AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Sổ Bìa Đen Trò lừa đảo

Tài liệu hướng dẫn loại bỏ túi để giúp quý vị có thể nhận ra, tránh những trò lừa đảo và bảo vệ bản thân

Sổ Bìa Đen Trò lừa đảo

Tài liệu hướng dẫn loại bỏ túi để giúp quý vị có thể nhận ra, tránh những trò lừa đảo và bảo vệ bản thân

ISBN 978 1 920702 00 7

Ủy hội Đặc trách Cạnh tranh và Người tiêu thụ Úc (Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129

www.accc.gov.au

Mục lục

Phần giới thiệu

Mỗi năm, những trò lừa đảo gây thiệt hại cho người Úc, doanh nghiệp và nền kinh tế hàng trăm triệu đô-la và gây tổn hại về mặt cảm xúc cho nạn nhân và gia đình họ.

Cách tốt nhất để bảo vệ chính quý vị là nhận thức và giáo dục. Ấn bản Sổ Bìa Đen Trò Lừa đảo *(The Little Black Book of Scams)* mới này do Ủy hội Đặc trách Cạnh tranh và Người tiêu thụ Úc (ACCC-Australian Competition and Consumer Commission), cơ quan bảo vệ người tiêu thụ toàn quốc cống hiến cho quý vị. Sổ Bìa Đen Trò Lừa đảo được quốc tế công nhận là công cụ quan trọng để người tiêu thụ và doanh nghiệp nhỏ tìm hiểu về những trò lừa đảo bao gồm:

- những trò lừa đảo phổ biến nhất để đề phòng
- những cách khác nhau mà bọn lừa đảo có thể tiếp xúc với quý vị
- những công cụ bọn lừa đảo sử dụng để lừa quý vị
- các dấu hiệu cảnh báo
- cách tự bảo vệ bản thân và
- quý vị có thể tìm sự giúp đỡ ở đâu.

Tại trang mạng www.accc.gov.au/littleblackbookofscams có *Sổ Bìa Đen Trò Lừa đảo*.

Tự bảo vệ bản thân— đăng ký với Scamwatch

Hãy đi trước bọn lừa đảo một bước, truy cập trang mạng Scamwatch—www.scamwatch.gov.au—của ACCC để tìm hiểu thêm, tại đây quý vị có thể đăng ký để nhận được các thông báo cảnh báo qua email miễn phí về những trò lừa đảo mới nhắm vào người tiêu thụ và doanh nghiệp nhỏ. Quý vị cũng có thể theo Scamwatch trên Twitter tại @scamwatch_gov hay http://twitter.com/scamwatch_gov.

Những trò lừa đảo hàng đầu cần tránh

Mọi người đều dễ bị lừa đảo vì vậy mọi người cần biết thông tin về cách nhận ra và tránh bị lừa đảo. Một số người nghĩ rằng chỉ có người cả tin và tham lam mới bị lừa đảo. Sự thật là bọn lừa đảo rất thông minh và nếu quý vị không biết phải để ý điều gì, bất kỳ ai cũng có thể bị lừa đảo.

Quý vị có từng nhận được lời đề nghị tốt đến mức khó tin là thật hay không, có lẽ là cuộc gọi điện thoại để giúp sửa máy vi tính của quý vị hoặc đe dọa đòi quý vị trả tiền nợ quý vị không thiếu, một cảnh báo từ ngân hàng hoặc công ty viễn thông về vấn đề liên quan đến tài khoản của quý vị hoặc thậm chí lời mời 'kết bạn' hoặc kết nối trực tuyến? Bọn lừa đảo biết những điểm yếu của quý vị để có đạt được những gì họ muốn.

Bọn họ ngày càng thông minh hơn, thay đổi theo thời thế để tận dụng công nghệ mới, sản phẩm hoặc dịch vụ mới và các sự kiện lớn để tạo ra những câu chuyện đáng tin nhằm thuyết phục quý vị chi tiền hoặc cho biết chi tiết cá nhân của quý vị.

Tuy nhiên, nhờ hàng chục ngàn báo cáo lừa đảo nhận được mỗi năm, ACCC đã soạn danh sách các trò lừa đảo phổ biến để tiết lộ những bí mật và mánh lới mà bọn lừa đảo không muốn quý vị biết.

Trò lừa đảo hẹn hò và ái tình

Trò lừa đảo hẹn hò và ái tình khiến người Úc tốn hàng triệu đô-la mỗi năm và có thể hủy hoại các cá nhân và gia đình.

Cách thức lừa đảo là như thế nào

Bọn lừa đảo **hẹn hò và ái tình** lập hồ sơ giả mạo trên các trang mạng hẹn hò hợp pháp, ứng dụng di động hoặc hình thức truyền thông xã hội như Facebook bằng các ảnh chụp và danh tính thường là những thứ đánh cắp của người khác. Bọn chúng sử dụng những hồ sơ này để tìm cách lập mối quan hệ với quý vị, có thể kéo dài trong nhiều tháng hoặc thậm chí nhiều năm, để bọn chúng có thể lấy tiền của quý vị. Kẻ lừa đảo sẽ xin quý vị cho họ tiền vì họ bị bệnh tật, thương tích, chi phí đi lại hoặc khủng hoảng gia đình. Họ là người vô lương tâm và sẽ nói dối để lợi dụng lòng tử tế của quý vị.

Bọn lừa đảo thường là ở nước ngoài và lấy cớ tại sao họ lại ở đó, chẳng hạn như đi lính, đi làm công việc kỹ sư hoặc chăm sóc bạn bè hoặc người thân. Họ không bao giờ thực sự là người họ tự nhận và một số kẻ lừa đảo xảo quyệt thậm chí có thể gửi những món quà nhỏ. Đây chỉ là một phần trong kế hoạch lớn của bọn chúng để lấy thêm nhiều tiền của quý vị hơn về sau này.

Tự bảo vệ bản thân

- Đừng bao giờ gửi tiền hoặc cung cấp thông tin cá nhân của quý vị cho người quý vị chỉ gặp trên mạng Internet (trực tuyến).
- Coi chừng nếu một người ái mộ trực tuyến yêu cầu giao tiếp bên ngoài trang mạng hẹn hò hoặc hình thức phương tiện truyền thông xã hội chỉ sau một vài lần 'liên lạc' hoặc cuộc trò chuyện, người này có thể là kẻ lừa đảo.
- Thực hiện việc tìm kiếm hình ảnh của người ái mộ quý vị để giúp xác định xem họ có thực sự là người họ tự nhận hay không. Quý vị có thể sử dụng các dịch vụ tìm kiếm hình ảnh như Google hoặc TinEye.
- Hãy thận trọng khi chia sẻ hình ảnh hoặc video thân mật trực tuyến. Được biết bọn lừa đảo sẽ tống tiền các đối tượng của chúng bằng hình ảnh hoặc video về quý vị mà quý vị không muốn ai khác nhìn thấy.

Trò lừa đảo đầu tư

'Đầu tư không rủi ro' hay cơ hội bất hạnh?

Cách thức lừa đảo là như thế nào

Trò lừa đảo đầu tư (Investment scams) có nhiều hình thức bao gồm mua tiền điện tử, giao dịch quyền chọn nhị phân, liên doanh kinh doanh, kế hoạch hưu bổng, quỹ được quản lý và bán hoặc mua cổ phiếu hoặc bất động sản. Bọn lừa đảo tô vẽ 'những cơ hội' này bằng các tài liệu quảng cáo và trang mạng chuyên nghiệp để che giấu các hoạt động gian lận của bọn chúng. Trò lừa đảo này thường bắt đầu bằng kẻ lừa đảo gọi điện thoại hoặc gửi email bất ngờ đề nghị cơ hội 'không thể bỏ qua', 'lợi nhuận cao' hoặc 'được bảo đảm'. Kẻ lừa đảo thường hoạt động ở nước ngoài và sẽ không có giấy phép Dịch vụ Tài chính Úc (Australian Financial Services licence).

Trò lừa đảo phần mềm máy vi tính tiên đoán (Computer prediction software scams) hứa sẽ tiên đoán chính xác diễn biến thị trường chứng khoán, kết quả các cuộc đua ngựa, các sự kiện thể thao hoặc xổ số. Chúng chỉ đơn giản là hình thức đánh bạc được ngụy trang thành các khoản đầu tư. Hầu hết các kế hoạch hoặc chương trình này đều vô dụng và người mua không thể lấy lại tiền. Trong nhiều trường hợp, nhà cung cấp chỉ đơn giản biến mất.

Trò lừa đảo hưu bổng (Superannuation scams) đề nghị cung cấp cho quý vị quyền rút hưu bổng của quý vị sớm, thường thông qua quỹ hưu bổng tự quản lý hoặc có tính lệ phí. Kẻ lừa đảo có thể yêu cầu quý vị đồng ý về một câu chuyện nào đó để quý vị được phép rút hưu bổng sớm và sau đó, với tư cách là cố vấn tài chính của quý vị, họ sẽ lừa công ty hưu bổng của quý vị trả hưu bổng của quý vị thẳng cho họ. Một khi tiền của quý vị đã vào túi chúng, kẻ lừa đảo có thể trừ 'lệ phí' lớn hoặc không để lại cho quý vị một cắc nào hết.

Tự bảo vệ bản thân

- Đừng để bất cứ ai gây áp lực khiến quý vị quyết định về tiền bạc hoặc khoản đầu tư của mình—đặc biệt là nếu lời đề nghị đến với quý vị bất ngờ.
- Trước khi chi tiền, quý vị hãy tự nghiên cứu về công ty đầu tư và kiểm tra www.moneysmart.gov.au để xem họ có Giấy phép Dịch vụ Tài chính của Úc không. Hãy tự hỏi: nếu một người lạ biết bí quyết để kiếm tiền, tại sao họ lại chia sẻ điều đó?

Nếu chưa đến tuổi nghỉ hưu, quý vị hãy coi chừng những lời đề nghị quảng bá dễ dàng rút tiền hưu bổng được bảo tồn của quý vị (your preserved superannuation benefits). Nếu quý vị rút tiền hưu bổng sớm trái phép, quý vị có thể phải gánh chịu các hình phạt theo luật thuế.

Trò lừa đảo kiểu đe dọa và biện pháp phạt

Nếu cơ quan chính phủ hoặc công ty đáng tin cậy nói quý vị phải giải quyết, quý vị hãy dừng lại, suy nghĩ và kiểm tra kỹ.

Cách thức lừa đảo là như thế nào

Thay vì đề nghị giải thưởng, tiền hoặc giảm giá, những trò lừa đảo này sử dụng các mối đe dọa với dụng ý làm cho quý vị sợ hãi rồi giao tiền của quý vị cho kẻ lừa đảo. Kẻ lừa đảo có thể gọi điện cho quý vị và đe dọa quý vị **sẽ bị bắt** hoặc gửi email cho quý vị nói rằng quý vị nợ tiền vì **bị phạt lái xe quá tốc độ, nợ sở thuế** hoặc **hóa đơn chưa thanh toán**.

Trong cuộc gọi điện thoại, bọn lừa đảo sẽ ép quý vị trả tiền ngay và cho quý vị biết cảnh sát sẽ được phái đến nhà quý vị nếu quý vị từ chối. Được biết bọn lừa đảo nhắm vào những người dễ bị thiệt thòi trong cộng đồng chúng ta, chẳng hạn như di dân mới đến. Họ giả vờ là viên chức Bộ Di trú và đe dọa các nạn nhân sẽ **bị trục xuất** trừ khi họ trả các khoản phí để sửa lỗi trong thị thực của họ. Trong một trò lừa đảo rất giống trò lừa đảo này, kẻ lừa đảo giả danh Sở Thuế Úc nói với nạn nhân rằng họ có hóa đơn thuế chưa thanh toán.

Bọn lừa đảo cũng giả vờ là **công ty đáng tin cậy** chẳng hạn như ngân hàng, công ty ga, điện, nước hoặc công ty điện thoại của quý vị. Họ sẽ đe dọa cắt dịch vụ của quý vị hoặc tính lệ phí phạt rất cao nếu quý vị không thanh toán hóa đơn ngay. Đôi khi, họ có thể mạo danh doanh nghiệp như Australia Post nói rằng quý vị có món hàng đợi quý vị đến nhận hoặc quý vị sẽ phải trả khoản lệ phí giữ món hàng mỗi ngày quý vị không trả tiền. Dù thế nào đi nữa, bọn chúng tìm cách làm cho quý vị lo lắng và hành động mà không có thời gian dừng lại để suy nghĩ và kiểm tra xem câu chuyện họ nói có đúng hay không.

Nếu trò lừa đảo được gửi qua email, rất có thể sẽ có tệp đính kèm hoặc dòng liên kết đến trang mạng giả mạo, tại đây quý vị sẽ được yêu cầu tải xuống bằng chứng 'hóa đơn', 'giấy phạt' hoặc 'chi tiết giao hàng'. Khi mở tệp đính kèm ra hoặc tải xuống tệp đính kèm, phần mềm độc hại sẽ xâm nhập máy vi tính của quý vị (xin đọc ở trang 16).

Tự bảo vệ bản thân

- Đừng để người gọi điện thoại có tính cách đe dọa gây áp lực lên quý vị. Hãy dừng lại, suy nghĩ và kiểm tra xem câu chuyện của họ có đúng hay không.
- Cơ quan chính phủ hoặc công ty đáng tin cậy sẽ không bao giờ yêu cầu quý vị thanh toán bằng các hình thức khác thường như thẻ tặng (gift card), điện chuyển khoản ngân hàng (wire transfers) hoặc Bitcoin.
- Hãy xác minh danh tính người liên lạc bằng cách gọi điện thẳng cho tổ chức liên quan—hãy tìm họ thông qua nguồn độc lập như niên giám điện thoại, hóa đơn cũ hoặc tìm trên mạng (trực tuyến).
- Đừng sử dụng chi tiết liên lạc được cung cấp trong email hoặc quý vị được cung cấp trong cuộc gọi điện thoại. Một lần nữa, hãy tìm chi tiết này thông qua nguồn độc lập.

Trò lừa đảo tiền bạc bất ngờ

Nếu được yêu cầu trả tiền trước khi nhận hàng hóa hoặc tiền, quý vị hãy suy nghĩ kỹ.

Cách thức lừa đảo là như thế nào

Bọn lừa đảo nói với quý vị rằng quý vị có quyền nhận tiền, đá quý, vàng hoặc cổ phiếu có giá trị nhưng quý vị cần phải **trả tiền trước (upfront payments)** để nhận được những món này. Quý vị sẽ không bao giờ nhận được những gì đã hứa và sẽ luôn có lý do vì sao quý vị phải trả nhiều tiền hơn. Nếu trả lệ phí, quý vị sẽ bị mất tiền.

Các trò lừa đảo hoàn tiền hoặc đòi lại tiền (Rebate or reclaim scams) liên quan đến kẻ lừa đảo nói với quý vị rằng họ nợ quý vị tiền vì những lý do như thuế trả dư, lệ phí ngân hàng hoặc tiền bồi thường gì đó. Tuy nhiên, trước khi có thể nhận được tiền của mình, quý vị phải trả một ít chi phí hành chính.

Với **trò lừa đảo thừa kế (inheritance scams)**, bọn lừa đảo giả làm luật sư, nhân viên ngân hàng hoặc viên chức nước ngoài và nói với quý vị rằng quý vị có quyền hưởng gia tài kết sù hoặc đề nghị quý vị hưởng một phần trong một kế hoạch nào đó vì quý vị có cùng tên với người quá cố. Họ thường sử dụng các giấy tờ nhìn rất thực và yêu cầu quý vị trả lệ phí và thuế trước khi quý vị có thể nhận được gia tài. Họ cũng có thể hỏi chi tiết cá nhân của quý vị để điền vào 'giấy tờ chính thức'. Điều này có nghĩa là quý vị có thể bị đánh cắp danh tính lẫn tiền của quý vị.

Thường gọi là **trò lừa đảo Nigeria (Nigerian scams)**, trò lừa đảo này có thể có nguồn gốc từ Tây Phi nhưng có thể đến từ bất cứ nơi nào trên thế giới. Trò lừa đảo này liên quan đến bọn lừa đảo nói với quý vị rằng họ cần quý vị giúp đỡ để lấy được khoản tài sản lớn mà họ đang cố gắng hết sức

để chuyển ra khỏi nước của họ. Họ có thể nói rằng khoản tài sản này là khối tiền giấu giếm, vàng hoặc tài sản bị chính phủ hoặc viên chức tham nhũng bỏ rơi và nếu quý vị đồng ý nhận nó, họ sẽ cho quý vị một phần lớn khi an toàn để làm như vậy. Tương tự tất cả những trò lừa đảo kiểu này, họ sẽ nói rằng trước tiên quý vị cần phải trả thuế, lệ phí ngân hàng hoặc lệ phí chống khủng bố và các khâu kiểm tra rửa tiền trước khi họ có thể gửi tiền.

Những trò lừa đảo này thường đến từ nước ngoài và yêu cầu thanh toán bằng hình thức điện chuyển khoản ngân hàng nhưng cũng có thể yêu cầu thanh toán bằng hình thức chuyển khoản ngân hàng hoặc các hình thức thanh toán khác.

Nếu bị mắc bẫy những trò lừa đảo này, quý vị sẽ không bao giờ nhận được bất cứ thứ gì từ kẻ lừa đảo và mất bất kỳ khoản tiền nào quý vị đã gửi.

Tự bảo vệ bản thân

- Hãy nhớ rằng không có chương trình nào giúp làm giàu trong một sớm một chiều: nếu nghe có vẻ đáng nghi ngờ vì nó quá tốt thì có lẽ nó là như vậy.
- Tránh mọi thỏa thuận với người lạ yêu cầu thanh toán trước bằng lệnh phiếu, điện chuyển khoản ngân hàng, chuyển tiền quốc tế, thẻ nạp sẵn tiền hoặc tiền điện tử. Rất hiếm khi quý vị có thể lấy lại được tiền đã gửi theo những cách này.
- Nếu email bất ngờ, có vẻ đáng ngờ, quý vị chỉ cần xóa nó đi. Đừng bấm vào bất kỳ dòng liên kết nào hết.
- Các cơ quan chính phủ, ngân hàng hoặc các công ty điện, ga, nước sẽ không bao giờ liên lạc với quý vị yêu cầu quý vị trả tiền trước để xin lấy lại lệ phí hoặc hoàn tiền.
- Nếu không chắc chắn, quý vị hãy kiểm tra danh tính người liên lạc một cách độc lập. Đừng sử dụng chi tiết liên lạc đã được cung cấp trong tin nhắn gửi đến cho quý vị—hãy lấy chi tiết liên lạc đúng thông qua nguồn độc lập như niên giám điện thoại hoặc tìm kiếm trên mạng (trực tuyến).
- Thực hiện việc tìm kiếm trực tuyến bằng cách sử dụng đúng chính xác từ ngữ của lời đề nghị—quý vị có thể xác định được nhiều trò lừa đảo theo cách này.

Trò lừa đảo giải thưởng và xổ số

Đừng để bị dụ dỗ vì trúng tiền/ thưởng bất ngờ—chỉ có kẻ lừa đảo là người trúng số tiền lớn mà thôi.

Cách thức lừa đảo là như thế nào

Những trò lừa đảo này tìm cách lừa quý vị đưa tiền trước hoặc thông tin cá nhân của quý vị để nhận giải thưởng từ cuộc xổ số, rút thăm trúng thưởng hoặc thi đua mà quý vị chưa bao giờ tham gia. Bọn lừa đảo nói rằng quý vị cần phải trả lệ phí hoặc thuế trước khi 'khoản tiền trúng' hoặc giải thưởng của quý vị có thể được trả cho quý vị. Quý vị cũng có thể phải gọi điện hoặc gửi tin nhắn đến số điện thoại tính cước đắt đỏ để nhận giải thưởng của mình.

Trò lừa đảo Cạo vé (Scratchie scams) liên quan đến việc nhận thư có tài liệu quảng cáo hào nhoáng và một số vé cạo, một trong số những vé cạo đó sẽ là vé trúng. Để làm cho nó đáng tin hơn, trò lừa đảo này thường sẽ có giải thưởng hạng nhì hoặc hạng ba. Khi quý vị gọi điện để nhận giải thưởng của mình, bọn lừa đảo sẽ yêu cầu quý vị trả lệ phí hoặc thuế trước khi quý vị có thể nhận được phần trúng của mình.

Trò lừa đảo xổ số (Lottery scams) có thể sử dụng tên của giải xổ số thực tế ở nước ngoài để nói rằng quý vị đã trúng tiền mặt, mặc dù quý vị chưa bao giờ tham gia giải xổ số này. Bọn lừa đảo thường đòi lệ phí hoặc thuế để giao tiền cho quý vị. Họ cũng sẽ cho quý vị biết họ cần thông tin cá nhân của quý vị để chứng minh quý vị đúng là người trúng nhưng sau đó

sử dụng thông tin này để lấy cắp danh tính hoặc tiền trong tài khoản ngân hàng của quý vị.

Phiếu và thẻ tặng giả (Fake vouchers and gift cards) liên quan đến bọn lừa đảo gửi cho quý vị email hoặc tin nhắn hoặc tin nhắn truyền thông xã hội nói là quý vị đã trúng thẻ tặng của tiệm bán lẻ nổi tiếng nhưng quý vị cần cung cấp một số chi tiết trước khi quý vị có thể nhận được thẻ tặng này. Đây là hình thức tìm cách lấy thông tin cá nhân có thể được sử dụng để đánh cắp danh tính hoặc nhắm vào quý vị với trò lừa đảo khác. Cũng được biết rằng các đề nghị như thế này sẽ cài phần mềm tống tiền (ransomware) vào thiết bị của quý vị (hãy đọc ở trang 17).

Trò lừa đảo giải thưởng du lịch (Travel prize scams) liên quan đến bọn lừa đảo nói rằng quý vị đã trúng kỳ nghỉ mát hoặc vé máy bay miễn phí. Trên thực tế, những gì quý vị thực sự trúng được là cơ hội mua phiếu chỗ ở hoặc chuyến bay. Những phiếu du lịch này thường tính lệ phí và kèm các điều kiện ẩn hoặc có thể là giả và chẳng có giá trị gì hết. Tương tự, bọn lừa đảo có thể cung cấp cho quý vị các gói kỳ nghỉ giảm giá tuyệt vời hoàn toàn không có.

Tự bảo vệ bản thân

- Hãy nhớ rằng: quý vị không thể trúng tiền xổ số hoặc cuộc thi đua trừ khi quý vị có tham gia.
- Các cuộc thi và xổ số không yêu cầu quý vị phải trả khoản lệ phí để nhận được tiền thưởng—hãy tìm kiếm trực tuyến bằng cách sử dụng đúng chính xác từ ngữ của lời đề nghị. Nó có thể giúp quý vị xác nhận rằng đó là trò lừa đảo.
- Suy nghĩ kỹ trước khi gọi điện hoặc nhắn tin đến số điện thoại bắt đầu bằng số '19'—những số điện thoại này tính cước đắt đỏ.

Trò lừa đảo mua sắm, rao vặt và đấu giá trực tuyến

Bọn lừa đảo cũng rất thích tình trạng dễ dàng khi mua sắm trực tuyến.

Cách thức lừa đảo là như thế nào

Người tiêu thụ và doanh nghiệp ngày càng mua và bán trên mạng Internet (trực tuyến) nhiều hơn. Đáng tiếc rằng bọn lừa đảo thích chọn lựa nạn nhân trên mạng Internet (trực tuyến).

Kẻ lừa đảo có thể tạo ra **các trang mạng bán lẻ giả (fake retailer websites)** rất giống, trông giống như thật, kể cả trên phương tiện truyền thông xã hội như Facebook. Chi tiết quan trọng nhất khiến quý vị nghi rằng trang mạng bán lẻ là trang mạng lừa đảo là hình thức thanh toán – hãy cảnh giác nếu quý vị được yêu cầu thanh toán bằng điện chuyển khoản hoặc các hình thức khác thường khác.

Trò lừa đảo đấu giá trực tuyến (online auction scam) liên quan đến kẻ lừa đảo nói rằng quý vị có cơ hội thứ hai để mua món hàng quý vị đã đấu giá vì người thắng cuộc đấu giá đã rút lui. Kẻ lừa đảo sẽ yêu cầu quý vị thanh toán bên ngoài cách thức thanh toán an toàn của trang đấu giá; nếu quý vị làm thế, quý vị sẽ bị mất tiền, quý vị sẽ không nhận được những gì quý vị đã trả tiền và trang mạng đấu giá sẽ không thể giúp quý vị.

Trò lừa đảo rao vặt trực tuyến (online classifieds scam) là trò lừa đảo phổ biến nhắm vào cả người mua lẫn người bán. Người mua nên cẩn thận đối với bọn lừa đảo đăng quảng cáo giả trên các trang mạng rao vặt hợp

pháp. Các mục quảng cáo có thể là về mọi thứ, từ nhà cho thuê cho đến thú cưng, xe hơi hoặc máy ảnh đã qua sử dụng và giá thường sẽ rẻ. Nếu quý vị cho thấy quý vị để ý đến món hàng, kẻ lừa đảo có thể nói rằng họ đang đi du lịch hoặc đã chuyển ra nước ngoài và một đại diện sẽ giao hàng sau khi họ nhận được tiền trả. Sau khi trả tiền, quý vị sẽ không nhận được hàng hoặc không thể liên lạc với người bán.

Đối với người bán, kẻ lừa đảo rao vặt sẽ trả lời quảng cáo của quý vị bằng lời đề nghị hào phóng. Nếu quý vị chấp nhận, kẻ lừa đảo sẽ trả tiền bằng séc (cheque) hoặc lệnh phiếu (money order). Tuy nhiên, số tiền quý vị nhận được sẽ nhiều hơn giá đã thỏa thuận. Trong **trò lừa đảo thanh toán dư** này, 'người mua' có thể nói với quý vị rằng đây là điều sai lầm và sẽ yêu cầu quý vị hoàn trả số tiền trả dư bằng cách chuyển tiền. Kẻ lừa đảo hy vọng rằng quý vị sẽ chuyển tiền trước khi quý vị phát hiện ra rằng séc của họ đã bị hủy (séc lủng) hoặc lệnh phiếu là lệnh phiếu giả. Quý vị sẽ bị mất tiền, cũng như món hàng quý vị đã bán nếu quý vị đã gửi hàng đi rồi.

