Tóm tắt trình bày trực tuyến

Australian Government

Be Connected
Every Australian online.

Tự bảo vệ chống lừa đảo

Những kẻ lừa đảo ngày càng tinh vi hơn trong nỗ lực lấy tiền hoặc thông tin cá nhân của quý vị. Lừa đảo nhắm vào mọi người thuộc mọi thành phần, lứa tuổi và mức thu nhập trên khắp nước Úc. Lừa đảo trực tuyến thường được điều hành bởi một người có hồ sơ hoặc doanh nghiệp giả mạo hoặc họ giả vờ đến từ một tổ chức nổi tiếng. Vì vậy, trong khi internet có thể là một nơi tuyệt vời để khám phá, quý vị nên thận trọng! Hãy cảnh giác và tự bảo vệ mình khỏi bị lừa đảo bằng cách làm theo các mẹo của chúng tôi.

Bảo vệ thông tin cá nhân của quý vị

Những kẻ lừa đảo giả vờ đến từ các tổ chức mà quý vị biết và tin tưởng như doanh nghiệp mà quý vị giao dịch, cơ quan chính phủ hoặc dịch vụ chống lừa đảo để cố gắng khiến quý vị tiết lộ thông tin cá nhân và tài chính quan trọng. Họ có thể liên hệ với quý vị qua điện thoại, email, tin nhắn hoặc qua mạng xã hội. Kẻ lừa đảo sẽ sử dụng thông tin cá nhân của quý vị để ăn cắp tiền của quý vị hoặc phạm tội khác.

Để lừa quý vị cung cấp thông tin cá nhân hoặc thông tin tài chính của quý vị, những kẻ lừa đảo có thể yêu cầu quý vị:

- xác minh quý vị là ai hoặc cập nhật thông tin chi tiết của quý vị
- bấm vào một đường liên kết
- cấp cho họ quyền truy cập từ xa vào máy tính của quý vị
- trả nợ
- mua một phiếu để nộp phạt
- yêu cầu quý vị chuyển tiền hoặc gửi tiền ra nước ngoài.

Những dấu hiệu nhận biết lừa đảo

- email, tin nhắn hoặc cuộc gọi bất ngờ hoặc từ người mà quý vị không biết
- những lời hứa về lợi ích tài chính
- những đe dọa về tiền phạt hoặc nợ nần
- những đe dọa đóng hoặc khóa tài khoản của quý vị
- những liên kết trông không thật, ví dụ: địa chỉ trang mạng khác thường
- có cảm giác nguy cấp hoặc thời hạn thực hiện bất thường.

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.

Tự bảo vệ ra sao

- Hãy cảnh giác với thực tế là có tồn tại những trò lừa đảo và luôn xem xét khả năng một tin nhắn, email hoặc cuộc gọi điện thoại có thể là một trò lừa đảo.
- Biết quý vị đang giao dịch với ai. Nếu quý vị không chắc liệu một tin nhắn hoặc cuộc gọi có phải là thật hay không, đừng sử dụng chi tiết liên hệ đã cung cấp, thay vào đó hãy tìm kiếm trên internet số điện thoại hoặc địa chỉ email của tổ chức.
- Không cung cấp thông tin tài chính cá nhân.
- Không mở các văn bản đáng ngờ, cửa sổ bật lên hoặc nhấp vào liên kết hoặc tập tin đính kèm trong email – hãy xóa chúng.
- Không trả lời các cuộc gọi điện thoại về việc yêu cầu quyền truy cập từ xa máy tính của quý vị – gác máy – ngay cả khi họ đề cập đến một công ty nổi tiếng như Telstra.

Cẩn thận khi kết bạn qua mạng

Những kẻ lừa đảo liên hệ với mọi người, thường là qua mạng xã hội, trang mạng hẹn hò hoặc thậm chí qua trò chơi trực tuyến. Họ sẽ rất thân thiện, thú vị và muốn xây dựng tình bạn hoặc mối quan hệ với quý vị. Những kẻ lừa đảo có thể kiên nhẫn một cách đáng ngạc nhiên. Mối quan hệ giả tạo có thể tiếp tục trong nhiều tuần, hoặc thậm chí một năm, để họ có thể chiếm được lòng tin của quý vị và yêu cầu quý vị cung cấp tiền, thông tin cá nhân, hình ảnh thân mật hoặc lừa quý vị làm điều gì đó bất hợp pháp.

Những dấu hiệu nhận biết lừa đảo

Coi chừng những người:

- thể hiện tình cảm sâu sắc một cách nhanh chóng và liên lạc với quý vị thường xuyên
- không thể gặp trực tiếp hoặc yêu cầu tiền cho chuyến đi để họ có thể đi gặp quý vị
- cố chuyển quý vị ra khỏi phần mềm hoặc ứng dụng mà quý vị đã gặp để chuyển sang một kênh liên lạc riêng tư hơn, chẳng hạn như nhắn tin trực tiếp hoặc gửi email
- tuyên bố là ổn định về tài chính nhưng yêu cầu quý vị cho tiền
- kể cho quý vị những câu chuyện phức tạp về những rắc rối tài chính
- hỏi về tình trạng tài chính của quý vị
- trở nên đeo bám, trực diện hơn hoặc thậm chí hung tợn hơn khi quý vị không gửi tiền
- dường như có sự mâu thuẫn trong các câu chuyện và hồ sơ trực tuyến của họ – ví dụ: ảnh của họ trông khác với mô tả của họ
- mắc lỗi chính tả và ngữ pháp
- cho quý vị biết họ đang làm việc ở nước ngoài (ví dụ: nhân viên cứu trợ hoặc làm việc trong quân đội).

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 để giúp xác định xem họ có thực sự là người mà họ nói không. 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, sự mâu thuẫn trong câu chuyện của họ.
- Không đồng ý mang vác những gói hàng quốc tế hoặc chuyển tiền cho người khác, vì quý vị có thể đang phạm tội mà không biết.
- 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 tài liệu gây tổn hại nếu tiết lộ.
- Dừng mọi liên lạc nếu người đó bắt đầu nhờ quý vị giúp đỡ hoặc xin tiền.
- Tránh mọi thỏa thuận với người lạ yêu cầu thanh toán qua chuyển tiền, chuyển khoản ngân hàng, chuyển tiền quốc tế, thẻ nạp sẵn hoặc tiền điện tử, như Bitcoin. Rất hiếm khi lấy lại tiền được gửi theo cách này.

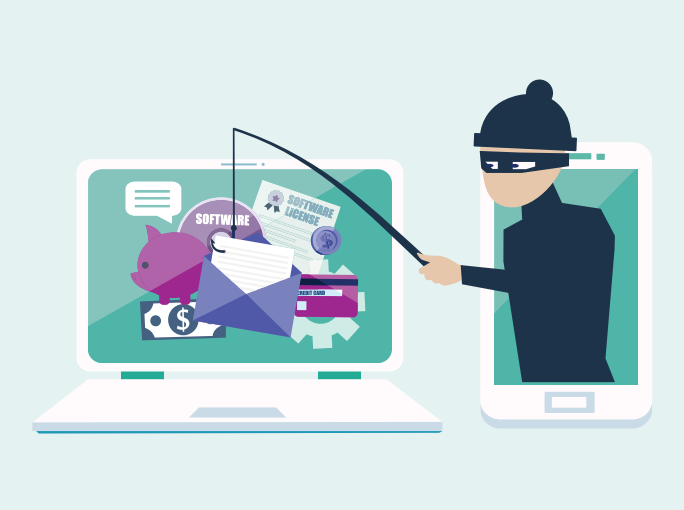
Coi chừng các lừa đảo đầu tư

Lừa đảo đầu tư liên quan đến những lời hứa về khoản thanh toán lớn, tiền lời nhanh chóng hoặc lợi nhuận được đảm bảo. Luôn nghi ngờ về bất kỳ cơ hội đầu tư nào hứa hẹn lợi nhuận cao với ít rủi ro hoặc không có rủi ro.

Người Úc mất nhiều tiền hơn cho các vụ lừa đảo đầu tư hơn bất kỳ vụ lừa đảo nào khác. Có thể khó phát hiện ra chúng, vì những kẻ lừa đảo đã nỗ lực rất nhiều để tạo ra những câu chuyện thuyết phục và tạo ra các trang mạng và tài liệu quảng cáo chuyên nghiệp. Trước khi đầu tư, hãy luôn tìm kiếm lời khuyên pháp lý hoặc tư vấn tài chính độc lập từ một cố vấn tài chính có đăng ký với Ủy ban Chứng khoán và Đầu tư Úc (ASIC)

Một số cách phổ biến nhất mà lừa đảo đầu tư có thể hoạt động bao gồm:

- liên hệ với quý vị qua email hoặc điện thoại với cơ hội đặc biệt để nhận được tiền hoàn trả nhanh chóng hoặc được đảm bảo
- sử dụng xác nhận giả của người nổi tiếng để lừa đảo có vẻ hợp pháp
- thuyết phục quý vị nhận tiền hưu sớm hoặc nhận một lần
- các hội thảo đầu tư (thường qua video trực tuyến, Zoom hoặc tương tự) miễn phí hoặc tính phí tham dự cao.



Tiền hưu bổng

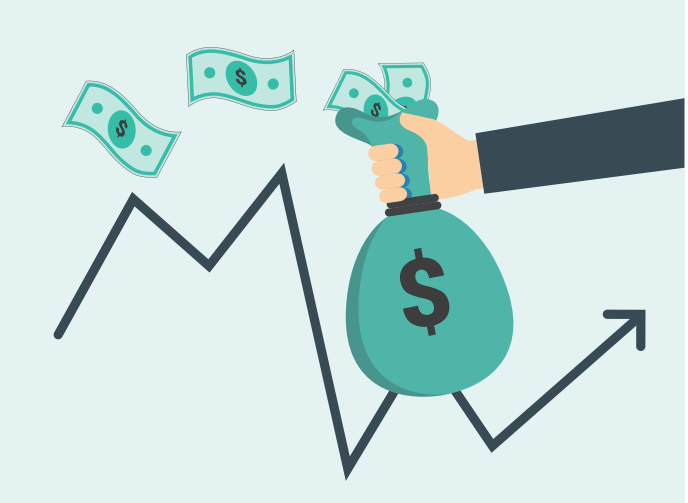
Lừa đảo tiền hưu bổng đề nghị cung cấp cho quý vị quyền truy cập sớm vào quỹ hưu bổng của mình, thường thông qua quỹ hưu bổng tự quản lý hoặc có tính phí. Lời đề nghị có thể đến từ một kẻ lừa đảo giả làm cố vấn tài chính.

Họ có thể yêu cầu quý vị đồng ý với một câu chuyện để đảm bảo tiền của quý vị được trả sớm và sau đó, đóng vai trò là cố vấn tài chính của quý vị, họ lừa dối công ty hưu bổng của quý vị thanh toán trực tiếp các khoản trợ cấp hưu bổng của quý vị cho họ. Khi lấy được tiền của quý vị, kẻ lừa đảo có thể thu số tiền 'phí' lớn từ số tiền được trả hoặc không để lại cho quý vị một chút tiền nào.

Lưu ý: Thông thường, quý vị không thể sử dụng hợp pháp phần hưu bổng được bảo toàn của mình cho đến khi quý vị ở độ tuổi từ 55 đến 60, tùy thuộc vào năm sinh của quý vị. Có một số ngoại lệ nhất định như túng quẫn tài chính nghiêm trọng hoặc các lý do thương cảm - nhưng bất cứ ai đề nghị trả sớm tiền hưu bổng của quý vị đều đang hành động bất hợp pháp. Để biết thêm thông tin, hãy truy cập: moneysmart.gov.au/how-super-works/superannuation-scams

Chia sẻ các chương trình khuyến mãi và mẹo hay

Những kẻ lừa đảo có thể liên hệ với quý vị qua email, phương tiện truyền thông xã hội hoặc đăng một tin nhắn trong một diễn đàn để khuyến khích quý vị mua cổ phiếu của một công ty mà chúng dự đoán là sắp tăng giá trị. Thông báo giống như một mẹo trong đó và thường sẽ nhấn mạnh rằng quý vị cần phải hành động nhanh chóng. Kẻ lừa đảo đang cố thuyết phục quý vị mua cổ phiếu để tăng giá cổ phiếu để họ có thể bán cổ phiếu mà họ đã mua và kiếm được lợi nhuận khổng lồ. Giá trị cổ phiếu sau đó sẽ giảm xuống đáng kể.



Lừa đảo được bảo chứng bởi người nổi tiếng

Những kẻ lừa đảo sử dụng hình ảnh, tên và đặc điểm cá nhân của những người nổi tiếng mà không có sự cho phép của họ để lôi kéo quý vị đầu tư vì nó được hỗ trợ bởi người mà quý vị tin tưởng. Những trò gian lận này thường xuất hiện dưới dạng quảng cáo trực tuyến hoặc câu chuyện quảng cáo đăng trên truyền thông xã hội hoặc các trang mạng có vẻ hợp pháp, đáng tin cậy.

Dấu hiệu cảnh báo lừa đảo đầu tư

Quý vị được liên lạc bất ngờ qua cuộc gọi điện thoại, tin nhắn, email hoặc tin nhắn mạng xã hội từ một người nào đó đưa ra lời khuyên đầu tư không mong muốn và họ:

- sử dụng các chiến thuật gây áp lực cao, bao gồm liên hệ với quý vị nhiều lần và gây áp lực buộc quý vị phải đưa ra quyết định nhanh chóng.
- hứa hẹn rủi ro thấp với lợi nhuận cao hoặc được đảm bảo.
- không có giấy phép dịch vụ tài chính Úc (AFS) hoặc nói rằng họ không cần.
- có bản thông báo đầu tư chưa được đăng ký với ASIC.
- sử dụng xác nhận hoặc hình ảnh của người nổi tiếng: Đây thường là giả mạo. Những người nổi tiếng hiếm khi thảo luận về các khoản đầu tư hoặc quyết định tài chính của họ trước công chúng.
- hướng quý vị đến một trang mạng giả mạo.
- cố gắng ngăn quý vị rút khỏi thỏa thuận.

Tự bảo vệ ra sao

- Hãy nghi ngờ những cơ hội có vẻ quá tốt để trở thành sự thật.
- Cảnh giác với những quảng cáo hoặc câu chuyện được bảo chứng bởi những người nổi tiếng.
- Đừng để ai gây áp lực lên quý vị.
- Nếu quý vị dưới 55 tuổi, hãy coi chừng những đề nghị chào mời dễ dàng tiếp cận các khoản trợ cấp hưu bổng.
- Tự nghiên cứu và tìm kiếm tư vấn tài chính hoặc pháp lý tin cậy hoặc độc lập.
- Không cung cấp thông tin cá nhân hoặc tài chính cho đến khi:
  - quý vị đã kiểm tra xem cố vấn tài chính và công ty của họ đã được đăng ký qua trang mạng ASIC chưa asic.gov.au/online-services/search-asic-s-registers/
  - quý vị đã kiểm tra danh sách của ASIC về các công ty không nên giao dịch moneysmart.gov.au/scams/companies-you-should-not-deal-with

Mẹo hàng đầu để tránh lừa đảo

Dừng lại

- Hãy dành thời gian 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 đến 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 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 hỏi một người quý vị đáng tin cậy hoặc thành viên gia đình 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 đi.

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 với 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.
- Phổ biến thông tin 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.