Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

AN NINH MẠNG CÁ NHÂN

NHỮNG BƯỚC ĐẦU TIÊN

cyber.gov.au

An ninh Mạng Cá nhân Nhiều phần

Hướng dẫn ***An ninh Mạng Cá nhân: Những Bước Đầu tiên*** là phần hướng dẫn thứ nhất trong loạt ba hướng dẫn được thiết kế nhằm giúp cho người dân Úc chân chính hiểu cơ bản về an ninh mạng. Học cách bạn có thể hành động để bảo vệ bản thân khỏi những mối đe dọa mạng phổ biến.

Những bước Đầu tiên

Những baước Tiếp theo

Những bước Nâng cao

Mục lục

Giới thiệu

An ninh mạng cá nhân là gì?

Trong một thế giới ngày càng được thúc đẩy bởi công nghệ, các thiết bị và tài khoản chúng ta sử dụng hàng ngày dễ bị đe dọa bởi các mối đe dọa trên mạng:

- Thiết bị của bạn có thể bao gồm máy vi tính, điện thoại di động, máy tính bảng di động với màn hình cảm ứng và các thiết bị kết nối internet khác.
- Có thể bạn còn sử dụng các tài khoản trực tuyến cho email, giao dịch ngân hàng, mua sắm, mạng xã hội, để chơi trò chơi điện tử, và hơn thế nữa.

An ninh mạng cá nhân là các bước liên tục mà bạn có thể thực hiện để bảo vệ các tài khoản và thiết bị của mình khỏi các mối đe dọa trên mạng.

Tập hướng dẫn này có thể giúp bảo vệ tôi khỏi các mối đe dọa trên mạng thế nào?

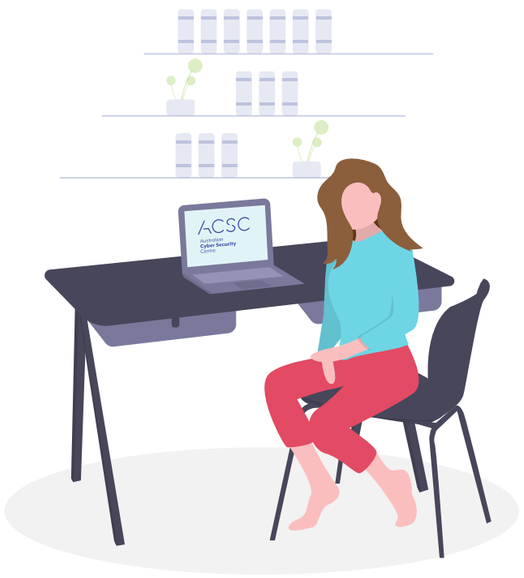
Nếu đây là lần đầu tiên bạn đang tìm hiểu về an ninh mạng, hoặc đang cập nhật kiến thức cho mình, thì tập hướng dẫn này là nơi tuyệt vời để bắt đầu. Bảo mật Mạng Cá nhân: Hướng dẫn Các bước Đầu tiên (First Steps guide) là tập hướng dẫn đầu tiên trong loạt ba tập hướng dẫn được thiết kế để giúp bạn nắm được những kiến thức cơ bản về an ninh mạng.

Các mối đe dọa trên mạng là gì?

Các mối đe dọa mạng chính ảnh hưởng đến người Úc hàng ngày là **lừa đảo và phần mềm độc hại**.

- **Phần mềm độc hại là một thuật ngữ chung được sử dụng để mô tả lập trình** được thiết kế để gây hại. Phần mềm này có thể bao gồm vi-rút, sâu, phần mềm gián điệp, trojans(là một loại phần mềm độc hại tải xuống máy tính được ngụy trang dưới dạng một chương trình hợp pháp) và phần mềm tống tiền. Tội phạm mạng sử dụng phần mềm độc hại để đánh cắp thông tin và tiền bạc của bạn, đồng thời kiểm soát các thiết bị và tài khoản của bạn.
- **Lừa đảo là những tin nhắn được tội phạm mạng gởi đi** nhằm đánh lừa để bạn cung cấp thông tin nhạy cảm, hoặc để kích hoạt phần mềm độc hại trên thiết bị của bạn.

Những cuộc tấn công này có thể có tác động đáng kể về mặt cá nhân và tài chính đối với nạn nhân. Chúng liên tục phát triển về độ tinh vi và mức độ thường xuyên.

