BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC, KỸ NĂNG BẢO ĐẢM AN TOÀN THÔNG TIN CHO THIẾT BỊ KHÔNG DÂY"

Hà Nội, năm 2023

I. AN TOÀN MẠNG KHÔNG DÂY CỦA CÁ NHÂN

1. Mạng không dây là gì?

a) Khái niệm mạng không dây

Mạng không dây (tiếng Anh: Wireless Network) là mạng điện thoại hoặc mạng máy tính sử dụng hệ thống thiết bị mạng kết nối có khả năng thu và phát sóng với nhau mà không dùng dây dẫn. Nền tảng cơ bản của mạng không dây là các thiết bị sử dụng sóng vô tuyến được truyền trong không gian thông qua các trạm, thiết bị phát sóng radio làm sóng truyền dẫn.

b) Những ưu điểm mạng không dây

- Khả năng chia sẻ tài nguyên dữ liệu dùng chung mạnh mẽ, rất được tin dùng trong môi trường kết nối mạng của các gia đình, cơ quan, tổ chức và doanh nghiệp, văn phòng. Vì là không dây nên rất tiện lợi, khi di chuyển cũng không quá khó khăn.

- Khắc phục được sự tốn kém về chi phí nối dây so với các loại mạng sử dụng kết nối có dây truyền thống.

- Khi lắp đặt và kết nối khá nhanh và dễ dàng, kết nối được đến những nơi mà mạng có dây không thể kết nối tới.

- Mặc dù chi phí của các thiết bị vô tuyến không dây ban đầu có thể sẽ cao hơn các loại có dây nhưng xét về mặt lâu dài thì kết nối có dây tiết kiệm và kinh tế hơn hẳn. Bên cạnh đó độ bền của các thiết bị không dây cũng cao hơn.

- Có nhiều cấu hình mạng, quy mô khác nhau, dễ dàng thay đổi phục vụ cho tùy nhu cầu sử dụng mạng như hộ gia đình hay đến các khu vực rộng lớn như khu dân cư hay giữa các văn phòng công sở,...

- Thuận tiện trong việc mở rộng khi có số lượng lớn người cùng có nhu cầu truy cập.

c) Nhược điểm mạng không dây là gì?

Bên cạnh những ưu điểm thì mạng không dây vẫn không thể tránh khỏi một số nhược điểm:

- Bởi vì tín hiệu được truyền đi là sóng vô tuyến trong không gian nên việc bảo mật là một nhược điểm lớn. Nguy cơ các kẻ xấu tấn công vào mạng là rất lớn.

- Phạm vi hoạt động của mạng không dây còn hạn chế. Hiện nay, các mạng dây WiFi hiện đại nhất cũng chỉ có khả năng phát sóng trong khu vực từ 250m trở xuống, phổ biến tối đa chủ yếu là 150m nên có thể chưa đáp ứng được cho các khu vực rộng lớn.

- Vì là tín hiệu sóng nên rất dễ bị nhiễu sóng do các thiết bị phát sóng khác dẫn đến việc sóng truyền đi bị ngắt quãng hay giảm tốc độ truyền.

- Tốc độ truyền của mạng còn tùy thuộc vào băng thông.

2. Các loại mạng không dây phổ biến tại Việt Nam hiện nay

Trong số các loại mạng không dây thì WiFi, 4G (5G) và Bluetooth là ba loại mạng được sử dụng phổ biến nhất hiện nay.

a) WiFi

Đây là loại mạng phổ biến nhất, có số lượng người sử dụng chiếm tổng số 60% trên tất cả các loại mạng truyền tải Internet.

Mạng WiFi theo chuẩn 802.11n, phát ở tần số 2.4 GHz, tốc độ truyền dữ liệu tối đa đạt 450 megabit/giây. Đây là loại được sử dụng phổ biến nhất ở Việt Nam hiện nay, hoạt động ở 2 dải tần 2.4GHz và 5GHz, phạm vi kết nối lên đến 250m tùy thuộc vào môi trường.

b) Bluetooth

Hiện nay, bluetooth xuất hiện hầu hết ở các thiết bị như máy tính, điện thoại/ smartphone,…Đây cũng là loại sóng truyền tải quan trọng.

Bluetooth ngoài việc dùng để truyền dữ liệu giữa các thiết bị di động và kết nối tai nghe với điện thoại, thì nó còn xuất hiện trong một số thiết bị khác nhau như máy ảnh, laptop, Loa Bluetooth, và đầu máy chơi game.

