BỘ CÔNG AN

CÔNG AN TỈNH HÀ TĨNH

CẨM NANG

NHẬN DIỆN VÀ PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

Hà Tĩnh, 01/2024

Tài liệu được tổng hợp từ Bộ Công an, Bộ Thông tin và Truyền thông

MỤC LỤC

I. TÌNH HÌNH CHUNG

1. Tổng hợp các hình thức lừa đảo phổ biến

Lừa đảo trên không gian mạng là vấn đề phức tạp trong tình hình hiện nay. Các đối tượng xấu lợi dụng bối cảnh bùng nổ công nghệ thông tin, sử dụng nhiều thủ đoạn hết sức tinh vi thực hiện hành vi lừa đảo, gây thiệt hại lớn về tài sản cho người dân. Trong đó, có 3 nhóm lừa đảo chính (giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác) với **26 hình thức lừa đảo** đang diễn ra trên không gian mạng phổ biến như:

1. Lừa đảo "combo du lịch giá rẻ"
2. Lừa đảo cuộc gọi video Deepfake
3. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao, nợ cước; lừa nâng cấp sim 4G…
4. Giả mạo biên lai chuyển tiền thành công
5. Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu
6. Chiêu trò lừa đảo tuyển người mẫu nhí, làm nhiệm vụ qua ứng dụng
7. Giả danh các công ty tài chính, ngân hàng để cho vay tiền
8. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen...
9. Giả mạo các website của các cơ quan, doanh nghiệp, bảo hiểm xã hội, ngân hàng...
10. Phát tán tin nhắn giả mạo thương hiệu (SMS Brandname)
11. Lừa đảo đầu tư chứng khoán quốc tế, tiền ảo
12. Lừa đảo tuyển dụng cộng tác viên bán hàng online
13. Chiếm đoạt (hack) hoặc mạo danh tài khoản mạng xã hội (Facebook, zalo...) nhắn tin lừa đảo người thân, bạn bè
14. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo
15. Lừa đảo trong mua bán hàng hóa trực tuyến
16. Đánh cắp thông tin Căn cước công dân đi vay tín dụng
17. Lừa đảo "chuyển nhầm tiền" vào tài khoản ngân hàng
18. Lừa đảo dịch vụ lấy lại tiền
19. Lừa đảo lấy cắp Telegram OTP
20. Lừa đảo tung tin giả về cuộc gọi mất tiền như FlashAI
21. Lừa đảo dịch vụ lấy lại Facebook
22. Lừa đảo tình cảm, lừa gửi quà
23. Lừa thông báo trúng thưởng
24. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook
25. Lừa đảo cho số đánh lô đề
26. Lừa đảo chuyển tiền từ thiện

2. Phải làm gì để phòng ngừa bị lừa đảo trên không gian mạng

*** Thực hiện nghiêm khẩu hiệu "4 không, 2 phải", gồm:**

- "4 không" là: [(1)]*Không sợ* (không hoảng sợ khi nhận được điện thoại, tin nhắn, các thông tin mà người lạ gửi đến có nội dung xấu liên quan đến cá nhân và người thân, thông báo có liên quan đến các vụ việc, vụ án…); ***[(2)]Không tham***

(không tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một cách dễ dàng, những lợi nhuận "phi thực tế" mà không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ, lương cao"...); [3]***Không kết bạn với người lạ*** (khi có người lạ mặt trên mạng xã hội kết bạn làm quen, mời tham gia các hội, nhóm mà không rõ là ai, mục đích thì không nên kết bạn, bắt chuyện, tham gia, nhất là không được cung cấp các thông tin cá nhân để đối tượng có thể lợi dụng); [4]***Không chuyển khoản*** (không chuyển tiền cho bất kỳ ai khi chưa xác thực rõ thông tin, khi các cá nhân không quen biết yêu cầu chuyển tiền hay làm một số việc thì tuyệt đối không được làm theo, không có cơ quan điều tra nào yêu cầu người dân phải chuyển khoản).

- **"2 phải" là:** [1]***Phải thường xuyên cảnh giác*** (chủ động bảo mật các thông tin cá nhân, nhất là các thông tin quan trọng như: Thông tin thẻ căn cước công dân; thông tin tài khoản ngân hàng; thông tin tài khoản mạng xã hội...); [2]***Phải tố giác ngay với cơ quan chức năng khi có nghi ngờ*** (khi nhận được các cuộc gọi, tin nhắn hoặc các nội dung nghi ngờ là hoạt động lừa đảo hoặc không có cơ sở khẳng định nội dung thì phải báo ngay cho cơ quan chức năng để được hướng dẫn xử lý).

*** Hành động nhanh nếu đã bị lừa đảo:** Nếu bạn đã bị lừa đảo, hãy ngay:

- Không tiếp tục gửi tiền và chặn tất cả các liên lạc từ kẻ lừa đảo.

- Liên hệ ngay lập tức với ngân hàng và tổ chức tài chính của bạn để báo cáo lừa đảo và yêu cầu họ dừng mọi giao dịch.

- Thu thập và lưu lại bằng chứng, tố giác tới cơ quan Công an nơi cư trú.

- Cảnh báo cho gia đình và bạn bè của bạn về trò lừa đảo này để họ có thể đề phòng những trò lừa đảo tiếp theo có thể xảy ra.

- Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại Cổng không gian mạng quốc gia (khonggianmang.vn); Cổng thông tin điện tử Công an tỉnh.

*** Nếu đã chuyển tiền cho một kẻ lừa đảo:** Nếu bạn đã chuyển tiền cho kẻ lừa đảo theo bất kỳ cách nào trong số này, đây sẽ là những việc cần làm:

- Thẻ tín dụng/thẻ ghi nợ: Hãy liên hệ ngay với ngân hàng của bạn để báo cáo hành vi lừa đảo và yêu cầu họ dừng mọi giao dịch.

