10 mẹo hàng đầu để bảo vệ bản thân khỏi

Lừa đảo mạo danh

Vietnamese | Tiếng Việt

Australian Government | Be Connected
Every Australian online.

Australian Government | National Anti-Scam Centre

SCAMWATCH

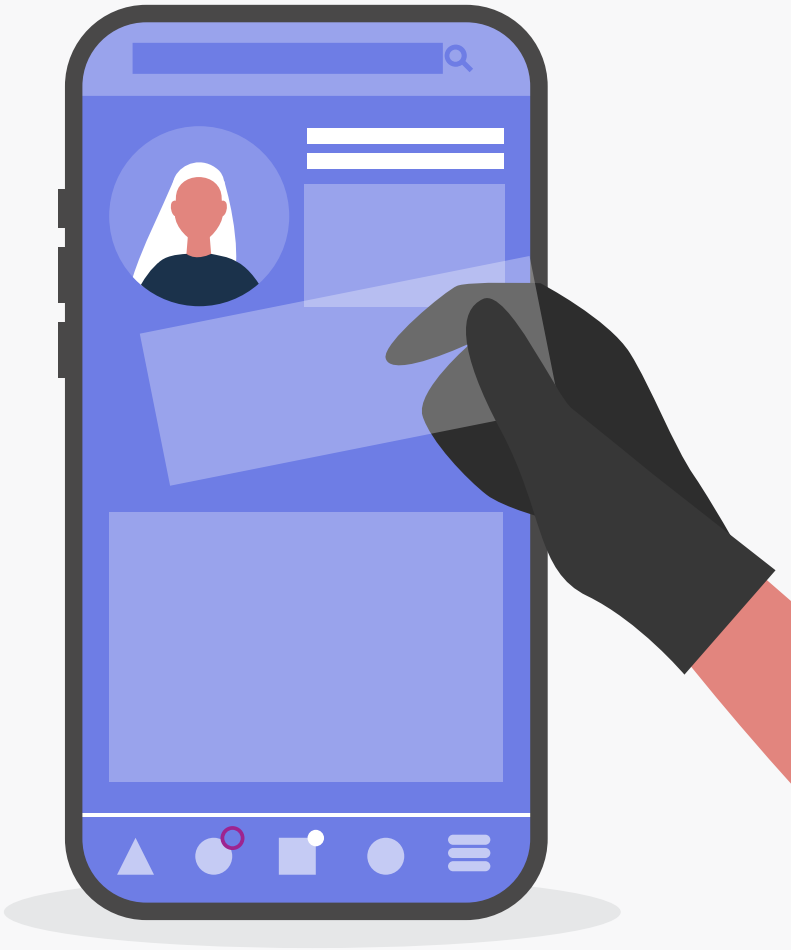
Các trò lừa đảo ngày nay ngày càng tinh vi. Trước đây, lỗi chính tả và ngữ pháp kém khiến các vụ lừa đảo dễ bị phát hiện, nhưng công nghệ mới khiến các chiêu trò lừa đảo ngày càng khó nhận biết hơn.

Trung tâm Chống Lừa đảo Quốc gia đã phối hợp với chính phủ, các chuyên gia ngành, các cơ quan thực thi pháp luật và các tổ chức cộng đồng để chống lại các trò lừa đảo. Nhưng cũng có các bước để quý vị có thể thực hiện để bảo vệ bản thân khỏi bị lừa đảo. Một trong những biện pháp bảo vệ tốt nhất là cập nhật thường xuyên về các chiêu trò lừa đảo mới và đang nổi lên, để quý vị có thể nhận biết các dấu hiệu lừa đảo.

Be Connected đã hợp tác với Scamwatch của Trung Tâm Chống Lừa Đảo Quốc Gia để cung cấp hướng dẫn này giúp quý vị nhận biết các trò lừa đảo mạo danh, bảo vệ bản thân và biết nơi để tìm sự trợ giúp nếu quý vị trở thành nạn nhân của lừa đảo.

Tất cả các ví dụ cung cấp trong hướng dẫn này đều là các vụ lừa đảo có thật.

Nội dung hướng dẫn này bao gồm



Lừa đảo mạo danh là gì?

