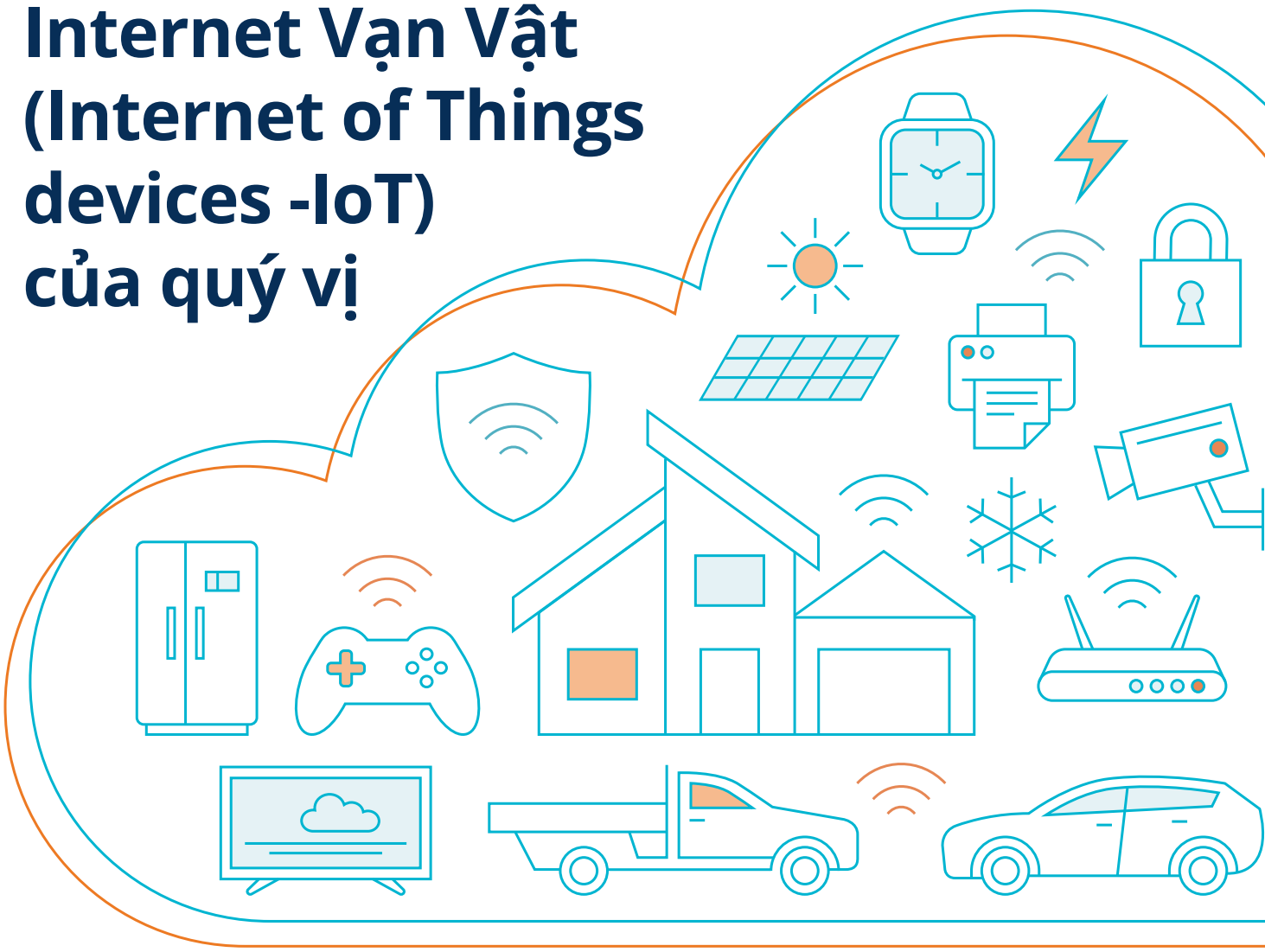
Mẹo để bảo mật thiết bị Internet Vạn Vật (Internet of Things devices -IoT) của quý vị



Trung tâm An ninh mạng Úc (Australian Cyber Security Centre) đã soạn thảo thông tin này nhằm giúp cộng đồng mua và sử dụng các thiết bị Internet Vạn Vật (IoT) một cách an toàn. Thiết bị IoT là những vật dụng hằng ngày được tích hợp khả năng kết nối với internet. Ví dụ về thiết bị IoT bao gồm máy quan sát trẻ em, máy bay không người lái, camera an ninh, tivi thông minh và bộ biến tần năng lượng mặt trời. Các thiết bị IoT trong gia đình và doanh nghiệp thường sử dụng hệ thống mạng lưới Wi-Fi hoặc mạng di động như 4G hoặc 5G để kết nối với internet.

