Phòng Tránh Lừa Đảo Trên Mạng

Lừa Đảo trên mạng (Online Scams) là gì?

Lừa Đảo trên mạng là những hành động gian trá, lừa lọc được thực hiện qua thư điện tử (email), tin nhắn, mạng xã hội hay điện thoại với mục đích là để lấy thông tin cá nhân và/hay tiền bạc của bạn.

Theo thống kê thì vào năm 2019 tại nước Úc, số tiền của những người bị mất vì lừa đảo lên đến $634,000,000 so với $489,700,000 từ năm 2018.

Những hình thức lừa đảo phổ biến

1. Mạo danh (Phishing Scam/ Impersonation scam)

Lừa đảo qua hình thức mạo danh là hình thức lừa đảo phổ biến nhất trên mạng. Đối tượng lừa đảo này thường bắt đầu bằng một email hoặc một tin nhắn hoặc một cuộc gọi điện thoại mạo danh là từ một tổ chức hay từ một cơ quan, doanh nghiệp mà bạn tin tưởng. Họ báo cáo là tài khoản của bạn có vấn đề, cần được bạn xác nhận và giải quyết ngay bằng cách cung cấp cho họ những thông tin cá nhân của mình. Sau khi nắm được thông tin đó, đối tượng lừa đảo bèn truy cập vào tài khoản cũng như thực hiện các giao dịch trái phép trên danh nghĩa của bạn.

Để tránh bị lừa như vậy thì bạn

Nên:

- Kiểm tra địa chỉ email của người gởi.
- Liên lạc và kiểm tra với cơ quan mà bạn nghi ngờ đã bị đối tượng lừa đảo mạo danh.
- Xoá email/tin nhắn đó.
- Báo cáo (sẽ hướng dẫn cách báo cáo ở phần sau).

Không nên:

- Nhấp vào bất cứ đường dẫn (link) nào trong email hay trong tin nhắn của họ.
- Tiết lộ mật mã của bạn.
- Trả lời.

2. Kết bạn trên mạng xã hội (Online Dating)

Đây là thủ đoạn lừa đảo đã khiến nhiều người Úc mất hằng triệu đô la mỗi năm. Đối tượng lừa đảo có khuynh hướng nhắm vào những người nhẹ dạ, yếu đuối để lợi dụng. Thông thường chúng dành một thời gian dài để xây dựng quan hệ trước khi dựng lên một câu chuyện đáng tin để lừa tiền. Để cảnh giác, bạn

Nên:

- Dùng những dịch vụ nhắn tin miễn phí qua điện thoại như WhatsApp, Skype, Google Voice và Facebook Messenger để thoải mái nhắn tin với đối tượng mà không phải lo số điện thoại bị tiết lộ.

- Cho người mà bạn tin tưởng biết nếu muốn gặp gỡ thì bạn sẽ gặp mặt đối mặt với người đó.
- Gặp ở nơi công cộng hoặc đem theo một người thân của bạn.
- Liên lạc ngân hàng nếu bạn nghi là chi tiết ngân hàng của bạn đã bị tiết lộ.
- Báo cáo.

Không nên:

- Tiết lộ số điện thoại thật của bạn.
- Chia sẻ chi tiết ngân hàng của bạn.
- Chia sẻ chi tiết thẻ tín dụng của bạn.
- Gởi tiền cho họ.
- Chia sẻ hình và phim ảnh riêng tư và nhạy cảm của bạn.
- Mủi lòng quá sớm.

3. <u>Mua bán trên mạng</u>

Trong khi có những dịch vụ buôn bán đàng hoàng, chính thức trên mạng thì cũng có những kẻ lợi dụng hình thức này để lừa gạt người mua.

Để tránh những thủ đoạn này:

Nên

- Kiểm soát xem địa chỉ trang mạng đó có bắt đầu bằng **https://** hay không. Mẫu tự "**s**" là chữ tắt của "secure" nghĩa là "an toàn".
- Dùng Paypal để trả tiền.
- Kiểm soát xem họ viết có đúng chính tả hay không.

Không nên

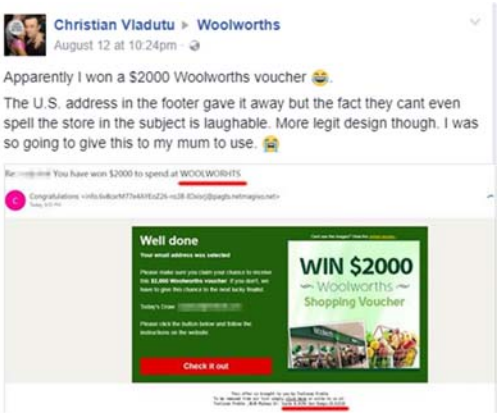
- Gởi money order.
- Chuyển tiền.

4. <u>Trúng số hay trúng thưởng bất ngờ</u>

Bạn được báo tin trúng số/trúng thưởng mà bạn không hề tham gia. Kẻ lừa đảo thường lấy tiền của bạn bằng cách yêu cầu bạn đóng tiền lệ phí trước khi nhận giải. Ngoài ra kẻ lừa đảo cũng có thể đòi bạn cung cấp các thông tin cá nhân cũng như những chi tiết về tài khoản ngân hàng để họ chuyển tiền trúng số vào nhưng thực ra họ sau đó sẽ dùng những chi tiết này để lấy tiền của bạn.

Nên

- Điều tra thực hư bằng cách tìm trên mạng chi tiết của cuộc sổ số này.
- Liên lạc và xin xác nhận trực tiếp với cơ quan đề cập. Tránh dùng đường dây liên lạc hoặc số điện thoại cung cấp bởi kẻ tình nghi.



Không nên

- Gởi tiền hoặc cho biết chi tiết thẻ tín dụng, chi tiết tài khoản ngân hàng của bạn.

5. Lợi dụng Covid-19 để lừa đảo

Đây là hình thức lừa đảo mới nhất. Bọn lừa đảo lợi dụng sự hoang mang, lo sợ của bạn để tung ra những chiêu lừa độc hại. Họ có thể mạo danh những cơ quan chính phủ, Bưu Điện hay cơ quan Y Tế để lấy thông tin của bạn.

Nên

- Kiểm tra trang mạng của họ xem có an toàn không. Một trang mạng an toàn khi địa chỉ của trang đó bắt đầu bằng **https://** và phải có mẫu tự "**s**" sau mẫu tự "**p**".
- Thiết lập và cập nhật thường xuyên hệ thống bảo vệ máy tính, chống vi khuẩn (anti virus).
- Báo cáo sự lừa đảo đến cơ quan trách nhiệm.

Không nên

- Tiết lộ chi tiết cá nhân.
- Cho phép họ xâm nhập máy computer của bạn từ xa (remote access).
- Mở những hồ sơ kèm theo (attachments) hay nhấn vào những đường dẫn được cung cấp.
- Làm theo áp lực của họ.
- Chuyển tiền cho họ.

Nói chung, các bạn cần cảnh giác, nắm vững tình hình, luôn luôn cẩn thận và không hoảng hốt.

Làm cách nào để báo cáo hành vi lừa đảo

Nơi tốt nhất để bạn báo cáo và học hỏi thêm về việc lừa đảo trên mạng là cơ quan Australian Competition and Consumer Commission's Scamwatch. Đây là một cơ quan của chính phủ mà bạn có thể tìm thấy qua địa chỉ mạng sau đây:

www.scamwatch.gov.au

Ngoài ra ở Nam Úc bạn có thể liên lạc với:

Catalyst Foundation Office
Địa chỉ 149 Currie Street, Adelaide

Hộp Thơ PO Box 1645, Adelaide SA 5001

Điện Thoại (08) 8168 8776

Email information@catalystfoundation.com.au

(Nguồn: Catalyst Foundation; Australian Competition and Consumer Commission's Scamwatch)

(Tóm tắt và chuyển ngữ: Hanh P)