Các lừa đảo mạo danh được thiết kế để trông giống như chúng đến từ các tổ chức hợp pháp mà quý vị biết. Chúng có thể xuất hiện như là của ngân hàng, nhà cung cấp dịch vụ internet, cơ quan chính phủ, nhà bán lẻ, hoặc thậm chí là kẻ lừa đảo giả dạng thành bạn bè hoặc người thân trong gia đình.

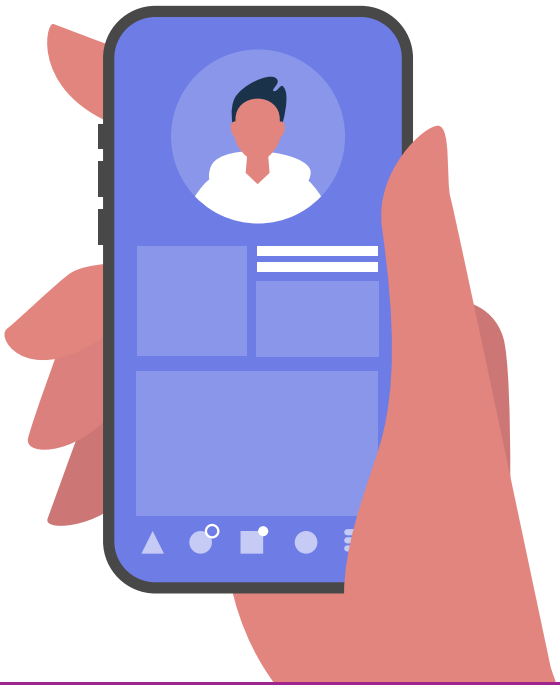
Bằng cách giả dạng người quý vị tin tưởng, kẻ lừa đảo thường tạo cảm giác khẩn cấp để đánh lừa quý vị chuyển tiền hoặc cung cấp thông tin cá nhân, như mật khẩu quan trọng, chi tiết thẻ tín dụng hoặc thông tin ngân hàng.

Những kẻ lừa đảo sử dụng nhiều phương thức để tiếp cận quý vị, bao gồm tin nhắn văn bản, cuộc gọi điện thoại, email, bài đăng trên mạng xã hội và các trang mạng giả mạo trông giống hệt như các trang mạng chính thức.

Giả mạo (Spoofing) là gì?

Kẻ lừa đảo có thể giả mạo các tổ chức mà quý vị biết bằng cách sử dụng công nghệ để làm cho cuộc gọi hoặc tin nhắn của họ có vẻ đến từ một nguồn đáng tin cậy. Điều này được gọi là giả mạo (spoofing).

Hãy cảnh giác với lừa đảo và nghi ngờ mọi liên lạc lạ khi các liên lạc này yêu cầu thông tin cá nhân, như mật khẩu hoặc yêu cầu thanh toán dưới bất kỳ hình thức nào. Hãy liên hệ trực tiếp với tổ chức mà họ giả danh để xác nhận.



Có nhiều loại kỹ thuật giả mạo khác nhau, bao gồm:

01. **Giả mạo số điện thoại (Caller ID spoofing):** Kẻ lừa đảo thay đổi ID người gọi để hiển thị một số điện thoại khác với số thực tế đang dùng, khiến cuộc gọi có vẻ như đến từ một số hợp pháp.

02. **Giả mạo tin nhắn SMS (SMS spoofing hoặc alpha tags):** Kẻ lừa đảo thay đổi số điện thoại của chúng để xuất hiện dưới một tên doanh nghiệp (ví dụ: AusPost). Điều này có thể khiến tin nhắn giả mạo xuất hiện trong cùng một cuộc trò chuyện hoặc chuỗi các tin nhắn thật của tổ chức đó.

03. **Giả mạo email (Email spoofing):** Kẻ lừa đảo thay đổi địa chỉ email hoặc tên người gửi để làm ra một email giống như đến từ một nguồn đáng tin cậy. Chúng có thể giả mạo tên hiển thị trong 'From' (‘ Người gửi’) hoặc địa chỉ email, thường bằng cách thay đổi hoặc thêm vào một chữ cái hoặc con số vào tên miền hợp pháp (ví dụ: @amaz0n.com thay vì @amazon.com).