Tự bảo vệ bản thân

- Hãy tìm hiểu chính xác quý vị đang giao dịch với ai. Nếu đó là nhà bán lẻ ở Úc, quý vị sẽ dễ có thể giải quyết vấn đề hơn nhiều nếu có sự cố xảy ra.
- Hãy kiểm tra xem người bán có uy tín hay không, có các chính sách hoàn tiền và dịch vụ giải quyết khiếu nại hay không.
- Tránh mọi thỏa thuận yêu cầu thanh toán trước bằng lệnh phiếu, điện chuyển khoản ngân hàng, chuyển tiền quốc tế, thẻ nạp tiền sẵn hoặc tiền điện tử. Rất hiếm khi quý vị lấy lại được tiền đã gửi theo cách này. Đừng bao giờ gửi tiền hoặc cung cấp chi tiết thẻ tín dụng hoặc chi tiết tài khoản trực tuyến cho bất kỳ ai quý vị không biết hoặc tin tưởng và đừng bao giờ cung cấp chi tiết bằng email.
- Chỉ thanh toán bằng hình thức thanh toán an toàn của trang mạng—hãy để ý tìm địa chỉ trang mạng bắt đầu bằng 'https' và biểu tượng ổ khóa đang khóa lại.
- Đừng bao giờ chấp nhận séc hoặc lệnh phiếu trả nhiều hơn số tiền quý vị đã thỏa thuận hoặc chuyển tiền cho bất kỳ ai.

Trò lừa đảo nhắm vào máy vi tính và thiết bị di động

Hãy nhớ rằng: bất cứ cái gì kết nối với internet đều có thể bị hại.

Cách thức lừa đảo là như thế nào

Kẻ lừa đảo truy cập từ xa (Remote access scammers) gọi điện thoại cho quý vị nói rằng máy vi tính của quý vị bị nhiễm vi-rút. Nếu quý vị làm theo lời hướng dẫn của họ thì họ sẽ có thể truy cập và kiểm soát máy vi tính của quý vị, trong trường hợp này họ có thể đánh cắp thông tin hoặc cài đặt phần mềm độc hại. Họ cũng có thể tìm cách thuyết phục quý vị mua phần mềm 'chống vi-rút', thường với giá đắt hoặc có sẵn miễn phí trên mạng internet.

Phần mềm độc hại (Malware) là thuật ngữ nói đến bất kỳ phần mềm độc hại nào có thể được cài đặt trong máy vi tính của quý vị hoặc các thiết bị khác bao gồm vi-rút, phần mềm gián điệp, phần mềm tống tiền, trojan horse và keystroke loggers.

Keystroke loggers và phần mềm gián điệp (Keystroke loggers and spyware) cho phép bọn lừa đảo ghi lại chính xác những gì quý vị gõ trên bàn phím để tìm ra mật khẩu và chi tiết ngân hàng hoặc truy cập thông tin cá nhân và gửi thông tin này đến bất cứ nơi nào họ muốn. Sau khi cài đặt xong, bọn lừa đảo có thể kiểm soát email và tài khoản truyền thông xã hội của quý vị và lấy bất kỳ thông tin nào trên thiết bị của quý vị, bao gồm mật khẩu. Họ cũng có thể sử dụng tài khoản của quý vị để gửi thêm các trò lừa đảo đến cho bạn bè và gia đình của quý vị.

Phần mềm tống tiền (Ransomware) là loại phần mềm độc hại sẽ mã hóa hoặc khóa thiết bị của quý vị để ngăn quý vị sử dụng cho đến khi quý vị đã trả tiền để mở khóa. Trả tiền không bảo đảm thiết bị của quý vị sẽ được mở khóa hoặc không có vi-rút ẩn, chúng cũng có thể lây lan và lây nhiễm các máy vi tính hoặc thiết bị khác trên mạng của quý vị.

Phần mềm độc hại thường được gửi qua email và có vẻ là từ các nơi hợp pháp, chẳng hạn như công ty điện, ga, nước của quý vị, cơ quan chính phủ hoặc thậm chí cảnh sát với lý do sẽ phạt tiền. Đừng bấm vào dòng liên kết hoặc mở bất kỳ tệp đính kèm nào mà quý vị không biết chắc. Quý vị nhiều khi sẽ tải phần mềm độc hại chứ không tải gì khác. Những trò lừa đảo này nhắm vào cả cá nhân lẫn doanh nghiệp.

Tự bảo vệ bản thân

- Hãy cảnh giác với lời mời tải xuống miễn phí cung cấp nhạc, trò chơi, phim và truy cập vào các trang mạng người lớn. Những thứ này có thể cài đặt các chương trình độc hại mà quý vị không hay biết.
- Hãy giữ an ninh cho mạng văn phòng, máy vi tính và thiết bị di động của quý vị. Cập nhật phần mềm an ninh của quý vị, thường xuyên đổi mật khẩu và sao lưu dữ liệu của quý vị. Lưu trữ bản sao lưu của quý vị ở chỗ khác và không nối với mạng Internet. Trang mạng www.staysmartonline.gov.au giải thích cách sao lưu dữ liệu của quý vị và bảo đảm an ninh các thiết bị di động của quý vị.
- Đừng mở tệp đính kèm hoặc bấm vào liên kết trong email hoặc tin nhắn truyền thông xã hội quý vị đã nhận được từ người lạ—chỉ cần bấm xóa đi.

Trộm cắp danh tính

Tất cả các trò lừa đảo quý vị đều có nguy cơ bị trộm cắp danh tính. Bảo vệ bản thân đối với những trò lừa đảo cũng có nghĩa là giữ an ninh thông tin cá nhân của quý vị.

Trộm cắp danh tính là mối đe dọa trong mọi trò lừa đảo

Hầu hết mọi người đều cho rằng lừa đảo là để tìm cách lừa gạt để lấy tiền của quý vị. Tuy nhiên, thông tin của quý vị cũng có giá trị đối với bọn lừa đảo. Bọn lừa đảo đánh cắp thông tin cá nhân của quý vị để thực hiện các hoạt động lừa đảo như mua hàng trái phép bằng thẻ tín dụng của quý vị hoặc sử dụng danh tính của quý vị để mở tài khoản ngân hàng hoặc tài khoản điện thoại. Bọn chúng có thể lấy tên quý vị để vay tiền hoặc thực hiện các hoạt động kinh doanh bất hợp pháp khác. Bọn chúng thậm chí có thể bán thông tin của quý vị cho bọn lừa đảo khác để bọn này sử dụng vào những việc phi pháp.

Khi bị đánh cắp danh tính, quý vị có thể bị thiệt hại khủng khiếp cả về tài chính lẫn cảm xúc. Quý vị có thể phải mất vài tháng để lấy lại danh tính của mình và tác động của việc bị đánh cắp danh tính có thể kéo dài trong nhiều năm.

Phishing—kẻ lừa đảo bất ngờ liên lạc quý vị bằng email, điện thoại, Facebook hoặc tin nhắn giả vờ là từ doanh nghiệp hợp pháp như ngân hàng, công ty điện thoại hoặc dịch vụ internet. Bọn này dẫn đường quý vị đến trang mạng giả mạo của doanh nghiệp, hỏi thông tin cá nhân của quý vị để xác minh hồ sơ khách hàng vì đã xảy ra lỗi kỹ thuật. Bọn này có thể gọi điện giả vờ là tiệm bán hàng xa xỉ, nói rằng có ai đó đang tìm cách xài thẻ tín dụng của quý vị. Họ khuyên quý vị nên liên lạc với ngân hàng của quý vị nhưng họ không cúp máy và vẫn còn ở trên đường dây. Khi quý vị tìm cách gọi điện cho ngân hàng, quý vị vẫn nói chuyện với bọn lừa đảo, làm như là cuộc gọi thực sự, giả vờ là nhân viên ngân hàng và hỏi chi tiết

tài khoản và chi tiết bảo mật của quý vị. Trong cả hai trường hợp, kẻ lừa đảo lấy bất kỳ thông tin nào quý vị cung cấp cho họ và sau đó sử dụng thông tin đó để truy cập tài khoản của quý vị.

Cuộc thăm dò ý kiến giả mạo (Fake surveys)—Bọn lừa đảo cung cấp giải thưởng hoặc phần thưởng như thẻ tặng của các tiệm bán lẻ nổi tiếng để đổi lấy việc hoàn tất cuộc thăm dò ý kiến trực tuyến. Cuộc thăm dò ý kiến này yêu cầu quý vị trả lời các câu hỏi khác nhau bao gồm tiết lộ chi tiết nhận dạng hoặc chi tiết ngân hàng quan trọng.

Dính líu đến mọi trò lừa đảo—Bọn lừa đảo thường hỏi thông tin cá nhân giống như trong các trò lừa đảo khác. Trong trò lừa đảo xổ số, bọn lừa đảo thường hỏi bằng lái xe hoặc hộ chiếu để 'chứng minh danh tính của quý vị trước khi họ có thể cho quý vị được hưởng tiền thưởng'. Trong các trò lừa đảo hẹn hò và ái tình, bọn chúng có thể hỏi thông tin 'để bảo lãnh đơn xin thị thực của họ đến thăm quý vị ở Úc'.

Xin nhớ rằng: Cung cấp thông tin cá nhân cho kẻ lừa đảo có thể cũng tai hại không kém như đưa tiền cho họ. Hãy giữ kín thông tin cá nhân của quý vị và giữ chúng an toàn.

Tự bảo vệ bản thân

- **Suy nghĩ kỹ về những gì quý vị nói và làm trong môi trường trực tuyến**

  Hãy cẩn thận khi chia sẻ thông tin về bản thân quý vị trên mạng Internet (trực tuyến), bao gồm phương tiện truyền thông xã hội, bài viết trực tuyến (blog) và các diễn đàn trực tuyến khác. Hãy dừng lại và suy nghĩ trước khi điền chi tiết trong các cuộc thăm dò ý kiến, tham gia các cuộc thi, bấm vào dòng liên kết hoặc tệp đính kèm hoặc thậm chí 'kết bạn', 'thích' hoặc 'chia sẻ' một cái gì đó trực tuyến.