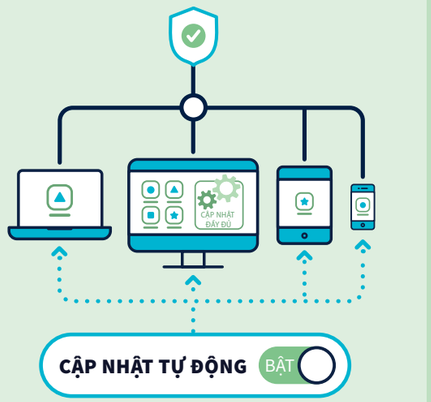


Bật tính năng tự động cập nhật

Cập nhật là gì?

Bản cập nhật là phiên bản cải tiến của phần mềm (lập trình, ứng dụng và hệ điều hành) mà bạn đã cài đặt trên máy vi tính, và thiết bị di động của mình.

- **Các bản cập nhật phần mềm giúp bảo vệ thiết bị** của bạn bằng cách sửa các 'lỗi' phần mềm (lỗi mã hóa hoặc lỗ hổng bảo mật). Tội phạm mạng và phần mềm độc hại có thể sử dụng những 'lỗi' này để truy cập vào thiết bị của bạn và đánh cắp dữ liệu cá nhân, tài khoản, thông tin tài chính và danh tính của bạn.
- **Những 'lỗi' phần mềm mới liên tục bị tội phạm mạng tìm thấy** và khai thác. Cập nhật phần mềm trên thiết bị của bạn sẽ giúp bảo vệ bạn khỏi các cuộc tấn công mạng.



Làm cách nào để thiết lập tính năng tự động cập nhật?

Cập nhật tự động là chế độ mặc định hoặc chế độ 'đặt và quên'. Chế độ này cài đặt các bản cập nhật mới ngay khi có sẵn.

- **Bật và xác nhận tính năng tự động** cập nhật trên tất cả các phần mềm và thiết bị.
- **Cách thức bạn bật tính năng tự động cập nhật có thể khác nhau** tùy thuộc vào phần mềm và thiết bị.
- **Chọn thời gian thuận tiện để tự động cập nhật nếu có thể**, chẳng hạn như khi bạn đang ngủ hoặc không thường sử dụng thiết bị của mình.

Thiết bị của bạn phải được bật nguồn, cắm điện và có dung lượng lưu trữ chưa sử dụng.

Mẹo: Nếu bạn nhận được lời nhắc nhở để cập nhật phần mềm của thiết bị, bạn nên thực hiện việc này càng sớm càng tốt.

Bạn có thể tìm thêm thông tin chi tiết hơn về các cách để bật tính năng tự động cập nhật bằng cách tìm kiếm sử dụng từ 'Updates'(Cập nhật) trên trang mạng cyber.gov.au

Nếu chế độ tự động cập nhật không có sẵn thì sao?

Nếu chế độ tự động cập nhật không có sẵn, bạn nên thường xuyên kiểm tra để biết và cài đặt các bản cập nhật mới qua menu chế độ của phần mềm hoặc thiết bị của bạn.

Nếu thiết bị và phần mềm cũ hơn của tôi không nhận được bất kỳ bản cập nhật nào thì sao?

Nếu thiết bị, hệ điều hành hoặc phần mềm của bạn quá cũ, thì nó có thể không còn được nhà sản xuất hoặc nhà phát triển hỗ trợ nữa.

Khi các sản phẩm đạt đến giai đoạn 'kết thúc hỗ trợ này, chúng sẽ không còn nhận được cập nhật nữa. Điều này có thể khiến bạn dễ bị tấn công mạng. Ví dụ về các sản phẩm đã kết thúc hỗ trợ bao gồm Hệ điều hành Windows 7 và iPhone 7.

Nếu thiết bị, hệ điều hành hoặc phần mềm của bạn đã hết thời gian được hỗ trợ, ACSC khuyến nghị nâng cấp càng sớm càng tốt để luôn an toàn.

Để biết thêm thông tin, hãy tìm kiếm 'End of support' (Kết thúc hỗ trợ) trên trang cyber.gov.au

Kích hoạt tính năng xác thực đa yếu tố (MFA).

MFA là gì?

Bạn có thể sử dụng tính năng xác thực đa yếu tố (MFA) để cải thiện tính bảo mật cho các tài khoản quan trọng nhất của mình. MFA yêu cầu bạn tạo cách kết hợp hai hoặc nhiều cách hơn để xác thực trước khi cấp quyền truy cập vào tài khoản.