Bluetooth mới nhất là Bluetooth 5.0 với tốc độ truyền tải được cải thiện và tăng cường tính bảo mật.

c) Mạng 4G (5G)

4G LTE là mạng di động có tốc độ kết nối cao nhất hiện nay. Mạng 4G LTE có thể tải xuống dữ liệu từ 5-12 megabit/giây, cho phép truyền trực tiếp video và thời gian đáp ứng tốt hơn cho các trò chơi trực tuyến nhiều người chơi game.

Mạng 4G LTE tốc độ cao đã hoàn thành cơ sở hạ tầng ở Việt Nam hiện nay và đã dần trở nên phổ biến, chính thức thay thế 3G trở thành chuẩn cơ bản trên hầu hết các thiết bị di động.

Có thể thấy với công nghệ không dây hiện nay, hàng tỷ người trên thế giới này có thể kết nối với nhau một cách rất dễ dàng nhờ vào các ứng dụng công nghệ hiện đại hoạt động trên nền tảng mạng không dây.

3. Bảo đảm an toàn mạng không dây cá nhân

3.1. Bảo đảm an toàn khi kết nối bằng Bluetooth

Khi việc trao đổi thông tin qua Bluetooth trên thiết bị cá nhân trở nên phổ biến, thì người dùng cũng trở thành mục tiêu của tin tặc để đánh cắp thông tin cá nhân. Dưới đây là một số lưu ý cơ bản giúp người dùng phòng tránh rủi ro mất an toàn thông tin khi sử dụng Bluetooth.

(1) Tắt kết nối Bluetooth khi không dùng

Luôn bật kết nối Bluetooth là nguyên nhân chính dẫn đến tin tặc có cơ hội tấn công người dùng. Tin tặc chỉ chờ để tấn công những người dùng bất cẩn hay quên không tắt kết nối Bluetooth dù không sử dụng đến. Do đó, người dùng cần tắt kết nối Bluetooth khi không sử dụng, đặc biệt là khi đang ở những nơi đông người.

(2) Không chia sẻ thông tin nhạy cảm

Song song với thời đại công nghệ hóa là sự gia tăng của các lỗ hổng bảo mật, người dùng không nên chia sẻ những thông tin nhạy cảm qua Bluetooth. Các thông tin nhạy cảm như: thông tin ngân hàng, mật mã, những hình ảnh riêng tư....

(3) Thay đổi chế độ Bluetooth thành “Not Discoverable”

Nhiều tấn công qua Bluetooth được thực hiện trong khu vực bị phát hiện. Đây là cách mà các tin tặc thực hiện để tìm kiếm nạn nhân cho cuộc tấn công của chúng. Khi bật chế độ "Not Discoverable" các thiết bị khác sẽ không thể tìm thấy cũng như ghép đôi với thiết bị của người dùng. Do đó, người dùng nên sử dụng chế độ này để đảm bảo an toàn.

(4) Cẩn thận với những thiết bị được kết nối

Đừng đồng ý với bất kỳ yêu cầu kết nối nào trừ khi người dùng biết rõ mình đang kết nối với thiết bị nào. Đây là cách mà các tin tặc thường xuyên thực hiện để có được quyền truy cập vào thiết bị của nạn nhân.

(5) Tránh ghép đôi thiết bị tại nơi công cộng

Những nơi công cộng đông người thường được tin tặc lợi dụng để tấn công vào thiết bị. Nếu người dùng buộc phải kết nối với thiết bị nào đó lần đầu tiên, tốt nhất nên thực hiện chúng ở nhà hoặc trong khu vực an toàn. Hãy đảm bảo rằng tin tặc không thể tìm ra kết nối Bluetooth khi người dùng mở chế độ có thể tìm thấy khi kết nối.

(6) Đừng quên ngắt kết nối

Nếu thiết bị Bluetooth từng kết nối với thiết bị của người dùng bị mất hoặc bị đánh cắp, hãy ngắt kết nối chúng trong danh sách những thiết bị từng kết nối. Thực tế, người dùng nên làm điều này với tất cả các thiết bị Bluetooth không dùng tới nữa.

(7) Thường xuyên cập nhật các bản vá lỗi

Người dùng sẽ không biết các lỗ hổng bảo mật nào đang tồn tại trên thiết bị của mình. Do đó, người dùng nên cập nhật mới thường xuyên các bản vá lỗi để đảm bảo thiết bị được luôn an toàn.

3.2. Bảo đảm an toàn khi kết nối WiFi

(1) Sử dụng mạng riêng ảo

Tạo ra mạng riêng ảo (VNP) (mạng riêng ảo là một mạng dành riêng để kết nối các máy tính lại với nhau thông qua mạng Internet công cộng. Những máy tính tham gia mạng riêng ảo sẽ "nhìn thấy nhau" như trong một mạng nội bộ - LAN. Đây là một trong những cách tốt nhất để giữ cho phiên duyệt web luôn an toàn). Khi sử dụng VPN để truy cập internet, nó sẽ tự động thiết lập một kết nối mạng dựa trên chính nền tảng mạng không dây được mã hóa các gói tin truyền đi và nhận về, đồng thời chuyển hướng truy cập giúp người dùng ẩn danh dễ dàng trên mạng internet. Tuy nhiên, chính vì yếu tố bảo mật cao này mà VPN sẽ làm suy giảm một phần tốc độ mạng.

(2) Thay đổi mật khẩu quản trị

Các wifi thường được đặt mật khẩu quản trị mặc định. Để đảm bảo an toàn, cần thay đổi mật khẩu mặc định, nên để mật khẩu từ 8 ký tự trở nên và có các ký tự phức tạp như #, $, &..., hạn chế sử dụng các chuỗi dễ đoán được như ngày sinh, số chứng minh nhân dân, số điện thoại….

(3) Thận trọng khi chia sẻ dữ liệu

Nếu việc chia sẻ tệp tin không cần thiết thì nên tắt chức năng chia sẻ dữ liệu trên máy tính. Không nên chia sẻ toàn bộ ổ cứng, nếu cần chia sẻ tệp tin thì nên tạo ra một thư mục dành riêng cho việc chia sẻ và chuyển những tệp tin cần chia sẻ tới thư mục đó. Sử dụng mật khẩu để bảo vệ tệp tin cần chia sẻ, nên sử dụng mật khẩu kết hợp các ký tự phức tạp (#, $, &...).

(4) Cập nhật thường xuyên phần mềm, bản vá lỗi cho wifi

Các nhà sản xuất thường công bố các bản vá, bổ sung cho phần mềm trên wifi. Người sử dụng nên thường xuyên kiểm tra bản vá, bổ sung trên website của nhà sản xuất.

(5) Bảo mật mạng không dây ở nhà

Khi sử dụng các thiết bị không dây ở nhà, nếu không bảo mật các thiết bị đó thì có thể bị lợi dụng để truy cập Internet, thậm chí các hoạt động của người dùng trên mạng có thể bị theo dõi, các tệp tin trên máy tính có thể bị truy cập trái phép… Hãy thực hiện theo các bước dưới đây để đảm bảo mạng được an toàn: Thay đổi ID mặc định của wifi; thay đổi mật khẩu mặc định của hệ thống; tắt tính năng "quảng bá wifi"; mã hóa thông tin trao đổi; sử dụng tường lửa được xây dựng sẵn trong wifi để ngăn chặn truy nhập trái phép; cập nhật phần mềm thường xuyên cho hệ thống.

II. AN TOÀN MẠNG KHÔNG DÂY CỦA CƠ QUAN, TỔ CHỨC

Có thể nói, Mạng không dây đã trở thành một phần không thể thiếu trong hoạt động của các cơ quan, tổ chức và doanh nghiệp hiện nay. Đây là một công nghệ tiện lợi cho phép cán bộ, nhân viên kết nối và truy cập vào tài nguyên mạng từ bất kỳ đâu trong cơ quan tổ chức. Tuy nhiên, bên cạnh những tiện lợi, khi sử dụng mạng không dây, các cơ quan, tổ chức cũng đối mặt với những rủi ro liên quan đến an toàn, bảo mật. Mạng không dây của của các cơ quan, tổ chức có thể bị truy cập từ bên ngoài tòa nhà đặt nó. Khi mạng không dây được kết nối với mạng LAN của tổ chức rất có thể nó sẽ trở thành một điểm yếu gây ra mất an toàn lớn nhất cho toàn bộ hệ thống mạng của tổ chức.

Vì vậy, triển khai các biện pháp bảo mật phù hợp để chống lại những tấn công vào mạng không dây, việc bảo đảm an toàn thông tin, bảo vệ mạng không dây trở thành một nhiệm vụ quan trọng đối với cơ quan, tổ chức. Trong phần này, chúng ta sẽ tìm hiểu về các biện pháp quan trọng về bảo đảm an toàn bảo vệ mạng

không dây mà một cơ quan tổ chức cần triển khai để bảo vệ hệ thống và dữ liệu của mình.

1. Xác định chính sách an toàn mạng không dây

Đầu tiên, cơ quan tổ chức cần xác định và triển khai một chính sách an toàn mạng không dây cụ thể. Chính sách này nên gồm các quy định và quy tắc về việc sử dụng mạng không dây, bao gồm yêu cầu sử dụng mật khẩu mạng mạnh, thời hạn đổi mật khẩu định kỳ, và hướng dẫn cho người dùng về các biện pháp an toàn khi sử dụng mạng không dây.

2. Sử dụng mã hóa mạnh

Đối với mạng không dây, việc sử dụng mã hóa là một biện pháp quan trọng để bảo vệ dữ liệu. Cơ quan, tổ chức nên sử dụng giao thức mã hóa mạnh hiện nay như WPA2 hoặc WPA3 để bảo vệ mạng không dây khỏi việc bị đánh cắp thông tin hoặc xâm nhập trái phép. Ngoài ra, việc sử dụng mã hóa cũng nên được áp dụng cho các dịch vụ mạng khác như VPN (Virtual Private Network) để đảm bảo an toàn khi truyền dữ liệu qua mạng.

3. Cập nhật phần mềm và Firmware

Các thiết bị mạng không dây cần được cập nhật phần mềm và Firmware đều đặn. Việc này giúp vá các lỗ hổng bảo mật mới được tìm thấy và nâng cao tính ổn định của hệ thống. Thông thường, các nhà cung cấp thiết bị sẽ phát hành các bản vá bảo mật để khắc phục các lỗ hổng. Cơ quan tổ chức cần có quy trình để kiểm tra và cập nhật các thiết bị mạng không dây của mình đều đặn để đảm bảo rằng chúng luôn được bảo vệ với phiên bản phần mềm mới nhất.

4. Sử dụng các biện pháp xác thực mạnh

Một trong những yếu tố quan trọng để đảm bảo an toàn mạng không dây là sử dụng các biện pháp xác thực mạnh mẽ. Thay vì chỉ sử dụng mật khẩu mạng đơn giản, cơ quan tổ chức nên áp dụng xác thực hai yếu tố hoặc sử dụng chứng chỉ số để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào mạng không dây.

5. Thiết lập các mạng con riêng (VLAN)

Sử dụng VLAN (Virtual LAN) để phân chia mạng không dây thành các mạng con riêng biệt là một biện pháp quan trọng để ngăn chặn sự truy cập trái phép từ mạng không dây đến các mạng và tài nguyên quan trọng khác trong tổ chức. Bằng cách phân chia mạng không dây thành các mạng con riêng, người

quản trị mạng có thể kiểm soát và giám sát truy cập từng mạng con một cách hiệu quả, đồng thời giảm thiểu khả năng lây lan của các cuộc tấn công mạng.

6. Thiết kế vùng mạng không dây tách riêng, độc lập với các vùng mạng khác của cơ quan, tổ chức

Cần triển khai thiết kế vùng mạng không dây tách riêng, độc lập với các vùng mạng khác. Đây là yêu cầu bắt buộc về triển khai quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ theo Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Trường hợp cơ quan, tổ chức có thiết lập mạng không dây để phục vụ khách hàng, những người đến làm việc (chẳng hạn như họp, hội nghị, v.v….) không phải là cán bộ, công chức, nhân viên của cơ quan, tổ chức. Lời khuyên trong trường hợp này là tách vùng mạng này không có kết nối liên thông với mạng nội bộ, các mạng quan trọng của cơ quan, tổ chức với các lý do chính như sau:

- Phòng chống nguy cơ hệ thống mạng của cơ quan, tổ chức mình bị nhiễm mã độc trong trường hợp máy tính của khách bị nhiễm mã độc, mã độc từ máy tính, thiết bị của khách hàng có thể lây lan sang hệ thống mạng của cơ quan, tổ chức chúng ta trong trường hợp không ngăn chặn được loại mã độc mới này.

- Tránh trường hợp kẻ xấu có thể lợi dụng để tấn công leo thang hệ thống thông tin quan trọng bên trong cơ quan, tổ chức.

Hiện nay, các các xã, phường, thị trấn… đều có mạng nội bộ LAN, được xác định tối thiểu là cấp độ 2, thì việc thiết kế cần tách biệt mạng không dây (nếu có) với các vùng mạng còn lại.