- **Hãy coi chừng bất kỳ yêu cầu muốn biết chi tiết hoặc lấy tiền của quý vị**

  Bọn lừa đảo sẽ tìm cách lừa quý vị cho chúng biết dữ liệu của quý vị bằng cách sử dụng tên các công ty nổi tiếng hoặc các cơ quan chính phủ. Nếu cho rằng đó là trò lừa đảo, quý vị đừng hồi đáp. Hãy sử dụng niên giám điện thoại hoặc tìm kiếm trực tuyến để kiểm tra chi tiết liên lạc của tổ chức đó. Đừng bao giờ sử dụng các chi tiết liên lạc được cung cấp trong yêu cầu ban đầu.

Nếu đã cung cấp thông tin nhận dạng cá nhân cho bọn lừa đảo, quý vị hãy liên lạc với IDCARE qua số 1300 432 273.

Trò lừa đảo công việc và việc làm

Lương cao—bảo đảm? Khó tin được!

Cách thức lừa đảo là như thế nào

Trò lừa đảo công việc và việc làm liên quan đến các đề nghị làm việc tại nhà hoặc thiết lập và đầu tư vào 'cơ hội kinh doanh'. Bọn lừa đảo hứa hẹn công việc, lương cao hoặc lợi tức đầu tư lớn sau khi đã trả các khoản thanh toán trả trước ban đầu. Các khoản thanh toán này có thể là cho 'kế hoạch kinh doanh', khóa huấn luyện, phần mềm, đồng phục, quyền được tiếp cận thông tin mật (security clearance), thuế hoặc lệ phí. Nếu quý vị trả lệ phí, quý vị có thể không nhận được bất cứ thứ gì hoặc không như những gì quý vị kỳ vọng hoặc như đã hứa.

Một số lời mời làm việc có thể là vỏ ngoài của **các hoạt động rửa tiền bất hợp pháp**, khi quý vị được yêu cầu đóng vai trò là 'người quản lý tài khoản' hoặc 'trợ lý cá nhân', nhận các khoản tiền trả vào tài khoản ngân hàng của quý vị để được hưởng hoa hồng, sau đó chuyển tiền đến cho công ty nước ngoài. Trò lừa đảo công việc thường được quảng bá thông qua email rác hoặc các mục quảng cáo trong các trang rao vặt nổi tiếng và trên các trang mạng tìm việc làm—ngay cả các trang mạng tìm việc làm của chính phủ.

Mối nguy hiểm lớn đối với những trò lừa đảo công việc là quý vị có thể được yêu cầu cho biết rất nhiều chi tiết cá nhân mà quý vị không nên cung cấp bao gồm số hồ sơ thuế và bản sao hộ chiếu hoặc bằng lái xe của quý vị. Thông tin này có thể được sử dụng sau này để đánh cắp danh tính.

Tự bảo vệ bản thân

- Coi chừng các đề nghị hoặc kế hoạch tuyên bố bảo đảm thu nhập hoặc yêu cầu trả tiền trước.
- Đừng bao giờ đồng ý chuyển tiền cho người khác—đây là hoạt động rửa tiền và bất hợp pháp.
- Đừng cung cấp số hồ sơ thuế, bằng lái xe hoặc hộ chiếu khi nộp đơn xin việc. Quý vị có thể cần cung cấp thông tin này nhưng chỉ sau khi quý vị đã bắt đầu làm việc.

Rửa tiền là tội hình sự: đừng đồng ý chuyển tiền giùm người lạ.

Trò lừa đảo từ thiện và y tế

Bọn lừa đảo là bọn vô lương tâm và có thể ra tay vào những lúc người ta cần được giúp đỡ nhiều nhất.

Cách thức lừa đảo là như thế nào

Bọn lừa đảo lợi dụng những người muốn quyên góp cho một mục đích chính đáng hoặc tìm câu trả lời cho một vấn đề sức khỏe.

Trò lừa đảo từ thiện (Charity scams) liên quan đến bọn lừa đảo thu tiền bằng cách giả vờ làm việc cho một mục đích hợp pháp hoặc từ thiện, hoặc một mục đích hư cấu họ đã tạo ra. Thông thường bọn lừa đảo sẽ khai thác vụ thiên tai hoặc trường hợp khủng hoảng xảy ra gần đây đã được loan tin.

Những trò lừa đảo này chuyển số tiền quyên góp rất cần thiết của các tổ chức từ thiện hợp pháp qua chỗ khác. Các tổ chức từ thiện phải có đăng ký với chính phủ—hãy tự tin tặng tiền bằng cách kiểm tra tình trạng đăng ký của họ trước.

Trò lừa đảo **phép lạ chữa lành bệnh (miracle cure)** cung cấp các sản phẩm và dịch vụ khác nhau có thể là thuốc thay thế hợp pháp, thường hứa hẹn các phương thuốc chữa bệnh nhanh chóng và hiệu quả cho các bệnh nặng. Các phương pháp điều trị thường được quảng bá bằng cách sử dụng lời chứng thực sai lệch của những người đã được 'chữa khỏi'.

Trò lừa đảo giảm cân (Weight loss scams) hứa giảm cân rất nhanh, ít tốn công sức hoặc không cần tốn công sức. Trò lừa đảo loại này có thể liên quan đến chế độ ăn kiêng khác thường hoặc hạn chế, tập thể dục mang tính cách mạng, thiết bị 'làm tan mỡ', thuốc, miếng dán hoặc kem mang tính đột phá. Quý vị có thể được yêu cầu ứng trước khoản tiền lớn hoặc ký kết hợp đồng dài hạn để nhận được nguồn cung cấp liên tục.

Nhà thuốc trực tuyến giả mạo cung cấp dược phẩm và thuốc giả giá rất rẻ, và đôi khi cung cấp mà không cần toa bác sĩ. Những loại thuốc này có thể có ít hoặc không có các hoạt chất, và có thể gây hậu quả chết người cho người tiêu thụ.

Tự bảo vệ bản thân

- Nếu có người quyên tiền từ thiện trên đường phố tới gặp quý vị, quý vị hãy yêu cầu được xem thông tin nhận dạng của họ. Nếu nghi ngờ về bất kỳ điểm nào về nhân thân của họ, quý vị đừng đưa tiền cho họ.
- Kiểm tra danh sách các tổ chức từ thiện không vì lợi nhuận của Hiệp hội Vô vị lợi Từ thiện Úc (Australian Charities Not for Profit Association).
- Hỏi ý kiến chuyên viên chăm sóc sức khỏe của quý vị nếu quý vị đang cân nhắc lời tự nhận 'thần kỳ' hoặc 'chữa hết tức thời' về thuốc, chất bổ sung hoặc các phương pháp điều trị khác.
- Tự hỏi bản thân: nếu đây thực sự là phương thuốc thần kỳ, chắc chuyên viên chăm sóc sức khỏe của quý vị đã nói cho quý vị biết về điều đó rồi, đúng không?

Trò lừa đảo kinh doanh

Bọn lừa đảo lợi dụng tình trạng bận rộn của nhiều doanh nghiệp để lừa đảo họ.

Cách thức lừa đảo là như thế nào

Bọn lừa đảo nhắm vào các doanh nghiệp có thể sử dụng vô số chiêu bài và có lẽ sẽ ra tay vào những lúc bận rộn nhất, như cuối năm tài chính.

Trò lừa đảo gửi hóa đơn sai (false billing scam) là mánh lới phổ biến nhất mà bọn lừa đảo sử dụng đối với các doanh nghiệp. Bọn lừa đảo gửi hóa đơn giả cho việc đăng trong danh sách, quảng cáo, sản phẩm hoặc dịch vụ không cần hoặc trái phép. **Trò lừa đảo danh bạ doanh nghiệp (business directory scam)** là ví dụ nổi tiếng, khi quý vị nhận được hóa đơn cho việc đăng trong danh sách trong danh bạ được cho là nổi tiếng. Bọn lừa đảo lừa quý vị đăng ký bằng cách ngụy trang đề nghị dưới dạng hóa đơn chưa thanh toán hoặc đăng trong danh sách miễn phí, nhưng với một thỏa thuận đăng ký ẩn viết chữ cỡ nhỏ.

Trò lừa đảo tên miền (domain name scam) là mánh lới khác mà bọn lừa đảo sử dụng, khi quý vị bị lừa ký tên để đăng ký tên miền internet không do yêu cầu rất giống với tên miền của chính quý vị. Quý vị cũng có thể nhận được giấy thông báo gia hạn giả cho tên miền thực của mình và trả tiền mà không hay biết.

Trò lừa đảo nguồn cung cấp vật dụng văn phòng (office supply scam) liên quan đến việc quý vị nhận và bị tính tiền cho các sản phẩm mà quý vị không đặt hàng. Những trò lừa đảo này thường liên quan đến các sản phẩm hoặc dịch vụ quý vị thường xuyên đặt hàng như văn phòng phẩm và vật dụng dọn dẹp vệ sinh. Bọn lừa đảo thường gọi điện thoại cho doanh

nghiệp của quý vị giả vờ rằng một dịch vụ hoặc sản phẩm đã được đặt hàng.