- **Thông tin bạn biết** (ví dụ: mã PIN, mật mã hoặc cụm mật mã)
- **Thứ bạn có** (ví dụ: thẻ thông minh, mã thông báo vật lý, ứng dụng xác thực, SMS hoặc email)
- **Thứ gì đó của bạn** (ví dụ: dấu vân tay, nhận diện khuôn mặt hoặc quét tròng mắt)

MFA khiến tội phạm mạng khó có được quyền truy cập lần đầu vào tài khoản của bạn hơn. Nó thêm nhiều lớp xác thực hơn, đòi hỏi thêm thời gian, công sức, tiền bạc và phương tiện để phá vỡ.

Bằng cách nào tôi có thể kích hoạt MFA để bảo vệ tài khoản quan trọng nhất của mình?

Các bước để kích hoạt MFA sẽ khác nhau, tùy thuộc vào tài khoản, thiết bị hoặc phần mềm ứng dụng. Bạn nên kích hoạt MFA ngay bây giờ, bắt đầu với các tài khoản quan trọng của bạn:

- Tất cả các tài khoản ngân hàng và tài chính trực tuyến (ví dụ: ngân hàng của bạn, PayPal)
- Tất cả các tài khoản email (ví dụ: Gmail, Outlook, Hotmail, Yahoo!)

Nếu bạn có nhiều tài khoản email, hãy ưu tiên những tài khoản được liên kết với ngân hàng trực tuyến của bạn hoặc các dịch vụ quan trọng khác.

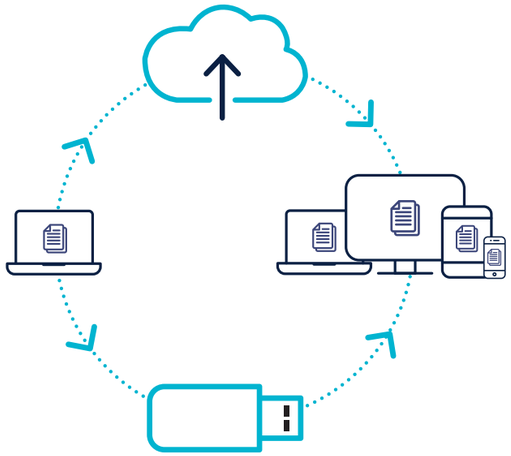
Bạn có thể đọc thêm về cách thức để bật tính năng xác thực đa yếu tố bằng cách tìm kiếm theo cụm từ 'Multi-factor authentication' (Xác thực đa yếu tố) hoặc 'MFA' trên trang cyber.gov.au

Thường xuyên sao lưu các thiết bị của bạn

Sao lưu là gì?

Bản sao lưu là một bản sao kỹ thuật số của thông tin của bạn. Điều này có thể bao gồm những thứ như hình ảnh, thông tin tài chính hoặc hồ sơ mà bạn đã lưu vào một thiết bị lưu trữ bên ngoài, hoặc trên đám mây(cloud).

Sao lưu thông tin của bạn là một biện pháp phòng ngừa để có thể khôi phục thông tin nếu thông tin bị mất, bị đánh cắp hoặc bị hư hỏng.



Làm thế nào để sao lưu các thiết bị và các tập hồ sơ của tôi?

Bạn nên thường xuyên sao lưu các tập hồ sơ và thiết bị của mình. Thường xuyên thế nào là do ở bạn, hàng ngày, hàng tuần hay hàng tháng, cuối cùng đều tùy thuộc vào bạn. Số lần bạn sao lưu có thể phụ thuộc vào số lượng:

- các tập hồ sơ mới mà bạn tải vào thiết bị của mình,
- những thay đổi bạn thực hiện đối với các tập hồ sơ.

Mẹo: Hãy kiểm tra các bản sao lưu của bạn thường xuyên để bạn quen với quá trình khôi phục. Luôn phải bảo đảm rằng các bản sao lưu của bạn đang hoạt động bình thường.

Bạn có thể tìm thêm thông tin chi tiết hơn về cách thức để sao lưu thông tin của mình, bằng cách tìm kiếm sử dụng từ 'Backups'(sao lưu) trên trang cyber.gov.au

Sử dụng cụm mật mã để bảo mật các tài khoản quan trọng của bạn

Xác thực đa yếu tố (MFA) là một trong những cách hiệu quả nhất để bảo vệ tài khoản của bạn khỏi tội phạm mạng. Nếu không có MFA, thì một cụm mật mã mạnh độc đáo có thể giúp bảo vệ tài khoản của bạn tốt hơn so với một mật mã đơn giản.

Cụm mật mã là gì?

Cụm mật mã bao gồm bốn từ ngẫu nhiên trở lên để trở thành mật mã của bạn.

Ví dụ: 'bánh quy đất sét hành pha lê'.

- **Cụm mật mã là cách bảo mật tốt hơn** so với mật mã đơn giản.
- Các cụm mật mã rất **khó bị tội phạm mạng** đoán ra, nhưng **bạn lại dễ nhớ**.

Bằng cách nào tôi có thể tạo cụm mật mã?

Tạo cụm mật mã:

- **Dài:** dài ít nhất 14 ký tự, sử dụng bốn từ ngẫu nhiên trở lên. Cụm mật mã của bạn càng dài thì càng an toàn.
- **Không thể đoán trước:** sử dụng kết hợp ngẫu nhiên ít nhất bốn từ không liên quan. Không nên dùng cụm từ nổi tiếng, những câu phát biểu lừng lẫy hoặc lời bài hát.
- **Độc đáo:** không được sử dụng trên nhiều tài khoản.

Nếu một trang web hoặc dịch vụ đòi hỏi một mật mã phức tạp bao gồm các ký hiệu, chữ hoa, hoặc số, bạn có thể bao gồm những đặc điểm này trong cụm mật mã của mình. Cụm mật mã của bạn vẫn phải dài, không thể đoán trước và độc nhất vô nhị để bảo mật tốt nhất.

Tôi nên bảo mật những tài khoản nào bằng cụm mật mã?

Nếu các tài khoản quan trọng nhất của bạn không được bảo vệ bằng MFA, hãy thay đổi mật mã của bạn thành cụm mật mã mạnh độc đáo, bắt đầu với:

- Tài khoản ngân hàng và tài chính trực tuyến
- Các tài khoản email

Nếu bạn có nhiều tài khoản email, hãy ưu tiên những tài khoản được liên kết với ngân hàng trực tuyến của bạn hoặc các dịch vụ quan trọng khác.

Thông thường, bạn có thể thay đổi mật mã của mình thành cụm mật mã mạnh, độc đáo, thông qua menu cài đặt tài khoản của mình.

Mẹo: Nếu bạn gặp khó khăn trong việc nhớ tất cả các cụm mật mã của mình, hãy cân nhắc sử dụng lập trình quản lý mật mã. Với lập trình quản lý mật mã, bạn chỉ cần nhớ một mật mã, lập trình quản lý mật mã đó sẽ lo phần còn lại. Tìm kiếm sử dụng cụm từ 'password manager' (quản lý mật mã) trên trang mạng cyber.gov.au để có thêm lời khuyên.

Bạn có thể tìm thêm thông tin chi tiết hơn về cách thức để tạo cụm mật mã an toàn bằng cách tìm kiếm sử dụng từ 'Passphrases'(Cụm mật mã) trên trang mạng cyber.gov.au

Bảo mật thiết bị di động của bạn

Ngày nay điện thoại thông minh và máy tính bảng được sử dụng trong cuộc sống hàng ngày. Chúng ta sử dụng chúng để kết nối, mua sắm, làm việc, giao dịch ngân hàng, theo dõi tình trạng sức khỏe của mình, và hoàn thành hàng trăm việc vào bất kỳ lúc nào, và từ bất kỳ địa điểm nào.

Điều gì có thể xảy ra nếu thiết bị di động của tôi bị xâm nhập, bị mất hoặc bị đánh cắp?

- Nó có thể bị tội phạm mạng sử dụng để đánh cắp tiền bạc hoặc danh tính của bạn. Họ làm điều này bằng cách sử dụng thông tin được lưu trữ trên thiết bị của bạn, bao gồm cả tài khoản mạng xã hội và email.
- Bạn có thể mất các dữ liệu không thể thay thế được như hình ảnh, các ghi chép hoặc tin nhắn (nếu không được sao lưu).
- Tội phạm mạng có thể sử dụng số điện thoại của bạn để lừa đảo người khác.

Làm thế nào để bảo mật thiết bị di động của tôi?