- Thẻ quà tặng: Báo cáo cho công ty phát hành thẻ.

- Chuyển tiền ngân hàng: Báo cáo với công ty chuyển khoản ngân hàng hoặc ngân hàng mà bạn đang sử dụng.

- Ứng dụng chuyển tiền: Báo cáo với nhà cung cấp ứng dụng (người bán hoặc nhà phát triển, không phải cửa hàng ứng dụng).

- Tiền điện tử: Báo cáo cho nền tảng hoặc công ty bạn đã sử dụng để gửi tiền vì tiền điện tử không thể thu hồi được.

- Tiền mặt: Nếu bạn gửi qua thư hoặc chuyển phát, hãy liên hệ với Bưu điện hoặc dịch vụ chuyển phát đã sử dụng để xem liệu họ có thể chặn gói hàng hay không.

- Chuyển khoản trái phép: Nếu một kẻ lừa đảo đã chuyển tiền mà không có sự chấp thuận của bạn, hãy báo ngay cho ngân hàng của bạn để yêu cầu đóng băng tài khoản và giao dịch của bạn.

- Thu thập và lưu lại bằng chứng, làm đơn tố giác gửi tới cơ quan Công an.

*** Nếu một kẻ lừa đảo có thông tin cá nhân của bạn:** Nếu thông tin cá nhân của bạn (tên, số điện thoại, email, địa chỉ, giấy tờ tùy thân) đã bị rò rỉ do vi phạm dữ liệu, bạn cần làm:

- Báo cáo vi phạm dữ liệu cho các tổ chức tài chính của bạn.

- Tạo một mật khẩu mới mạnh hơn: Đảm bảo rằng bạn chưa từng sử dụng mật khẩu đó trước đây. Nếu bạn đã sử dụng mật khẩu bị rò rỉ ở bất kỳ nơi nào khác, hãy thay đổi mật khẩu ở đó.

- Coi chừng liên lạc đáng ngờ: Chặn hoặc không trả lời bất kỳ ai mà bạn không biết và không nhấp vào bất kỳ liên kết đáng nghi nào.

- Theo dõi chặt chẽ tài khoản ngân hàng của bạn.

*** Nếu kẻ lừa đảo đã truy cập vào máy tính hoặc điện thoại của bạn:** Nếu kẻ lừa đảo đã đánh cắp mật khẩu và thông tin tài chính của bạn:

- Nếu những kẻ lừa đảo truy cập vào máy tính của bạn: Hãy cập nhật phần mềm bảo mật và quét vi-rút. Xóa mọi thứ được xác định là có vấn đề và đặt lại mật khẩu của bạn.

- Nếu những kẻ lừa đảo truy cập vào điện thoại của bạn: Hãy báo cáo với nhà cung cấp dịch vụ điện thoại của bạn. Cập nhật phần mềm bảo mật và quét vi-rút. Thay đổi mật khẩu hoặc mã pin của bạn, chặn các cuộc gọi lừa đảo và xem xét thay đổi số điện thoại của mình.

- Nhờ chuyên gia công nghệ thông tin kiểm tra trực tiếp thiết bị của mình.

*** Liên hệ đường dây nóng của Công an tỉnh Hà Tĩnh:**

- Trực ban hình sự: 069.292.8312

- Phòng Cảnh sát hình sự: 069.292.8231

- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao: 069.292.8639

- Đường dây nóng Công an cấp xã nơi bạn đang cư trú *(Công an cấp xã đã công khai số điện thoại trên địa bàn)*

- Thường xuyên theo dõi, cập nhật các thông tin, tình huống, dấu hiệu cảnh báo về tội phạm trên không gian mạng tại **Cổng thông tin điện tử Công an tỉnh**, địa chỉ https://conganhatinh.gov.vn

Cổng thông tin điện tử Công an tỉnh

II. DẤU HIỆU NHẬN BIẾT VÀ CÁCH PHÒNG TRÁNH MỘT SỐ THỦ ĐOẠN PHỔ BIẾN

1. Lừa đảo "combo du lịch giá rẻ"

**** Dấu hiệu nhận diện:***

- Đăng tải bài viết quảng cáo bán tour du lịch, phòng khách sạn giá rẻ trên mạng Internet, mạng xã hội với nhiều tiện ích kèm theo, đề nghị nạn nhân chuyển tiền đặt cọc (từ 30-50% giá trị) để đặt cọc tour du lịch, phòng khách sạn, từ đó chiếm đoạt số tiền đặt cọc.

- Đăng bài viết quảng cáo dịch vụ làm visa (thị thực) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa. Sau khi nạn nhân chuyển khoản thanh toán chi phí hoặc một phần chi phí, các đối tượng sẽ để nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ… Sau đó lấy lý do nạn nhân khai thông tin bị thiếu và không trả lại tiền.

- Làm giả website/fanpage của công ty du lịch uy tín, làm giả ảnh chụp biên lai, hóa đơn thanh toán và đề nghị nạn nhân chuyển khoản thanh toán chi phí tour du lịch. Sau khi khách hàng chuyển khoản để thanh toán dịch vụ du lịch các đối tượng sẽ chặn liên lạc và xóa mọi dấu vết.

- Làm giả/chiếm đoạt tài khoản của người dùng mạng xã hội, liên lạc với người thân trong danh sách bạn bè cho biết đang bị mắc kẹt khi du lịch tại nước ngoài và cần một khoản tiền ngay lập tức.

- Các đối tượng mạo danh đại lý bán vé máy bay, tự tạo ra các website, trang mạng xã hội, với địa chỉ đường dẫn, thiết kế tương tự kênh của các hãng hoặc đại lý chính thức, sau đó quảng cáo với các mức giá rất hấp dẫn so với mặt bằng chung để thu hút khách hàng.

- Nếu khách hàng liên hệ, các đối tượng sẽ đặt chỗ vé máy bay, gửi mã đặt chỗ để làm tin và yêu cầu khách hàng thanh toán. Sau khi nhận thanh toán, các đối tượng không xuất ra vé máy bay và ngắt liên lạc. Do mã đặt chỗ chưa được xuất ra vé máy bay, nên sẽ tự hủy sau một thời gian và khách hàng thường chỉ biết được việc này khi đã đến sân bay nếu không thường xuyên kiểm tra mã đặt chỗ trên hệ thống.

**** Biện pháp phòng tránh:***

- Cần tìm hiểu kỹ thông tin khi lựa chọn các gói du lịch, nên lựa chọn dịch vụ đặt tour, đặt phòng, đặt vé máy bay của những công ty uy tín hoặc qua các App du lịch (ứng dụng du lịch). Để yên tâm hơn, người dân có thể đề nghị phía đối tác cho xem giấy phép hoạt động kinh doanh, giấy tờ, chứng chỉ hành nghề… của công ty lữ hành, du lịch.

- Cảnh giác khi nhận được lời mời chào mua gói du lịch với mức giá quá rẻ (rẻ hơn 30-50% so với giá chung của thị trường); đặc biệt thận trọng khi đơn vị du lịch yêu cầu chuyển tiền đặt cọc để giữ chỗ, nên thực hiện thanh toán trực tiếp.

- Chú ý các dấu hiệu nhận biết website giả mạo thông qua tên website và tên miền. Thông thường tên các website giả sẽ gần giống với tên các website thật nhưng sẽ có thêm hoặc thiếu một số ký tự. Tên miền giả thường sử dụng những đuôi lạ như .cc, .xyz, .tk…

- Nếu thông qua các trang mạng xã hội (Fanpage) để mua bán, nên chọn các trang mạng xã hội có dấu tích xanh (tài khoản đã đăng ký) hoặc chọn các trang mạng xã hội có uy tín mà mình biết rõ thông tin của người bán.

- Xác nhận lại thông tin đặt phòng, đặt vé máy bay trên các trang web chính thống, phòng vé của hãng bay, khách sạn để kịp thời phát hiện dấu hiệu lừa đảo, trình báo cho cơ quan Công an nơi gần nhất để được hướng dẫn giải quyết.

2. Lừa đảo cuộc gọi video Deepfake

Các đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video hoặc hình ảnh giả, sao chép chân dung để tạo ra các đoạn video giả người thân, bạn bè để thực hiện các cuộc gọi lừa đảo trực tuyến.

**** Dấu hiệu nhận biết:***

- Thời gian gọi thường rất ngắn chỉ vài giây.

- Khuôn mặt thiếu tính cảm xúc và khá "trơ" khi nói, hoặc tư thế trông lúng túng, không tự nhiên, hoặc là hướng đầu và cơ thể trong video không nhất quán với nhau…

- Màu da của nhân vật trong video bất thường, ánh sáng kỳ lạ và bóng đổ không đúng vị trí; điều này có thể khiến cho video trông rất giả tạo và không tự nhiên.

- Âm thanh có thể sẽ không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.

- Ngắt giữa chừng, bảo là mất sóng, sóng yếu...

- Yêu cầu chuyển tiền mà tài khoản chuyển tiền không phải của người đang thực hiện cuộc gọi.

**** Biện pháp phòng tránh:*** Khi nhận được một cuộc gọi yêu cầu chuyển tiền gấp, trước tiên hãy bình tĩnh và xác minh thông tin:

- Liên lạc trực tiếp với người thân, bạn bè thông qua một kênh khác xem có đúng là họ cần tiền không.

- Kiểm tra kỹ số tài khoản được yêu cầu chuyển tiền. Nếu là tài khoản lạ, tốt nhất là không nên tiến hành giao dịch.

- Nếu cuộc gọi từ người tự xưng là đại diện cho ngân hàng, hãy gác máy và gọi trực tiếp cho ngân hàng để xác nhận cuộc gọi vừa rồi có đúng là ngân hàng thực hiện hay không.

- Các cuộc gọi thoại hay video có chất lượng kém, chập chờn là một yếu tố để bạn nghi ngờ người gọi cũng như tính xác thực của cuộc gọi.

3. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao, nợ cước; lừa nâng cấp sim 4G…

**** Dấu hiệu nhận diện:***

- Các đối tượng mạo danh là cán bộ, nhân viên của cơ quan quản lý Nhà nước hoặc nhà mạng gọi điện và thông báo số điện thoại của người sử dụng sẽ bị khóa 2 chiều trong 2 tiếng với các lý do như "chưa nộp phạt", "thuê bao sai thông tin", "nợ cước"…

- Đối tượng yêu cầu cung cấp thông tin cá nhân, thông tin thuê bao, mã OTP...

- Sau khi yêu cầu cung cấp thông tin, chúng sẽ tiếp tục hướng dẫn người dùng thực hiện một số bước tiếp theo như: thực hiện các cú pháp sang tên đổi chủ thông tin số điện thoại, cú pháp chuyển hướng cuộc gọi...

- Khi đã chiếm được quyền nhận cuộc gọi, các đối tượng sẽ đăng nhập ứng dụng ví điện tử, tài khoản mạng xã hội… của nạn nhân và khai báo quên mật khẩu đăng nhập, chọn tính năng nhận cuộc gọi thông báo mã OTP. Từ đó, chúng dễ dàng chiếm đoạt tài khoản mạng xã hội, kiểm soát chiếm đoạt tiền trong ví, tài khoản ngân hàng liên kết với ví điện tử.