Nhiều thiết bị IoT thường thấy tại các hộ gia đình và doanh nghiệp ở Úc không được thiết kế với yếu tố bảo mật làm trọng tâm. Điều này khiến các thiết bị dễ bị tấn công và xâm nhập thông qua internet. Những vụ xâm nhập như vậy có thể cho phép tội phạm mạng truy cập trái phép vào thiết bị và dữ liệu cá nhân của quý vị để thực hiện các mục đích độc hại.

Trước khi mua một thiết bị IoT

Tìm hiểu thiết bị trước khi mua là việc rất quan trọng, vì các nhà sản xuất cung cấp mức độ bảo mật khác nhau. Trước khi đưa ra quyết định mua, hãy so sánh các thiết bị tương tự được bán bởi các nhà sản xuất khác nhau. Những yếu tố cần cân nhắc bao gồm:

1. **Thiết bị có được sản xuất bởi một công ty có uy tín và được bán bởi một cửa hàng đáng tin cậy không?** Các công ty nổi tiếng và có uy tín thường có xu hướng sản xuất thiết bị với yếu tố bảo mật được cân nhắc ngay từ đầu. Các cửa hàng có uy tín thường chỉ bán sản phẩm từ những công ty có uy tín, và có chuỗi cung ứng nghiêm ngặt hơn, bảo đảm thiết bị đến tay quý vị đúng như nhà sản xuất dự định.

2. **Quý vị có thể thay đổi mật mã không?** Việc thay đổi mật mã luôn là một thói quen tốt. Tuy nhiên, nếu thiết bị được cài sẵn mật mã mặc định yếu, thì việc thay đổi mật mã càng trở nên quan trọng hơn. Một thiết bị có bảo mật tốt nên có mật mã duy nhất, khó đoán, phức tạp và không thể suy đoán được, vì mật mã mặc định yếu là cách dễ nhất để tấn công một thiết bị.

3. **Nhà sản xuất có cung cấp bản cập nhật không?** Việc các công ty cung cấp bản cập nhật để khắc phục các lỗ hổng bảo mật khi chúng được phát hiện là rất quan trọng. Ví dụ, nếu phần mềm trên thiết bị tồn tại các lỗ hổng đã biết hoặc tác nhân phát triển các phương thức mới để xâm nhập thiết bị của quý vị, thì các bản cập nhật là việc cần thiết để vá và khắc phục các vấn đề đó.

4. **Thiết bị sẽ thu thập dữ liệu gì và dữ liệu đó sẽ được chia sẻ với ai?** Thông tin về loại dữ liệu mà thiết bị sẽ thu thập và cách sử dụng dữ liệu đó nên được công khai trên trang mạng của nhà sản xuất hoặc trong chính sách về quyền riêng tư của họ. Việc cân nhắc kỹ lưỡng những thông tin mà ứng dụng trực tuyến hoặc ứng dụng di động thu thập luôn là điều quan trọng.

5. **Thiết bị có thực hiện đúng chức năng quý vị cần không?** Mua một thiết bị có nhiều tính năng hơn nhu cầu thực tế của quý vị, đặc biệt là những thiết bị có khả năng kết nối với internet, có thể làm giảm mức độ an toàn bảo mật. Các chức năng của thiết bị mà quý vị không sử dụng, có thể làm tăng nguy cơ bị tấn công mà không mang lại lợi ích gì cho quý vị cả.

Thiết bị IoT

Hãy ghi nhớ một vài câu hỏi đơn giản khi thiết lập thiết bị của quý vị, để giúp bảo vệ hệ thống mạng lưới và dữ liệu cá nhân tốt hơn.

1. **Thiết bị có thật sự cần kết nối với internet không?** Chỉ vì thiết bị có thể kết nối với internet, không có nghĩa là quý vị phải kết nối chúng. Những thiết bị không kết nối với internet có nguy cơ bị xâm nhập thấp hơn rất nhiều. Nếu quý vị không sử dụng các tính năng yêu cầu kết nối với internet, hãy cân nhắc xem liệu thiết bị có cần kết nối không.

2. **Thiết bị có được đặt ở vị trí an toàn không?** Nếu thiết bị không cần phải lắp đặt ở khu vực không an toàn, việc đặt nó ở một vị trí an toàn có thể giảm nguy cơ chúng bị xâm phạm trực tiếp.