7. Thiết lập bảo vệ, theo dõi và giám sát

Để đảm bảo an toàn mạng không dây, cơ quan tổ chức cần thiết lập phương án bảo vệ để kiểm soát truy cập giữa vùng mạng không dây với các vùng mạng khác của cơ quan, tổ chức (trong trường hợp có kết nối), thiết lập các hệ thống giám sát mạng để theo dõi hoạt động và phát hiện các hành vi bất thường. Các giải pháp bảo vệ, giám sát mạng có thể cung cấp thông tin về việc kết nối, lưu lượng mạng, và các hoạt động không bình thường, giúp phát hiện sớm các vấn đề bảo mật và can thiệp kịp thời.

8. Đào tạo nhân viên về an toàn mạng không dây

Cuối cùng, cơ quan tổ chức cần đào tạo nhân viên về an toàn mạng không dây. Điều này bao gồm cung cấp cho nhân viên kiến thức và kỹ năng cần thiết để hiểu và tuân thủ chính sách an toàn mạng không dây của tổ chức. Nhân viên cần được đào tạo về việc phát hiện các mối đe dọa tiềm ẩn, xác thực mạng không dây và biện pháp bảo mật, và các biện pháp phòng ngừa tấn công mạng.

An toàn mạng không dây là một yếu tố cần thiết trong việc bảo vệ thông tin và hệ thống của cơ quan tổ chức. Bằng cách triển khai các biện pháp an toàn mạng không dây như xác định chính sách an toàn, sử dụng mã hóa mạnh, cập nhật phần mềm và firmware, sử dụng các biện pháp xác thực mạnh, thiết lập VLAN, thiết kế vùng mạng không dây độc lập và giám sát mạng, cơ quan tổ chức có thể đảm bảo rằng mạng không dây của họ được bảo vệ một cách tốt nhất. Ngoài ra, việc đào tạo nhân viên về an toàn mạng không dây cũng đóng vai trò quan trọng trong việc nâng cao nhận thức và sự chuẩn bị của cơ quan tổ chức trước các mối đe dọa bảo mật mạng không dây.

III. AN TOÀN MÁY TÍNH KẾT NỐI MẠNG KHÔNG DÂY

Trong thời đại số ngày nay, máy tính và mạng không dây đã trở thành một phần không thể thiếu trong cuộc sống và công việc của chúng ta. Tuy nhiên, việc sử dụng máy tính kết nối mạng không dây cũng mang đến những rủi ro bảo mật. Đặc biệt, khi chúng ta kết nối máy tính của mình với mạng không dây công cộng hoặc kết nối đến mạng không dây trong cơ quan tổ chức, chúng ta cần đảm bảo rằng máy tính của mình được bảo vệ và an toàn. Trong phần này, chúng ta sẽ tìm hiểu về các biện pháp an toàn máy tính kết nối mạng không dây quan trọng để bảo vệ thông tin và dữ liệu của chúng ta, cụ thể 05 biện pháp như sau:

1. Về cập nhật hệ điều hành và phần mềm

Việc cập nhật hệ điều hành và phần mềm là một biện pháp quan trọng để đảm bảo an toàn máy tính. Hãy đảm bảo rằng hệ điều hành của bạn và tất cả các chương trình và ứng dụng trên máy tính đều được cập nhật phiên bản mới nhất. Các bản vá bảo mật được phát hành định kỳ để vá các lỗ hổng bảo mật mới được tìm thấy. Việc cập nhật đều đặn giúp bảo vệ máy tính khỏi các cuộc tấn công và lợi dụng lỗ hổng bảo mật.

Bởi khi chúng ta kết nối mạng không dây, đặc biệt là các mạng không dây công cộng, kẻ xấu hay hacker có thể khai thác lỗ hổng chưa được vá trên máy tính

của chúng ta để xâm nhập, cài đặt các mã độc hoặc đánh cắp dữ liệu trên máy tính.

2. Sử dụng phần mềm diệt virus và tường lửa

Đảm bảo rằng máy tính của bạn được trang bị phần mềm diệt virus và tường lửa mạnh. Phần mềm diệt virus giúp phát hiện và loại bỏ các phần mềm độc hại và virus khỏi máy tính, trong khi tường lửa giúp ngăn chặn các cuộc tấn công từ bên ngohài vào máy tính của bạn. Hãy đảm bảo rằng phần mềm diệt virus và tường lửa của bạn được cập nhật thường xuyên để đảm bảo khả năng bảo vệ tối đa.