Trò lừa đảo chuyển khoản tiền trả sang nơi nhận khác (Payment redirection scams) liên quan đến kẻ lừa đảo sử dụng thông tin họ lấy được bằng cách 'hack' hệ thống máy vi tính của quý vị. Sau đó, họ giả là một trong những nhà cung cấp thường xuyên của quý vị và nói với quý vị rằng chi tiết ngân hàng của họ đã thay đổi. Họ có thể nói với quý vị rằng gần đây họ đã đổi ngân hàng và có thể sử dụng tiêu đề thư (letterhead) và thương hiệu đã sao chụp để thuyết phục quý vị rằng họ hợp pháp. Họ sẽ cung cấp cho quý vị số tài khoản ngân hàng mới và yêu cầu tất cả các khoản thanh toán trong tương lai được trả vào tài khoản này. Trò lừa đảo thường chỉ bị phát hiện khi nhà cung cấp thường xuyên của quý vị hỏi tại sao họ chưa được trả tiền.

Phần mềm tống tiền (Ransomware) có thể cực kỳ tai hại đối với bất kỳ doanh nghiệp nào. Cách phòng ngừa tốt nhất là thường xuyên sao lưu dữ liệu của quý vị và lưu trữ bản sao lưu của quý vị ở chỗ khác và không nối với mạng Internet. Xem thêm chi tiết ở trang 17.

Tự bảo vệ bản thân

- Đừng đồng ý với các lời mời hoặc giao dịch ngay lập tức—luôn luôn yêu cầu họ cung cấp lời mời bằng văn bản và hỏi ý kiến độc lập nếu việc giao dịch có liên quan đến tiền bạc, thời gian hoặc cam kết lâu dài.
- Đừng bao giờ cung cấp chi tiết ngân hàng, tài chính và kế toán của doanh nghiệp của quý vị cho người nào bất ngờ liên lạc với quý vị và quý vị không biết và không tin tưởng.
- Các thủ tục quản lý hiệu quả có thể có ích đáng kể đối với việc ngăn chặn các trò lừa đảo—quý vị nên có các tiến trình xác định rõ ràng để xác minh và thanh toán tài khoản và hóa đơn và xem xét rất kỹ các yêu cầu thay đổi chi tiết ngân hàng.
- Huấn luyện nhân viên của quý vị để họ nhận ra những trò lừa đảo.
- Sao lưu dữ liệu kinh doanh của quý vị rồi cất giữ ở chỗ khác và không nối với mạng Internet.
- Cảnh giác đối với các email yêu cầu thay đổi chi tiết thanh toán. Luôn xác minh các thay đổi về chi tiết thanh toán thẳng với doanh nghiệp hoặc cá nhân.

Cách thức của trò lừa đảo là như thế nào—cơ cấu của trò lừa đảo

Hầu hết các trò lừa đảo đều theo cùng một kiểu dạng và một khi hiểu điều này, quý vị sẽ dễ nhận ra các mánh lới của kẻ lừa đảo hơn.

Nếu xem xét kỹ tất cả các loại trò lừa đảo khác nhau được nêu trong tập sách này, quý vị sẽ sớm nhận ra rằng hầu hết các trò lừa đảo đều diễn ra theo ba giai đoạn: (1) tiếp xúc; (2) giao tiếp; và (3) tiền trả.

Hiểu các phần cơ bản của trò lừa đảo sẽ giúp quý vị tránh được các trò lừa đảo hiện tại và cảnh giác đối với những trò lừa đảo mới sẽ xuất hiện trong tương lai.

1. Tiếp xúc: phương thức thực hiện

Khi bọn lừa đảo tiếp xúc quý vị, bọn chúng sẽ luôn có câu chuyện được dàn dựng để khiến quý vị tin vào lời nói dối. Kẻ lừa đảo sẽ giả vờ là một cái gì đó mà thực ra không phải là họ, viên chức chính phủ, nhà đầu tư chuyên gia, viên chức xổ số hoặc thậm chí là người tơ tưởng quý vị.

Để cung cấp những lời nói dối này đến cho quý vị, bọn lừa đảo sẽ sử dụng các phương thức liên lạc khác nhau.

Trực tuyến

Bọn lừa đảo rình rập trong môi trường ẩn danh của internet.

Email là phương thức thực hiện trò lừa đảo được ưa chuộng, cung cấp cách liên lạc rẻ tiền và đơn giản đến rất nhiều người. Email phishing 'tìm cách lấy' thông tin cá nhân của quý vị là loại lừa đảo phổ biến nhất bằng email.

Hình thức mạng xã hội, trang mạng hẹn hò và diễn đàn trực tuyến cho phép bọn lừa đảo 'kết bạn' với quý vị và xâm nhập vào cuộc sống cá nhân của quý vị để tìm biết các chi tiết cá nhân của quý vị, sau đó có thể được sử dụng để làm hại quý vị hoặc gia đình và bạn bè của quý vị.

Các trang mạng mua sắm, rao vặt và đấu giá trực tuyến được bọn lừa đảo sử dụng để nhắm vào người mua và người bán, với lần tiếp xúc ban đầu thường được thực hiện thông qua các trang mạng uy tín và đáng tin cậy hoặc các trang mạng giả trông giống như thật. Hãy để ý tìm các hình thức thanh toán an toàn và hãy cẩn thận với các hình thức thanh toán khác thường như điện chuyển khoản ngân hàng, Bitcoin hoặc thẻ nạp tiền sẵn. Thẻ tín dụng thường có thể bảo vệ quý vị phần nào.

Qua điện thoại

Kẻ lừa đảo cũng gọi điện thoại và gửi SMS.

Bọn lừa đảo **gọi điện thoại** cho các nhà dân và doanh nghiệp trong nhiều trò lừa đảo khác nhau, từ trò lừa đảo đe dọa thuế cho đến đề nghị giải thưởng hoặc 'trợ giúp' với vi-rút máy vi tính. Vì cước gọi Truyền giọng nói trên giao thức IP (VOIP-Voice Over Internet Protocol) rẻ nên các trung tâm điện thoại có thể hoạt động ở nước ngoài với các số điện thoại trông giống như số điện thoại địa phương. Nhân dạng của người gọi có thể dễ dàng ngụy trang và là một trong nhiều thủ đoạn mà bọn lừa đảo sử dụng để khiến quý vị tin rằng họ là người khác.

Bọn lừa đảo sử dụng **tin nhắn SMS** để gửi hàng loạt các trò lừa đảo bao gồm trò lừa đảo thi đua hoặc trò lừa đảo giải thưởng. Nếu quý vị trả lời, quý vị có thể bị tính cước đắt hoặc thấy mình đã đăng ký sử dụng dịch vụ. Điều an toàn hơn là quý vị không trả lời hoặc bấm vào dòng liên kết trong tin nhắn trừ khi quý vị biết người gọi là ai. Chúng cũng có thể có tệp đính kèm hoặc dòng liên kết đến phần mềm độc hại ngụy trang là hình ảnh, bài hát, trò chơi hoặc ứng dụng.

Trước cửa nhà quý vị

Hãy coi chừng—một số kẻ lừa đảo sẽ đến tận nhà quý vị để tìm cách lừa đảo quý vị.

Lừa đảo dạo trực tiếp (Door-to-door scams) thường liên quan đến kẻ lừa đảo quảng bá hàng hóa hoặc dịch vụ quý vị sẽ không nhận được hoặc chất lượng rất kém. Quý vị thậm chí có thể bị gửi hóa đơn cho công việc mà quý vị không muốn hoặc không đồng ý. Một trò lừa đảo mà những con buôn tinh ranh thường thực hiện khi đi từ nơi này sang nơi khác là thực hiện công việc sửa chữa nhà cửa kém chất lượng hoặc chỉ lấy tiền của quý vị và bỏ trốn.

Các doanh nghiệp hợp pháp có thể bán hàng tận cửa nhà nhưng phải xác định rõ ràng danh tính và công ty của họ và tuân theo các điều luật khác. Quý vị có các quyền cụ thể khi nói đến các cách thức bán hàng tận cửa nhà, bao gồm có cơ hội để đổi ý—hãy tìm hiểu thêm tại www.accc.gov.au/doortodoor.

Bọn lừa đảo có thể **giả làm** nhân viên **từ thiện** để thu tiền quyên góp. Họ sẽ lợi dụng các sự kiện xảy ra gần đây như lũ lụt và cháy rừng.Trước khi tặng tiền, quý vị hãy yêu cầu được xem giấy tờ chứng minh và xem sổ biên nhận chính thức của họ.

Hình thức gửi thư hàng loạt vẫn được sử dụng để gửi **những trò lừa đảo xổ số và rút thăm trúng thưởng, cơ hội đầu tư, trò lừa đảo Nigeria** và **thư thừa kế giả**. Một tờ thông tin hào nhoáng không bảo đảm rằng lời mời là hợp pháp.