**** Biện pháp phòng tránh:***

- Chủ động kiểm tra thông tin đã chuẩn hóa hay chưa thông qua các công cụ, hướng dẫn từ nhà mạng. Chỉ thực hiện theo các thông báo cập nhật, chuẩn hóa thông tin từ các kênh chính thức của các doanh nghiệp viễn thông di động sử dụng cho mục đích nhắn tin, gọi điện thông báo đề nghị chuẩn hóa thông tin thuê bao. Đối với các thuê bao đã bị khóa hai chiều, người dân phải đến trực tiếp các điểm giao dịch của các nhà mạng để thực hiện chuẩn hóa và mở khóa liên lạc lại.

- Không thực hiện theo các yêu cầu khi nghe cuộc gọi từ số điện thoại lạ; không cung cấp mã OTP, thông tin cá nhân, thông tin thuê bao...

- Nếu cần biết thêm thông tin chi tiết có thể truy cập vào các trang web hoặc gọi điện đến tổng đài chăm sóc khách hàng của doanh nghiệp di động để được hỗ trợ, hướng dẫn.

4. Giả mạo biên lai chuyển tiền thành công

**** Dấu hiệu nhận diện:***

- Thủ đoạn của các đối tượng lừa đảo là mua hàng số lượng lớn, sau đó vay thêm tiền mặt của nạn nhân rồi chuyển khoản trả.

- Đối tượng đề nghị chuyển khoản theo hình thức Internet Banking cho người bán hàng. Nhưng thực chất là không có việc chuyển tiền thật, mà các đối tượng dùng các phần mềm tạo dựng bill thanh toán giả rồi đưa cho người bán hàng xem nhằm chứng minh là đã thực hiện việc chuyển khoản.

- Đối tượng gửi biên lai chuyển tiền thành công nhưng tài khoản ngân hàng chưa nhận được tiền, đối tượng giải thích với các lý do là ngân hàng bảo trì, giao dịch vào ngoài giờ hành chính...

- Biên lai chuyển tiền giả thường có một số đặc điểm khác với hình ảnh từ ngân hàng chính thống về màu sắc, phông chữ, thời gian...

**** Biện pháp phòng tránh:***

- Không vội vàng: Phải xem kỹ hóa đơn chuyển khoản, kiểm tra tiền đã về tài khoản hay chưa, không giao hàng hóa cho bất kỳ ai khi chưa nhận được tiền trong tài khoản ngân hàng, kể cả khi kẻ gian cung cấp hình ảnh đã chuyển khoản thành công.

- Chờ thông báo tiền về: Người tham gia giao dịch nên chờ thông báo đã nhận được tiền từ ngân hàng thay vì chỉ tin tưởng vào ảnh chụp giao diện chuyển tiền thành công. Với việc chuyển khoản 24/7 thường sẽ nhận được thông báo trong 15 phút.

- Không cung cấp tên đăng nhập, mật khẩu ứng dụng, mã xác thực OTP, email… cho bất kỳ ai kể cả khi người đó tự xưng là nhân viên ngân hàng, cơ quan nhà nước.

- Lưu ý các dấu hiệu khác lạ trong biên lai chuyển tiền.

5. Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu

**** Dấu hiệu nhận biết:***

- Các đối tượng lừa đảo tự xưng là giáo viên/nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con em/ người thân họ đang cấp cứu trong tình trạng nguy kịch. Những "thầy cô giáo tự xưng" này thay phiên nhau gọi điện thúc giục cha mẹ chuyển tiền cứu con, nếu không hoặc chậm nộp tiền thì con của họ sẽ nguy hiểm đến tính mạng.

- Các đối tượng đánh vào tâm lý, tình cảm của nạn nhân, hình thành trạng thái bất an, lo sợ và hoảng loạn cho phụ huynh.

- Các đối tượng thường trình bày không rõ ràng, sử dụng những ngôn từ tiêu cực nhằm kích động cảm xúc như nguy kịch, bị thương nặng, có thể không qua khỏi…

- Cách xưng hô khác thường ngày, thường không thể cung cấp thông tin cá nhân của mình một cách rõ ràng, thời gian gọi điện vào giờ nghỉ trưa, giữa đêm hay giờ tan tầm…

**** Biện pháp phòng tránh:***

- Hạn chế chia sẻ thông tin, hình ảnh cá nhân, con cái, danh tính của mình lên mạng xã hội. Hủy bỏ những dịch vụ mình đã đăng ký mà hiện không còn nhu cầu nữa để hạn chế bớt việc các đơn vị giữ thông tin của mình.

- Không cung cấp thông tin cá nhân, số điện thoại, số chứng minh thư (căn cước công dân), địa chỉ nhà ở, số tài khoản ngân hàng, mã OTP trên điện thoại cá nhân... cho bất kỳ ai không quen biết hoặc khi chưa biết rõ nhân thân, lai lịch.

- Khi nhận các cuộc điện thoại, tin nhắn có dấu hiệu bất thường, người dân cần bình tĩnh xác minh thông tin, xem xét một cách tỉnh táo, cẩn thận, không vội vã trả lời hay thực hiện theo nội dung mà đối tượng đưa ra.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ hoặc không rõ nguồn gốc. Không đăng nhập tài khoản cá nhân vào những địa chỉ này.

- Không chuyển tiền cho đối tượng nếu chưa xác thực rõ thông tin.

- Trong trường hợp nghi vấn đối tượng giả mạo để lừa đảo, chiếm đoạt tài sản, cần báo ngay cho cơ quan Công an gần nhất để được hỗ trợ, xử lý kịp thời.