Đối với việc cài đặt phần mềm diệt Virus, chúng ta có thể đầu tư để cài đặt phần mềm của nhà cung cấp dịch vụ chuyên nghiệp, tại Việt Nam có các sản phẩm của các nhà cung cấp Việt Nam nổi tiếng như Bkav, CMC, Cyrada hay VNPT, v.v…, các phần mềm của các hãng nước ngoài nổi tiếng có Kaspersky, Trend Micro, McAfee, … Trường hợp chưa đầu tư để cài đặt phần mềm Anti-virus chuyên nghiệp, chúng ta nên bật phần mềm phòng chống virus có sẵn trên hệ điều hành. Đối với hệ điều hành Windows, phần mềm này là Windows Defender (tùy thuộc vào phiên bản hệ điều hành, tên gọi có thể khác).

Đối với thiết lập tường lửa: Hiện nay, trên các máy tính hệ điều hành Microsoft Windows đề có tích hợp sẵn công cụ tường lửa (Windows Firewall), chúng ta nên tận dụng công cụ này

Để thiết lập tường lửa, chúng ta thực hiện như sau:

(1) Trên máy tính cài hệ điều hành Windows

Vào mục Control Panel, chọn "System and Security" và sau đó lựa chọn "Windows Firewall", bạn kiểm tra xem đang bật (on hoặc enable) hay tắt (off hoặc disable).

(2) Trên máy Macbook

Vào mục "System Preferences", chọn "Security & Privacy", sau đó chọn "Firewall" nhấn vào thanh để bật “enable” tính năng tường lửa

3. Sử dụng kết nối an toàn

Khi kết nối máy tính với mạng không dây công cộng hoặc mạng không dây trong cơ quan tổ chức, hãy sử dụng kết nối an toàn như giao thức mã hóa WPA2

hoặc WPA3. Điều này giúp mã hóa thông tin truyền qua mạng và ngăn chặn kẻ tấn công nghe trộm hoặc đánh cắp dữ liệu.

4. Tắt chia sẻ tệp tin (Turn off File-Sharing)

Một biện pháp an toàn quan trọng là tắt chia sẻ tập tin trên máy tính khi kết nối với mạng không dây công cộng. Việc tắt chia sẻ tập tin ngăn chặn người khác truy cập vào các tập tin và thư mục trên máy tính của bạn và giữ cho dữ liệu của bạn an toàn.

Một số hiệu điều hành như Windows sẽ tắt chế độ chia sẻ tệp tin cho bạn khi chọn tuy chọn Public khi kết nối vào một mạng mới đối với lần đầu tiên.

Các bước để tắt chế độ chia sẻ tệp tin

Trên máy tính chạy hệ điều hành Windows:

1. Vào mục Network and Sharing Center.

2. Sau đó chọn Change advanced sharing settings.

3. Chọn “Turn off file and printer sharing”

Đối với máy Macbooks:

1. Vào mục System Preferences.

2. Chọn mục Choose Sharing.

3. Bỏ lựa chọn chia sẻ mọi thứ

4. Tiếp theo, trong Finder, chọn AirDrop, và chọn mục Allow me to be discovered by: No One.

5. Sử dụng mạng riêng ảo (VPN)

Khi truy cập vào mạng không dây công cộng hoặc muốn tăng cường tính bảo mật, sử dụng mạng riêng ảo (VPN) là một lựa chọn tốt. VPN tạo ra một kênh kết nối bảo mật giữa máy tính của bạn và mạng đích, mã hóa thông tin và ẩn địa chỉ IP của bạn. Điều này giúp bảo vệ dữ liệu của bạn khỏi nguy cơ đánh cắp hoặc xâm nhập.

Thông thường, để phục vụ nhân viên có nhu cầu làm việc từ xa, kết nối vào tài nguyên của cơ quan, tổ chức, các đơn vị này sẽ thường thiết lập kênh VPN để đảm bảo an toàn thông tin mạng.

6. Đào tạo và nâng cao nhận thức bảo mật

Cuối cùng, việc đào tạo và nâng cao nhận thức bảo mật cho người dùng máy tính là rất quan trọng. Cung cấp cho nhân viên của cơ quan tổ chức kiến thức về các nguy cơ bảo mật, các biện pháp phòng ngừa, và quy tắc an toàn mạng không dây là cách hiệu quả nhất để nâng cao an toàn máy tính kết nối mạng không dây. Nhân viên cần được đào tạo về cách phân biệt các email lừa đảo, tránh nhấp vào các liên kết đáng ngờ và tránh cung cấp thông tin cá nhân nhạy cảm trên các mạng không dây công cộng.

