các khóa thật). Nếu chúng ta viết một bí mật ra giấy rồi gửi cho bạn mình, thì bất kỳ ai cầm mảnh giấy đều có thể biết được bí mật này. Nhưng giả sử, đích thân chúng ta trao cho bạn mình một chiếc chìa khóa dự phòng, sau đó gửi bí mật vào trong những chiếc hộp tương ứng. Khi đó, dù có ai cố mở chiếc hộp ra mà không có chìa, thì cũng khó thấy được bí mật bên trong. Và nếu họ cố đánh tráo chiếc hộp đó bằng một chiếc khác tương tự, thì chúng ta sẽ thấy chìa khóa của mình không mở được hộp. SSL/TLS cũng hoạt động như vậy đó, nhưng là với trang web.

Các chỉ báo bảo mật trên trình duyệt cũng sẽ cho biết thông tin chứng chỉ Xác thực mở rộng (EV). Chứng chỉ EV được cung cấp để các trang web xác minh danh tính qua một nhà cung cấp chứng chỉ. Trong các trình duyệt, đôi khi chỉ báo EV sẽ xuất hiện dưới dạng tên trang web hoặc thực thể đã đăng ký bên cạnh thanh địa chỉ. Nếu nghi ngờ nội dung trên một trang web cụ thể, chúng ta có thể kiểm tra xem URL trong chứng chỉ có khớp với URL trong trình duyệt hay không. Để thực hiện việc này, hãy nhấp vào “Xem chứng chỉ”. [Sẽ rất hữu ích nếu chúng ta có thể minh họa trên màn hình máy chiếu để học viên biết cách tìm cụm từ “Xem chứng chỉ” để nhấp vào.] Tùy theo trình duyệt mà cụm từ này nằm ở những nơi khác nhau. Ví dụ: trên Chrome, trong phần “Xem”, hãy nhấp vào “Nhà phát triển”, sau đó nhấp vào “Công cụ dành cho nhà phát triển”. Từ “Công cụ dành cho nhà phát triển”, hãy nhấp vào tab “Bảo mật” rồi nhấp vào “Xem chứng chỉ”.

Hỏi học viên

Chúng ta nên suy xét những gì khi kết nối với một mạng mới bất kỳ?

1. Đó có thể là: vị trí (hoặc chủ sở hữu mạng đó), quyền truy cập (hoặc người nào khác được kết nối với mạng đó) và hoạt động (hoặc chúng ta đang làm gì trên mạng đó).

Ai là chủ sở hữu mạng Wi-Fi tại nhà của chúng ta? Tại trường học? Tại quán cà phê?

1. Cha mẹ/người chăm sóc là chủ sở hữu mạng Wi-Fi tại nhà của chúng ta, phòng hành chính và/hoặc quận (huyện) sở hữu mạng tại trường học và chủ quán cà phê sở hữu mạng tại quán.

Cá nhân chúng ta có quen biết những người này không? Chúng ta có tin tưởng họ không?

1. Hãy cho học viên thảo luận về các mức độ tin tưởng khác nhau mà họ dành cho những người này.

Nói với học viên

Chủ sở hữu mạng Wi-Fi nên là người mà chúng ta biết và tin tưởng. Đôi khi, chúng ta có thể xác định chủ sở hữu thông qua SSID của mạng.

Tên mạng (SSID) là tên mà nhà cung cấp dịch vụ đặt cho mạng Wi-Fi. Chúng ta sẽ thấy tên này hiển thị khi kết nối với mạng đó. SSID thường dùng để biết thông tin về chủ sở hữu mạng cũng như các thông tin chi tiết khác về mạng đó. Tuy nhiên, chúng ta nên thận trọng bởi vì gần như bất kỳ ai (biết cách) cũng có thể tạo SSID. Ví dụ: ai đó có thể tạo một SSID giống hệt SSID mà chúng ta sử dụng ở trường học. Đây là ví dụ về việc giả mạo một mạng đã biết và đáng tin cậy, nhằm có thể thu thập tên người dùng và mật khẩu.

Khi biết rõ ai là chủ sở hữu mạng, chúng ta có thể xác định mạng đó có bảo mật hay không. Nếu mạng đó thuộc sở hữu của một cá nhân hay tổ chức mà mình tin tưởng, thì chúng ta có thể yên tâm kết nối. Tuy nhiên, nếu đó là mạng không xác định, thì chúng ta không nên làm thế vì không biết ai là chủ sở hữu bộ định tuyến mà mình đang kết nối. Do tất cả lưu lượng truy cập trên mạng đó đều đi qua bộ định tuyến, nên chủ sở hữu mạng có thể giám sát hoặc ghi lại lưu lượng truy cập web của chúng ta.

Khi kết nối với Wi-Fi, thiết bị của chúng ta sẽ kết nối với một mạng cục bộ gồm các thiết bị và mạng đó lại kết nối với mạng Internet rộng hơn. Vì thiết bị của chúng ta đang trao đổi thông tin qua mạng này, nên quan trọng là chúng ta cũng phải tin tưởng những thiết bị khác mà mình được kết nối - nghĩa là mọi thiết bị trong mạng đó. Điều này cũng tương tự như khi làm việc nhóm tại trường học. Những người mà chúng ta làm việc cùng nên là những người mà chúng ta có thể tin tưởng được.

Sử dụng mật khẩu trên mạng sẽ phần nào hạn chế những người có thể kết nối với mạng. Điều này có nghĩa là chúng ta sẽ biết rõ hơn những ai đang sử dụng mạng, bất kể đó là người thân, bạn bè hay những khách hàng khác trong quán cà phê, so với nếu đó là mạng mở hoàn toàn.

Việc chúng ta có quyết định tham gia một mạng có vẻ đáng ngờ hay không tùy thuộc vào những ưu nhược điểm mà chúng ta sẵn sàng chấp nhận xét về khía cạnh bảo

mật online. Chúng ta có thể cân nhắc giữa nguy cơ tài khoản bị xâm phạm và sự thuận tiện khi tham gia một mạng có sẵn.

Hỏi học viên

Chúng ta có nên đọc blog/tin tức online qua mạng Wi-Fi tại nhà không? Tại trường học? Tại quán cà phê?

1. Giải thích rằng nhìn chung, nội dung trang web không phải thông tin nhạy cảm. Chúng ta có thể đọc blog/tin tức online trên bất kỳ mạng nào.

Chúng ta có nên gửi số thẻ tín dụng qua mạng Wi-Fi tại nhà không? Tại trường học? Tại quán cà phê? Tại sao?

1. Hãy cùng thảo luận với mọi người về lý do việc gửi số thẻ tín dụng qua mạng Wi-Fi tại nhà là an toàn nhất và không nên gửi qua mạng Wi-Fi của quán cà phê. Ngoài ra, hãy thảo luận vì sao mà mạng ở trường học tuy có thể đáng tin cậy nhưng lại không đáng để chúng ta liều lĩnh, bởi đây là thông tin rất nhạy cảm.

Chúng ta có nên kiểm tra email cá nhân khi sử dụng mạng Wi-Fi tại nhà không? Tại trường học? Tại quán cà phê?

1. Hãy thảo luận vì sao kiểm tra email bằng mạng tại nhà có thể là an toàn nhất, tùy vào nội dung của tài khoản email đó. Ví dụ: một số người có rất nhiều tài khoản email dùng cho những mục đích khác nhau (chẳng hạn như một tài khoản dùng cho các email marketing/quảng cáo; một tài khoản khác cho các email của bạn bè và gia đình).

Nói với học viên

Thông tin nhạy cảm, bao gồm cả mật khẩu và thông tin về ngân hàng, nên được gửi/xem bằng một mạng an toàn và riêng tư, trên các trang web sử dụng giao thức SSL/TLS thay vì một mạng công khai dùng chung. Thông tin riêng tư này sẽ có nguy cơ bị tấn công nếu chúng ta gửi hoặc truy cập trên một mạng dùng chung với những người mà mình không biết hoặc không tin tưởng.

Cũng có thể không xác định được rõ ràng thế nào là thông tin nhạy cảm và không nhạy cảm, bởi mỗi người lại có một quan điểm khác nhau về quyền riêng tư. Chúng ta phải cân nhắc từng tình huống để xác định xem mình có nên kết nối với mạng đó hay không. Trước khi quyết định có kết nối hay không, hãy tự hỏi xem chúng ta có tin tưởng chủ sở hữu mạng và những người kết nối với mạng đó không, chúng ta đang thực hiện hành động nào trên mạng, cũng như chúng ta đang chia sẻ thông tin nào.

Mạng an toàn và mạng không an toàn

Phần 1

Tương tác trong lớp

Lưu ý: Một phần nội dung trong hoạt động này đã được đề cập ở “Hoạt động số 2: Chọn mạng Wi-Fi”. Tùy bạn đánh giá xem mình có cần lặp lại hay bỏ qua nội dung này không.

Nói với học viên

Như đã đề cập trước đó, các mạng Wi-Fi không bảo mật là những mạng không yêu cầu mật khẩu đăng nhập. Việc sử dụng mạng không bảo mật gây rủi ro cho dữ liệu mà chúng ta truyền và nhận qua mạng đó.

Các mạng Wi-Fi bảo mật là những mạng yêu cầu mật khẩu và đã bật mã hóa. Người cấu hình mạng này chính là người quyết định có bật mã hóa hay không. Tính năng mã hóa sẽ xáo trộn thông tin chúng ta gửi và nhận qua mạng, nhờ vậy tin tặc sử dụng cùng mạng Wi-Fi sẽ khó xem được nội dung chúng ta đang gửi hoặc nhận hơn rất nhiều.