6. Chiêu trò lừa đảo tuyển người mẫu nhí, làm nhiệm vụ trực tuyến để nhận tiền

**** Dấu hiệu nhận biết:***

- Thủ đoạn của đối tượng là lợi dụng lòng tham của người bị hại khi chỉ cần thực hiện những thao tác đơn giản mà cũng có thể kiếm ra tiền; nạn nhân vì nhẹ dạ, chỉ thấy được cái lợi trước mắt mà dễ dàng dính bẫy lừa đảo.

- Các đối tượng là thông qua mạng xã hội như Facebook, Zalo, Telegram… kết bạn, mời tham gia ứng tuyển người mẫu nhí cho hãng thời trang hay tham gia làm các nhiệm vụ trên các ứng dụng để kiếm tiền. Sau khi nạn nhân "cắn câu", các đối tượng lừa đảo sẽ đưa vào một group chat để mời tham gia thử thách.

- Thử thách cho người chơi là những công việc khá đơn giản, như xem, like, share video, bài viết; chuyển khoản để mua sản phẩm hàng hiệu, cho con em mình làm mẫu chụp ảnh để giới thiệu, quảng bá sản phẩm trên mạng xã hội.

- Thông thường ban đầu chúng trả hoa hồng và tiền làm nhiệm vụ để "kích thích" phụ huynh tham gia; nhưng khi số tiền chuyển vào tài khoản tăng cao, chúng xóa tung tích nhằm chiếm đoạt số tiền đã chuyển.

- Các tài khoản đăng tải thông tin nếu là tài khoản ảo, thông tin liên hệ không rõ ràng, không xác định được định danh thì khả năng cao đều lập ra với mục đích lừa đảo. Thông tin đăng tải là tin giả, thường sẽ bị lỗi chính tả hoặc có bố cục lộn xộn, các hình ảnh, video trong thường bị chỉnh sửa, cắt ghép, thay đổi nội dung, ngày tháng của sự kiện thường bị thay đổi.

**** Biện pháp phòng tránh:***

- Không cung cấp những thông tin cá nhân cho người lạ, người không quen biết trên không gian mạng; không kết bạn, không vào các nhóm Zalo, Facebook, Telegram… không quen biết.

- Đặc biệt cẩn trọng đối với các chương trình tuyển mẫu nhí trên không gian mạng và hạn chế gửi hình ảnh của con nhằm phòng ngừa đối tượng lợi dụng với mục đích xấu. Trường hợp cần thiết để tham gia tuyển mẫu nhí phụ huynh nên đề nghị được gặp mặt trực tiếp để phòng tránh các chiêu trò lừa đảo qua mạng.

- Kiểm tra tác giả, đọc kỹ nội dung để xác định thông tin thật hay giả.

- Không làm việc với nhà tuyển dụng mà yêu cầu ứng viên phải chuyển tiền, nộp tiền trước. Chỉ thực hiện giao dịch chuyển tiền khi xác định chắc chắn định danh của người mình trao đổi và tuyệt đối không click vào những đường link lạ.

7. Giả danh các công ty tài chính, ngân hàng để cho vay tiền

**** Dấu hiệu nhận biết:***

- Thủ đoạn của các đối tượng là đánh vào tâm lý những người cần vay số tiền lớn nhưng không đủ điều kiện vay vốn tại các tổ chức tài chính; từ đó, đối tượng mạo danh ngân hàng và các công ty tài chính để chào mời cho vay.

- Đối tượng lừa đảo lập tài khoản facebook ảo, tham gia vào các hội nhóm, diễn đàn, đăng bài quảng cáo cho vay tín chấp với lãi suất thấp (chỉ 01%/ tháng), thủ tục vay đơn giản, không cần gặp trực tiếp; nợ xấu vẫn vay được; không thế chấp, không thẩm định, chỉ cần Chứng minh nhân dân hoặc Căn cước công dân và có tài khoản ngân hàng/thẻ ATM là có thể vay được tiền...

- Khi có người vay tiếp cận, các đối tượng sẽ dẫn dụ, yêu cầu người vay truy cập vào các trang web, ứng dụng (các ứng dụng này sẽ thu thập các thông tin trên điện thoại) và cung cấp thông tin cá nhân, như: họ tên, số điện thoại, ảnh chụp CMND/CCCD, ảnh chụp chân dung… phục vụ làm hồ sơ vay.

- Đối tượng yêu cầu người vay đóng các loại phí bảo hiểm, xác minh, duyệt khoản vay.

- Sau khi người vay chuyển tiền, đối tượng tiếp tục viện dẫn hàng loạt các lý do khoản vay không được giải ngân xuất phát từ lỗi khai hồ sơ của người vay *(như khai sai tên người hưởng thụ, đổi cách viết tên người hưởng thụ từ chữ in thường sang in hoa, không đủ điều kiện vay, thừa hoặc sai một số trên số căn cước công dân…).* Từ đó, chúng yêu cầu người vay phải nộp thêm tiền. Tuy nhiên, khi người vay chuyển tiền vào số tài khoản của các đối tượng cung cấp, các đối tượng sẽ lập tức chiếm đoạt và ngắt liên lạc.

**** Biện pháp phòng tránh:***

- Không tham gia vào các hoạt động "tín dụng đen" trên không gian mạng, vay tiền qua các ứng dụng, trang web không rõ nguồn gốc. Khi có nhu cầu vay tiền, cần liên hệ trực tiếp với các tổ chức tín dụng, chi nhánh ngân hàng để được tư vấn, hướng dẫn làm thủ tục vay vốn.