Các trò lừa đảo mạo danh phổ biến

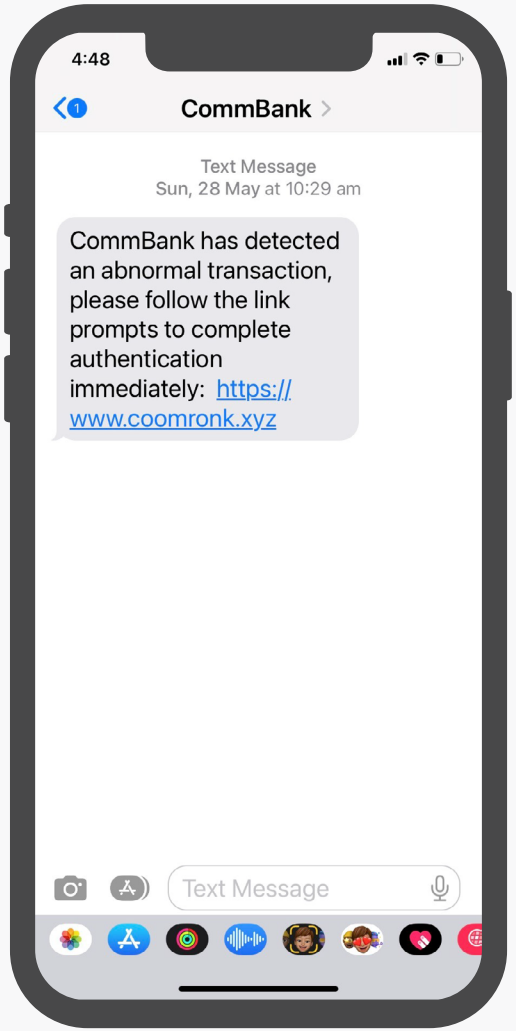
Các trò lừa đảo mạo danh ngân hàng

- Quý vị nhận được cuộc gọi hoặc tin nhắn văn bản từ một người tự xưng là từ bộ phận an ninh của ngân hàng. Họ thông báo cho quý vị về một giao dịch đáng ngờ, tuyên bố rằng tài khoản của quý vị đã bị xâm phạm. Họ thúc giục quý vị chuyển tiền sang một tài khoản khác để 'giữ an toàn' hoặc để 'điều tra thêm'.
- Quý vị nhận được tin nhắn văn bản hoặc email yêu cầu quý vị nhấp vào một liên kết để xác minh thông tin chi tiết về tài khoản của mình. Liên kết sẽ đưa quý vị đến một trang mạng giả mạo được thiết kế để đánh cắp tên người dùng, mật khẩu và thông tin cá nhân khác của quý vị.

Làm sao quý vị biết đó là lừa đảo?

Mặc dù ngân hàng của quý vị có thể liên hệ với quý vị nếu có hoạt động đáng ngờ trên tài khoản của quý vị, nhưng họ sẽ không bao giờ yêu cầu quý vị chuyển tiền sang một tài khoản khác. Họ cũng không hỏi bất kỳ thông tin tài khoản hoặc thông tin cá nhân nào, bao gồm mật khẩu, số PIN hoặc mã xác thực một lần qua tin nhắn văn bản, email hoặc một cuộc gọi điện thoại lạ.