Bảo mật thiết bị:

- **Khóa** thiết bị của bạn bằng cụm mật mã, mật khẩu, mã PIN hoặc mật mã. Làm cho khó đoán – tội phạm mạng có thể dễ dàng luận ra ngày sinh và khuôn mẫu khóa của bạn. Sử dụng cụm mật mã để bảo mật tối ưu (xem trang 6). Bạn cũng có thể cân nhắc sử dụng tính năng nhận diện khuôn mặt hoặc dấu vân tay để mở khóa thiết bị của mình.
- **Phải chắc chắn** là thiết bị của bạn được cài đặt để tự động khóa sau một thời gian ngắn không hoạt động.
- **Không** sạc thiết bị của bạn tại trạm sạc công cộng và tránh sạc từ bên thứ ba.
- **Coi** điện thoại của bạn như ví bóp của bạn. Giữ nó an toàn và luôn ở với bạn vào mọi lúc.

Bảo mật phần mềm và ứng dụng:

- **Sử dụng** tính năng tự động cập nhật của thiết bị để cài đặt các bản cập nhật của hệ điều hành và ứng dụng mới ngay khi có sẵn.
- **Cài đặt** cho thiết bị tính năng yêu cầu phải có cụm mật mã/mật mã trước khi cài đặt ứng dụng. Tính năng dành cho phụ huynh để kiểm soát cũng có thể được sử dụng cho mục đích này.
- **Kiểm tra** kỹ các quyền riêng tư khi cài đặt ứng dụng mới trên thiết bị của bạn, đặc biệt là đối với các ứng dụng miễn phí. Chỉ cài đặt ứng dụng từ các nhà cung cấp có uy tín.

Bảo mật dữ liệu:

- **Kích hoạt** chức năng khóa và xóa từ xa nếu thiết bị của bạn có chức năng này.
- **Phải chắc** chắn là bạn đã xóa bỏ triệt để dữ liệu cá nhân khỏi thiết bị của bạn trước khi bán hoặc vứt bỏ nó.

Bảo mật khi kết nối:

- **Tắt** Bluetooth và Wi-Fi khi bạn không sử dụng chúng.
- **Phải chắc chắn** là thiết bị của bạn không tự động kết nối với các mạng Wi-Fi mới.

Để có thêm thông tin chi tiết hơn về việc bảo mật điện thoại di động của mình, bạn có thể truy cập trang mạng cyber.gov.au và tìm kiếm sử dụng cụm từ 'Secure your mobile phone'(Bảo mật điện thoại di động của bạn).

Nâng cao sự suy nghĩ của bạn về an ninh mạng

An ninh mạng cá nhân không chỉ là thay đổi cài đặt, mà còn là thay đổi suy nghĩ và hành vi của bạn.

Coi chừng các trò lừa đảo trên mạng

Tội phạm mạng thường hay sử dụng email, tin nhắn, phương tiện truyền thông xã hội hoặc các cuộc gọi điện thoại để thử và lừa đảo người Úc. Họ có thể giả vờ là một cá nhân hoặc tổ chức mà bạn nghĩ rằng bạn biết, hoặc nghĩ rằng bạn có thể tin tưởng.

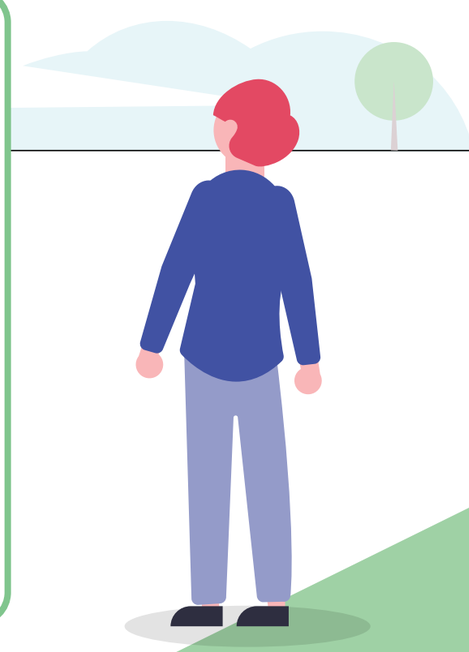
Tin nhắn và cuộc gọi của họ nhằm lừa để bạn thực hiện các hành động cụ thể, chẳng hạn như:

- Tiết lộ chi tiết tài khoản ngân hàng, mật mã và số thẻ tín dụng,
- Cấp quyền truy cập từ xa vào máy vi tính của bạn,
- Mở tập hồ sơ đính kèm có thể chứa phần mềm độc hại,
- Gửi tiền hoặc thẻ quà tặng.

Làm thế nào để tôi nhận ra tin nhắn lừa đảo?

Bạn có thể khó nhận ra các tin nhắn lừa đảo. Tội phạm mạng thường sử dụng một số phương pháp để đánh lừa bạn. Thông điệp của họ có thể bao gồm:

- **Quyền hạn:** có phải tin nhắn đó tự xưng là từ một người nào đó chính thức, chẳng hạn như ngân hàng của bạn không?
- **Khẩn cấp:** có phải bạn được thông báo là có vấn đề gì đó, hoặc bạn chỉ có một thời gian giới hạn để trả lời hoặc thanh toán không?
- **Cảm xúc:** tin nhắn đó có khiến bạn hoang mang, hy vọng hay tò mò không?
- **Sự khan hiếm:** nội dung của thông điệp đó hứa hẹn là sẽ cung cấp thứ gì đó đang khan hiếm, hay hứa hẹn một giao dịch béo bở không?
- **Sự kiện hiện tại:** có phải nội dung của thông điệp đó là về một câu chuyện thời sự hoặc sự kiện lớn không?



Hãy tìm hiểu cách phát hiện tin nhắn lừa đảo hoặc lừa đảo bằng cách truy cập 'Learn the basics' (Tìm hiểu kiến thức cơ bản) trên trang mạng cyber.gov.au

Tôi nên làm gì nếu nhận được tin nhắn lừa đảo?

Nếu bạn nhận được tin nhắn hoặc cuộc gọi lừa đảo, bạn nên bỏ qua, xóa hoặc trình báo với Scamwatch của ACCC tại trang mạng scamwatch.gov.au

Bạn cũng có thể liên lạc với Đường dây nóng về An ninh Mạng của ACSC qua số **1300 CYBER1** (1300 292 371) nếu bạn lo ngại về tình hình an ninh mạng của mình.

Nếu bạn đã vướng vào một vụ lừa đảo và nghĩ rằng tài khoản ngân hàng, thẻ tín dụng hoặc thẻ ghi nợ của bạn có thể gặp rủi ro, hãy liên lạc với tổ chức tài chính của bạn ngay lập tức. Họ có thể đóng tài khoản của bạn hoặc ngăn chặn giao dịch.

Nếu tôi không chắc liệu một tin nhắn nào đó có phải là lừa đảo hay không?

Nếu bạn nghĩ rằng một tin nhắn hoặc cuộc gọi nào đó có thể thực sự đến từ một tổ chức mà bạn tin tưởng (chẳng hạn như ngân hàng của bạn), hãy tìm một phương thức liên lạc khác mà bạn có thể tin tưởng. Tìm kiếm trang mạng chính thức, gọi đến số điện thoại được quảng cáo của họ, hoặc ghé đến một cửa hàng hoặc chi nhánh. Không sử dụng các đường dẫn hoặc các chi tiết liên lạc trong tin nhắn được gởi tới bạn, hoặc được cung cấp qua điện thoại vì chúng có thể là giả mạo.

Mẹo:
Hãy Suy nghĩ Trước khi Bạn Nhấp chuột.

Nếu bạn cho rằng mình là nạn nhân của tội phạm mạng, hãy trình báo điều đó qua ReportCyber của ACSC trên trang cyber.gov.au/report hoặc gọi cho Đường dây nóng về An ninh Mạng của chúng tôi qua số 1300 CYBER1 (1300 292 371).

Bạn cũng có thể được cập nhật về các mối đe dọa mới nhất bằng cách đăng ký dịch vụ cảnh báo miễn phí của ACSC. Tìm kiếm sử dụng cụm từ 'Subscribe to the ACSC alert service'(Đăng ký dịch vụ cảnh báo ACSC) trên trang cyber.gov.au
Chúng tôi sẽ gởi cho bạn cảnh báo khi chúng tôi phát hiện mối đe dọa mạng mới.

An ninh mạng cá nhân: Những bước Đầu tiên

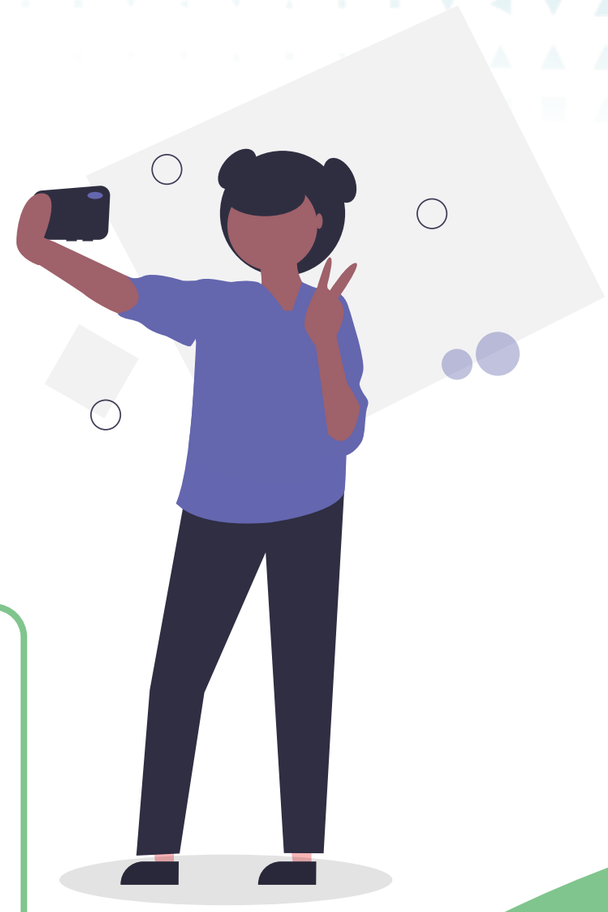
Dừng lại và suy nghĩ trước khi bạn chia sẻ trên phương tiện truyền thông xã hội

Tội phạm mạng có thể sử dụng thông tin mà bạn đã đăng công khai trên các tài khoản truyền thông xã hội của mình để lừa đảo và tấn công mạng.

Hãy nhớ rằng các thông tin đăng trên internet là vĩnh viễn và bạn có thể không bao giờ xóa được hoàn toàn những gì đã được đăng.

Làm thế nào để tôi có thể dừng lại và suy nghĩ trước khi đăng?

- **Hãy suy nghĩ:** Bằng cách nào tội phạm mạng có thể sử dụng thông tin này để nhắm vào tôi hoặc các tài khoản của tôi?
- **Hãy suy nghĩ:** Tôi có cảm thấy thoải mái khi tiết lộ thông tin hoặc hình ảnh này cho một người hoàn toàn xa lạ không?



Tôi nên tránh chia sẻ những thông tin nào?

Tránh chia sẻ thông tin (bao gồm hình ảnh) trực tuyến mà tội phạm mạng có thể sử dụng để nhận dạng bạn, thao túng bạn qua trò lừa đảo, hoặc đoán được các câu hỏi khôi phục tài khoản của bạn. Các thông tin này có thể bao gồm:

- Nơi sinh và ngày sinh.
- Địa chỉ và số điện thoại.
- Nhà tuyển dụng và quá trình làm việc.
- Bạn đã đi học ở đâu.
- Bất kỳ thông tin cá nhân nào khác có thể được sử dụng để gài bẫy bạn.

Danh sách Kiểm tra Tóm tắt

Bạn đã hoàn thành mọi thứ trong tập hướng dẫn này chưa?

Sử dụng danh sách kiểm tra hữu ích này để theo dõi tiến trình của bạn:

- **Tôi đã bật tính năng tự động cập nhật cho tất cả các thiết bị của tôi:**
  - Máy vi tính (máy vi tính để bàn và máy vi tính xách tay).
  - Điện thoại di động.
  - Máy tính bảng.
- **Tôi đã kích hoạt tính năng xác thực đa yếu tố trên các tài khoản quan trọng nhất của tôi:**
  - Tất cả các tài khoản tài chính và ngân hàng trực tuyến của tôi (ví dụ: ngân hàng của bạn, PayPal).
  - Tất cả các tài khoản email của tôi (ví dụ: Gmail, Outlook, Hotmail, Yahoo!).
- **Tôi thường xuyên sao lưu các thiết bị của mình:**
  - Máy vi tính (máy vi tính để bàn và máy vi tính xách tay).
  - Điện thoại di động.
  - Máy tính bảng di động với màn hình cảm ứng.
- **Tôi sử dụng các cụm mật mã mạnh độc đáo trên các tài khoản quan trọng nhất của mình mà không được MFA bảo vệ:**
  - Tài khoản ngân hàng và tài chính trực tuyến.
  - Các tài khoản email.
- **Tôi đã bảo mật các thiết bị di động của mình:**
  - Máy vi tính xách tay.
  - Điện thoại di động.
  - Máy tính bảng di động với màn hình cảm ứng.
- **Tôi luôn suy nghĩ về an ninh mạng mỗi ngày:**
  - Tôi có thể nhận ra các tin nhắn lừa đảo.
  - Tôi biết phải làm gì nếu nhận được tin nhắn lừa đảo.
  - Tôi biết cách kiểm tra xem một tin nhắn nào đó có phải là lừa đảo hay không nếu tôi không chắc chắn.
  - Tôi suy nghĩ trước khi nhấp vào đường dẫn và tập hồ sơ đính kèm.
  - Tôi suy nghĩ trước khi chia sẻ bất cứ điều gì trên mạng xã hội.
- **Tôi biết đến đâu để được giúp đỡ nếu tôi là nạn nhân của tội phạm mạng hoặc lừa đảo.**

Bảng Chú Giải

Khôi phục tài khoản
Là một quy trình trong đó bao gồm một bộ câu hỏi hoặc các phương pháp xác minh khác được sử dụng để khôi phục hoặc lấy lại quyền truy cập vào tài khoản hoặc để thay đổi cụm mật mã/mật mã của tài khoản.

Phần mềm độc hại
Phần mềm độc hại được sử dụng để giành quyền truy cập và kiểm soát máy vi tính của người dùng một cách trái phép, đánh cắp thông tin và làm gián đoạn hoặc vô hiệu hóa mạng lưới.

Ứng dụng
Còn được gọi là ứng dụng di động, ứng dụng là thuật ngữ để chỉ phần mềm thường được sử dụng cho điện thoại thông minh hoặc máy tính bảng di động với màn hình cảm ứng.

Tập hồ sơ đính kèm
Một tập tin được gửi cùng với một thông điệp email.

Hệ điều hành
Phần mềm được cài đặt trên ổ cứng của máy vi tính cho phép phần cứng máy tính giao tiếp và chạy các chương trình máy vi tính. Ví dụ: Microsoft Windows, Apple macOS, iOS, Android.

Mã thông báo vật lý
Một thiết bị vật lý thường có thể vừa với móc khóa(móc đeo chìa khoá nhà/xe), nhằm tạo mã bảo mật được sử dụng để xác nhận danh tính của người dùng máy vi tính sử dụng MFA.

Ứng dụng xác thực
Một ứng dụng được sử dụng để xác nhận danh tính của người dùng máy vi tính nhằm để cho phép truy cập thông qua xác thực đa yếu tố (MFA).

Đám mây
Một mạng lưới các máy chủ từ xa cung cấp nguồn lực mạnh để xử lý và dung lượng lưu trữ lớn.

Truy cập từ xa
Giành quyền truy cập và kiểm soát các thiết bị và mạng từ một vị trí bên ngoài.

Tội phạm mạng
Bất kỳ cá nhân nào truy cập bất hợp pháp vào hệ thống máy vi tính hoặc tài khoản để làm hỏng hoặc lấy cắp thông tin.

Thiết bị
Một máy vi tính hoặc thiết bị truyền thông. Ví dụ: máy vi tính để bàn, máy vi tính xách tay, điện thoại di động hoặc máy tính bảng di động với màn hình cảm ứng.

Phần mềm
Thường được gọi là lập trình, tập hợp các hướng dẫn cho phép người dùng tương tác với máy vi tính, phần cứng của máy vi tính hoặc thực hiện các nhiệm vụ.

Kết thúc hỗ trợ
Kết thúc hỗ trợ để cập đến tình huống khi một công ty ngừng hỗ trợ cho một sản phẩm hoặc dịch vụ. Điều này thường được áp dụng với các sản phẩm phần cứng và phần mềm khi một công ty phát hành phiên bản mới và chấm dứt hỗ trợ cho các phiên bản trước đó.

Bãi miễn trách nhiệm
Tài liệu trong hướng dẫn này có tính chất tổng quát và không nên được coi là lời khuyên pháp lý hoặc được trông cậy vào để làm sự hỗ trợ trong bất kỳ hoàn cảnh cụ thể hoặc tình huống khẩn cấp nào. Trong bất kỳ vấn đề quan trọng nào, bạn nên tìm kiếm lời khuyên chuyên nghiệp, độc lập, liên quan đến hoàn cảnh của riêng bạn.

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

Để biết thêm thông tin, hoặc để trình báo sự việc về an ninh mạng, hãy liên lạc với chúng tôi qua trang:

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

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

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre