Tự bảo vệ chống lừa đảo

Lừa đảo là một hành động không trung thực hoặc phạm pháp nhằm lừa người khác đưa tiền, thông tin cá nhân, hình ảnh thân mật hoặc vật có giá trị khác. Lừa đảo trực tuyến thường do người có hồ sơ giả mạo hoặc doanh nghiệp giả mạo thực hiện. Vì vậy, mặc dù internet có thể là nơi tuyệt vời để khám phá, quý vị cần thận trọng!

Nhận biết về những kẻ lừa đảo là một trong những bước quan trọng để tránh chúng. Một khi biết các thủ đoạn của chúng, quý vị dường như có thể phát hiện ra lừa đảo. Giữ tỉnh táo là sự bảo vệ tốt nhất của quý vị.

Dưới đây là một số mẹo hàng đầu để nhận biết và tránh lừa đảo.

Bảo vệ thông tin cá nhân của quý vị

Kẻ lừa đảo tìm cách truy cập thông tin cá nhân của quý vị bằng cách hỏi quý vị hoặc hướng dẫn cho quý vị thông qua điện thoại, email, tin nhắn hoặc truyền thông 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.

Kẻ lừa đảo yêu cầu gì?

Kẻ lừa đảo tìm cách chiếm được lòng tin của quý vị bằng cách giả vờ đến từ một tổ chức hoặc cơ quan nổi tiếng như NBN Co, Telstra, Microsoft, Australia Post, sở thuế vụ, cảnh sát hoặc Services Australia (MyGov, Centrelink, Medicare).

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

- khiến quý vị nhấp vào một liên kết
- yêu cầu quý vị cho họ quyền truy cập từ xa vào máy tính của quý vị
- yêu cầu quý vị trả một khoản nợ
- yêu cầu quý vị mua một phiếu trả tiền phạt
- yêu cầu quý vị chuyển tiền hoặc gửi tiền ra nước ngoài.

Những dấu hiệu nhận biết lừa đảo

Coi chừng:

- những email, tin nhắn hoặc cuộc gọi bất ngờ hoặc từ người quý vị không quen 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.

Mẹo: Nếu không chắc chắn tin nhắn hay cuộc gọi đó là thật hay giả, quý vị đừng sử dụng các chi tiết liên lạc được cung cấp, mà hãy tìm trên internet số liên lạc hoặc địa chỉ email của tổ chức đó.

Cẩn thận với những người quý vị kết bạn trên trực tuyến

Kẻ lừa đảo trực tuyến thường liên lạc với người khác qua truyền thông xã hội. Chúng dùng chiêu lừa đảo tình cảm hoặc hẹn hò. Chúng cũng nhắm đến những người chơi các trò chơi trực tuyến như Words with Friends và Scrabble. Mục tiêu của chúng là xây dựng mối quan hệ (không nhất thiết phải là tình cảm) để chiếm được lòng tin của quý vị để rồi hỏi quý vị về tiền, thông tin cá nhân, hình ảnh thân mật hoặc vật có giá trị khác.

Những dấu hiệu nhận biết lừa đảo

Coi chừng những người:

- nhanh chóng thể hiện tình cảm sâu sắc
- tìm cách đưa câu chuyện của quý vị từ trang mạng nơi quý vị gặp họ sang một kênh giao tiếp riêng tư hơn, như nhắn tin hoặc gửi email trực tiếp
- kể cho quý vị những câu chuyện phức tạp về những rắc rối tài chính
- nói rằng họ muốn gặp quý vị nhưng đưa ra những lý do không thể thực hiện, hoặc bảo quý vị đưa tiền để họ có thể 'đi' gặp quý vị
- 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
- hồ sơ trực tuyến của họ dường như không nhất quán - ví dụ, ảnh của họ trông khác với mô tả, hoặc họ nói rằng họ học đại học nhưng lại kém ngữ pháp.

Ngoài ra, cũng phổ biến là kẻ lừa đảo nhận là nhân viên cứu tế hoặc quân nhân hoặc chuyên gia làm việc ở nước ngoài.

Mẹo: Tìm kiếm hình ảnh trên một vài trang mạng như Google (images.google.com) hoặc Tineye (tineye.com), để kiểm tra xem họ có đúng như họ nói không

Tự bảo vệ ra sao

- Không cung cấp thông tin cá nhân hoặc tài chính cho những người quý vị chưa từng gặp trực tiếp.
- Không thực hiện thanh toán bất cứ khoản tiền nào bằng lệnh chuyển tiền, chuyển khoản, chuyển tiền quốc tế hoặc tiền điện tử như bitcoin. (Khó có thể lấy lại tiền chuyển đi theo cách này nếu sau này phát hiện là lừa đảo.)
- 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 thân mật hoặc dùng webcam trong một khung cảnh thân mật.
- Dừng mọi liên lạc nếu người đó bắt đầu nhờ quý vị giúp đỡ hoặc xin tiền.
- Cảnh giác với lỗi chính tả, ngữ pháp kém và sự không nhất quán trong câu chuyện của họ.

Coi chừng lừa đảo đầu tư

Những kẻ lừa đảo đầu tư dành rất nhiều thời gian, công sức và tiền bạc tạo nên những câu chuyện thuyết phục, những trang mạng lạ mắt và các tờ rơi quảng cáo để lừa đảo những người Úc lớn tuổi đang muốn phát triển 'trứng yến' hoặc tiền tiết kiệm của mình.

Làm thế nào kẻ lừa đảo khiến quý vị quan tâm?

Dưới đây là một số phương pháp đầu tư kẻ lừa đảo sử dụng:

- Chúng dẫn quý vị đến một trang mạng giả mạo, tuyên bố sai về những khoản đầu tư có hiệu suất và lợi nhuận rất tốt.
- Chúng đăng quảng cáo hoặc bài viết trên mạng xã hội như Facebook.
- Chúng gửi yêu cầu 'kết bạn' với quý vị trên truyền thông xã hội bằng cách tự nhận là người quý vị biết hoặc có kết nối, để truy cập thông tin hồ sơ của quý vị và gửi cho quý vị lời đề nghị đầu tư phù hợp.

Những dấu hiệu nhận biết lừa đảo

- Kẻ lừa đảo liên tục gọi điện hoặc gửi email cho quý vị.
- Chúng cho quý vị nói chuyện với nhiều người khác nhau - lúc đầu một người cấp thấp nói chuyện với quý vị, sau đó là người cao cấp hơn để cố gắng đóng giao dịch.
- Chúng gây sức ép buộc quý vị phải hành động nhanh chóng nếu không quý vị sẽ bị lỡ cơ hội.
- Chúng nói rằng chúng không có giấy phép dịch vụ tài chính Úc (AFS) hoặc không cần giấy phép đó
- Chúng cố gắng ngăn không cho quý vị rút khỏi giao dịch đó.

Tiền hưu bổng

Kẻ lừa đảo đầu tư đưa ra những cách nhanh chóng và dễ dàng 'giải phóng' sớm tiền hưu bổng của quý vị. Chúng có thể yêu cầu quý vị đồng ý với một câu chuyện để đảm bảo giải phóng sớm tiền của quý vị, sau đó với vai trò cố vấn tài chính cho quý vị, chúng lừa dối công ty hưu bổng trả trực tiếp cho chúng tiền hưu bổng của quý vị.

Khi lấy được tiền của quý vị, kẻ lừa đảo có thể thu số tiền 'phí' lớn từ số tiền được giải phóng hoặc không để lại cho quý vị một tí gì cả.

Ghi chú! Thông thường, theo pháp luật quý vị không thể truy cập phần tiền hưu bổng bị phong toả cho đến khi quý vị từ 55 đến 60 tuổi, tùy thuộc quý vị sinh năm nào. 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 giải phóng sớm tiền hưu bổng của quý vị đều đang hành động bất hợp pháp.

Tăng giả tạo giá cổ phiếu

Kẻ lừa đảo đầu tư mua cổ phiếu một công ty nhỏ ở mức giá thấp, sau đó đưa ra các lời khuyên sai trái rằng công ty có triển vọng lớn. Khi nhiều người đầu tư vào công ty, giá cổ phiếu tăng lên và kẻ lừa đảo bán ra cổ phiếu của chúng khi giá tăng lên cao nhất. Sau đó, giá cổ phiếu giảm và các cổ đông còn lại nắm giữ chúng ở mức giá sụt giảm.

Lừa đảo được bảo chứng bởi người nổi tiếng

Kẻ lừa đảo đầu tư giả mạo được bảo chứng bởi các doanh nhân thành công và được kính trọng hoặc những người nổi tiếng nhằm khiến người khác tin là giao dịch đó được bảo chứng bởi người họ tin tưởng. Những lừa đảo này thường xuất hiện dưới dạng các câu chuyện quảng cáo hoặc khuyến mại trực tuyến hoặc các dòng truyền thông xã hội hoặc các trang mạng trông có vẻ hợp pháp, tin cậy.

Tự bảo vệ ra sao

- Cảnh giác với những cơ hội có vẻ tốt đến mức không tưởng.
- 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, coi chừng những đề nghị về việc truy cập dễ dàng tiền 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 có đăng ký hay không thông qua trang mạng ASIC asic.gov.au/online-services/search-asics-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.

Giúp với, tôi nghi ngờ tôi 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. Quý vị có thể thực hiện một số bước để giải quyết vấn đề này:

- Liên lạc với ngân hàng của quý vị để dừng mọi khoản thanh toán tiếp theo cho kẻ lừa đảo.
- Liên lạc với ID Care idcare.org nếu thông tin cá nhân của quý vị bị xâm phạm hoặc sử dụng sai.
- Đối với mọi lừa đảo về Medicare, Centrelink hoặc myGov, hãy gọi Services Australia số 1800 941 126 hoặc email reportascam@servicesaustralia.gov.au.
- Trình báo vụ lừa đảo lên Ủy ban Cạnh tranh và Người tiêu dùng Úc tại scamwatch.gov.au để họ có thể tư vấn cho những người khác cách tránh nó.

Để được cập nhật về những gian lận mới nhất cần tránh, hãy đăng ký email cảnh báo Scamwatch scamwatch.gov.au/news/subscribe-to-scam-alert-emails

Dành thời gian tìm hiểu về Be Connected

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

beconnected.esafety.gov.au