- Cảnh giác, tìm hiểu kỹ, xác thực chính xác công ty tài chính, tư vấn viên trước khi tiến hành các thủ tục vay tiền bằng cách:

+ Kiểm tra mã số thuế, địa chỉ, người đại diện công ty.

+ Gọi điện đến các đường dây nóng, chăm sóc khách hàng của các công ty.

+ Kiểm tra kỹ các đường link trang web trước khi truy cập.

+ Nên tư vấn thêm ý kiến của người thân có nhiều kinh nghiệm trước khi làm các thủ tục vay.

- Không cung cấp bất kỳ thông tin cá nhân (Chứng minh nhân dân/Căn cước công dân, địa chỉ, hình ảnh nhận diện khuôn mặt…) khi chưa xác định chính xác website, ứng dụng và danh tính tư vấn viên.

- Tuyệt đối không cung cấp thông tin tài khoản ngân hàng, mã OTP được gửi vào hòm thư, điện thoại di động cho các đối tượng.

- Không chuyển tiền vào tài khoản do các đối tượng lạ cung cấp, dụ dỗ.

- Nhanh chóng trình báo cơ quan Công an nơi gần nhất khi phát hiện thủ đoạn lừa đảo chiếm đoạt tài sản.

8. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen...

**** Dấu hiệu nhận biết:***

- Lợi dụng tính năng cho phép đăng thông tin của trang web như đăng hỏi đáp, diễn đàn, tải tập tin, các đối tượng xấu đưa quảng cáo lên. Các ứng dụng vay tiền trực tuyến hay các link quảng cáo cờ bạc, cá độ thường được quảng cáo rộng rãi trên các trang web với những tiêu đề thu hút như "*Không cần thế chấp, lãi suất không đồng", "Vay siêu tốc, nhận tiền sau 30 phút, lãi suất thấp, nhận tiền ngay*"… hoặc nhắn tin qua số điện thoại kèm theo đường link đến ứng dụng… Người có nhu cầu tham gia chỉ cần ấn (click) vào những trang quảng cáo, tải các ứng dụng về máy tính hoặc điện thoại thông minh, nhập các thông tin cá nhân, số tài khoản ngân hàng nhận tiền, ảnh chứng minh nhân dân, ảnh cá nhân và đồng ý cho truy cập vào danh bạ cá nhân…

- Các app vay tiền biến tướng này thường mạo danh hoặc giả mạo là một công ty để gây dựng lòng tin ban đầu đối với nạn nhân.

- Khi người dùng đồng ý cấp quyền truy cập danh bạ, hình ảnh thì các ứng dụng này cũng sẽ sao lưu được các thông tin số điện thoại có trong danh bạ cũng như các hình ảnh được lưu trong điện thoại. Chính vì vậy, các đối tượng lừa đảo đã có được thông tin để đe dọa, làm phiền nạn nhân và người thân của họ. Các điều khoản, chính sách của các app này cũng chứa các nội dung bất lợi cho nạn nhân, bao gồm thỏa thuận buộc nạn nhân chấp nhận mọi hình thức thu hồi nợ, bất chấp đó là các hình thức đe dọa, khủng bố mạng, bôi nhọ danh dự nạn nhân.

**** Biện pháp phòng tránh:***

- Nếu cần vay tiền, bạn nên tìm đến các tổ chức cho vay uy tín như ngân hàng, hoặc các công ty tài chính hợp pháp.

- Tuyệt đối không cung cấp bất kỳ thông tin cá nhân, tài khoản ngân hàng trên các trang web và ứng dụng không tin cậy.

- Khi cài đặt bất kỳ ứng dụng nào, đặc biệt liên quan đến tài chính, bạn nên xem xét cẩn thận các quyền mà ứng dụng yêu cầu cũng như đọc kỹ các điều khoản, chính sách của ứng dụng này. Nếu phát hiện có điểm đáng ngờ, hãy hủy cài đặt ứng dụng ngay lập tức.

- Nếu phát hiện bất kỳ ứng dụng, website có dấu hiệu lừa đảo, có thể báo cáo với NCSC tại địa chỉ https://canhbao.khonggianmang.gov.vn

9. Giả mạo các website của các cơ quan, doanh nghiệp, bảo hiểm xã hội, ngân hàng…

**** Dấu hiệu nhận biết***

- Các đối tượng tạo trang web có giao diện gần giống trang web của cơ quan, doanh nghiệp từ hình ảnh, giao diện và nội dung để người dùng nhầm tưởng là trang web của đơn vị cung cấp. Sau đó, sử dụng tin nhắn giả mạo thương hiệu với các nội dung yêu cầu người dùng phải truy cập vào liên kết giả mạo, khai báo thông tin cá nhân, tài khoản ngân hàng hoặc giả danh nhân viên ngân hàng, cơ quan, doanh nghiệp liên hệ hướng dẫn nâng cấp app, nâng hạn mức thẻ tín dụng, hủy giao dịch... và từ đó thực hiện hành vi đánh cắp, chiếm đoạt thông tin dữ liệu người dùng, lừa đảo.

- Dấu hiệu nhận biết các website không an toàn:

+ Thông thường không được chú trọng nhiều về nội dung, đồng thời thông tin đăng tải khá cẩu thả, sai lỗi chính tả nhiều; thường có đường dẫn bất thường như là vn-cbs.xyz. vn-ms.top…

+ Các link website giả mạo thường được lồng ghép trong các cảnh báo, đe dọa hoặc các chương trình trúng thưởng hấp dẫn với nhiều phần quà có giá trị để dụ dỗ người dùng truy cập vào các đường link này từ đó đánh cắp dữ liệu cá nhân, hoặc điều hướng truy cập đến những website không an toàn khác có chứa mã độc hại.

+ Trang không có các biểu tượng bảo mật như khóa SSL hay "https://" trước URL, cuối trang web chưa có logo của Bộ Công Thương, đó có thể là dấu hiệu của một trang web mới được tạo ra, chưa có độ an toàn hoặc giả mạo.

+ Khi người dùng vừa truy cập website mà đã yêu cầu cung cấp những thông tin cá nhân như địa chỉ nhà, số điện thoại, số CMND/CCCD.

**** Biện pháp phòng tránh:***

- Kiểm tra kỹ địa chỉ URL: Luôn kiểm tra URL của trang web trước khi cung cấp thông tin cá nhân. Hãy chắc chắn rằng địa chỉ URL chính xác và tương ứng với trang web mà bạn mong muốn truy cập; các website chính thức của các tổ chức thường sử dụng giao thức https và kết thúc bằng đuôi ".vn".

- Sử dụng trình duyệt an toàn: Sử dụng trình duyệt web có tính năng bảo mật cao và cập nhật phiên bản mới nhất. Các trình duyệt như Google Chrome, Mozilla Firefox và Safari thường có các cơ chế bảo mật tích hợp giúp ngăn chặn truy cập vào trang web độc hại.

- Kiểm tra kết nối an toàn: Bằng cách kiểm tra xem trang web có chứng chỉ SSL hợp lệ hay không; nếu trang không có các biểu tượng bảo mật như khóa SSL hay "https://" trước URL, đó có thể là dấu hiệu của một trang web giả mạo và thông tin của bạn có thể bị đánh cắp.

- Cẩn thận với email và liên kết: Tránh nhấp vào liên kết trong email không xác định hoặc không mong muốn.

- Hạn chế cung cấp thông tin cá nhân: Chỉ cung cấp thông tin cá nhân trên các trang web đáng tin cậy và an toàn. Không cung cấp thông tin cá nhân như địa chỉ nhà, số điện thoại, số CMND/CCCD, mật khẩu, số thẻ tín dụng, mã OTP hoặc tài khoản ngân hàng trên các trang web không xác định hoặc không đáng tin.

- Sử dụng phần mềm bảo mật: Cài đặt và duy trì phần mềm diệt virus, phần mềm chống độc, tường lửa và các công cụ bảo mật khác trên thiết bị của bạn.

- Giữ tỉnh táo và cảnh giác: Luôn cảnh giác khi truy cập vào các trang web và giao dịch trực tuyến.

- Kiểm tra đánh giá và phản hồi: Trước khi thực hiện giao dịch hoặc cung cấp thông tin cá nhân, hãy kiểm tra các đánh giá và phản hồi từ người dùng khác về trang web đó; nếu có nhiều phản hồi tiêu cực hoặc cảnh báo về lừa đảo, không truy cập vào trang web đó.

- Sử dụng các phương pháp xác thực bổ sung như xác thực hai yếu tố hoặc sử dụng mã OTP để bảo vệ tài khoản của bạn.

- Đừng dễ tin vào thông báo đột xuất: Cẩn thận với các thông báo đột xuất yêu cầu cập nhật thông tin cá nhân hoặc yêu cầu thay đổi mật khẩu. Luôn truy cập vào trang web chính thức của dịch vụ và thực hiện các thay đổi thông qua đó, thay vì truy cập qua liên kết trong email hoặc thông báo không xác định.

- Nếu phát hiện một trang web giả mạo, hãy báo cáo cho nhà cung cấp dịch vụ trực tuyến hoặc cơ quan chức năng có thẩm quyền để ngăn chặn, xử lý.

10. Phát tán tin nhắn giả mạo thương hiệu (SMS Brandname)

**** Dấu hiệu nhận biết:***

- Các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới điện thoại người dùng.

- Nội dung tin nhắn giả mạo luôn kèm đường dẫn đến trang web giả mạo do đối tượng quản lý (các trang web này có tên gần giống với trang web chính thức của ngân hàng, tổ chức...), khi người dùng truy cập vào đường dẫn, sẽ yêu cầu điền thông tin cá nhân, tên đăng nhập, mật khẩu, OTP...

- Mỗi thiết bị BTS giả có thể phát tán tới mấy chục nghìn tin nhắn/1 ngày.

**** Biện pháp phòng tránh:***

- Đọc kỹ nội dung tin nhắn, kiểm tra các lỗi chính tả, xem xét một cách tỉnh táo, cẩn thận, không vội vã trả lời hay thực hiện theo nội dung trong tin nhắn. Các ngân hàng, đơn vị cung cấp dịch vụ... thường không yêu cầu khách hàng cung cấp thông tin cá nhân thông qua SMS, email, phần mềm chat,... vì vậy, việc xuất hiện các tin nhắn có nội dung yêu cầu cung cấp thông tin cá nhân là điều bất thường.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ hoặc không rõ nguồn gốc; không đăng nhập tài khoản cá nhân vào những địa chỉ này.

- Không cung cấp tên, mật khẩu đăng nhập ngân hàng trực tuyến, mã xác thực OTP, số thẻ ngân hàng qua điện thoại, email, mạng xã hội và các trang web. Chỉ sử dụng dịch vụ ngân hàng điện tử thông qua website chính thức của ngân hàng, có thể liên hệ với tổng đài ngân hàng để lấy thông tin trang chính thức.

- Khi nhận được các tin nhắn có dấu hiệu bất thường phải liên lạc ngay với đơn vị chủ quản của brandname thông qua hotline; luôn gọi điện thoại lên công ty, tổ chức có liên quan để kiểm chứng.

- Lưu lại các bằng chứng, phản ánh tới Doanh nghiệp viễn thông để yêu cầu xử lý.

