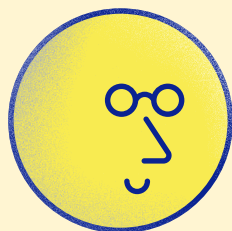


Làm thế nào để phát hiện và tránh được các trò lừa đảo



Hướng dẫn về cách bảo vệ
bản thân khỏi các trò lừa
đảo



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

Lời Tri ân Đất nước

ACCC tri ân các chủ nhân truyền thống và những người trông coi Đất nước trên khắp nước Úc và công nhận sự kết nối liên tục của họ với vùng đất, vùng sông nước và cộng đồng. Chúng tôi bày tỏ lòng kính trọng của mình đối với họ và các nền văn hóa của họ; và đối với các Trưởng lão trong quá khứ, hiện tại và tương lai.

Australian Competition and Consumer Commission (Ủy hội Cạnh tranh và Người Tiêu dùng Úc)
Ngunnawal

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Bản quyền của Liên bang Úc Năm 2023

Tài liệu này được bảo vệ bản quyền. Ngoài việc sử dụng được cho phép theo *Đạo luật về Bản quyền Năm 1968*, tất cả tài liệu trong tài liệu này đều được cung cấp tuân theo giấy phép Creative Commons Attribution 4.0 (Ghi công sự Sáng tạo Chung Phiên bản 4.0) Úc Châu, ngoại trừ:

- Quốc Huy Liên bang
- các biểu trưng của ACCC và AER,
- bất kỳ hình minh họa, biểu đồ, hình ảnh hay đồ họa nào mà Ủy ban Cạnh tranh và Người Tiêu dùng Úc không giữ bản quyền, nhưng có thể là một phần hoặc được bao gồm trong ấn phẩm này.

Chi tiết về các điều kiện của giấy phép có liên quan có thể được tìm thấy trên trang mạng của Creative Commons, cũng như mã pháp lý đầy đủ cho giấy phép CC BY 4.0 AUD.

Mọi yêu cầu và thắc mắc liên quan đến việc sao chép và các quyền, xin gửi tới Giám đốc, Truyền thông Doanh nghiệp, ACCC, GPO Box 3131, Canberra ACT 2601.

Thông báo quan trọng

Thông tin trong ấn phẩm này chỉ mang tính tổng quát mà thôi. Các thông tin này không phải là lời khuyên pháp lý hoặc chuyên môn, và không nên được xem như một điều luật trong bất kỳ thẩm quyền tài phán nào. Do các thông tin này được chú ý làm hướng dẫn tổng quát mà thôi, nên có thể bao gồm thông tin được khái quát hóa. Quý vị nên tìm kiếm lời khuyên chuyên môn nếu có bất kỳ quan ngại cụ thể nào.

ACCC đã thực hiện mọi nỗ lực hợp lý để cung cấp thông tin hiện hành và chính xác, nhưng ACCC không đưa ra bất kỳ sự bảo đảm nào về tính chính xác, hiện hành hay đầy đủ của các thông tin đó.

Các bên muốn tái xuất bản hoặc sử dụng thông tin trong ấn phẩm này phải kiểm tra tính chính xác và hiện hành của thông tin trước khi xuất bản. Việc này nên được làm trước mỗi phiên bản của ấn phẩm, bởi hướng dẫn của ACCC và luật lệ chuyển tiếp có liên quan, thường xuyên thay đổi. Mọi thắc mắc, xin gửi tới Giám đốc, Truyền thông Doanh nghiệp, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

Mục lục

Sự trợ giúp luôn sẵn có	1
Trò lừa đảo là gì	3
Các bước đơn giản để phát hiện và tránh được các trò lừa đảo	4
Các trò lừa đảo bằng tin nhắn hoặc SMS	7
Các trò lừa đảo bằng thư điện tử	7
Các trò lừa đảo qua điện thoại	7
Các trò lừa đảo trên trang mạng	19
Các trò lừa đảo trên mạng xã hội, ứng dụng và nhắn tin trực tuyến	23
Các trò lừa đảo phổ biến nhất mà quý vị nên biết	27
Tới đâu để trình báo các trò lừa đảo	31
Sự trợ giúp và hỗ trợ thêm	33



Hướng dẫn này do Trung tâm Quốc gia về Phòng chống Lừa đảo viết, và sẽ giúp quý vị phát hiện và bảo vệ bản thân khỏi những tổn hại do các trò lừa đảo gây ra.

Lừa đảo là một tội ác và những ai thực hiện các trò lừa đảo là những kẻ tội phạm. Nhiều người ở Úc đang bị lừa và bị mất tiền bạc, đôi khi thậm chí là cả những khoản tiền dành dụm cả đời. Các trò lừa đảo gây tổn hại đến cuộc sống của mọi người.

Các trò lừa đảo đang trở nên khó phát hiện hơn, vì vậy chúng ta cần phải làm việc cùng nhau để ngăn chặn chúng.

Trung tâm Quốc gia về Phòng chống Lừa đảo làm việc để giữ an toàn cho người dân Úc khỏi các trò lừa đảo.

Chúng tôi làm việc với chính phủ và kỹ nghệ để tìm ra những cách mới nhằm ngăn chặn những kẻ lừa đảo ăn cắp tiền bạc và thông tin cá nhân từ người dân Úc. Đây là một số cách để chúng tôi đạt được mục tiêu này.

Chúng tôi giúp mọi người phát hiện và tránh được các trò lừa đảo

Qua Scamwatch, chúng tôi chia sẻ thông tin cập nhật về các trò lừa đảo và các cách quý vị có thể bảo vệ bản thân khỏi các trò lừa đảo.

Chúng tôi phá vỡ hoạt động của những kẻ lừa đảo

Bằng việc thu thập và chia sẻ thông tin tình báo giữa chính phủ và kỹ nghệ, chúng tôi khiến những kẻ lừa đảo khó có thể tiếp tục phạm tội hơn và giúp mọi người trình báo các vụ lừa đảo dễ dàng hơn.



Sự trợ giúp luôn sẵn có

Nếu quý vị đang đọc những điều này, thì có khả năng là quý vị, hoặc ai đó mà quý vị biết, đã bị lừa gạt. Không may thay, quý vị không phải là trường hợp duy nhất. Các trò lừa đảo đang trở nên ngày một tinh vi, điều đó có nghĩa là bất kỳ ai cũng có thể bị lừa.

Nếu quý vị đã bị lừa, điều quan trọng là quý vị phải nhanh chóng hành động.

Nếu quý vị đã bị mất tiền vào tay một kẻ lừa đảo, hãy liên lạc với ngân hàng hoặc nhà cung cấp thẻ của quý vị.

Hãy liên lạc với IDCARE, **1800 595 160**, www.idcare.org.

Các trò lừa đảo thành công vì nó có vẻ thật. Những kẻ lừa đảo dựa vào việc quý vị không phát hiện ra các dấu hiệu cảnh báo do quý vị đang hành động gấp rút, thứ gì đó trông có vẻ là một món hời mà quý vị không muốn bỏ lỡ, hoặc bởi nó có vẻ như đến từ ai đó quý vị tin cậy.

Hãy bảo vệ bản thân khỏi các trò lừa đảo bằng cách làm theo 3 bước này:

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



Những kẻ lừa đảo sẽ đề nghị giúp quý vị hoặc yêu cầu quý vị xác minh quý vị là ai. Chúng sẽ giả là người từ các tổ chức mà quý vị biết và tin cậy như các nhà cung cấp dịch vụ, cảnh sát, ngân hàng của quý vị hoặc các dịch vụ của chính phủ.

Kiểm tra Hãy tự hỏi liệu tin nhắn hay cuộc gọi này có phải là giả mạo không?

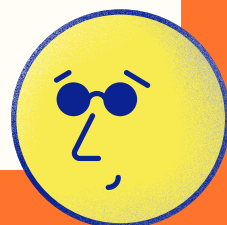


Đừng bao giờ nhấp chuột vào đường dẫn nào trong tin nhắn. Chỉ liên lạc với doanh nghiệp hoặc chính phủ bằng cách sử dụng các thông tin liên lạc mà quý vị tự tìm ra từ trang mạng hoặc ứng dụng chính thức của họ. Nếu quý vị không chắc chắn, hãy nói 'không' ('không'), rồi gác máy hoặc hủy bỏ.

Trình báo Hãy nhanh chóng hành động nếu có gì đó khiến quý vị cảm thấy không ổn.



Hãy liên lạc với ngân hàng của mình nếu quý vị nhận thấy hoạt động bất thường hoặc nếu một kẻ lừa đảo lấy được tiền bạc hoặc thông tin của quý vị. Hãy tìm kiếm sự giúp đỡ và trình báo vụ lừa đảo với ReportCyber và Scamwatch. Khi quý vị trình báo trò lừa đảo là quý vị đang giúp tất cả người dân Úc bằng cách xây dựng hàng rào bảo vệ chống lại các trò lừa đảo.



Trò lừa đảo là gì

Trò lừa đảo là khi ai đó lừa gạt quý vị để đánh cắp tiền hoặc thông tin cá nhân của quý vị.

Các trò lừa đảo là tội ác kinh tế do những kẻ tội phạm thực hiện. Những kẻ tội phạm thường rất có tổ chức và tinh vi.

Các trò lừa đảo:

-  do những kẻ tội phạm thực hiện
-  trông như thật
-  cùng với những câu chuyện đáng tin
-  tạo áp lực để quý vị thực hiện hành động

Trò lừa đảo KHÔNG phải là:

-  Việc xâm nhập vào hệ thống máy vi tính
-  Những điều khoản hợp đồng bất công
-  Các phương pháp tiếp thị phiền nhiễu

Điều quan trọng cần nhớ là, không phải tất cả các trải nghiệm tiêu cực đều là các trò lừa đảo. Quý vị có thể đã trả tiền cho một sản phẩm mà quý vị không bao giờ nhận được hoặc đã mua rồi thấy chất lượng kém. Mặc dù việc này gây thất vọng, nhưng đây không nhất thiết là trò lừa đảo. Luật lệ Người Tiêu dùng của Úc đưa ra những bảo vệ cho người tiêu dùng của Úc đối với những loại vấn đề này.

Muốn biết thêm thông tin, xin quý vị truy cập www.accc.gov.au/consumers

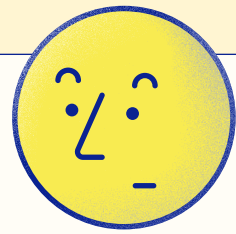
Các bước đơn giản để phát hiện và tránh được các trò lừa đảo

Các trò lừa đảo có thể xảy ra với bất kỳ ai trong chúng ta. Các trò lừa đảo thành công bởi vì những kẻ lừa đảo tạo ra các câu chuyện đáng tin để đánh cắp tiền của quý vị hoặc có được thông tin cá nhân của quý vị.

Các kẻ lừa đảo đang ngày một thông minh hơn và đang lợi dụng công nghệ, các sản phẩm, dịch vụ mới, và các sự kiện lớn để khiến quý vị tin các trò lừa đảo của chúng là thật.

Có thể rất khó phát hiện được trò lừa đảo. Đây là một số tình huống để đề phòng. Một số kẻ lừa đảo dùng sự kết hợp của các mảnh khốe này.

- 1. Các cơ hội để kiếm được hoặc tiết kiệm được tiền:** Một số kẻ lừa đảo sẽ lừa gạt quý vị để quý vị tin là mình đang có một giao dịch hoặc một chào mời tuyệt vời. Chúng sẽ tạo áp lực lên quý vị để quý vị nhanh chóng hành động sao để không bỏ lỡ. Xin nhớ là, những giao dịch có vẻ quá tốt đến mức khó có thật, thì thường là không thật.
- 2. Những câu chuyện buồn rồi kêu gọi xin giúp đỡ:** Những kẻ lừa đảo sẽ tìm cách dùng bản tính tốt bụng của quý vị để hại quý vị. Chúng sẽ chia sẻ với quý vị những câu chuyện đau lòng và buồn thảm rồi giải thích tại sao chúng cần sự giúp đỡ của quý vị và tiền của quý vị.
- 3. Các đường dẫn và các nội dung đính kèm:** Những kẻ lừa đảo sử dụng các đường dẫn để đưa quý vị đến các trang mạng lừa đảo được thiết kế để đánh cắp thông tin và tiền của quý vị. Những kẻ lừa đảo có thể còn yêu cầu quý vị mở các tập tin được đính kèm. Những thứ này có thể cài đặt các vi-rút đánh cắp thông tin của quý vị.



4. **Áp lực để nhanh chóng hành động:** Những kẻ lừa đảo không muốn quý vị dành thời gian suy nghĩ thấu đáo. Chúng muốn thúc ép quý vị nhanh chóng hành động. Kiểu này có thể bao gồm việc đưa ra những hăm dọa rằng điều gì đó xấu có thể xảy ra nếu quý vị không hành động nhanh.
5. **Yêu cầu quý vị trả tiền theo những cách bất bình thường hoặc theo những cách cụ thể:** Những kẻ lừa đảo thường yêu cầu quý vị trả tiền bằng cách dùng các phương thức không thường gặp, như thẻ ghi nợ đã có sẵn tiền, thẻ iTunes, hoặc tiền ảo như Bitcoin. Sau khi số tiền này đã được chi tiêu, quý vị không thể lấy lại được.
6. **Yêu cầu thiết lập các tài khoản hoặc PayID mới:** Những kẻ lừa đảo có thể yêu cầu quý vị thiết lập một tài khoản ngân hàng hoặc PayID mới để trả tiền cho chúng (hoặc được chúng trả tiền). Chúng có thể giả là ngân hàng của quý vị rồi bảo quý vị chuyển tiền của quý vị vào các tài khoản mới để giữ an toàn.

Nếu những kẻ lừa đảo đã thành công trong việc lấy được tiền của quý vị, chúng sẽ tìm cách tiếp tục lấy thêm tiền từ quý vị. Đáng tiếc là cứ trong ba nạn nhân của trò lừa này thì một nạn nhân đã bị lừa hơn một lần. Nếu quý vị bị lừa mất tiền, hãy đề phòng với những kẻ lừa đảo đề nghị giúp quý vị lấy lại tiền. Đây là một hình thức khác của trò lừa đảo liên tiếp.



Các trò lừa đảo bằng tin nhắn hoặc SMS

Kẻ lừa đảo gửi các tin nhắn giả là từ chính phủ, cơ quan thực thi luật pháp, các doanh nghiệp được tin cậy, hoặc thậm chí là từ gia đình hoặc bạn bè của quý vị.

Các tin nhắn này sẽ nghe có vẻ khẩn cấp và cố sao để quý vị nhanh chóng hành động. Các tin nhắn sẽ thường có đường dẫn mà sẽ đưa quý vị đến một trang mạng lừa đảo. Những kẻ lừa đảo có thể đánh cắp bất kỳ thông tin cá nhân nào được nhập vào các trang mạng lừa đảo này và dùng các thông tin đó để lấy tiền của quý vị hoặc thực hiện trò gian lận dưới tên của quý vị.

Để làm cho các tin nhắn này có vẻ thật, những kẻ lừa đảo sao chép và che giấu số điện thoại của chúng sau số điện thoại hoặc nhận dạng người gọi của các doanh nghiệp hợp pháp hoặc của những người mà quý vị biết.