3. **Tôi có nên thay đổi tên đăng nhập và mật mã mặc định không?** Việc sử dụng mật mã hoặc cụm mật mã mạnh là rất quan trọng. Nếu thiết bị của quý vị không được giao kèm mật mã duy nhất, khó đoán, phức tạp và không thể suy đoán, thì quý vị cần thay đổi mật mã đó. Tên đăng nhập và mật mã mặc định thường được thu thập và đăng tải trực tuyến, có thể khiến cho thiết bị của quý vị trở thành mục tiêu để tấn công.

4. **Hệ thống mạng lưới Wi-Fi của tôi đã được thiết lập an toàn chưa, và nó có mật mã bảo mật không?** Bảo mật hệ thống mạng lưới Wi-Fi và bộ định tuyến của quý vị để làm cho việc truy cập thiết bị và hệ thống mạng lưới của quý vị trở nên khó khăn hơn đối với kẻ tấn công.

Hãy cố gắng làm thêm những bước sau:

Thiết lập một hệ thống mạng lưới Wi-Fi bổ sung trên bộ định tuyến của quý vị chỉ dành riêng cho các thiết bị IoT. Hệ thống mạng lưới này có thể được đặt tên trên bộ định tuyến Wi-Fi của quý vị là hệ thống mạng lưới "khách" (guest network). Nếu các thiết bị IoT của quý vị không cần giao tiếp với nhau, hãy bật tính năng "cách ly khách" (client isolation). Việc giữ các thiết bị IoT tách biệt khỏi dữ liệu nhạy cảm của quý vị sẽ bảo đảm rằng, khi một thiết bị IoT bị xâm phạm, kẻ tấn công không thể truy cập vào các thiết bị hoặc dữ liệu khác của quý vị.

5. **Các tính năng không cần thiết của thiết bị đã được tắt chưa?** Nếu thiết bị của quý vị có các tính năng không mong muốn, hoặc không cần thiết (chẳng hạn như camera hoặc micro), hãy tắt chúng nếu có thể.

Hãy cố gắng làm thêm những bước sau

Tìm cài đặt cấu hình liên quan đến việc bật truy cập từ xa vào giao diện quản trị mạng của thiết bị từ mạng LAN nội bộ hoặc WAN/internet. Bảo đảm cài đặt này chỉ cho phép truy cập từ mạng LAN nội bộ, trừ khi quý vị thực sự cần truy cập từ xa.

Bảo trì thiết bị IoT

Có một số điều quan trọng cần nhớ sau khi quý vị đã thiết lập và sử dụng thiết bị IoT của mình. Bao gồm:

1. **Khởi động lại thiết bị của quý vị định kỳ.** Virus có thể hiện diện nếu thiết bị IoT bắt đầu hoạt động chậm hoặc không thể sử dụng được. Phần lớn phần mềm độc hại được lưu trữ trong bộ nhớ và có thể dễ dàng loại bỏ bằng cách khởi động lại thiết bị, tức là tắt và bật lại thiết bị. Nếu thiết bị vẫn chậm hoặc không hoạt động sau khi khởi động lại, hãy thử khôi phục cài đặt gốc (factory reset), nhưng cần lưu ý rằng thao tác này có thể xóa hết dữ liệu người sử dụng và các thiết lập cá nhân.

2. **Áp dụng các bản cập nhật thường xuyên.** Một số thiết bị tự động cập nhật các bản vá. Đối với những thiết bị không được tự động cập nhật, hãy thường xuyên kiểm tra với nhà sản xuất và áp dụng các bản cập nhật ngay khi có sẵn. Khi thiết bị của quý vị không còn nhận được các bản cập nhật nữa, hãy cân nhắc nâng cấp lên thiết bị mới hơn, có hỗ trợ cập nhật. Các thiết bị không được cập nhật bảo mật sẽ không được bảo vệ khi các lỗ hổng mới được phát hiện, và có thể trở thành nguy cơ đối với hệ thống mạng lưới, quyền riêng tư và dữ liệu của quý vị.

3. **Tắt thiết bị khi không sử dụng.** Để các thiết bị không sử dụng và không được giám sát, hoạt động và kết nối với hệ thống mạng lưới Wi-Fi trong thời gian dài, có thể làm tăng khả năng các thiết bị này bị tấn công. Một cách để tự động thực hiện việc này, là sử dụng bộ hẹn giờ ổ cắm điện, chỉ cấp điện cho thiết bị trong những giờ đã định trước.

4. **Hãy chú ý đến sự tăng đột biến đáng kể trong lượng sử dụng internet hằng tháng hoặc hóa đơn cước internet của quý vị.** Sự gia tăng đáng kể trong việc sử dụng internet; hoặc chi phí hóa đơn; có thể là dấu hiệu thiết bị của quý vị đã bị xâm phạm. Trừ khi bộ phận IT trong doanh nghiệp của quý vị sẽ điều tra vấn đề này, quý vị nên thực hiện khôi phục cài đặt gốc tuy nhiên, cần lưu ý rằng thao tác này có thể xóa hết dữ liệu người sử dụng và các thiết lập cá nhân, sau đó thay đổi mật mã.

