Tóm tắt trình bày trực tuyến

Australian Government

Be Connected
Every Australian online.

Quý vị có thể phát hiện ra trò lừa đảo (scam) hay không?

Nhận biết được các trò lừa đảo và cách chúng hoạt động là một trong những bước quan trọng để tránh chúng. Mỗi năm người Úc lớn tuổi mất hàng triệu đô la do lừa đảo. Mặc dù internet là một nơi tuyệt vời để khám phá và kết nối với người khác, nhưng không phải lúc nào chúng ta cũng có thể chắc chắn rằng mọi người đúng như những gì họ nói. Khi biết thủ đoạn của kẻ lừa đảo, quý vị sẽ có nhiều khả năng phát hiện ra trò lừa đảo hơn.

Lừa đảo

Lừa đảo là nỗ lực của những kẻ lừa đảo nhằm lừa quý vị tin rằng họ đến từ một tổ chức đáng tin cậy hoặc một người mà quý vị biết để yêu cầu quý vị cung cấp thông tin cá nhân như số tài khoản ngân hàng, mật khẩu và số thẻ tín dụng của quý vị.

Tin nhắn lừa đảo được thiết kế trông như thật và thường sao chép định dạng được sử dụng bởi tổ chức mà kẻ lừa đảo đang giả vờ đại diện, bao gồm cả thương hiệu và logo của họ. Những trò lừa đảo này có thể xuất hiện dưới nhiều hình thức bao gồm email, tin nhắn văn bản hoặc cuộc gọi điện thoại. Ví dụ: quý vị có thể nhận được:

- một tin nhắn văn bản từ ngân hàng của quý vị, yêu cầu quý vị xác nhận mật khẩu của mình
- một email từ nhà cung cấp internet của quý vị yêu cầu quý vị cập nhật thông tin chi tiết của mình
- tin nhắn từ một thành viên trong gia đình sử dụng số điện thoại mới cho quý vị biết họ bị mất điện thoại và cần quý vị gửi tiền gấp
- một cuộc điện thoại từ tổ chức tài chính của quý vị thông báo cho quý vị về 'hoạt động trái phép hoặc đáng ngờ trên tài khoản của quý vị' hoặc tài khoản của quý vị sẽ bị khóa nếu quý vị không cập nhật thông tin chi tiết của mình
- một thông báo trên Facebook từ một người mà quý vị biết giới thiệu một trang mạng.

Lừa đảo về Thuế và Medicare

Những kẻ lừa đảo mạo danh Văn phòng Thuế vụ Úc (ATO), Medicare và các tổ chức chính phủ khác để cố lừa quý vị trả tiền và chia sẻ thông tin cá nhân. Những kẻ lừa đảo này tạo các trang mạng giả mạo và sẽ gửi cho quý vị email, tin nhắn văn bản và gọi điện cho quý vị giả vờ là người của một tổ chức chính phủ.

ATO sẽ không bao giờ gửi email, nhắn tin hoặc gọi điện yêu cầu quý vị để:

- cung cấp thông tin cá nhân như số hồ sơ thuế, thẻ tín dụng hoặc chi tiết ngân hàng của quý vị
- trả một khoản phí để được hoàn thuế, hoặc để thoát khỏi việc bị bắt vì trốn thuế
- nhấp vào liên kết để nhập thông tin cá nhân của quý vị
- tải các tập tin xuống hoặc cài đặt phần mềm.

Nếu quý vị không chắc liệu thông tin liên lạc có phải từ ATO hay không, hãy gọi cho đường dây nóng về Lừa đảo của ATO (ATO Scams hotline) theo số 1800 008 540 hoặc truy cập ato.gov.au/scams.

Tự bảo vệ ra sao

- Hãy từ từ. Đọc lại tin nhắn. Hãy tự hỏi bản thân tin nhắn hoặc cuộc gọi đó có thể là giả mạo không?
- Đây có phải là một địa chỉ email chính thức hay nó hoàn toàn không đúng?
- Nó gửi đến cho ai? Hãy cảnh giác nếu nó ghi là "Kính gửi khách hàng" thay vì tên của quý vị.
- Nó có chứa lỗi đánh máy hoặc lỗi ngữ pháp không? Đây có thể là dấu hiệu cho thấy nó đến từ một kẻ lừa đảo.
- Không sử dụng các chi tiết liên lạc được cung cấp trong tin nhắn, chúng có thể là giả mạo. Thực hiện tìm kiếm trên internet cho số điện thoại và trang mạng chính thức của tổ chức.
- Không nhấp vào bất kỳ liên kết nào hoặc mở bất kỳ tập tin đính kèm nào vì chúng có thể tải vi-rút xuống thiết bị của quý vị – chỉ cần nhấn xóa.
- Đừng tiết lộ các chi tiết cá nhân của quý vị như số hồ sơ thuế (TFN), ngày sinh, tài khoản ngân hàng hoặc thẻ tín dụng.

Hãy nhớ rằng: Những kẻ lừa đảo có thể cố gắng nói theo cảm xúc của quý vị để khiến quý vị phản ứng và không dành thời gian suy nghĩ kỹ về tình huống. Chiến thuật của họ có thể bao gồm đe dọa hoặc phạt tiền, cho quý vị biết rằng đã có khoản chi tiêu trái phép từ tài khoản của quý vị hoặc giả vờ là một thành viên gia đình cần giúp đỡ.

Lừa đảo tình bạn và tình cảm

Những kẻ lừa đảo lợi dụng những người đang tìm kiếm bạn bè hoặc đối tác tình cảm, thường thông qua các trang mạng hẹn hò, ứng dụng, mạng xã hội hoặc thậm chí là trò chơi trực tuyến bằng cách giả vờ là bạn đồng hành tiềm năng. Mục đích của họ là lấy lòng tin của quý vị để khiến quý vị cung cấp tiền, quà, hình ảnh thân mật hoặc thông tin cá nhân.

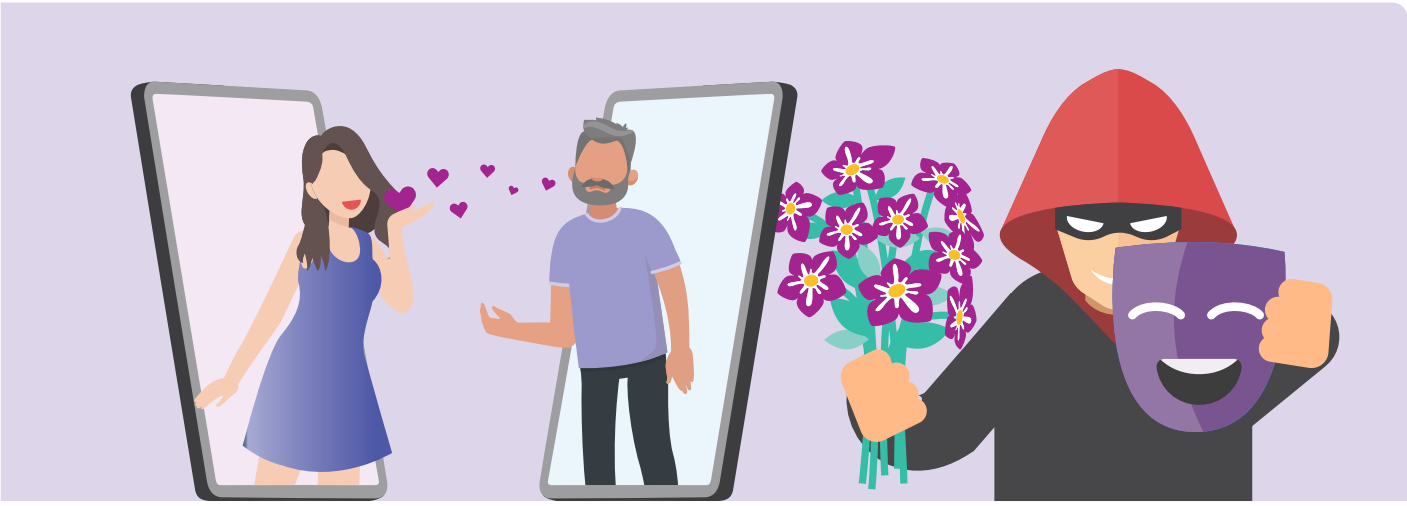
Quý vị có thể làm gì để hiểu biết và an toàn?

Coi chừng những người:

- thể hiện tình cảm sâu sắc đối với quý vị rất nhanh chóng
- sau khi có được lòng tin của quý vị – thường là chờ đợi hàng tuần, hàng tháng hoặc thậm chí hàng năm – kể cho quý vị một câu chuyện phức tạp và yêu cầu tiền hoặc khoản vay, quà tặng hoặc thông tin chi tiết về tài khoản ngân hàng/thẻ tín dụng của quý vị
- tránh gặp mặt trực tiếp với quý vị và viện lý do tại sao họ không thể đến gặp quý vị
- có một hồ sơ trực tuyến với chi tiết không phù hợp với những gì họ nói với quý vị về bản thân họ.

Tự bảo vệ ra sao

- Không bao giờ gửi tiền hoặc cung cấp chi tiết thẻ tín dụng, chi tiết tài khoản trực tuyến hoặc bản sao tài liệu cá nhân quan trọng cho người mà quý vị chưa gặp trực tiếp.
- Thực hiện tìm kiếm hình ảnh trên Google đối với ảnh của người đó để giúp xác định xem họ có thực sự là người mà họ nói hay không hoặc ảnh được lấy từ một nơi nào khác trên internet. Truy cập vào images.google.com và nhấp vào biểu tượng máy ảnh.
- Hãy nghi ngờ khi họ bắt đầu đề cập đến vấn đề tiền bạc hoặc cần tiền cho trường hợp khẩn cấp.
- Hãy cảnh giác với những thứ như lỗi chính tả và ngữ pháp và sự không nhất quán trong câu chuyện của họ.
- Không chia sẻ hình ảnh hoặc video thân mật. Những kẻ lừa đảo được biết là tống tiền các mục tiêu của chúng bằng cách sử dụng vật liệu hay tài liệu gây tổn hại nếu tiết lộ.



Lừa đảo hỗ trợ kỹ thuật

Những trò lừa đảo này thường bắt đầu bằng một cuộc gọi hoặc email có vẻ là từ một công ty máy tính hoặc viễn thông lớn, chẳng hạn như Telstra, NBN hoặc Microsoft để cho quý vị biết rằng quý vị gặp sự cố về máy tính hoặc internet và họ có thể khắc phục sự cố đó. Sau đó, họ sẽ yêu cầu quyền truy cập từ xa vào máy tính của quý vị để 'tìm hiểu vấn đề là gì' hoặc cố thuyết phục quý vị mua phần mềm hoặc dịch vụ không cần thiết để 'sửa chữa' máy tính.

Cách tự bảo vệ quý vị

- Nếu quý vị nhận được một cuộc gọi điện thoại bất ngờ về máy tính của mình và yêu cầu truy cập từ xa – hãy gác máy.
- Không cung cấp cho người gọi không mong muốn quyền truy cập từ xa vào máy tính của quý vị.
- Không chia sẻ thông tin cá nhân của quý vị như tài khoản ngân hàng hoặc chi tiết thẻ tín dụng.
- Không mua phần mềm từ các cuộc gọi hoặc email lạ.
- Lờ đi các tin nhắn bật lên yêu cầu quý vị gọi hỗ trợ kỹ thuật.

Mẹo hàng đầu để tránh lừa đảo

Dừng lại

- Hãy dành thời gian để xem xét trước khi đưa tiền hoặc thông tin cá nhân cho bất kỳ ai.
- Những kẻ lừa đảo sẽ đề nghị giúp đỡ quý vị hoặc yêu cầu xác minh quý vị là ai. Họ sẽ giả vờ là từ các tổ chức mà quý vị biết và tin tưởng như doanh nghiệp mà quý vị giao dịch, hoặc cảnh sát, chính phủ hoặc dịch vụ chống lừa đảo.

Suy nghĩ

- Hãy tự hỏi bản thân tin nhắn hoặc cuộc gọi đó có thể là giả mạo không?
- Không bao giờ nhấp vào một liên kết trong tin nhắn và hãy hỏi một người bạn đáng tin cậy hoặc thành viên gia đình là họ sẽ làm gì. Chỉ liên hệ với các doanh nghiệp hoặc chính phủ bằng cách sử dụng thông tin liên hệ từ trang mạng chính thức của họ hoặc thông qua các ứng dụng bảo mật của họ. Nếu quý vị không chắc chắn, hãy nói không, gác máy hoặc xóa tin nhắn.

Bảo vệ

- Hành động nhanh chóng nếu cảm thấy có gì đó không ổn.
- Liên hệ với ngân hàng của quý vị ngay lập tức nếu quý vị bị mất tiền hoặc thông tin cá nhân hoặc nếu quý vị nhận thấy một số hoạt động bất thường trên thẻ hoặc tài khoản của mình. Tìm kiếm sự giúp đỡ từ các tổ chức như IDCARE và báo cáo tội phạm trực tuyến cho ReportCyber. Giúp đỡ người khác bằng cách báo cáo các trò lừa đảo tới Scamwatch.

Hãy giúp tôi với, tôi nghi ngờ mình đang bị lừa đảo

Nếu quý vị nghĩ rằng quý vị là nạn nhân một vụ lừa đảo, đừng xấu hổ và đừng giữ nó cho riêng mình. Có các bước quý vị có thể thực hiện để khắc phục sự cố:

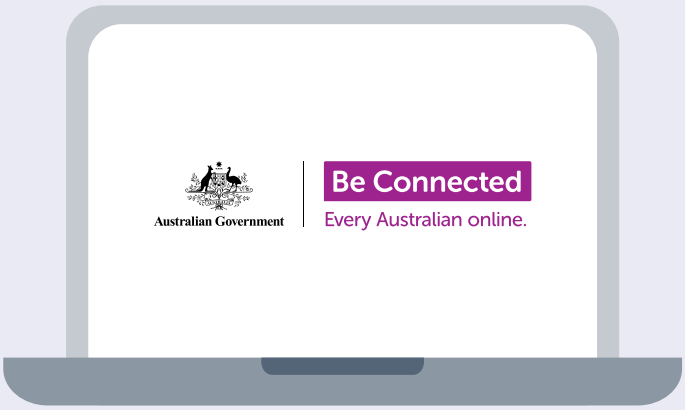
- Liên lạc với tổ chức tài chính của quý vị để dừng mọi khoản thanh toán tiếp theo cho kẻ lừa đảo.
- Nếu quý vị gặp phải tội phạm trên mạng và bị mất tiền trực tuyến, quý vị có thể báo cảnh sát qua ReportCyber hoặc truy cập: cyber.gov.au
- Nếu lo lắng rằng thông tin cá nhân của quý vị đã bị tiết lộ và sử dụng sai, hãy liên lạc với Dịch vụ Hỗ trợ Danh tính và Cyber Toàn quốc Úc IDCARE số 1300 432 273 hoặc idcare.org
- Báo cáo vụ lừa đảo cho ACCC qua trang scamwatch.gov.au/report-a-scam. Điều này giúp cảnh báo mọi người về các trò gian lận hiện tại, theo dõi các xu hướng và phá vỡ các trò lừa đảo nếu có thể.
- Truyền bá thông tin này cho bạn bè và gia đình của quý vị để bảo vệ họ.

Hãy nhớ rằng: Luôn có người có thể giúp đỡ – cho dù đó là những người ở cyber.gov.au hay scamwatch.gov.au, một người bạn hoặc thành viên gia đình có đầu óc kỹ thuật hay thậm chí là một câu lạc bộ máy tính địa phương

Để cập nhật những trò lừa đảo mới nhất cần tránh, hãy đăng ký nhận thông tin cảnh báo qua email của Scamwatch.

Dành thời gian để khám phá Be Connected

Be Connected là một trang mạng toàn diện với các tài liệu miễn phí được thiết kế đặc biệt để hỗ trợ người Úc lớn tuổi kết nối trực tuyến an toàn và tự tin khám phá thế giới kỹ thuật số. Trang mạng này cũng hữu ích cho các gia đình và tổ chức cộng đồng, những người muốn giúp các thành viên cộng đồng cao niên hưởng mọi lợi ích của internet.



hãy truy cập beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Chương trình này được xây dựng bởi eSafety nằm trong sáng kiến Be Connected.