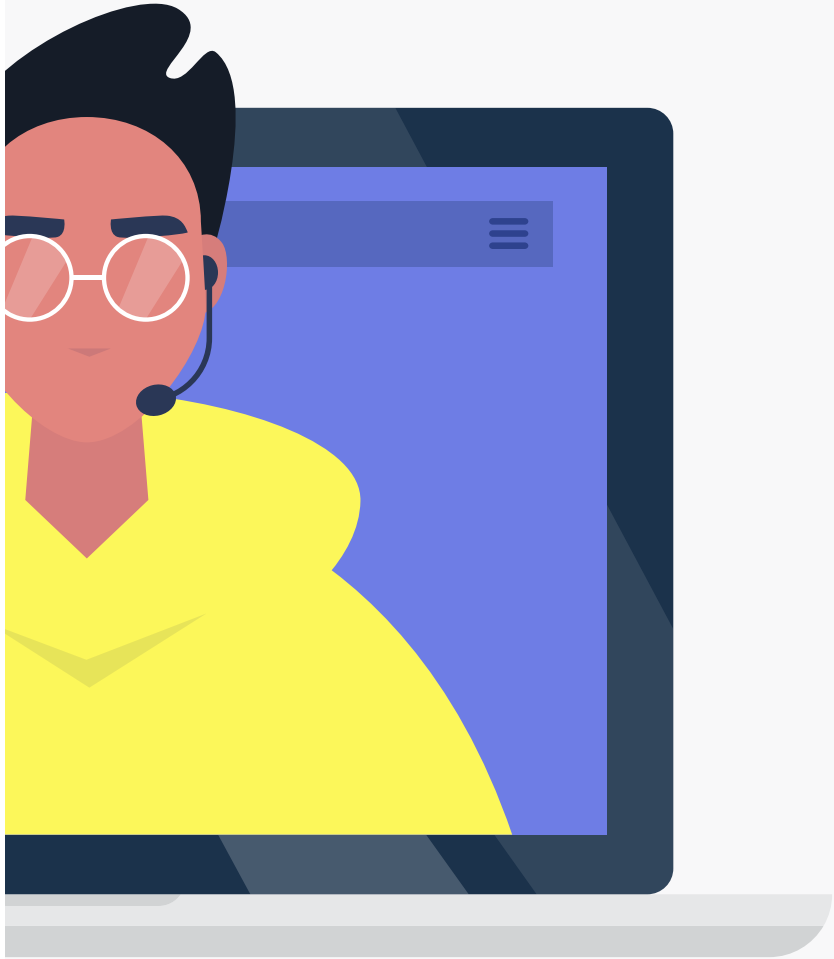
Kẻ lừa đảo có thể làm một số điện thoại trông giống như ID người gọi của ngân hàng quý vị, nhưng đừng coi đó là bằng chứng xác nhận người đang gọi là thật. Chúng cũng có thể giả vờ có thông tin về quý vị, nhưng rất có thể những thông tin đó đã bị lấy cắp do hành vi gian lận.



Ví dụ về tin nhắn mạo danh ngân hàng từ một số điện thoại giả mạo yêu cầu quý vị nhấp vào liên kết để xác minh thông tin cá nhân.

Lừa đảo hỗ trợ kỹ thuật

- Người gọi tự xưng là từ nhà cung cấp dịch vụ internet, công ty viễn thông hoặc máy tính, thông báo cho quý vị rằng có sự cố với internet hoặc máy tính của quý vị. Họ có thể nói rằng máy tính đã bị hack, nhiễm vi-rút, chạy chậm hoặc sắp bị ngắt kết nối. Họ sẽ hướng dẫn quý vị tải về ứng dụng hoặc phần mềm để cho phép họ truy cập từ xa máy tính cho việc 'sửa chữa'.
- Trên màn hình máy tính có thể xuất hiện cảnh báo yêu cầu quý vị ngay lập tức gọi số điện thoại được liệt kê để được trợ giúp về một vấn đề đã được phát hiện.



Làm sao quý vị biết đó là lừa đảo?

Các công ty hợp pháp sẽ không bao giờ gọi điện để báo rằng kết nối internet hoặc máy tính của quý vị có vấn đề (họ mong đợi quý vị liên hệ với họ khi có vấn đề). Họ sẽ không bao giờ yêu cầu quý vị tải xuống bất kỳ loại phần mềm hoặc ứng dụng nào cho phép họ truy cập vào thiết bị của quý vị.

Đóng các thông báo bật lên đáng ngờ bằng cách nhấp vào dấu ‘x’ ở góc trên bên phải của hộp. Nếu cách đó không hiệu quả, hãy thử nhấp ra bên ngoài hộp hoặc đóng trang mạng mà thông báo đó xuất hiện. Nếu cửa sổ bật lên vẫn chưa biến mất, hãy thử giữ phím ALT và F4 trên máy tính Windows của quý vị để đóng trình duyệt mạng. Trên máy tính Apple, chọn Thoát Cưỡng bức (Force Quit) từ menu Apple và chọn trình duyệt quý vị muốn đóng.

Lừa đảo đình chỉ tài khoản

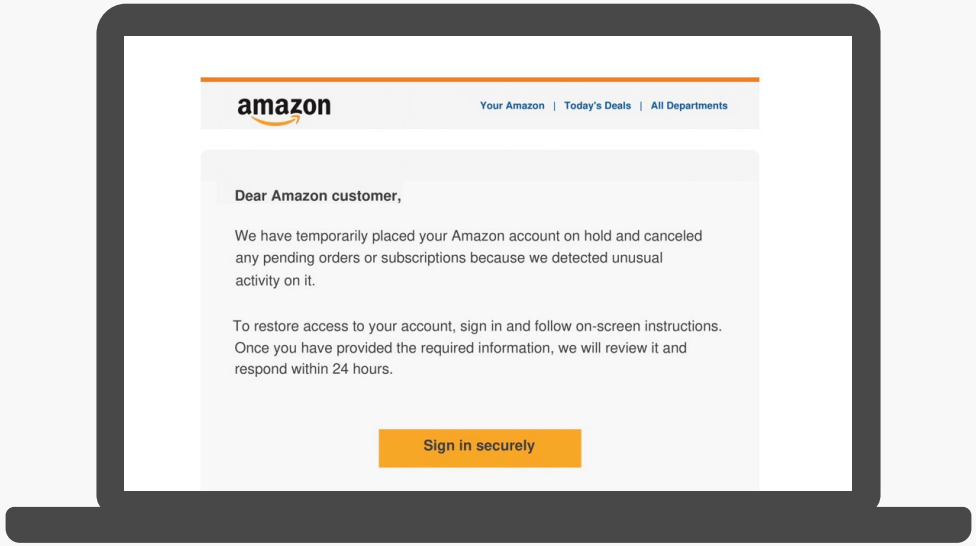
Quý vị nhận được một email hoặc tin nhắn văn bản tự xưng là từ một tổ chức mà quý vị biết, chẳng hạn như Amazon, PayPal hoặc Netflix. Email hay tin nhắn thông báo rằng tài khoản của quý vị đã bị đình chỉ do hoạt động đáng ngờ và quý vị cần nhấp vào một đường liên kết để xác nhận danh tính, nhằm chứng minh quý vị chính là chủ tài khoản.

Kẻ lừa đảo dùng chiêu bài hù dọa để dẫn quý vị đến trang mạng giả mạo, nơi chúng sẽ lấy cắp các thông tin cá nhân như tên đăng nhập, mật khẩu, thông tin ngân hàng hoặc thẻ tín dụng.

Làm sao quý vị biết đó là lừa đảo?

Amazon, PayPal và Netflix sẽ không bao giờ yêu cầu thông tin cá nhân như mật khẩu, thông tin ngân hàng hoặc thẻ tín dụng của quý vị thông qua một liên kết trong một email hoặc tin nhắn không mong đợi. Mỗi tổ chức có cách liên lạc với khách hàng khác nhau, nhưng tốt nhất quý vị nên thận trọng với những email, tin nhắn hoặc cuộc gọi kiểu này.

Nếu quý vị không chắc tin nhắn có thật sự đến từ doanh nghiệp đó không, hãy tìm kiếm thông tin liên hệ thật sự của họ trên mạng và liên hệ trực tiếp. Không bao giờ sử dụng thông tin liên hệ có trong email, tin nhắn hay cuộc gọi đáng ngờ.



Ví dụ về email lừa đảo tự nhận là từ Amazon, thúc giục quý vị nhấp vào liên kết để cung cấp thông tin cá nhân của mình.

Hãy cẩn thận với các chiêu trò hù dọa

Kẻ lừa đảo sử dụng các chiêu trò hù dọa để tạo cảm giác cấp bách khiến quý vị phải hành động. Dưới đây là một số điều họ có thể nói để thu hút sự chú ý của quý vị:

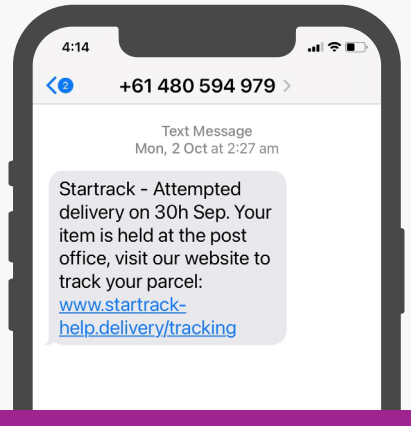
- Phát hiện hoạt động bất thường trên tài khoản
- Các nỗ lực đăng nhập trái phép
- Tài khoản của quý vị đã bị chặn / khóa
- Thanh toán của quý vị đã bị từ chối
- Không thể xác thực thông tin thanh toán của quý vị

Lừa đảo không giao được hàng

Quý vị nhận được email hoặc tin nhắn từ Australia Post hoặc các công ty chuyển phát như FedEx thông báo có vấn đề hoặc chậm trễ trong việc giao hàng cho quý vị. Để nhận gói hàng, quý vị sẽ phải trả phí vận chuyển hoặc 'cập nhật thông tin cá nhân'.