Vất bỏ thiết bị IoT

Việc vất bỏ thiết bị (bằng cách loại bỏ hoặc bán đi) có thể tạo điều kiện cho người khác dễ dàng truy cập vào thông tin cá nhân hoặc dữ liệu của quý vị. Các cách thức để ngăn chặn việc truy cập này bao gồm:

1. **Xóa tất cả dữ liệu và thông tin cá nhân.** Nhà sản xuất nên cung cấp phương pháp để quý vị có thể xóa dữ liệu và thông tin cá nhân khỏi cả thiết bị và các ứng dụng liên quan. Việc xóa thông tin cá nhân của quý vị sẽ bảo đảm rằng không ai có thể truy cập vào dữ liệu đó sau khi quý vị đã vất bỏ thiết bị. Xóa tài khoản trực tuyến của quý vị nếu không còn cần sử dụng cùng với thiết bị IoT nữa.

2. **Thực hiện khôi phục cài đặt gốc cho thiết bị.** Khôi phục cài đặt gốc được thiết kế để xóa dữ liệu lưu trữ cục bộ và đặt lại mật mã, tên đăng nhập cùng các thiết lập về mặc định. Kiểm tra hướng dẫn sử dụng thiết bị hoặc trang mạng của nhà sản xuất để biết cách thực hiện khôi phục cài đặt gốc.

3. **Ngắt kết nối thiết bị với điện thoại di động và các thiết bị khác.** Vất bỏ một thiết bị mà vẫn có quyền truy cập vào các thiết bị khác, hệ thống mạng lưới hoặc tài khoản trực tuyến của quý vị, có thể tạo điều kiện cho người khác có cơ hội truy cập vào chúng. Hãy chắc chắn kiểm tra các thiết bị khác của quý vị và loại bỏ mọi liên kết (pairing) với thiết bị mà quý vị định vứt bỏ. Xóa bỏ bất kỳ quyền truy cập nào đã cấp cho ứng dụng di động mà quý vị không còn cần sử dụng.

4. **Tháo bỏ bất kỳ phương tiện lưu trữ di động nào (ví dụ: USB flash drive, thẻ nhớ, v.v.) gắn với thiết bị.** Phương tiện lưu trữ di động có thể chứa dữ liệu cá nhân không bị xóa khi quý vị khôi phục cài đặt gốc, và nên được tháo ra, tiêu hủy và xử lý riêng biệt với thiết bị.

Giúp đỡ

Liên lạc với Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) qua email: asd.assist@defence.gov.au hoặc gọi cho đường dây nóng 24 giờ mỗi ngày, 7 ngày một tuần để được giúp đỡ khẩn cấp theo số **1300 CYBER1 (1300 292 371)**.

Trình báo tội phạm mạng qua ReportCyber tại trang mạng www.cyber.gov.au/report

Liên lạc IDCARE qua trang mạng www.idcare.org nếu danh tính của quý vị đã từng bị đánh cắp.

Truy cập trang mạng www.cyber.gov.au để nhận lời khuyên hữu ích cho quý vị và gia đình. Đăng ký dịch vụ Cảnh báo miễn phí về các mối đe dọa trực tuyến gần đây của Trung tâm An ninh Mạng Úc (ACSC).

Hãy cùng nhau làm cho nước Úc trở thành nơi kết nối trực tuyến an toàn nhất.

Để nhận lời khuyên về an ninh mạng, hãy truy cập trang mạng www.cyber.gov.au

Tuyên bố miễn trừ trách nhiệm

Tài liệu trong hướng dẫn này mang tính chất tổng quát và không nên được coi là cố vấn pháp lý hoặc được dựa vào để được giúp đỡ trong bất kỳ trường hợp cụ thể hoặc tình huống khẩn cấp nào. Đối với bất kỳ vấn đề quan trọng nào, quý vị nên tìm kiếm lời khuyên chuyên môn, độc lập và thích hợp liên quan đến hoàn cảnh của mình.

Chính phủ Liên bang không chịu trách nhiệm hoặc trách nhiệm pháp lý nào đối với bất kỳ thiệt hại, mất mát hoặc chi phí nào phát sinh do việc trông cậy vào thông tin có trong hướng dẫn này.

Muốn biết thêm thông tin, hoặc muốn trình báo vấn đề an ninh mạng, hãy liên lạc với chúng tôi:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Số điện thoại này chỉ được sử dụng ở trong nước Úc mà thôi.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre