

Tóm tắt trình bày trên mạng



Be Connected

Every Australian online.

Bảo vệ thông tin cá nhân của quý vị khi hoạt động trên mạng (Protecting your personal information online)

Hầu như mọi ứng dụng, nền tảng mạng xã hội hoặc trang mạng đều yêu cầu quý vị cung cấp ít nhất một số thông tin cá nhân. Thông tin cá nhân của quý vị bao gồm mọi chi tiết hoặc dữ liệu có thể được sử dụng để xác định danh tính của quý vị, chẳng hạn như thông tin xác định nơi quý vị đang ở hoặc nơi quý vị sống và các chi tiết cụ thể khác. Điều quan trọng là phải luôn suy nghĩ kỹ trước khi chia sẻ thông tin cá nhân.



Bảo vệ thông tin cá nhân của quý vị là điều quan trọng

Việc bảo vệ thông tin cá nhân của quý vị là rất quan trọng vì kẻ lừa đảo và kẻ đánh cắp danh tính có thể sử dụng thông tin này để giả mạo quý vị. Họ có thể tạo tài khoản giả mạo dưới tên quý vị và thực hiện hành vi có thể ảnh hưởng đến quý vị ngay hiện tại hoặc trong tương lai. Điều này có thể bao gồm sự lừa gạt, chẳng hạn như ăn cắp tiền từ tài khoản ngân hàng của quý vị hoặc vay tiền dưới tên quý vị.

Kẻ lừa đảo có thể sử dụng riêng rẽ thông tin của quý vị hoặc kết hợp với thông tin khác. Thông tin có thể bao gồm những thứ hàng ngày cụ thể đối với quý vị, như:

Thông tin cá nhân

- Họ tên đầy đủ
- Địa chỉ nhà
- Số điện thoại
- Ngày sinh
- Số giấy phép lái xe
- Chi tiết tài khoản ngân hàng
- Địa chỉ email
- Tên người dùng và mật khẩu

Giấy tờ tùy thân

- Giấy phép lái xe
- Hộ chiếu
- Giấy khai sinh
- Thẻ Medicare
- Giấy chứng nhận quốc tịch hoặc thị thực Úc
- Thẻ ImmiCard



Hãy ý thức những gì quý vị muốn chia sẻ

Phương tiện truyền thông xã hội

Quý vị nên tránh chia sẻ thông tin cá nhân trên các tài khoản mạng xã hội của mình. Kẻ lừa đảo có thể biết được nhiều điều về quý vị thông qua thông tin quý vị chia sẻ trên mạng. Đôi khi, chúng tạo ra các cuộc thi đố hoặc hỏi các câu hỏi nhằm lừa quý vị chia sẻ thông tin cá nhân. Chúng sử dụng thông tin này để đoán mật khẩu tài khoản của quý vị hoặc nhằm mục tiêu vào quý vị bằng các trò lừa đảo khác.

Hãy nhớ: Chỉ chấp nhận yêu cầu kết bạn từ những người quý vị biết trong cuộc sống thực, đặt tài khoản mạng xã hội ở chế độ riêng tư và xem xét ai có thể xem những gì quý vị chia sẻ.

Sử dụng các ứng dụng

Chỉ tải xuống các ứng dụng từ các cửa hàng ứng dụng chính thức và đọc chính sách bảo mật cũng như đánh giá trước khi tải xuống bất kỳ ứng dụng nào. Quý vị cũng có thể giới hạn thông tin mà ứng dụng có thể truy cập. Một số ứng dụng yêu cầu quyền truy cập không cần thiết vào danh bạ, máy ảnh, bộ nhớ, vị trí và micrô của quý vị. Xem lại và điều chỉnh quyền hạn của ứng dụng trong menu cài đặt trên thiết bị thông minh của quý vị.

Giữ thông tin của quý vị an toàn

Sử dụng bảo mật dành cho thiết bị

Sử dụng phần mềm bảo mật trên máy tính là một trong những cách đơn giản nhất để bảo vệ bản thân và quyền riêng tư của quý vị. Việc bảo mật máy tính tốt là bao gồm cài đặt phần mềm chống gián điệp, chống vi-rút và phần mềm tường lửa có uy tín. Quý vị cũng nên cập nhật các công cụ và ứng dụng bảo mật trực tuyến của mình bằng cách bật tính năng cập nhật tự động. Sử dụng khóa màn hình có hẹn giờ và tự động hoặc trình bảo vệ màn hình được bảo vệ bằng mật khẩu và tự động khóa sau nhiều lần đăng nhập không thành công.

Mẹo: Ứng dụng quản lý mật khẩu cũng có thể giúp quý vị tạo và lưu trữ cụm mật khẩu phức tạp, khó đoán hoặc bẻ khóa. Quý vị có thể tìm thông tin về [trình quản lý mật khẩu](#) và cách thiết lập chúng trên trang mạng Be Connected.

Cụm mật khẩu

Giữ tài khoản của quý vị an toàn bằng cụm mật khẩu mạnh. Cụm mật khẩu là phiên bản mật khẩu có tính an toàn hơn và bao gồm bốn hoặc nhiều từ ngẫu nhiên.

Hãy thử nghĩ ra một cụm mật khẩu khác nhau cho mỗi tài khoản của quý vị và đừng sử dụng lại bất kỳ mật khẩu cũ nào.

Khi quý vị chọn mật khẩu, hãy đặt mật khẩu:

- **Dài** – có ít nhất 14 ký tự
- **Không thể đoán trước** – sử dụng bốn hoặc nhiều từ ngẫu nhiên với số, ký hiệu và chữ hoa và chữ thường
- **Duy nhất** – không sử dụng lại mật khẩu của quý vị

Ví dụ: *Yellow So Hey Plant > Yell*w-SOheyPl@nt!*

Mẹo: Kiểm tra độ mạnh của mật khẩu bằng công cụ kiểm tra độ mạnh mật khẩu của Chính phủ NSW tại nsw.gov.au/id-support-nsw/be-prepared/passwords

Tính xác thực đa yếu tố

Bật xác thực đa yếu tố cho tài khoản của quý vị luôn là một ý tưởng hay. Tính xác thực đa yếu tố (còn gọi là xác thực 2 bước) gia tăng thêm một tầng bảo mật cho tài khoản của quý vị. Điều này có nghĩa là khi quý vị đăng nhập vào tài khoản bằng mật khẩu, quý vị có thể được yêu cầu thực hiện thêm một bước để xác nhận đó là quý vị – như nhập mã số từ tin nhắn văn bản hoặc sử dụng nhận dạng khuôn mặt.

Mua sắm trực tuyến an toàn

Khi mua sắm trực tuyến, hãy đảm bảo quý vị sử dụng người/nơi bán hàng đáng tin cậy và xem các đánh giá của khách hàng. Trước khi nhập thông tin cá nhân, hãy kiểm tra xem trang mạng đó có sử dụng 'https' ở đầu tên miền hay có biểu tượng bảo mật, thường là ổ khóa nhỏ trên trình duyệt để biểu thị rằng đây là trang mạng an toàn hơn không. Khi mua hàng, hãy sử dụng phương thức thanh toán an toàn như PayPal, BPAY hoặc thẻ tín dụng của quý vị.

Sử dụng kết nối an toàn

Khi quý vị cần truy cập vào các tài khoản quan trọng, gửi thông tin nhạy cảm hoặc nhập mật khẩu, hãy kết nối với một kết nối mạng đáng tin cậy, chẳng hạn như ở nhà hoặc tại nơi làm việc, hoặc sử dụng dữ liệu di động của riêng quý vị nếu có. Wi-Fi công cộng không an toàn bằng Wi-Fi tại nhà hoặc nơi làm việc của quý vị.

Các trò lừa đảo và xâm phạm dữ liệu

Bảo vệ bản thân khỏi các trò lừa đảo

Nhận thức được các trò lừa đảo và cách chúng hoạt động là một trong những bước quan trọng để tránh chúng. Những kẻ lừa đảo giả danh là từ một tổ chức hoặc một người mà quý vị biết để lừa quý vị cung cấp thông tin cá nhân. Những hành vi này được gọi là các trò lừa đảo mạo danh.



Hãy nhớ:

Dừng lại – không đưa tiền hoặc thông tin cá nhân cho bất kỳ ai nếu không chắc chắn

Kẻ lừa đảo thường yêu cầu quý vị xác minh danh tính hoặc yêu cầu quý vị trả tiền.

Suy nghĩ – tự hỏi liệu tin nhắn hoặc cuộc gọi đó có phải là giả mạo không?

Hãy cẩn thận với các cuộc gọi, tin nhắn và email bất ngờ. Nếu quý vị không chắc chắn về tin nhắn nào đó, hãy gọi trực tiếp đến tổ chức đó bằng số điện thoại trên trang mạng của họ.

Bảo vệ – hành động nhanh nếu có điều gì đó không ổn

Liên lạc với ngân hàng nếu quý vị nhận thấy bất kỳ hoạt động bất thường nào hoặc nếu kẻ lừa đảo lấy được tiền hoặc thông tin của quý vị.

Mẹo: Truy cập trang mạng Be Connected để xem miễn phí [những hướng dẫn về các trò lừa đảo mạo danh](#) do Scamwatch phát triển.

Xâm phạm dữ liệu

Xâm phạm dữ liệu xảy ra khi thông tin cá nhân do một tổ chức nắm giữ bị truy cập hoặc bị tiết lộ mà không được phép hoặc bị mất. Nhiều tổ chức và cơ quan chính phủ có trách nhiệm pháp lý phải thông báo cho quý vị nếu thông tin cá nhân của quý vị liên quan đến vụ xâm phạm dữ liệu mà có khả năng gây tổn hại nghiêm trọng cho quý vị.

Nếu thông tin của quý vị có liên quan đến một vụ xâm phạm dữ liệu, hãy đảm bảo quý vị hành động nhanh chóng và nhận lời khuyên từ [Văn phòng Ủy viên Thông tin Úc](#). Hành động mà quý vị thực hiện phụ thuộc vào thông tin liên quan. Giữ hồ sơ ghi nhận những gì quý vị làm. Quý vị cũng có thể nhận được hỗ trợ và tư vấn miễn phí từ [IDCARE](#).

Để tìm hiểu xem trang mạng hoặc ứng dụng quý vị sử dụng có bị xâm phạm dữ liệu hay không, quý vị có thể kiểm tra các dịch vụ như [haveibeenpwned.com](#). Nếu điều này xảy ra, hãy thay đổi mật khẩu ngay lập tức.

Lừa gạt về danh tính

Nếu quý vị biết hoặc nghi ngờ danh tính của mình đã bị đánh cắp:

- Gửi báo cáo tới Trung tâm An ninh Mạng Úc thuộc Cục Tín hiệu Úc tại [ReportCyber](#).
- Liên hệ với cảnh sát theo số 131 444. Hỏi xin bản báo cáo của cảnh sát hoặc số tham chiếu làm bằng chứng cho thấy quý vị đã trình báo với cảnh sát.
- Nếu quý vị biết hoặc nghi ngờ loại thông tin cá nhân nào đó đã bị đánh cắp, hãy liên hệ với cơ quan hoặc tổ chức có liên quan để thông báo cho họ biết.
- Hãy thông báo cho tổ chức tài chính của quý vị ngay khi có thể.
- Hãy báo cáo với Trung tâm Chống Lừa đảo Quốc gia ở [Scamwatch](#) nếu đó là một trò lừa đảo.

Hãy dành thời gian để khám phá Be Connected

Be Connected là một trang mạng toàn diện với các nguồn tài liệu miễn phí được thiết kế riêng để hỗ trợ người Úc lớn tuổi kết nối trực tuyến an toàn và điều hướng thế giới kỹ thuật số một cách tự tin. Trang mạng này cũng hữu ích cho các gia đình và tổ chức cộng đồng muốn giúp những thành viên lớn tuổi trong cộng đồng tiếp cận mọi lợi ích của Internet.



Hãy truy cập [beconnected.esafety.gov.au](#)



Chương trình này được eSafety biên soạn như một phần của sáng kiến Be Connected.