



**Hành động ngay.
Giữ an toàn.**

actnowstaysecure.gov.au

Quý vị đang mạo hiểm điều gì trên mạng?

Với công nghệ đang trên đà phát triển nhanh chóng và chúng ta cũng dành nhiều thời gian trên mạng hơn, người dân Úc tiếp tục dễ bị tấn công mạng.

Cuộc vận động Hành động ngay. Giữ an toàn. nhằm giáo dục người dân Úc về các hành động đơn giản trên mạng để giữ an toàn mà ai cũng có thể làm được để tự bảo vệ bản thân trên mạng.

Hành động ngay. Giữ an toàn.

Làm thế nào để giữ an toàn trên mạng

Hãy sử dụng cụm mật khẩu độc đáo duy nhất và mạnh cho mỗi tài khoản

Sử dụng cụm mật khẩu độc đáo duy nhất và mạnh cho mỗi tài khoản trên mạng là một trong những hành động hiệu quả nhất quý vị có thể làm để giữ an toàn trên mạng.

Cụm mật khẩu là một mật khẩu an toàn hơn. Cụm mật khẩu gồm có một dãy các từ ngẫu nhiên. Các từ này làm cho quý vị dễ nhớ hơn nhưng khiến cho tội phạm mạng khó đoán hơn.

Để tạo một cụm mật khẩu mạnh và độc đáo duy nhất, hãy chắc chắn cụm mật khẩu:

- ✓ có từ bốn từ ngẫu nhiên trở lên
- ✓ gồm có 15 ký tự trở lên
- ✓ là khác nhau cho mỗi tài khoản
- ✓ không bao gồm các thông tin nhận dạng như là họ tên, ngày sinh hoặc địa chỉ
- ✓ bao gồm các biểu tượng, chữ hoa, hoặc số, nếu trang mạng hoặc dịch vụ yêu cầu.

Hãy cân nhắc sử dụng trình quản lý mật khẩu để tạo ra và lưu giữ các cụm mật khẩu độc đáo duy nhất của quý vị.

Hãy cài đặt các cập nhật phần mềm để giữ an toàn cho thiết bị của quý vị

Luôn luôn cài đặt cập nhật phần mềm cho tất cả các thiết bị nối mạng internet (như là điện thoại di động, máy tính xách tay hoặc đồng hồ đeo tay thông minh) là việc rất quan trọng để quý vị bảo vệ an toàn bản thân trên mạng.

Cập nhật phần mềm sẽ khắc phục các điểm yếu hoặc lỗ hổng về mặt an ninh trên thiết bị. Thường xuyên cài đặt cập nhật sẽ giữ an toàn cho thiết bị và làm cho tội phạm mạng khó xâm nhập vào thiết bị hơn.

Hãy bật cập nhật tự động và chắc chắn cài đặt cập nhật khi xuất hiện lời nhắc.

Hãy luôn luôn thiết lập xác thực đa nhân tố

Hãy bật xác thực đa nhân tố ở chỗ nào có xác thực này để tăng thêm một lớp bảo vệ an toàn cho tất cả các tài khoản trên mạng của mình.

Xác thực đa nhân tố yêu cầu phải có từ hai phương pháp xác thực trở lên mới đăng nhập được vào tài khoản. Ví dụ như, sau khi nhập mật khẩu hoặc nhập cụm mật khẩu, quý vị sẽ được nhắc phải cung cấp xác thực thứ hai như là nhập mã số gửi vào điện thoại cho quý vị thông qua một ứng dụng, email hoặc tin nhắn dùng để xác thực.

Xác thực đa nhân tố bảo vệ tài khoản của quý vị ngay cả trong trường hợp một trong những cách xác thực khác (như là cụm mật khẩu) bị lộ.



**Hành động ngay.
Giữ an toàn.**

actnowstaysecure.gov.au

Muốn biết thêm những cách khác để giữ an toàn trên mạng?

Quý vị đang tìm thêm cách để giữ an toàn trên mạng? Đây là một số các hành động khác mà quý vị có thể làm để tự bảo vệ bản thân trên mạng.

Hãy thận trọng khi sử dụng Wi-Fi công cộng

Khi sử dụng Wi-Fi công cộng, không nên truy cập bất cứ thông tin nào là nhạy cảm hoặc thông tin cá nhân nào bởi vì kết nối công cộng không được an toàn. Điều này bao gồm truyền thông xã hội, email hoặc ngân hàng trực tuyến. Bất cứ thông tin nào quý vị nhập vào có thể bị tội phạm mạng tiếp cận.

Hãy kiểm tra và cập nhật cài đặt bảo mật riêng tư và định vị của quý vị thường xuyên

Quan trọng là hãy kiểm tra cài đặt bảo mật riêng tư và định vị vị trí thường xuyên để chắc chắn là quý vị không vô tình chia sẻ thông tin cá nhân hoặc thông tin xác định bản thân với công chúng.

Các cài đặt cần kiểm tra bao gồm cài đặt bảo mật riêng tư trên tài khoản truyền thông xã hội và việc theo dõi vị trí địa lý trên các ứng dụng và thiết bị của quý vị.

Hãy nói chuyện với bạn bè và gia đình về cách thức bảo vệ an toàn trên mạng.

Việc giáo dục và nâng cao nhận thức là điều rất quan trọng để giữ an toàn trên mạng cho bản thân, cho gia đình và bạn bè – nhất là nếu quý vị dùng chung thiết bị kết nối mạng. Trao đổi về vấn đề này với mạng lưới của quý vị sẽ đặt vấn đề an toàn mạng lên hàng đầu và chắc chắn họ nhận được thông tin mới nhất về cách tự bảo vệ bản thân trên mạng.

Tìm hiểu cách nhận ra vụ lừa đảo

Kẻ lừa đảo gạt mọi người trả tiền hoặc cung cấp thông tin cá nhân.

Không bao giờ đưa tiền hoặc thông tin cá nhân cho bất cứ ai nếu quý vị không chắc chắn là mình đang giao dịch với ai. Hãy kiểm tra bằng cách liên lạc với cá nhân hoặc tổ chức đó qua chi tiết liên lạc mà quý vị tự tìm thấy từ trang mạng hoặc ứng dụng chính thức của nơi đó.

Hãy trình báo các vụ tấn công mạng hoặc sự cố mạng

Việc trình báo các vụ lừa đảo hoặc sự cố mạng là việc hết sức quan trọng để giúp chính phủ xác định được các xu hướng mới, cảnh báo cho cộng đồng và giúp quý vị hồi phục từ các sự cố mạng.

Hãy tìm hiểu các bước đơn giản để tự bảo vệ mình tại actnowstaysecure.gov.au



**Hành động ngay.
Giữ an toàn.**

actnowstaysecure.gov.au