An toàn máy tính kết nối mạng không dây là một yếu tố quan trọng để bảo vệ hệ thống thông tin, thông tin và dữ liệu của cơ quan, tổ chức. Bằng cách thực hiện các biện pháp an toàn như cập nhật hệ điều hành và phần mềm, sử dụng phần mềm diệt virus và tường lửa, sử dụng kết nối an toàn, tắt chia sẻ tập tin, sử dụng VPN và đào tạo nhân viên, chúng ta có thể đảm bảo rằng máy tính của mình được bảo vệ một cách an toàn khi kết nối với mạng không dây. Việc bảo đảm an toàn mạng không dây là trách nhiệm chung của cả cá nhân và tổ chức, và chúng ta cần làm việc cùng nhau để đảm bảo an toàn trong thế giới kỹ thuật số ngày nay.

IV. AN TOÀN ĐIỆN THOẠI KẾT NỐI MẠNG KHÔNG DÂY

Trong thời đại công nghệ số hiện đại, điện thoại di động đã trở thành một công cụ không thể thiếu trong cuộc sống hàng ngày của chúng ta. Thiết bị này ngoài những tính năng cơ bản của một chiếc điện thoại di động như nghe, gọi, nhắn tin…, thì còn tích hợp những ứng dụng vô cùng hiện đại với nhiều chức năng khác hỗ trợ đắc lực cho sinh hoạt, học hành và công việc như đọc tin tức, học trực tuyến, soạn thảo văn bản, chuyển khoản thanh toán ngân hàng, đặt xe di chuyển, mua bán hàng, đầu tư chứng khoán… Ngoài ra, nó còn như nhật ký (lưu trữ thông tin, hình ảnh…). Có thể nói, với chiếc điện thoại thông minh (smartphone), ngoài tài sản là giá của điện thoại của chúng ta, chiếc điện thoại chứa rất nhiều tài sản cả về tài sản vô hình là dữ liệu và tài sản hữu hình là tài khoản ngân hàng, ví điện tử, tài khoản chứng khoán,...

Do vậy, việc bảo đảm an toàn điện thoại nói chung và bảo đảm an toàn điện thoại khi kết nối mạng không dây, đặc biệt là đối với mạng không dây công cộng trở nên rất quan trọng, giúp bảo vệ thông tin, dữ liệu được lưu trữ trên những chiếc điện thoại thông minh và hạn chế các nguy cơ bị lộ lọt hoặc đánh cắp thông tin, dữ liệu.

Tương tự như bảo đảm an toàn cho máy tính kết nối mạng không dây, sau

đây là 06 biện pháp bảo đảm an toàn điện thoại kết nối mạng không dây để bảo vệ thông tin và dữ liệu của chúng ta.

Biện pháp 1. Cập nhật hệ điều hành và ứng dụng

Đảm bảo rằng điện thoại di động của bạn được cập nhật hệ điều hành và ứng dụng phiên bản mới nhất. Việc cập nhật hệ điều hành và ứng dụng giúp vá các lỗ hổng bảo mật mới được tìm thấy và nâng cao tính ổn định của hệ thống. Hãy đảm bảo rằng điện thoại di động của bạn tự động cập nhật hoặc thường xuyên kiểm tra cập nhật để bảo vệ thông tin và dữ liệu của bạn khỏi các cuộc tấn công bảo mật.

Do đó, điều quan trọng là bạn phải cài đặt các bản cập nhật hệ điều hành của mình. Bất cứ khi nào có bản cập nhật iOS mới xuất hiện, hãy tải xuống và cài đặt nó vào iPhone của bạn. Khi Google tung ra các bản cập nhật mới, hãy cài đặt chúng trên thiết bị Android của bạn. Bạn lo ngại về giới hạn bộ nhớ? Sao lưu hoặc đồng bộ hóa dữ liệu quan trọng lên đám mây, sau đó tạo dung lượng, xóa ứng dụng để có thể tải xuống và sử dụng các bản cập nhật đã cài đặt.

Biện pháp 2. Sử dụng phần mềm diệt virus hoặc công cụ bảo mật cho điện thoại di động

Đảm bảo rằng điện thoại di động của bạn được cài đặt phần mềm bảo mật hoặc phần mềm diệt vi-rút. Mặc dù điều này không áp dụng nhiều với người dùng iOS nhưng Android có vấn đề với phần mềm độc hại. Phần mềm như vậy sẽ cung cấp tường lửa và quét và loại bỏ phần mềm độc hại.

Những lý do rất rõ ràng. Nếu bạn kết nối với mạng Wi-Fi mở không bảo mật, bạn có nguy cơ tiếp xúc với phần mềm độc hại từ các thiết bị khác trên mạng. Điều này có thể là ngẫu nhiên - có thể là một con sâu máy tính tự lây lan từ thiết bị bị nhiễm này sang thiết bị bị nhiễm khác - hoặc có thể là cố ý, được gửi bởi một người dùng độc hại có thể ngồi khá gần.

Biện pháp 3. Tránh các giao dịch tài chính mà không được bảo vệ

Nên hạn chế sử dụng dịch vụ Ngân hàng trực tuyến và mua sắm qua kết nối Wi-Fi công cộng, không an toàn. Những kẻ hoặc hacker thể sử dụng các công cụ mà để đánh cắp một số dữ liệu không được mã hóa. Đương nhiên, các anh/chị chỉ nên thực hiện giao dịch tài chính, mua sắm với những công ty bảo mật mật khẩu của bạn.

Vậy bạn có thể làm gì để đảm bảo an toàn? Một cách là chuyển sang kết

nối internet di động của riêng bạn, nếu có thể và thực hiện giao dịch một cách an toàn theo cách đó. Bạn cũng có thể sử dụng VPN để mã hóa tất cả lưu lượng truy cập internet của bạn.

Nếu bạn đang sử dụng dịch vụ ngân hàng trực tuyến, hãy đảm bảo bạn đang sử dụng ứng dụng chính thức của ngân hàng và ứng dụng này cung cấp mã hóa đầy đủ. Tương tự, hãy sử dụng các ứng dụng chính thức, bảo mật để mua sắm trực tuyến. Nếu chúng không an toàn, đừng mua sắm cho đến khi bạn có thể chắc chắn rằng nó an toàn!

Biện pháp 4. Kiểm tra ứng dụng trước khi cài đặt

Trước khi cài đặt bất kỳ ứng dụng nào trên điện thoại di động của bạn, hãy kiểm tra tính phù hợp và đáng tin cậy của ứng dụng đó. Lựa chọn ứng dụng từ các nguồn tin cậy và kiểm tra đánh giá và nhận xét từ người dùng khác. Điều này giúp tránh cài đặt ứng dụng độc hại hoặc nguy hiểm, và đảm bảo an toàn cho dữ liệu và thông tin trên điện thoại di động của bạn.

Lời khuyên là nên sử chỉ cài đặt các phần mềm từ các kho ứng dụng như Apple Store đối với điện thoại iPhone, sử dụng hệ điều hành iOS và từ kho ứng dụng Google Play đối với các điện thoại dụng hệ điều hành Android, bởi những phần mềm đưa lên 02 kho ứng dụng này cơ bản đã được xét duyệt.

Biện pháp 5. Quản lý quyền riêng tư và ứng dụng

Kiểm tra và quản lý quyền riêng tư trên điện thoại di động của bạn. Hãy kiểm tra và kiểm soát quyền truy cập của các ứng dụng đến thông tin cá nhân và dữ liệu trên điện thoại di động. Cung cấp quyền truy cập tối thiểu và chỉ cho phép những ứng dụng đáng tin cậy và cần thiết truy cập thông tin cá nhân của bạn. Điều này giúp bảo vệ quyền riêng tư và ngăn chặn việc sử dụng thông tin cá nhân của bạn một cách trái phép.

Biện pháp 6. Sao lưu và mã hóa dữ liệu

Thực hiện sao lưu định kỳ dữ liệu quan trọng trên điện thoại di động và mã hóa các tập tin và thông tin nhạy cảm. Việc sao lưu dữ liệu đảm bảo rằng bạn không mất dữ liệu quan trọng trong trường hợp xảy ra sự cố hoặc mất mát thiết bị. Mã hóa dữ liệu giúp bảo mật thông tin cá nhân và dữ liệu quan trọng của bạn trong trường hợp điện thoại di động bị đánh cắp hoặc mất mát.

An toàn điện thoại kết nối mạng không dây là một yếu tố quan trọng để bảo vệ thông tin và dữ liệu cá nhân. Bằng cách thực hiện các biện pháp an toàn như cập

nhật hệ điều hành và ứng dụng, sử dụng mã hóa và kết nối an toàn, sử dụng phần mềm diệt virus và tường lửa, kiểm tra ứng dụng trước khi cài đặt, quản lý quyền riêng tư và ứng dụng, sao lưu và mã hóa dữ liệu, và biện pháp không thể thiếu là nâng cao nhận thức bảo mật, chúng ta có thể đảm bảo rằng điện thoại di động của chúng ta được bảo vệ một cách an toàn khi kết nối với mạng không dây./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG