



Australian Government



Hành động ngay.
Giữ an toàn.

Làm thế nào để quý vị giữ an toàn khi trực tuyến?

Phiên bản đọc dễ hiểu



Cách sử dụng cuốn hướng dẫn này



Chúng tôi là Chính phủ Úc.

Chúng tôi đã biên soạn cuốn hướng dẫn này.



Chúng tôi có viết một số từ bằng **chữ in đậm**.

Chúng tôi sẽ giải thích ý nghĩa của những từ này.

Ở trang 28 cũng có danh sách các từ này.



Quý vị có thể nhờ người mà quý vị tin tưởng hỗ trợ:

- đọc cuốn hướng dẫn này
- tìm thêm thông tin.



Đây là bản tóm tắt Đọc Dễ Hiểu của một cuốn hướng dẫn khác.

Nó chỉ bao gồm những ý tưởng quan trọng nhất.



Quý vị có thể tìm thấy cuốn hướng dẫn khác trên trang mạng của chúng tôi.

www.actnowstaysecure.gov.au

Nội dung cuốn hướng dẫn này có gì?

Giới thiệu về cuốn hướng dẫn này	4
----------------------------------	---

Giữ an toàn cho các tài khoản của quý vị	6
--	---

Kiểm tra phần cài đặt để bảo vệ thông tin cá nhân của quý vị	10
--	----

Bảo vệ các thiết bị của quý vị	16
--------------------------------	----

Các trò lừa đảo	20
-----------------	----

Hãy lên tiếng	25
---------------	----

Danh sách các từ	28
------------------	----

Liên lạc với chúng tôi	30
------------------------	----

Giới thiệu về cuốn hướng dẫn này



Tất cả chúng ta cần suy nghĩ về cách giữ an toàn khi trực tuyến.

Chúng tôi gọi đây là an toàn **mạng (cyber)**.



Mạng có nghĩa là điều gì đó liên quan đến internet.



Cuốn hướng dẫn này giải thích một số điều quý vị có thể làm để bảo vệ bản thân trên mạng.

Ví dụ, đối với **tội phạm mạng (cyber crime)**.



Tội phạm mạng là khi tội phạm sử dụng internet để thực hiện hành vi phạm tội.

Ví dụ, họ có thể sử dụng internet để:

- đánh cắp thông tin cá nhân của quý vị
- chiếm đoạt tài khoản hoặc hồ sơ trực tuyến của quý vị.

Tội phạm mạng có thể xảy ra trên bất kỳ thiết bị nào.



Bao gồm:

- máy tính
- điện thoại thông minh
- đồng hồ thông minh.



Có một số việc quý vị có thể làm để tự bảo vệ mình khỏi tội phạm mạng.



Chúng tôi sẽ giải thích những việc quý vị có thể làm ở các trang tiếp theo.

Giữ an toàn cho các tài khoản của quý vị



Quý vị nên suy nghĩ về cách giữ an toàn cho các tài khoản trực tuyến của mình.

Sử dụng các mật khẩu dạng cụm từ mạnh và khác nhau



Mật khẩu dạng cụm từ (passphrase) là một loại mật khẩu mạnh hơn.

Người khác rất khó đoán được.



Sử dụng các mật khẩu dạng cụm từ mạnh và khác nhau là một trong những cách tốt nhất để bảo vệ các tài khoản của quý vị.



Quý vị nên sử dụng một mật khẩu dạng cụm từ khác nhau cho mỗi tài khoản trực tuyến của mình.



Các mật khẩu dạng cụm từ mạnh bao gồm:

- 4 từ ngẫu nhiên trở lên
- 15 chữ cái và số trở lên.



Quý vị có thể thêm một vài chữ cái viết hoa.



Quý vị cũng có thể sử dụng các ký hiệu như:

- dấu gạch ngang
- dấu đô la
- ký hiệu @ của email.



Quý vị không nên sử dụng bất kỳ thông tin cá nhân nào trong các mật khẩu dạng cụm từ của mình.



Ví dụ:

- sinh nhật của quý vị
- tên các thành viên trong gia đình hoặc thú cưng của quý vị.

Thêm các bước bổ sung để đăng nhập vào tài khoản của quý vị



Quý vị có thể bảo vệ các tài khoản trực tuyến của mình bằng **xác thực đa-yếu tố (MFA)**.

MFA là khi quý vị sử dụng từ 2 phương thức khác nhau trở lên để đăng nhập vào tài khoản của mình mỗi lần.



Ví dụ, quý vị có thể cần nhập mật khẩu dạng cụm từ trước.

Sau đó, quý vị nhập mã mà quý vị nhận được trên điện thoại của mình.

Quý vị có thể chọn cách:



- tải một ứng dụng trên điện thoại để nhận mã



- nhận mã qua email



- nhận mã qua tin nhắn.



Xác thực đa yếu tố (MFA) khiến người khác khó truy cập vào các tài khoản trực tuyến của quý vị hơn.

Ngay cả khi họ tìm ra mật khẩu dạng cụm từ của quý vị.

Kiểm tra phần cài đặt để bảo vệ thông tin cá nhân của quý vị



Quý vị có thể kiểm tra xem phần cài đặt của quý vị có đang bảo vệ thông tin trực tuyến của quý vị hay không.



Điều này bao gồm phần cài đặt trên:

- các tài khoản trực tuyến
- các thiết bị
- các ứng dụng.



Quý vị có thể:

- thay đổi phần cài đặt của quý vị
- chọn ứng dụng nào được phép sử dụng thông tin của quý vị.

Quý vị có thể tìm thấy phần cài đặt trên thiết bị của mình bằng cách:



- tìm biểu tượng bánh răng
- hoặc
- nhập từ khóa 'settings' vào thanh tìm kiếm trên thiết bị của quý vị.

Quý vị có thể tìm thấy phần cài đặt trong một ứng dụng hoặc tài khoản trực tuyến bằng cách mở menu.



Menu thường được trình bày dưới dạng 3 vạch kẻ thẳng.

Một số cài đặt này có thể chia sẻ thông tin về:



- quý vị là ai
- quý vị đang ở đâu
- nơi quý vị sống.



Việc chia sẻ thông tin này trên mạng có thể khiến quý vị gặp rủi ro trở thành nạn nhân của tội phạm mạng.



Tội phạm mạng có thể sử dụng thông tin của quý vị để giả mạo quý vị.

Ví dụ, chúng có thể sử dụng các thông tin như:



- nơi quý vị sống



- tên các thành viên trong gia đình quý vị



- tên các thú cưng của quý vị.



Quý vị có thể thiết lập các tài khoản của mình sao cho chỉ những người quý vị quen biết mới có thể xem được hồ sơ mạng xã hội của quý vị.

Ví dụ, trang cá nhân Facebook của quý vị.



Phần cài đặt này thường được gọi là cài đặt quyền riêng tư.



Quý vị cũng có thể tùy chỉnh **phần cài đặt vị trí** của mình.

Cài đặt vị trí hiển thị vị trí thiết bị của quý vị.



Quý vị có thể bật hoặc tắt cài đặt vị trí.

Quý vị cũng có thể chọn ứng dụng nào được phép sử dụng cài đặt vị trí của mình.



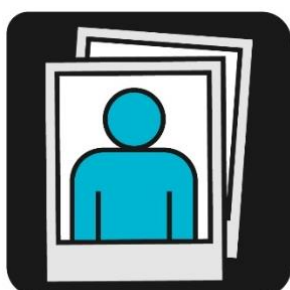
Quý vị có thể làm điều này cho:

- các tài khoản trực tuyến
- các thiết bị
- các ứng dụng.

Một số ứng dụng cũng có thể hỏi quý vị xem chúng có thể:



- sử dụng máy ảnh của quý vị



- xem ảnh của quý vị.



Quý vị chỉ nên cho phép các ứng dụng mà quý vị quen thuộc sử dụng camera và ảnh của mình.

Bảo vệ các thiết bị của quý vị



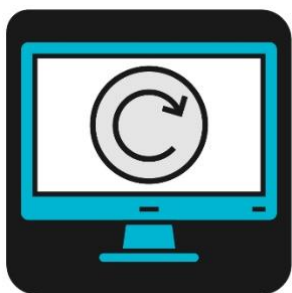
Quý vị nên suy nghĩ về cách bảo vệ các thiết bị của mình để giúp quý vị giữ an toàn khi trực tuyến.

Ví dụ, điện thoại hoặc đồng hồ thông minh của quý vị.



Điều này rất quan trọng đối với các thiết bị kết nối internet.

Cập nhật các thiết bị của quý vị



Quý vị có thể cập nhật các thiết bị của mình để giữ an toàn cho chúng khi trực tuyến.

Ví dụ, điện thoại và máy tính xách tay của quý vị.



Thiết bị của quý vị có thể gọi đây là cập nhật phần mềm.



Các bản cập nhật giúp thiết bị tự bảo vệ mình khỏi tội phạm mạng.



Quý vị có thể thiết lập để thiết bị tự động cập nhật.



Quý vị có thể tìm hiểu thêm về cách cập nhật thiết bị của mình trên trang mạng của chúng tôi.

www.actnowstaysecure.gov.au/cyber-safe-actions

Mạng Wi-Fi công cộng



Quý vị nên cẩn thận khi sử dụng **Wi-Fi công cộng**.



Wi-Fi công cộng là mạng internet không dây miễn phí mà quý vị có thể sử dụng ở những nơi công cộng.



Ví dụ, tại một:

- quán cà phê
- sân bay
- khách sạn.



Quý vị nên cẩn thận với những thông tin mình nhập vào trang mạng khi sử dụng Wi-Fi công cộng.



Ví dụ:

- thông tin ngân hàng
- các tài khoản email
- các mạng xã hội của quý vị



Một số tội phạm mạng có thể sử dụng Wi-Fi công cộng để:

- xem những gì quý vị đang làm trực tuyến
- đánh cắp thông tin của quý vị.

Lý do là vì:



- ai cũng có thể sử dụng nó



- việc bảo vệ các thiết bị của quý vị sẽ khó khăn hơn.



Quý vị có thể tìm hiểu cách giữ an toàn khi sử dụng Wi-Fi công cộng trên trang mạng của chúng tôi.

www.actnowstaysecure.gov.au/cyber-safe-actions

Các trò lừa đảo



Chúng ta gọi đó là **trò lừa đảo (scam)** khi ai đó tìm cách:

- lừa quý vị
- lấy tiền của quý vị.



Kẻ lừa đảo (scammer) là người thực hiện các hành vi lừa đảo.

Những kẻ lừa đảo có thể tìm cách lừa quý vị thông qua:



- một tin nhắn điện thoại hoặc cuộc gọi điện thoại
- một email
- mạng xã hội
- một trang mạng.



Chúng có vẻ thân thiện.

Nhưng chúng có thể lừa quý vị đưa thông tin của quý vị cho chúng

Bạn chúng có thể sử dụng những thông tin này để:



- truy cập vào các tài khoản trực tuyến của quý vị



- giả vờ là quý vị



- ăn cắp tiền của quý vị.

Những kẻ lừa đảo cũng có thể:



- tạo các tài khoản giả để lừa quý vị



- chia sẻ các liên kết và quảng cáo để quý vị nhấp vào.

Cách nhận biết một trò lừa đảo

Đó có thể là một trò lừa đảo nếu nó:



- yêu cầu quý vị làm việc gì đó nhanh chóng



- đề xuất mang lại cho quý vị rất nhiều tiền



- yêu cầu quý vị đưa tiền



- yêu cầu quý vị nhấp vào một liên kết.



Những kẻ lừa đảo cũng có thể giả danh là một tổ chức mà quý vị biết và tin tưởng.

Ví dụ, ngân hàng của quý vị.



Những kẻ lừa đảo làm vậy để quý vị chia sẻ thông tin cá nhân với chúng.



Quý vị nên ngừng nói chuyện với người đó nếu quý vị nghi ngờ họ là kẻ lừa đảo.



Quý vị nên kiểm tra xem người đó có đúng là người mà họ tự xưng hay không.

Quý vị có thể liên lạc với cá nhân hoặc tổ chức đó bằng những thông tin mà quý vị tin tưởng và đã tự tìm được.



Hãy hành động nhanh chóng để bảo vệ bản thân nếu cảm thấy có điều gì đó không ổn.

Trình báo trò lừa đảo



Scamwatch giúp đỡ người dân Úc:

- hiểu rõ các trò lừa đảo
- trình báo các trò lừa đảo.



Scamwatch cũng hỗ trợ người dân Úc đã từng là nạn nhân của các trò lừa đảo.



Quý vị có thể trình báo một trò lừa đảo trên trang mạng của Scamwatch.

www.scamwatch.gov.au/report-a-scam

Hãy lên tiếng



Quý vị nên lên tiếng về cách những người khác có thể tự bảo vệ mình trên mạng.

Việc này bao gồm:



- trình báo tội phạm mạng



- chia sẻ những gì quý vị biết với gia đình và bạn bè.



Chúng tôi sẽ giải thích cách quý vị có thể lên tiếng ở các trang tiếp theo.

Trình báo tội phạm mạng

Việc trình báo tội phạm mạng giúp chính phủ:



- tìm hiểu cách tội phạm mạng tấn công mọi người



- bảo vệ được nhiều người hơn.



Quý vị có thể trình báo tội phạm mạng trên trang mạng ReportCyber.

www.cyber.gov.au/report

Hãy trò chuyện với gia đình và bạn bè về cách giữ an toàn khi trực tuyến



Quý vị nên chia sẻ những lời khuyên về cách giữ an toàn trực tuyến với gia đình và bạn bè.

Quý vị cũng có thể học hỏi từ họ.



Quý vị có thể bảo vệ bản thân và những người xung quanh bằng cách chia sẻ những kiến thức về cách giữ an toàn trên mạng.



Điều này cũng rất quan trọng nếu quý vị dùng chung các thiết bị với người khác.

Danh sách các từ

Danh sách này giải thích ý nghĩa của các từ **in đậm** trong cuốn hướng dẫn này.



Mạng (cyber)

Mạng có nghĩa là điều gì đó liên quan đến internet.



Tội phạm mạng (cyber crime)

Tội phạm mạng là khi tội phạm sử dụng internet để thực hiện hành vi phạm tội.

Ví dụ, chúng có thể sử dụng internet để:

- đánh cắp thông tin cá nhân của quý vị
- chiếm quyền kiểm soát các tài khoản trực tuyến của quý vị.



Cài đặt vị trí

Cài đặt vị trí hiển thị vị trí thiết bị của quý vị.



Xác thực đa-yếu tố (MFA)

MFA là khi quý vị sử dụng từ 2 phương thức khác nhau trở lên để đăng nhập vào tài khoản của mình mỗi lần.



Mật khẩu dạng cụm từ (passphrase)

Mật khẩu dạng cụm từ là một loại mật khẩu mạnh hơn.

Người khác rất khó đoán được.



Wi-Fi công cộng

Wi-Fi công cộng là mạng internet không dây miễn phí mà quý vị có thể sử dụng ở những nơi công cộng.



Trò lừa đảo (scam)

Chúng ta gọi đó là trò lừa đảo khi ai đó tìm cách:

- lừa quý vị
- lấy tiền của quý vị.



Những kẻ lừa đảo (scammers)

Kẻ lừa đảo là người thực hiện các hành vi lừa đảo.

Liên lạc với chúng tôi



Quý vị có thể gọi đến Đường dây nóng An ninh Mạng Úc.

1300 292 371



Quý vị có thể truy cập trang mạng của chúng tôi.

www.actnowstaysecure.gov.au



Quý vị có thể trình báo tội phạm mạng trên trang mạng ReportCyber.

www.cyber.gov.au/report



Information Access Group đã soạn thảo tài liệu Đọc Dễ Hiểu này bằng cách sử dụng ảnh có sẵn và hình ảnh tùy chỉnh. Không được phép sử dụng lại các hình ảnh nếu không có sự cho phép. Mọi thắc mắc về hình ảnh, vui lòng truy cập www.informationaccessgroup.com. Vui lòng ghi rõ mã số công việc 6342.