Làm sao quý vị biết đó là lừa đảo?

Australia Post, FedEx và các công ty chuyển phát nhanh hợp pháp khác sẽ không bao giờ yêu cầu thông tin cá nhân hoặc thanh toán qua tin nhắn, email hoặc cuộc gọi. Nếu quý vị đang chờ giao hàng, tốt nhất nên theo dõi việc giao hàng của mình qua ứng dụng bảo mật của đơn vị vận chuyển hoặc qua dịch vụ theo dõi trực tuyến có trong email xác nhận đơn hàng. Nếu quý vị không có thông tin đó, hãy gọi trực tiếp cho công ty chuyển phát để hỏi về tình trạng bưu kiện của mình.



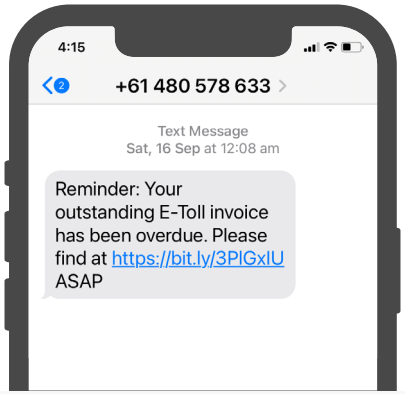
Ví dụ về tin nhắn giả mạo là từ công ty chuyển phát.

Lừa đảo phí đường bộ

Quý vị nhận được tin nhắn từ đơn vị thu phí đường bộ thông báo rằng phí đường bộ của quý vị đã quá hạn. Quý vị cần xử lý ngay để tránh bị phạt, kèm theo một đường liên kết để thanh toán, nhưng đó là trang mạng giả mạo nhằm đánh cắp thông tin tài chính của quý vị.

Làm sao quý vị biết đó là lừa đảo?

Nếu quý vị nhận được tin nhắn báo rằng quý vị có một khoản phí cầu đường quá hạn hoặc tài khoản không đủ tiền – đó có thể là trò lừa đảo. Truy cập trang mạng hoặc ứng dụng của nhà điều hành thu phí để đăng nhập vào tài khoản của quý vị nhằm kiểm tra hoạt động gần đây của quý vị.



Ví dụ về tin nhắn lừa đảo phí đường bộ.

Lừa đảo đầu tư giả

Quý vị thấy một cơ hội đầu tư hấp dẫn được một người nổi tiếng hoặc người có ảnh hưởng trong lĩnh vực tài chính đề xuất. Đề xuất hứa hẹn lợi nhuận cao đảm bảo với rủi ro thấp hoặc không có rủi ro. Khi quý vị hỏi thông tin, quý vị được dẫn đến một trang mạng giống như chuyên nghiệp và nhận được tài liệu quảng cáo tinh vi.

Làm sao quý vị biết đó là lừa đảo?

Nếu một thỏa thuận nghe như là thật, có thể đó là lừa đảo. Kẻ lừa đảo sử dụng các chiến thuật gây áp lực cao để thuyết phục quý vị hành động nhanh chóng để quý vị không 'bỏ lỡ'. Cảnh giác với các email, trang mạng hoặc quảng cáo có lời chứng thực và những hứa hẹn quá mức về các lợi nhuận to lớn.

Người 'cố vấn' hỗ trợ quý vị có thể nói rằng họ không cần giấy phép dịch vụ tài chính Úc (AFS). Nếu họ cung cấp giấy phép, hãy kiểm tra xem người quý vị đang giao dịch có thực sự sở hữu giấy phép đó không.

Lừa đảo qua trang mạng giả mạo

Quý vị thấy một quảng cáo trên Facebook về một thương hiệu BBQ nổi tiếng đang được bán với giá 100 đô la, trong khi giá bình thường là 900 đô la. Quý vị nhấp vào liên kết đến trang bán hàng và thấy rằng nếu thanh toán bằng thẻ tín dụng sẽ bị tính thêm phí 2.99%, vì vậy quý vị chọn chuyển khoản ngân hàng để được giảm thêm 5%. Quý vị nhận được email xác nhận, nhưng không bao giờ nhận được BBQ.

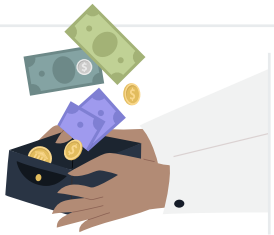
Làm sao quý vị biết đó là lừa đảo?

Các trang mạng giả mạo có mức giá quá rẻ đến mức khó tin, phương thức thanh toán bất thường và các dấu hiệu cảnh báo khác như URL trông giống như URL của cửa hàng chính thức (ví dụ: webberbbqs.com so với weber.com thật).

Kẻ lừa đảo cũng có thể trả tiền cho quảng cáo trên mạng xã hội và các công cụ tìm kiếm như Google (gọi là quảng cáo được tài trợ), vì vậy hãy cẩn thận khi nhấp vào những loại quảng cáo này.

10 mẹo hàng đầu để bảo vệ bản thân

01. Cảnh giác với những cuộc gọi có số lạ. Hãy để các cuộc gọi từ số lạ chuyển sang hộp thư thoại.



02. Dừng lại và suy nghĩ trước khi cung cấp thông tin về cá nhân hoặc tài chính qua các cuộc liên lạc không có yêu cầu. Hãy tự hỏi: liệu điều này có thể là giả mạo không?

03. Cẩn thận với email có nội dung đe dọa hoặc gây hoang mang. Kiểm tra tên và địa chỉ email hiển thị. Chúng có khớp nhau không? Ví dụ: Trường 'From' ('Người gửi') ghi là "Amazon Support" nhưng địa chỉ email là "amazonsupport830@gmail.com"

04. Đừng tin vào tin nhắn văn bản chỉ vì nó xuất hiện trong cùng một chuỗi với các tin nhắn cũ từ một tổ chức mà quý vị biết. Nó vẫn có thể là tin nhắn lừa đảo.

05. Nếu quý vị nghi ngờ về một tin nhắn hoặc cuộc gọi mà quý vị đã nhận, hãy liên hệ trực tiếp với tổ chức mà người đó tự xưng là đại diện. Liên hệ qua trang mạng chính thức của họ hoặc ứng dụng bảo mật trên điện thoại thông minh hoặc máy tính bảng của quý vị.

06. Không cung cấp mật khẩu, số PIN, hoặc mã xác thực một lần cho bất kỳ ai qua điện thoại, kể cả khi họ tự xưng là từ ngân hàng hoặc cơ quan chính phủ và đọc thông tin về tài khoản của quý vị.

07. Không bấm vào các liên kết trong tin nhắn văn bản. Mặc dù một số liên kết có thể vô hại, nhưng tốt nhất là nên thận trọng. Điều này cũng áp dụng cho các tệp đính kèm và liên kết trong email – chỉ mở khi quý vị chắc chắn về người gửi.

08. Không làm theo hướng dẫn từ người lạ gọi đến bất ngờ, yêu cầu quý vị tải xuống một ứng dụng hoặc cài đặt phần mềm cho phép họ quyền truy cập vào thiết bị của quý vị. Hãy lập tức cúp máy.

09. Không bao giờ đăng nhập vào tài khoản trực tuyến của quý vị qua một liên kết trong email hoặc tin nhắn. Thay vào đó, hãy nhập địa chỉ trang mạng chính thức (URL) vào trình duyệt hoặc sử dụng ứng dụng bảo mật của họ để truy cập tài khoản.

10. Trước khi thanh toán trực tuyến, luôn kiểm tra địa chỉ trang mạng URL (có phải là trang chính thức không?), hãy để ý các phương thức thanh toán bất thường và những phần thông tin mơ hồ hoặc thiếu sót ở các mục như Giới thiệu (About Us), Vận chuyển và Trả hàng lại (Shipping and Returns) và các phần khác ở cuối trang mạng.

Nếu quý vị có bất kỳ nghi ngờ nào, hãy tìm kiếm trực tuyến bằng cách nhập tên tổ chức hoặc trang mạng đang nghi vấn và từ 'lừa đảo' ('scam').

Quý vị nghĩ rằng mình đã bị lừa đảo?