Bất kể bọn họ sử dụng phương thức thực hiện nào, câu chuyện của họ luôn là mồi nhử và nếu quý vị cắn mồi, kẻ lừa đảo sẽ tìm cách chuyển quý vị sang giai đoạn tiếp theo.

2. Giao tiếp và dẫn dụ

Nếu quý vị cho họ cơ hội nói chuyện với quý vị, bọn lừa đảo sẽ bắt đầu sử dụng các mánh lới trong **hộp công cụ** của bọn chúng để thuyết phục quý vị chi tiền.

Các công cụ của bọn lừa đảo có thể liên quan đến các điều dưới đây:

- Bọn lừa đảo thêu dệt **những câu chuyện** cầu kỳ nhưng **đáng tin** để đạt được những gì họ muốn.
- Họ sử dụng **thông tin cá nhân** của quý vị để làm cho quý vị tin rằng quý vị đã từng tiếp xúc với bọn chúng trước đó và làm cho trò lừa đảo có vẻ hợp pháp.
- Bọn lừa đảo có thể **liên lạc với quý vị thường xuyên** để tạo niềm tin và thuyết phục quý vị rằng họ là bạn bè, đối tác của quý vị hoặc người tơ tưởng đến quý vị.
- Họ **đánh vào tâm lý của quý vị** bằng cách sử dụng sự phấn khích khi trúng/thắng, lời hứa tình yêu vĩnh cửu, sự cảm thông về tai nạn đáng tiếc, cảm giác tội lỗi về việc không giúp đỡ hoặc lo lắng và sợ bị bắt hoặc phạt tiền.
- Bọn lừa đảo rất thích tạo ra **cảm giác cấp bách** để quý vị không kịp suy nghĩ kỹ và phản ứng theo cảm xúc hơn lý trí.
- Tương tự, họ sử dụng **các mánh khóe bán hàng áp lực cao** nói rằng đó là khuyến mại có hạn, giá sẽ tăng hoặc thị trường sẽ thay đổi và cơ hội sẽ bị mất.
- Trò lừa đảo có thể có tất cả các đặc điểm của doanh nghiệp thực sự bằng cách sử dụng **tài liệu quảng cáo hào nhoáng** với thuật ngữ ngành kỹ thuật, bổ sung bằng mặt tiền văn phòng, trung tâm điện thoại và trang mạng chuyên nghiệp.
- Với dịch vụ internet và phần mềm thông minh, bọn lừa đảo có thể dễ dàng tạo ra **các giấy tờ** giả mạo và **nhìn như thật**. Một giấy tờ ra vẻ được chính phủ chấp thuận hoặc đầy rẫy thuật ngữ pháp lý có thể khiến giúp trò lừa đảo có uy quyền.

Các công cụ của kẻ lừa đảo là nhằm làm cho quý vị bớt đề phòng, tạo niềm tin vào câu chuyện và hành động nhanh chóng hoặc không sử dụng lý trí và tiến tới giai đoạn cuối cùng—gửi tiền.

3. Gửi tiền

Đôi khi manh mối rõ rệt nhất để quý vị nhận ra đó là trò lừa đảo là cách kẻ lừa đảo yêu cầu quý vị trả/chuyển/gửi tiền.

Yêu cầu tiền có thể xảy ra trong vòng vài phút sau khi trò lừa đảo diễn ra hoặc sau nhiều tháng mồi chài cẩn thận. Bọn lừa đảo có các ý thích riêng về cách quý vị gửi tiền.

Đã được biết rằng bọn lừa đảo thường yêu cầu nạn nhân đến địa điểm **chuyển tiền** gần nhất (bưu điện, dịch vụ diện chuyển khoản hoặc thậm chí ngân hàng) để gửi tiền. Đã được biết là bọn chúng vẫn không cúp điện thoại, sẽ chỉ dẫn cụ thể và thậm chí có thể gửi taxi để tiếp tay chuyện này. Bọn lừa đảo sẵn sàng chấp nhận tiền bằng mọi hình thức và điều này có thể bao gồm **chuyển khoản ngân hàng trực tiếp, thẻ trừ tiền tài khoản ngân hàng nạp tiền sẵn, thẻ tặng, Google Play, Steam** hoặc **thẻ iTunes** hoặc tiền ảo như **Bitcoin**. Bất kỳ yêu cầu thanh toán bằng hình thức khác thường nào cũng là dấu hiệu rõ ràng rằng nó dính líu đến trò lừa đảo.

Thẻ tín dụng thường bảo vệ quý vị phần nào và quý vị cũng nên tìm các hình thức thanh toán an toàn có 'https' trong địa chỉ mạng và trang mạng có biểu tượng ổ khóa đang khóa.

Đừng gửi tiền cho người quý vị chỉ gặp trên mạng Internet (trực tuyến) hoặc qua điện thoại, đặc biệt nếu họ ở nước ngoài.

Xin lưu ý bọn lừa đảo cũng có thể yêu cầu thanh toán dưới dạng hàng hóa có giá trị và những món quà đắt tiền như đồ trang sức hoặc đồ điện tử. Trả tiền cho bọn lừa đảo không chỉ là điều duy nhất quý vị lo ngại về vấn đề này—nếu giúp chuyển tiền cho người lạ, quý vị có thể vô tình dính líu vào hoạt động **rửa tiền bất hợp pháp**.

Những nguyên tắc vàng để bảo vệ chính mình

Hãy cảnh giác về điều thực tế là trò lừa đảo có thực. Khi tự dưng có người hoặc doanh nghiệp tiếp xúc với mình mà quý vị không mời, cho dù là qua điện thoại, thư tín, email, đích thân hoặc trên trang mạng xã hội, quý vị luôn xem xét khả năng là người hoặc doanh nghiệp này có thể là trò lừa đảo. Hãy nhớ rằng, nếu nó có vẻ tốt đến mức khó tin là thật, có lẽ nó là như vậy.

Biết quý vị đang tiếp xúc với ai. Nếu chỉ từng gặp ai đó trên mạng Internet (trực tuyến) hoặc không chắc chắn về tính hợp pháp của doanh nghiệp nào đó, quý vị hãy thư thả để nghiên cứu thêm một chút. Thực hiện việc tìm kiếm hình ảnh Google bằng các hình ảnh hoặc tìm kiếm trên mạng internet những người khác có thể đã từng tiếp xúc với họ.

Đừng mở các dòng chữ, cửa sổ tự động hiện ra hoặc email đáng ngờ—hãy xóa chúng đi. Nếu không chắc chắn, quý vị hãy xác minh danh tính người tìm cách liên lạc với quý vị thông qua nguồn độc lập như niên giám điện thoại hoặc tìm kiếm trực tuyến. Đừng sử dụng chi tiết liên lạc được cung cấp trong tin nhắn gửi cho quý vị.

Giữ thông tin cá nhân của quý vị an toàn. Gắn ổ khóa vào hộp thư của quý vị và cắt nhỏ hóa đơn của quý vị và các giấy tờ quan trọng khác trước khi vất bỏ. Cất mật khẩu và số pin của quý vị ở nơi an toàn. Hãy thật cẩn thận về lượng thông tin cá nhân quý vị chia sẻ trên các trang truyền thông xã hội. Kẻ lừa đảo có thể sử dụng thông tin và hình ảnh của quý vị để tạo ra danh tính giả hoặc thực hiện trò lừa đảo nhắm vào quý vị.

Coi chừng các hình thức thanh toán khác thường. Bọn lừa đảo thường yêu cầu thanh toán bằng hình thức điện chuyển khoản ngân hàng, thẻ nạp sẵn tiền và thậm chí cả thẻ Google Play, Steam hoặc iTunes và Bitcoin. Những thứ này hầu như luôn là dấu hiệu cho thấy nó dính líu đến trò lừa đảo.

Giữ an toàn cho thiết bị di động và máy vi tính của quý vị. Luôn sử dụng biện pháp bảo vệ mật khẩu, không chia sẻ quyền truy cập với người khác (bao gồm từ xa), cập nhật phần mềm bảo mật và sao lưu nội dung. Bảo vệ mạng WiFi của quý vị bằng mật khẩu và tránh sử dụng máy vi tính hoặc điểm truy cập WiFi công cộng để truy cập ngân hàng trực tuyến hoặc cung cấp thông tin cá nhân.

Cẩn thận chọn mật khẩu của quý vị. Hãy chọn mật khẩu mà người khác khó đoán ra và thường xuyên cập nhật mật khẩu. Mật khẩu khó giải phải có cả các mẫu tự hoa và thường, số và ký hiệu. Đừng sử dụng cùng một mật khẩu cho mọi tài khoản/hồ sơ và đừng cho bất kỳ ai biết mật khẩu của quý vị.

Cẩn thận với bất kỳ yêu cầu muốn biết chi tiết hoặc yêu cầu quý vị chi tiền. Đừng bao giờ gửi tiền hoặc cung cấp số thẻ tín dụng, chi tiết tài khoản trực tuyến hoặc bản sao giấy tờ cá nhân cho bất kỳ ai quý vị không biết hoặc không tin tưởng. Đừng đồng ý chuyển tiền hoặc hàng hóa cho người khác: rửa tiền là tội hình sự.

