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

Trên internet, chúng ta không thể luôn chắc chắn rằng người đang nói chính là họ. Nhận biết về những kẻ lừa đảo trên internet là một trong những điều quan trọng nhất để tránh họ. Một khi biết các thủ đoạn của họ, quý vị sẽ thấy dễ dàng hơn để phát hiện ra lừa đảo khi gặp phải.

Lừa đảo tấn công giả mạo (phishing)

Lừa đảo 'phishing' là hình thức lừa đảo phổ biến nhất trên mạng. Chúng có thể mạo danh là đến từ một tổ chức tin cậy và nhằm để lừa quý vị cung cấp các chi tiết cá nhân như tài khoản ngân hàng, số thẻ tín dụng, tên người dùng và mật khẩu.

Chúng có thể xuất hiện dưới nhiều hình thức:

- email, tin nhắn hoặc cuộc gọi bất ngờ yêu cầu quý vị xác nhận, cập nhật hoặc nhập lại thông tin cá nhân của quý vị
- tin nhắn khẩn cấp hoặc đe dọa thông báo có điều bất thường xảy ra với tài khoản của quý vị, hoặc nó sẽ bị đóng và quý vị cần phải nhấp chuột vào một đường liên kết để khắc phục việc này
- các email bất ngờ yêu cầu quý vị mở hoặc tải xuống một tệp '.exe' hoặc '.zip'.

Mẹo: Nếu không chắc chắn về tin nhắn nhận được, quý vị hãy tìm trên internet công ty gửi nó đến và liên lạc trực tiếp với họ.

Hãy từ từ. Đọc lại tin nhắn.

- Ai là người gửi? Đó có phải là một địa chỉ email chính thức không hay trông nó lạ hoắc?
- 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 ngữ pháp hoặc chính tả kém không? Đây có thể là dấu hiệu cho thấy nó đến từ một kẻ lừa đảo.

Đừng:

- nhấp vào bất cứ đường liên kết nào
- mở bất cứ tệp đính kèm nào, vì chúng có thể tải xuống một con vi-rút máy tính
- sử dụng các chi tiết liên lạc được cung cấp, chúng có thể là giả.

Lừa đảo về Thuế & Medicare

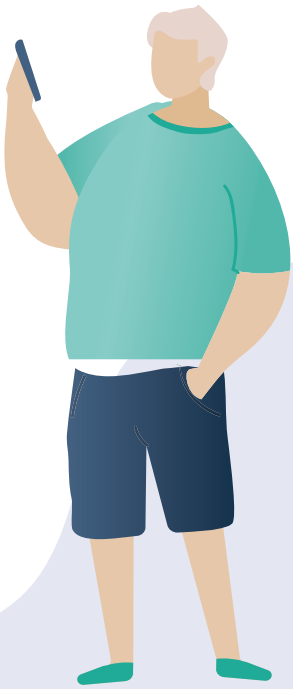
Những kẻ lừa đảo mạo danh Văn phòng Thuế vụ Úc, Medicare và các tổ chức chính phủ khác để moi tiền và thông tin cá nhân của các nạn nhân thông qua các trang mạng, email, tin nhắn và cuộc gọi giả mạo.

Điều quan trọng cần nhớ, Cơ quan Thuế vụ Úc (ATO) sẽ không bao giờ:

- gửi cho quý vị email hoặc tin nhắn yêu cầu thông tin cá nhân của quý vị bao gồm TFN, chi tiết thẻ tín dụng hoặc ngân hàng của quý vị
- yêu cầu quý vị trả một khoản phí để nhận tiền hoàn thuế, hoặc để không bị bắt về tội trốn thuế
- gửi cho quý vị email có đường dẫn đến một dịch vụ trực tuyến hỏi về các chi tiết cá nhân của quý vị
- gửi cho quý vị các tệp để tải xuống hoặc yêu cầu quý vị cài đặt phần mềm.

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

- Đừng nhấp vào bất cứ đường dẫn nào hoặc tải xuống bất cứ tệp đính kèm nào.
- 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.
- Nếu không chắc tin nhắn đó có thật hay không, quý vị đừng sử dụng các chi tiết liên lạc nó cung cấp, mà hãy tìm trên internet số liên lạc của tổ chức đó.
- Biết vấn đề thuế của quý vị – quý vị có khả năng được hoàn thuế hay nợ thuế?
- Đăng nhập vào tài khoản myGov chính thức của quý vị bằng cách tự tay gõ địa chỉ chứ không nhấp vào một đường dẫn.
- Kiểm tra xem email quý vị nhận được có phải đến từ địa chỉ thật của ATO kết thúc bằng @ato.gov.au hay không
- Ngay cả khi có vẻ như quý vị đang ở trên trang mạng ATO hoặc myGov, hãy kiểm tra xem địa chỉ đó có kết thúc bằng .gov.au hay không (chứ không phải .com.au, .org.au hay .net.au).
- Lưu ý đến ngữ pháp và chính tả kém.
- Cảnh giác với những thứ không đề tên quý vị là người nhận.



Lừa đảo về lãng mạn và hẹn hò

Kẻ lừa đảo tạo những hồ sơ trực tuyến giả trên các trang truyền thông xã hội hoặc hẹn hò để liên lạc với nạn nhân. Mục đích là để chiếm được lòng tin của quý vị trước khi hỏi về tiền.

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

Hãy coi chừng:

- những người nhanh chóng thể hiện tình cảm sâu sắc với quý vị trước khi hỏi xin hoặc 'vay' tiền
- những người tránh gặp mặt trực tiếp và lấy cớ không thể đến gặp quý vị
- những người có hồ sơ trực tuyến không khớp với những gì họ nói với quý vị về họ.

Hãy làm:

- kiểm tra xem hình có đúng là của họ không hay được lấy từ nơi khác bằng thao tác tìm kiếm hình ảnh Google. Truy cập images.google.com và nhấp vào biểu tượng camera
- cảnh giác khi họ bắt đầu đề cập đến chuyện tiền bạc hoặc cần tiền vì có việc 'khẩn cấp'.

Không làm:

- chuyển tiền cho người quý vị chỉ mới nói chuyện qua điện thoại hoặc email
- gửi thông tin cá nhân của quý vị như ngày sinh, chi tiết ngân hàng hoặc thẻ tín dụng.

Lừa đảo hỗ trợ kỹ thuật

Những trò lừa đảo này thường bắt đầu bằng một cuộc gọi hoặc email mạo danh là của một tổ chức lớn, nổi tiếng thông báo rằng quý vị có vấn đề về máy tính hoặc internet và họ có thể khắc phục nó.

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

- Không cho phép truy cập từ xa vào máy tính của quý vị.
- Không gửi cho họ thông tin cá nhân của quý vị như chi tiết tài khoản ngân hàng hoặc 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.

Các tổ chức lớn kỳ vọng quý vị gọi cho họ khi có vấn đề về internet hoặc máy tính của quý vị. Họ sẽ không gọi cho quý vị.

Giúp với, tôi nghi ngờ tôi bị lừa đảo

Nếu cho rằng quý vị là nạn nhân của một vụ lừa đảo, quý vị đừng xấu hổ và đừng giữ nó cho bản thân quý vị. Quý vị có thể thực hiện một số bước để khắc phục vấn đề:

- liên lạc với ngân hàng của quý vị và dừng mọi khoản thanh toán tiếp theo cho kẻ lừa đảo
- trình báo cáo lừa đảo lên Ủy ban Cạnh tranh và Người tiêu dùng Úc tại scamwatch.gov.au - họ có thể tư vấn thêm giúp quý vị
- nâng cao hiểu biết. Nếu biết ai đó là nạn nhân, quý vị hãy nói cho họ biết.

Nếu không chắc chắn tin nhắn quý vị nhận được có thực sự đến từ ATO, hay quý vị có phải là nạn nhân một vụ lừa đảo về thuế, hãy gọi cho **ATO Scam Hotline (Đường dây nóng Lừa đảo ATO)** số **1800 008 540**.

Luôn cập nhật về những gian lận ATO bằng cách truy cập ato.gov.au/scams

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 Quốc gia Úc **IDCARE** số **1300 432 273** hoặc idcare.org

Ghi nhớ:

Luôn có người có thể giúp - dù đó là những người ở scamwatch.gov.au, một người bạn hay thành viên gia đình hiểu kỹ thuật, hoặc thậm chí là một câu lạc bộ máy tính địa phương.

Những vụ lừa đảo nhằm mục đích lợi dụng sự tốt bụng của quý vị, nhưng internet có thể là nơi an toàn để khám phá nếu quý vị cẩn thận khi chia sẻ thông tin cá nhân trên trực tuyến, nghe theo trực giác khi gửi tiền cho người khác và đề cao cảnh giác.

Dành thời gian tìm hiểu về Be Connected

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

beconnected.esafety.gov.au