Nơi để tìm sự trợ giúp

Bị lừa đảo có thể ảnh hưởng đến tài chính và cảm xúc, vì vậy điều quan trọng là tìm kiếm sự giúp đỡ và hành động nhanh chóng. Dưới đây là một số bước quý vị có thể thực hiện:

1. Liên hệ ngay với ngân hàng của quý vị để ngăn các giao dịch tiếp theo.
2. Liên hệ IDCARE, dịch vụ hỗ trợ miễn phí cho những người bị lừa đảo hoặc mất cắp danh tính. Gọi 1800 595 160 hoặc truy cập idcare.org
3. Đổi mật khẩu ngay lập tức và đảm bảo mật khẩu đủ mạnh.
4. Báo cáo lừa đảo cho Scamwatch để cảnh báo người khác: scamwatch.gov.au/report-a-scam
5. Tìm sự hỗ trợ cho bản thân. Nếu quý vị không cảm thấy thoải mái khi nói chuyện với bạn bè hoặc gia đình, hãy liên hệ với Lifeline hoặc Beyond Blue để có một cuộc trò chuyện riêng tư. Và nếu quý vị đã mất một số tiền đáng kể, hãy nói chuyện với Đường dây Trợ giúp Nợ Quốc gia.

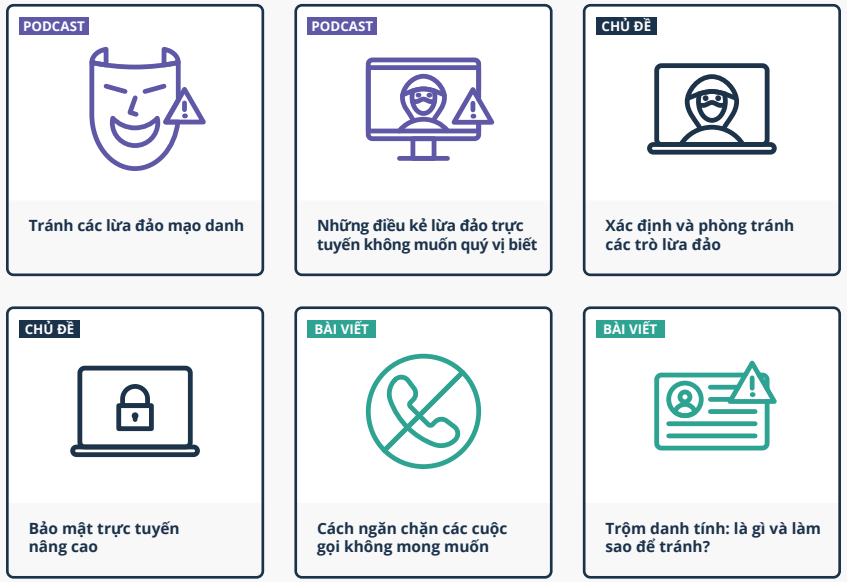
   Beyond Blue: 1300 22 4636 (24/7) hoặc truy cập beyondblue.org.au

   Lifeline: 13 11 14 (24/7) hoặc truy cập lifeline.org.au

   Đường dây Trợ giúp Nợ Quốc gia: 1800 007 007 (ngày thường, 9h30 sáng đến 4h30 chiều) hoặc truy cập ndh.org.au

Thông tin thêm

Nhấp vào các mục bên dưới để khám phá:



Cuốn Sách Nhỏ Về Các Trò Lừa Đảo là một công cụ được quốc tế công nhận, giúp quý vị tìm hiểu về các hình thức lừa đảo phổ biến và cách tự bảo vệ.

Truy cập trang mạng Scamwatch để cập nhật các hình thức lừa đảo mới nhất và các lời khuyên để tự bảo vệ.

Về Be Connected

Be Connected là một sáng kiến của chính phủ Úc cam kết xây dựng kỹ năng số, sự tự tin và an toàn trực tuyến cho người cao tuổi Úc với các lớp học máy tính miễn phí, các khóa học trực tuyến ngắn hạn và nhiều nội dung khác. Trang mạng và nội dung học của Be Connected được quản lý bởi Ủy viên An toàn điện tử (eSafety Commissioner).

Về Scamwatch

Scamwatch được điều hành bởi Trung tâm Chống Lừa đảo Quốc gia, với mục tiêu biến nước Úc thành mục tiêu khó tiếp cận hơn với các đối tượng lừa đảo. Scamwatch nâng cao nhận thức cộng đồng về lừa đảo, giúp mọi người nhận biết, tránh và báo cáo các hành vi lừa đảo. Trung tâm Chống Lừa đảo chia sẻ thông tin từ các báo cáo lừa đảo và làm việc với chính phủ, cơ quan thực thi pháp luật và lĩnh vực tư nhân để ngăn chặn và phòng ngừa lừa đảo.