Cẩn thận khi mua sắm trực tuyến. Coi chừng những lời đề nghị có vẻ quá tốt để tin là thực và luôn sử dụng dịch vụ mua sắm trực tuyến quý vị biết và tin tưởng. Hãy suy nghĩ kỹ trước khi sử dụng các loại tiền ảo (như Bitcoin)—tiền ảo không có các biện pháp bảo vệ giống như các hình thức giao dịch khác, điều đó có nghĩa là quý vị không thể lấy lại tiền của mình sau khi gửi đi.

Tìm trợ giúp hoặc nhờ trợ giúp ở đâu

Nếu quý vị đã bị mất tiền vì trò lừa đảo hoặc cung cấp thông tin cá nhân của quý vị cho kẻ lừa đảo, ít khi nào quý vị có thể lấy lại tiền của mình. Tuy nhiên, có những bước quý vị có thể thực hiện ngay để hạn chế thiệt hại và bảo vệ bản thân khỏi bị mất mát thêm.

Liên lạc với ngân hàng hoặc tổ hợp tín dụng (credit union) của quý vị

Nếu đã gửi tiền hoặc thông tin ngân hàng cá nhân cho kẻ lừa đảo, quý vị hãy liên lạc với ngân hàng hoặc tổ hợp tín dụng của quý vị ngay lập tức. Họ có thể chặn giao dịch chuyển tiền hoặc séc hoặc đóng tài khoản của quý vị nếu kẻ lừa đảo có chi tiết tài khoản của quý vị. Nhà cấp thẻ tín dụng của quý vị có thể thực hiện biện pháp 'lấy tiền lại' (đảo ngược giao dịch) nếu thẻ tín dụng của quý vị bị trừ tiền một cách gian lận.

Lấy lại danh tính bị đánh cắp của quý vị

Nếu nghi ngờ mình là nạn nhân vụ trộm cắp danh tính, điều quan trọng là quý vị phải hành động nhanh chóng để giảm thiểu rủi ro tổn thất tài chính hoặc các thiệt hại khác.

Liên lạc với **IDCARE**—dịch vụ miễn phí do chính phủ tài trợ. Dịch vụ này trợ giúp nạn nhân tội phạm danh tính. IDCARE có thể giúp quý vị lập kế hoạch ứng phó để thực hiện các bước thích hợp để sửa chữa thiệt hại đối với danh tiếng, quá trình tín dụng và danh tính của quý vị. Truy cập trang mạng IDCARE tại www.idcare.org hoặc gọi số 1300 432 273.

Nộp đơn xin **Giấy chứng nhận Nạn nhân do Liên bang cấp (Commonwealth Victims' Certificate)**—giấy chứng nhận này giúp ủng hộ lời khai của quý vị rằng quý vị là nạn nhân tội phạm danh tính và quý vị có thể sử dụng giấy này để giúp thiết lập lại tư cách (credentials) của quý vị với chính phủ hoặc tổ chức tài chính. Truy cập trang mạng Bộ Tổng chưởng lý tại www.ag.gov.au (hoặc gọi số 02 6141 6666) để tìm hiểu thêm về việc bảo vệ và phục hồi danh tính của quý vị.

Liên lạc với dịch vụ tư vấn hoặc trợ giúp

Nếu quý vị hoặc người quý vị quen đã bị lừa đảo và có thể đang bị căng thẳng hoặc trầm cảm, quý vị hãy nói chuyện với bác sĩ gia đình (GP), chuyên gia y tế địa phương hoặc người quý vị tin tưởng. Quý vị cũng có thể nghĩ đến liên lạc với các dịch vụ tư vấn hoặc trợ giúp, như:

Lifeline—Khi quý vị cần trợ giúp trong cuộc khủng hoảng, hãy liên lạc với Lifeline qua số 13 1114 (24/7) hoặc truy cập www.lifeline.org.au

Beyondblue—để biết thông tin về trầm cảm hoặc lo lắng, liên lạc với Beyondblue qua số 1300 224 636 hoặc truy cập www.beyondblue.org.au

Đường dây Trợ giúp Trẻ em (Kids helpline)—dịch vụ tư vấn và trợ giúp qua điện thoại và trực tuyến dành cho thanh thiếu niên từ năm đến 25 tuổi. Liên lạc với Đường dây Trợ giúp Trẻ em qua số 1800 551 800 hoặc truy cập www.kidshelpline.com.au

Tư vấn Tài chính Úc (Financial Counselling Australia)—nếu gặp khó khăn về tài chính, quý vị hãy gọi số 1800 007 007 để nói chuyện với nhân viên tư vấn tài chính miễn phí hoặc truy cập www.financialcounsellingaustralia.org.au.

Trình báo vụ lừa đảo ở đâu

Quý vị có thể giúp người khác bằng cách trình báo trò lừa đảo cho các cơ quan thích hợp. Thông tin của quý vị sẽ giúp các tổ chức này hiểu rõ tình hình hơn về những trò lừa đảo mới nhất và cảnh báo cho những người khác về những gì cần để ý coi chừng.

Các tổ chức dưới đây nhận các vụ trình báo các loại lừa đảo cụ thể.

Scamwatch

Trình báo các trò lừa đảo cho ACCC thông qua Scamwatch, truy cập www.scamwatch.gov.au

Hãy đi trước bọn lừa đảo một bước

Đi trước bọn lừa đảo một bước, truy cập trang mạng của Scamwatch để biết chi tiết các trò lừa đảo nhắm vào người tiêu thụ Úc và các doanh nghiệp nhỏ. Tìm hiểu thêm về cách hoạt động của các trò lừa đảo, cách tự bảo vệ bản thân và phải làm gì nếu bị lừa đảo.

Đăng ký với dịch vụ Scamwatch để nhận thông báo qua email miễn phí về các trò lừa đảo mới, đang xảy ra.

www.scamwatch.gov.au

Theo Scamwatch trên Twitter tại @scamwatch_gov hoặc http://twitter.com/Scamwatch_gov

Nếu gặp phải trò lừa đảo trên trang mạng hoặc hình thức truyền thông xã hội, quý vị hãy trình báo nó cho trang mạng để họ có thể điều tra và loại bỏ. Nếu bọn lừa đảo đang mạo danh tổ chức hợp pháp như bộ chính phủ hoặc ngân hàng, quý vị hãy thông báo cho họ biết để họ có thể cảnh báo những người khác.

Các cơ quan khác

Quý vị cũng nên nghĩ đến trình báo trò lừa đảo mình đã trải qua cho các cơ quan khác có liên quan cụ thể đến một số loại trò lừa đảo.

Loại trò lừa đảo	Cơ quan
Tội phạm mạng (Cybercrime)	Mạng Báo cáo Trực tuyến về Tội phạm Mạng của Úc (ACORN-Australian Cybercrime Online Reporting Network)—truy cập www.acorn.gov.au
Trò lừa đảo tài chính và đầu tư	Ủy hội Đầu tư và Chứng khoán Úc (ASIC-Australian Securities and Investments Commission)—truy cập www.moneysmart.gov.au hoặc gọi cho đường dây thông tin của ASIC qua số 1300 300 630
Gian lận và trộm cắp	Cảnh sát địa phương của quý vị—gọi số 13 1444
Email và tin nhắn SMS rác	Cơ quan Truyền thông và Giới Truyền thông Úc (ACMA-Australian Communications and Media Authority)—truy cập www.acma.gov.au hoặc gọi cho Trung tâm Dịch vụ Khách hàng ACMA qua số 1300 850 115
Lừa đảo liên quan đến thuế	Sở Thuế vụ Úc (ATO)—Trình báo trò lừa đảo thuế hoặc xác minh xem người liên lạc với quý vị từ ATO có hợp pháp không: • gọi số 1800 008 540 hoặc chuyển email lừa đảo thuế qua email tới ReportEmailFraud@ato.gov.au
Ngân hàng	Ngân hàng hoặc tổ chức tài chính của quý vị

Liên lạc với cơ quan bảo vệ người tiêu thụ địa phương của quý vị

Dù ACCC là cơ quan toàn quốc giải quyết các vấn đề bảo vệ người tiêu thụ nói chung, các cơ quan tiểu bang và lãnh thổ cũng có thể trợ giúp quý vị.

Văn phòng Dịch vụ Giám sát Lãnh thổ Thủ đô Úc (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
Cơ quan Bảo vệ Người tiêu thụ Victoria (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
Cơ quan Thương mại Công bằng New South Wales (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
Cơ quan Bảo vệ Người tiêu thụ Lãnh thổ Bắc Úc (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
Cơ quan Thương mại Công bằng Queensland (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
Dịch vụ Người tiêu thụ và Doanh nghiệp Nam Úc (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
Dịch vụ Người tiêu thụ, Xây dựng và Ngành nghề Tasmania (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
Bộ Hầm mỏ, Giám sát Ngành Công nghiệp và An toàn Tây Úc (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

Muốn biết thêm thông tin

Chính phủ Úc có một số tài liệu rất hay về cách giữ an ninh và an toàn trực tuyến.

- Dịch vụ Luôn Khôn ngoan trên mạng (Stay Smart Online Service)—www.staysmartonline.gov.au
- Trang mạng CyberSmart—www.cybersmart.gov.au
- Tài liệu Hướng dẫn Luôn Khôn ngoan trên mạng—có tại www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au