Các tin nhắn lừa đảo thậm chí có thể xuất hiện trong cùng chuỗi tin nhắn như các tin nhắn thật từ tổ chức này, làm cho quý vị càng khó phát hiện được ra đó là trò lừa đảo.

Các dấu hiệu khi một tin nhắn nào đó có thể là trò lừa đảo

Tin nhắn này:



Yêu cầu quý vị thực hiện hành động ngay tức thì, thực hiện một khoản thanh toán, hoặc chuyển tiền.



Yêu cầu quý vị nhấp vào một đường dẫn hoặc gọi số điện thoại được cung cấp trong tin nhắn.



Yêu cầu quý vị đăng nhập vào một tài khoản trực tuyến bằng tên người sử dụng và mật khẩu của quý vị hoặc cung cấp các thông tin cá nhân khác.



Từ một người thân trong gia đình hoặc từ một người bạn, nói rằng các chi tiết liên lạc của họ đã thay đổi.



Hăm dọa chấm dứt một dịch vụ nào đó hoặc tính phí với quý vị nếu quý vị không hành động.



Gợi ý rằng quý vị hoặc các tài khoản của quý vị đã bị tin tặc hoặc đã tham gia vào hoạt động gian lận.



Gợi ý rằng có một vấn đề nào đó với khoản thanh toán của quý vị hoặc với việc giao bưu phẩm của quý vị.

Các bước để bảo vệ bản thân mình khỏi các trò lừa đảo bằng tin nhắn

1. Nếu ai đó mà quý vị biết, gửi một tin nhắn nói rằng họ có số điện thoại mới:



- a. thử gọi cho họ vào số điện thoại của họ mà quý vị hiện có, và
 - b. nhắn tin cho họ vào số mới với một câu hỏi mà chỉ họ mới có thể biết câu trả lời, để kiểm tra xem họ có phải là người mà họ tự xưng không.
-



2. Đừng bao giờ nhấp vào các đường dẫn trong các tin nhắn.
-



3. Nếu một tin nhắn dẫn đến một trang mạng, thì đừng nhấp chuột vào đường dẫn đó. Thay vào đó, hãy tự mình tìm kiếm trực tuyến trang mạng đó, hoặc sử dụng ứng dụng chính thức.
-



4. Đừng trả lời tin nhắn văn bản bằng cách dùng số điện thoại được cung cấp.
-



5. Hãy gọi lại cho tổ chức hoặc người đó vào số điện thoại mà quý vị tự tìm thấy, chẳng hạn như từ trang mạng của tổ chức đó.
-



Các trò lừa đảo bằng thư điện tử

Những kẻ lừa đảo gửi các thư điện tử giả là từ chính phủ, cơ quan thực thi pháp luật và các doanh nghiệp. Những thư điện tử này làm ra vẻ khẩn cấp để buộc quý vị nhanh chóng hành động.

Những kẻ lừa đảo sử dụng cùng một biểu trưng và địa chỉ thư điện tử tương tự như tổ chức thật. Những kẻ lừa đảo còn có thể sao chép hoặc che giấu địa chỉ thư điện tử của chúng sau địa chỉ thư điện tử của một tổ chức hoặc doanh nghiệp để thư điện tử lừa đảo trông thật hơn.

Các dấu hiệu khi một thư điện tử nào đó có thể là trò lừa đảo

Thư điện tử đó:



Yêu cầu một khoản thanh toán nhưng các chi tiết tài khoản lại mới hoặc đã thay đổi kể từ lần thanh toán sau cùng quý vị thực hiện



Yêu cầu quý vị đăng nhập vào một tài khoản trực tuyến bằng tên người sử dụng và mật khẩu của quý vị hoặc cung cấp các thông tin cá nhân khác.



Không được mong chờ và đính kèm tài liệu có lời mời mở ra.



Yêu cầu quý vị xác nhận các chi tiết ngân hàng của quý vị để nhận được một khoản hoàn tiền hoặc một số tiền mà quý vị đang không chờ đợi.



Tuyên bố là có các thông tin về quý vị hoặc các hình ảnh về quý vị và đe dọa phát tán chúng.



Đề nghị giúp quý vị lấy lại tiền hoặc nhận được khoản bồi thường cho một vụ lộ dữ liệu hoặc đánh cắp danh tính.

Các bước quý vị có thể thực hiện để bảo vệ bản thân khỏi các trò lừa đảo bằng thư điện tử

1. Hãy kiểm tra xem thư điện tử đó có thật không, bằng cách:



- a. trực tiếp liên lạc với người hoặc tổ chức đó, sử dụng các chi tiết liên lạc mà quý vị tự mình tìm thấy, chẳng hạn như từ trang mạng của tổ chức đó hoặc,
- b. truy cập vào một tổ chức qua ứng dụng chính thức của họ (đừng bao giờ qua một đường dẫn).



2. Ngay lập tức chấm dứt liên lạc với bất kỳ ai đang cố hãm dọa hoặc làm cho quý vị lo sợ.



3. Đừng bao giờ cung cấp các chi tiết cá nhân hoặc trả tiền cho bất kỳ ai đang chào mời quý vị:
 - a. khoản bồi thường hoặc sự giúp đỡ để khôi phục lại từ vụ lừa đảo hoặc vụ lộ dữ liệu trước đó hoặc,
 - b. các kết quả thắng, các giải thưởng hoặc một món thừa kế.



4. Hãy dùng cách xác thực đa yếu tố những khi quý vị có thể. Cách này cung cấp thêm một tầng bảo vệ và có nghĩa là kẻ lừa đảo phải biết được mật khẩu thư điện tử của quý vị và số pin (số chứng minh riêng) được gửi tới máy điện thoại của quý vị thì mới có thể truy cập được vào tài khoản thư điện tử của quý vị.



Các trò lừa đảo qua điện thoại

Những kẻ lừa đảo gọi điện thoại, tự xưng là từ các tổ chức nổi tiếng. Họ bao gồm các tổ chức của chính phủ, cơ quan thực thi pháp luật, các công ty đầu tư và công ty luật, ngân hàng, và các công ty cung cấp dịch vụ viễn thông.

Những thư điện tử này làm ra vẻ khẩn cấp để buộc quý vị nhanh chóng hành động. Chúng có thể tìm cách thuyết phục để quý vị tin rồi cung cấp cho chúng các chi tiết cá nhân hoặc tài khoản ngân hàng của quý vị, hoặc cho chúng truy cập vào máy vi tính của quý vị.

Người gọi có thể đã có sẵn một số chi tiết về quý vị, chẳng hạn như tên hoặc địa chỉ của quý vị, khiến cho cuộc gọi có vẻ thật.

Các dấu hiệu khi một cuộc gọi điện thoại nào đó có thể là trò lừa đảo

Người gọi:



Yêu cầu việc thanh toán hoặc yêu cầu quý vị chuyển tiền vào một tài khoản mới.



Yêu cầu quý vị cung cấp mật khẩu, PIN, mã sử dụng một lần của quý vị, hoặc các thông tin an ninh khác.



Yêu cầu quý vị cung cấp các chi tiết tài chính của quý vị, như thẻ tín dụng hoặc các chi tiết giao dịch ngân hàng.



Yêu cầu quý vị hoàn tất một hành động nào đó trên máy điện thoại di động hoặc máy vi tính của quý vị, chẳng hạn như cài đặt phần mềm hoặc truy cập vào một tài khoản an toàn.



Tự xưng là từ cơ quan thực thi luật pháp và đe dọa quý vị bằng việc bắt giữ hoặc trục xuất ngay tức thì.



Nói rằng quý vị hoặc các tài khoản trực tuyến khác của quý vị đã bị tin tặc hoặc đã tham gia vào hoạt động gian lận.

Các bước quý vị có thể thực hiện để bảo vệ bản thân khỏi các trò lừa đảo qua điện thoại

1. Hãy kiểm tra xem cuộc gọi đó có thật không, bằng cách:



- a. trực tiếp liên lạc với người hoặc tổ chức đó, sử dụng các chi tiết liên lạc mà quý vị tự mình tìm thấy, chẳng hạn như từ trang mạng của tổ chức đó hoặc,
- b. truy cập vào một tổ chức qua ứng dụng chính thức của họ (đừng bao giờ qua một đường dẫn).



2. Nếu quý vị không biết chắc người gọi là ai, hoặc nếu họ hăm dọa hoặc làm cho quý vị lo sợ, hãy cúp máy ngay lập tức.



3. Đừng bao giờ cài đặt phần mềm cho phép ai đó truy cập được vào máy vì tính hoặc thiết bị của quý vị.



4. Quý vị có thể làm ngơ với cuộc gọi từ các số điện thoại quý vị không biết hoặc để cho cuộc gọi đó tới phần tin nhắn vào hộp thoại.



Nên biết!

Quý vị có thể vẫn nhận được các cuộc gọi lừa đảo ngay cả nếu quý vị đã đặt chế độ ẩn số hoặc trong Đăng bạ Đừng Gọi.



Các trò lừa đảo trên trang mạng

Trên mạng, những kẻ lừa đảo có thể giả là bất kỳ ai, bao gồm chính phủ, một doanh nghiệp thật, các nhân vật nổi tiếng hoặc bạn bè hay gia đình của quý vị.

Chúng có thể tạo ra các trang mạng giả để trông như các thương hiệu nổi tiếng. Chúng có thể giả là những người nổi tiếng và làm như thể họ đang quảng bá cho hàng hóa hoặc các dịch vụ. Những trang mạng này có thể có các nhận xét giả để khiến quý vị tin cậy.

Khi trên mạng, quý vị có thể thấy các biểu ngữ quảng cáo giả hoặc các ô cửa sổ nổi lên mà có các cảnh báo giả hoặc các thông điệp báo lỗi.

Các dấu hiệu khi một trang mạng nào đó có thể là trò lừa đảo

Trang mạng đó:



Chào mời các món đồ được bán với giá thấp hơn rất nhiều so với giá thông thường hoặc so với các trang mạng khác.



Mách cho quý vị cách để kiếm tiền nhanh, dễ dàng mà ít rủi ro hoặc ít vất vả.



Có một thông điệp cảnh báo khẩn cấp hoặc thông điệp báo lỗi yêu cầu quý vị nhấp vào đường dẫn.



Yêu cầu việc thanh toán theo các cách bất bình thường hoặc theo cách cụ thể, chẳng hạn như thẻ quà tặng hoặc tiền ảo như Bitcoin.



Chỉ bao gồm các nhận xét tích cực.

Các bước quý vị có thể thực hiện để tránh các trò lừa đảo trên trang mạng



1. So sánh giá. Nếu một chào mời nào đó có vẻ quá tốt đến mức khó có thật, thì có lẽ là không thật.



2. Tìm hiểu về tổ chức hoặc người mà quý vị đang giao dịch với họ, trước khi đưa tiền hoặc cung cấp thông tin cá nhân.



3. Đừng dựa vào các nhận xét được viết trên chính trang mạng đó. Tìm kiếm trang mạng đó hoặc tên doanh nghiệp đó cùng với từ ngữ 'scam' ('lừa đảo') hoặc 'reviews' ('các nhận xét').



4. Nếu một thông điệp cảnh báo hoặc thông điệp báo lỗi nổi lên trên màn hình của quý vị, đừng nhấp chuột vào nó, mà thay vào đó, hãy trực tiếp tới ứng dụng mà thông điệp đó nói đến, để kiểm tra xem liệu đó có phải là thật không.



5. Luôn cập nhật thiết bị mà quý vị sử dụng cho việc mua sắm trực tuyến, bằng cách cho phép 'tự động cập nhật' hệ điều hành hay các ứng dụng của quý vị.



Nên biết!

Các cách thiết thực để bảo vệ bản thân trên mạng luôn sẵn có trên trang mạng www.cyber.gov.au



Các trò lừa đảo trên mạng xã hội, ứng dụng và nhắn tin trực tuyến

Nếu ai đó quý vị không biết mà liên lạc với quý vị trên mạng xã hội, trên nền tảng nhắn tin như WeChat hoặc WeChat, hoặc qua một ứng dụng, thì đó có thể là trò lừa đảo.

Những kẻ lừa đảo giả là ai đó khác, sẽ thường dùng ảnh thật của người đó hoặc biểu trưng chính thức của công ty mà chúng đang giả danh, để làm cho trò lừa đảo của chúng khó phát hiện hơn.

Những kẻ lừa đảo trên mạng xã hội sẽ tạo ra các hồ sơ giả và giả là từ chính phủ, một doanh nghiệp, một chủ nhân, công ty đầu tư thật, hoặc thậm chí từ một người bạn, người thân trong gia đình hoặc một mối yêu đương.

Chúng có thể giả là những người nổi tiếng và làm như thể họ đang quảng bá cho hàng hóa hoặc các dịch vụ.

Những kẻ lừa đảo còn có thể biết rất nhiều về quý vị từ các chi tiết quý vị chia sẻ trên các tài khoản mạng xã hội. Chúng có thể dùng các thông tin này để đoán ra các mật khẩu tài khoản của quý vị hoặc nhắm đến quý vị với các trò lừa đảo khác.

Các dấu hiệu của trò lừa đảo trên mạng xã hội hoặc trên các ứng dụng

Hồ sơ mạng xã hội hoặc ứng dụng:



Mách cho quý vị cách để kiếm tiền nhanh, dễ dàng mà ít rủi ro hoặc ít vất vả.



Mời quý vị tham gia một cuộc thi hoặc chào mời chỉ có thời gian ngắn.



Yêu cầu chuyển cuộc trò chuyện khỏi ứng dụng, thí dụ ứng dụng hẹn hò, sang trò chuyện riêng tư hoặc thư điện tử.



Gợi ý rằng một người nổi tiếng công nhận hoặc ủng hộ một sản phẩm hoặc dịch vụ nào đó.



Nói rằng ai đó sẽ mua thứ quý vị đang bán mà không xem trước và mua ở giá cao.



Hăm dọa chia sẻ hình ảnh riêng tư của quý vị nếu quý vị không trả tiền cho chúng.



Liên lạc với quý vị để chào mời một công việc.



Nên biết!

Thông tin về những cách để giữ an toàn trên các nền tảng mạng xã hội khác nhau, có thể được tìm thấy trên trang mạng www.esafety.gov.au

Các bước quý vị có thể thực hiện để tránh các trò lừa đảo trên mạng xã hội và trên các ứng dụng



1. Kiểm tra xem liệu hồ sơ đó có thể là giả không. Tài khoản này có đang hoạt động không? Họ có bao nhiêu người bạn/người theo dõi và họ đăng tải trên mạng nhiều ở mức độ nào?



2. Tìm kiếm tên của hồ sơ đó trên mạng cùng với từ ngữ 'scam' ('lừa đảo').



3. Đừng bao giờ nhận một công việc quý vị được chào mời mà không có cuộc phỏng vấn, hoặc cuộc trao đổi về kinh nghiệm, sự phù hợp của quý vị cho công việc đó, và những người chứng nhận tư cách cho quý vị. Tìm hiểu về người tuyển dụng và doanh nghiệp hoặc cá nhân đang cung cấp vị trí đó. Liên lạc với đại lý tuyển dụng qua các số điện thoại có nguồn từ kết quả tìm kiếm độc lập trên internet. Đừng trả tiền trước chỉ để bảo đảm có được một công việc.



4. Chỉ nhận lời khuyên đầu tư từ ai đó có giấy phép hành nghề của Các Dịch vụ Tài chính của Úc (Australian Financial Services) cấp và kiểm tra xem công ty hoặc trang mạng nào đó có tên trên cổng cảnh báo của Tổ chức Chứng khoán Quốc tế (International Organization of Securities Commission - IOSCO) cho người đầu tư không.



5. Đừng bao giờ đưa tiền cho một người mà quý vị mới chỉ gặp trên mạng thôi. Những kẻ lừa đảo thường nói rằng chúng sống ở nước ngoài và không thể trực tiếp gặp quý vị được.



6. Đừng bao giờ gửi các hình kín đáo của quý vị cho ai đó mà quý vị mới chỉ gặp trên mạng thôi.

Muốn biết thêm thông tin về các trò lừa đảo bao gồm các cách khác mà những kẻ lừa đảo có thể liên lạc với quý vị, như đích thân và bằng thư từ, hãy truy cập trang mạng [Scamwatch](#).



Các trò lừa đảo phổ biến nhất mà quý vị nên biết

Đây là một vài trong số các loại lừa đảo thường gặp nhất để quý vị biết. Quý vị có thể tìm thêm thông tin về từng loại của những loại lừa đảo này, bao gồm các dấu hiệu cảnh báo và các bước để bảo vệ bản thân, trên trang mạng của [Scamwatch](#).

Các trò lừa đảo giả danh

Những kẻ lừa đảo dối trá để quý vị tưởng họ là từ các tổ chức được tin cậy như cảnh sát, chính phủ, ngân hàng, và các doanh nghiệp được nhiều người biết đến. Chúng có thể thậm chí còn giả là bạn bè hoặc người thân trong gia đình của quý vị. Những kẻ lừa đảo tìm kiếm để có thông tin về quý vị bằng cách gửi các thư điện tử hoặc tin nhắn giả mạo. Những thứ này được thiết kế để đánh cắp thông tin của quý vị. Chúng tìm cách thuyết phục để quý vị tin rồi cung cấp cho chúng các thông tin cá nhân, bằng cách giả là chúng từ một tổ chức chính thức hoặc chúng là ai đó mà quý vị biết và tin cậy.

Những kẻ lừa đảo dùng công nghệ để làm cho các cuộc gọi điện thoại hoặc các tin nhắn của chúng có vẻ như đến từ một số điện thoại hợp pháp. Chúng có thể làm cho các tin nhắn văn bản xuất hiện trong cùng chuỗi trò chuyện như các tin nhắn thật từ một tổ chức nào đó.

Các trò lừa đảo về đầu tư

Những kẻ lừa đảo dùng các mảnh khoe tiếp thị có sức thuyết phục và công nghệ mới để làm cho các đề xuất đầu tư nghe tuyệt vời đến mức không thể bỏ qua. Chúng hứa hẹn với quý vị những khoản cổ tức lớn mà ít rủi ro hoặc không có rủi ro. Chúng thường sử dụng các mảnh khoe áp lực để buộc quý vị phải hành động nhanh, sao để chúng có thể đánh cắp tiền của quý vị.

Các trò lừa đảo về công việc và việc làm

Những kẻ lừa đảo đưa ra các công việc trả lương hậu hĩnh mà ít vất vả. Chúng giả là đang thuê mướn người thay mặt cho các công ty nổi tiếng và trên các nền tảng mua sắm trực tuyến. Đôi khi, công việc mà chúng đăng, thậm chí không tồn tại. Những kẻ lừa đảo còn giả là các đại lý tuyển người được nhiều người biết đến. Đích của chúng là đánh cắp tiền và thông tin cá nhân của quý vị. Chúng có thể yêu cầu quý vị trả tiền trước để có thể được làm cho chúng.

Các trò lừa đảo về sản phẩm và dịch vụ

Những kẻ lừa đảo giả là người mua hoặc người bán để đánh cắp tiền của quý vị. Chúng tạo ra các trang mạng hoặc hồ sơ giả trên trang của các nhà kinh doanh lẻ hợp pháp, chào mời các sản phẩm hoặc dịch vụ ở giá hời đến mức khó có thật. Chúng đăng các quảng cáo giả và các nhận xét giả. Chúng có thể sử dụng các biểu trưng, một tên miền .com.au bị ẩn cấp và Số Doanh nghiệp Úc (Australian Business Number - ABN) bị ẩn cấp. Khó phát hiện được các trò lừa đảo này.

Những kẻ lừa đảo còn giả là các doanh nghiệp mà quý vị biết và tin cậy, để gửi cho quý vị các hóa đơn giả. Chúng thậm chí có thể thay đổi các chi tiết trên hóa đơn hợp pháp để khách hàng cuối cùng trả tiền cho kẻ lừa đảo, thay vì trả cho quý vị.

Các trò lừa đảo về yêu đương

Những kẻ lừa đảo dùng lời hứa yêu thương, hẹn hò, hoặc tình bạn để đánh cắp tiền bạc của quý vị. Chúng tìm mọi cách để khiến quý vị tin mỗi quan hệ là thật rồi thao túng quý vị cho chúng tiền.

Những kẻ lừa đảo tìm ra quý vị trên mạng xã hội, các ứng dụng và trang mạng hẹn hò hoặc trò chơi điện tử. Chúng có thể còn nhắn tin hoặc gửi thư điện tử cho quý vị. Chúng ẩn nấp sau các hồ sơ và danh tính giả, đôi khi là của những người nổi tiếng. Sau khi quý vị đã tin cậy chúng, chúng sẽ có 'tình huống khẩn cấp' rồi hỏi xin sự giúp đỡ của quý vị. Đây sẽ thường là các yêu cầu đưa tiền hoặc các sản phẩm khác.

Các trò lừa đảo là các hăm dọa và tổng tiền

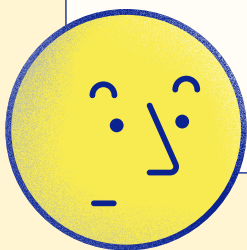
Những kẻ lừa đảo giả là từ một tổ chức được tin cậy và tuyên bố rằng quý vị cần phải trả tiền, bằng không điều gì đó tồi tệ sẽ xảy ra. Chúng có thể hăm dọa quý vị bằng việc bắt giữ, trục xuất, hoặc thậm chí hăm hại thể chất, nếu quý vị không đồng ý trả tiền cho chúng ngay lập tức.

Chúng còn có thể tổng tiền quý vị bằng cách dọa chia sẻ các tấm hình hoặc đoạn phim khỏa thân mà quý vị đã gửi cho chúng, nếu quý vị không gửi tiền cho chúng.

Các trò lừa đảo về món tiền không ngờ tới

Những kẻ lừa đảo tìm cách thuyết phục để quý vị tin là có nơi nợ quý vị tiền hay các kết quả thắng hoặc quý vị có quyền nhận được tiền hoặc kết quả thắng mà quý vị không mong đợi.

Kẻ lừa đảo yêu cầu quý vị trả một khoản phí hoặc cung cấp các chi tiết giao dịch ngân hàng hoặc danh tính trước khi quý vị có thể lấy được món tiền hoặc kết quả thắng đó. Đáng tiếc là không có tiền nào cho không cả.





Tới đâu để trình báo các trò lừa đảo

Chúng tôi đang làm việc để làm cho nước Úc trở thành mục tiêu khó khăn hơn đối với những kẻ lừa đảo, bằng cách nâng cao nhận thức về các cách nhận ra, tránh được, và trình báo các trò lừa đảo.

Chúng tôi chia sẻ thông tin từ các trình báo về trò lừa đảo và làm việc với chính phủ, cơ quan thực thi luật pháp, và khu vực tư nhân để phá vỡ hoạt động và ngăn chặn các trò lừa đảo.

Hãy giúp những người khác bằng cách trình báo với Scamwatch. Hãy trình báo với Scamwatch về trải nghiệm của quý vị về trò lừa đảo, qua mẫu đơn trình báo trên trang mạng của Scamwatch tại địa chỉ www.scamwatch.gov.au

Xin nhớ là, nếu quý vị là nạn nhân của một trò lừa đảo, điều quan trọng là quý vị hành động một cách nhanh chóng.

- Nếu quý vị đã bị mất tiền vào tay một kẻ lừa đảo, hãy liên lạc với ngân hàng hoặc nhà cung cấp thẻ của quý vị.
- Hãy liên lạc với ID CARE: 1800 595 160 | idcare.org



Sự trợ giúp và hỗ trợ thêm

Việc là nạn nhân của trò lừa đảo có thể khiến cảm thấy bị áp đảo. Điều quan trọng cần nhớ là, việc đó có thể xảy ra với bất kỳ ai, và sự hỗ trợ luôn sẵn có.

Nếu quý vị hoặc ai đó mà quý vị biết đã bị lừa gạt, hãy nói chuyện với một người nào đó về sự việc này. Quý vị có thể tìm sự giúp đỡ từ gia đình, bạn bè, GP (Bác sĩ Gia đình) của quý vị hoặc từ một trong các dịch vụ hỗ trợ sau.

Lifeline (Đường dây Giúp Cứu Mạng sống): 13 11 14 | lifeline.org.au
hoặc nhắn tin trực tuyến hỗ trợ trong khủng hoảng (24 giờ hàng ngày, 7 ngày trong tuần)

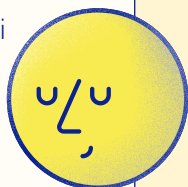
Beyond Blue (Đường dây Hỗ trợ về Sức khỏe Tâm thần): 1300 22 4636 | beyondblue.org.au
hoặc nhắn tin trực tuyến (24 giờ hàng ngày, 7 ngày trong tuần)

Kids Helpline (Đường dây Trợ giúp Dành cho Trẻ em): 1800 55 1800 | kidshelpline.com.au
(24 giờ hàng ngày, 7 ngày trong tuần)

Tác động tài chính do các trò lừa đảo gây ra, có thể là tàn khốc và làm cuộc đời thay đổi.

Nếu đang gặp khó khăn về tài chính, quý vị có thể nói chuyện với một tư vấn viên về tài chính qua **National Debt Helpline (Đường dây Trợ giúp Trên Toàn quốc về Nợ nần):**

1800 007 007 từ 9:30 sáng – 4:30 chiều, từ thứ Hai đến thứ Sáu hoặc vào Trò chuyện Trực tiếp, từ 9 giờ sáng – 8 giờ tối, từ thứ Hai đến thứ Sáu.



scamwatch.gov.au