Thế nhưng mạng được bảo mật cũng không có nghĩa là dữ liệu của chúng ta đã an toàn. Việc sử dụng mạng bảo mật chắc chắn là an toàn hơn so với mạng không bảo mật; tuy nhiên, tin tặc nếu quyết tâm vẫn có thể tìm ra cách để truy cập thông tin của chúng ta.

Có 3 giao thức mã hóa phổ biến dành cho mạng Wi-Fi, đó là: Wired Equivalent Privacy (WEP - Bảo mật tương đương mạng đi dây), Wi-Fi Protected Access (WPA - Truy cập Wi-Fi được bảo vệ) hoặc WPA2. WEP và WPA đã lỗi thời nên những mạng dựa vào hai giao thức này được xem là không bảo mật. Còn giao thức WPA2 thì cũng tỏ ra là dễ bị hack.

Để đảm bảo thông tin được bảo vệ đầy đủ nhất, hãy kiểm tra xem các trang web chúng ta đang sử dụng có được mã hóa bằng SSL/TLS hay không.

Hỏi học viên

Có ai biết ví dụ nào về mạng được bảo vệ bằng mật khẩu mà mình đã sử dụng không?

1. Một số ví dụ gồm có mạng Wi-Fi tại nhà, mạng Wi-Fi tại trường học và mạng Wi-Fi tại các địa điểm công cộng, chẳng hạn như quán cà phê.

Có ai biết ví dụ nào về mạng không bảo mật mà mình đã sử dụng không?

Ví dụ về mạng bảo mật thì sao?

Nói với học viên

Chúng ta có thể biết liệu một mạng Wi-Fi có được mã hóa hay không bằng cách kiểm tra cài đặt mạng hoặc cài đặt mạng không dây trên thiết bị của mình.

Phần 2

Tương tác trong lớp

Trước khi bắt đầu bài học này, hãy tìm kiếm trên Internet để xem lại cách kiểm tra loại mã hóa mạng Wi-Fi cho những hệ điều hành khác nhau. Sau đó, trình bày cách tìm ra loại mã hóa mà một mạng sử dụng. Ví dụ: trên hệ điều hành Mac, hãy nhấp vào Tùy chọn hệ thống -> Mạng -> Chọn Wi-Fi -> Chọn Tên mạng thích hợp. Trong tab Wi-Fi, chúng ta sẽ thấy một danh sách các mạng đã biết và một cột chỉ ra loại mã hóa nào được sử dụng.

Nói với học viên

Không phải tất cả các kết nối đều như nhau. Khi mạng không bảo mật, bất kỳ ai cũng có thể kết nối với mạng và khó xác minh được ai là người kiểm soát mạng. Việc tham gia một mạng không bảo mật sẽ khiến chúng ta dễ bị tấn công hơn, bởi thông tin mà chúng ta gửi và nhận, chẳng hạn như lưu lượng truy cập web (các trang, mật khẩu, v.v.), có nguy cơ bị xem bởi bất kỳ ai trên mạng đó nếu chúng ta không sử dụng kết nối SSL/TLS.

Tương tác trong lớp

Tùy vào kiến thức kỹ thuật của những học viên, bạn có thể thảo luận về việc sử dụng Mạng riêng ảo (VPN) như một lớp bảo mật bổ sung khi dùng Wi-Fi. Vui lòng tham khảo các liên kết VPN trong phần Tài nguyên để biết thêm thông tin.

Nhận diện mức độ an toàn của kết nối

Tiêu đề của phần

Tương tác trong lớp

Chia học viên thành các nhóm gồm 2-3 thành viên. Phát phiếu bài tập về Mức độ an toàn của kết nối: Phát phiếu bài tập cho học viên và chỉ định tình huống cho từng nhóm. Học viên có 5 phút để thảo luận về tình huống của mình. Sau đó, yêu cầu các nhóm chia sẻ câu trả lời của mình. Các câu trả lời có màu xanh lá trên phiếu bài tập.

Bài tập

Phần 1

Bài tập

Yêu cầu học viên:

1. Đưa ra thời gian biểu của một ngày thông thường, đánh dấu những mạng Wi-Fi mà họ kết nối.

2. Từ những mạng họ đã chọn và mô tả trong thời gian biểu, hãy yêu cầu học viên chọn lấy hai mạng rồi mô tả mỗi mạng bằng một đoạn ngắn - còn ai khác được kết nối với mạng đó nữa không? Độ bảo mật của mạng đó ra sao?

3. Ngoài ra, với hai mạng đã chọn, hãy yêu cầu học viên mô tả những cơ hội và rủi ro đi kèm khi họ kết nối với những mạng này.