11. Lừa đảo đầu tư chứng khoán quốc tế, tiền ảo

**** Dấu hiệu nhân biết:*** Các sàn đầu tư chứng khoán quốc tế, giao dịch vàng, ngoại hối, tiền ảo, bất động sản, kinh doanh đa cấp có nguy cơ lừa đảo chiếm đoạt tài sản thường có dấu hiệu:

- Lời hứa quá cao: Sàn đầu tư lừa đảo thường hứa lợi nhuận vượt trội, không thể tin được và quá cao so với thị trường thực tế.

- Thiếu thông tin minh bạch: Sàn không cung cấp đầy đủ thông tin về công ty, giấy phép hoạt động, lịch sử giao dịch và nhân sự quản lý.

- Yêu cầu chuyển tiền trước: Sàn yêu cầu người tham gia chuyển khoản tiền trước khi bắt đầu giao dịch, thường là dưới hình thức phí đăng ký, phí tham gia hoặc tiền ký quỹ.

- Thiếu sự kiểm soát và giám sát: Sàn không có sự kiểm soát từ các cơ quan quản lý hoặc không được cấp phép hoạt động đúng quy định.

- Đối tượng có thể can thiệp vào hệ thống để chiếm đoạt tiền của người tham gia

**** Biện pháp phòng tránh:***

- Tìm hiểu về hệ thống bảo mật: Đối với các sàn giao dịch và công ty trực tuyến, hãy tìm hiểu về hệ thống bảo mật và cơ chế bảo vệ thông tin cá nhân và tài sản của người dùng.

- Nghiên cứu đánh giá từ người dùng khác, tìm kiếm sự tư vấn chuyên gia đối với sàn giao dịch hoặc công ty mà bạn quan tâm.

- Cảnh giác với mức phí và chi phí: Hãy cẩn trọng với các khoản phí và chi phí không rõ ràng hoặc quá cao so với thị trường thông thường.

- Thận trọng với các lời mời giới thiệu: Hãy cẩn trọng khi người khác đề nghị hoặc giới thiệu các hoạt động đầu tư mà bạn không biết gì về.

- Luôn cảnh giác khi giao dịch, không tham gia đầu tư vào các sàn giao dịch chưa được cấp phép; không chuyển tiền cho một cá nhân khác để nhờ nộp tiền vào hệ thống nếu họ không đáng tin cậy.

12. Lừa đảo tuyển dụng cộng tác viên bán hàng online

**** Dấu hiệu nhận diện:***

- Thủ đoạn của đối tượng lừa đảo là:

+ Mạo danh nhân viên các công ty, doanh nghiệp, các trang thương mại điện tử (như Shopee, Lazada, Tiki...) lôi kéo người dân tham gia làm cộng tác viên bán hàng online với lợi nhuận hấp dẫn, "việc nhẹ lương cao".

+ Đối tượng thường giao nhiệm vụ cho cộng tác viên hết sức đơn giản (như đăng, chia sẻ bài trên facebook...) để nhận tiền; sau đó chúng cho đối tượng khác đóng vai "khách hàng" liên hệ cộng tác viên đặt mua hàng và gửi các hóa đơn giả chuyển tiền đặt cọc đến các tài khoản của công ty. Để hoàn thành đơn hàng, các công ty yêu cầu cộng tác viên chuyển thêm các khoản tiền cho công ty để lấy hàng về giao cho "khách hàng", sau đó các đối tượng "khách hàng" sẽ hủy hợp đồng và cắt liên lạc. Hoặc yêu cầu cộng tác viên nộp một khoản tiền tạm ứng ngay từ đâu trước khi bắt đầu công việc, sau đó chiếm đoạt và cắt đứt liên lạc.

+ Những đơn hàng đầu tiên có giá trị thấp đối tượng có thể sẽ trả đủ tiền cho cộng tác viên để dụ dỗ, "kích thích" con mồi; đến lần tiếp theo, khi cộng tác viên đặt hàng, tạm ứng với số tiền lớn thì đối tượng chiếm đoạt tiền đặt hàng, đồng thời yêu cầu nộp thêm tiền để hệ thống xử lý lỗi và hoàn trả lại tiền nhưng đều bị chiếm đoạt.

- Phải tạm ứng tiền khi chưa hoàn thành công việc.

- Phải cung cấp thông tin tài khoản cá nhân, bao gồm số thẻ tín dụng hoặc thông tin ngân hàng, với lý do để thực hiện thanh toán hoặc tạo tài khoản.

- Trang thanh toán đơn hàng không an toàn, có dấu hiệu giả mạo các trang web của ngân hàng.

- Quảng cáo công việc quá hấp dẫn và dễ dàng với thu nhập cao mà không yêu cầu kỹ năng hay kinh nghiệm đặc biệt.

- Thiếu thông tin, thông tin không rõ ràng hoặc không có thông tin liên hệ của công ty và người tuyển dụng.

- Thiếu hợp đồng hoặc thoả thuận rõ ràng trong việc cộng tác.

**** Biện pháp phòng tránh:***

- Tìm hiểu kỹ thông tin tuyển dụng và đối tượng đăng tin tuyển cộng tác viên bằng nhiều nguồn thông tin khác nhau.

- Kiểm tra về đánh giá và phản hồi tiêu cực đối với đối tượng đăng tin tuyển dụng, nếu có nhiều phản hồi tiêu cực hoặc đánh giá không tốt, hãy cân nhắc trước khi tham gia.

- Cảnh giác trước những lời mời chào hấp dẫn, hứa hẹn với hoa hồng cao bất thường, "việc nhẹ lương cao", công việc dễ dàng, không yêu cầu trình độ, kinh nghiệm...

- Nếu đối phương yêu cầu tạm ứng tiền, cung cấp thông tin cá nhân thì phải cảnh giác; không tạm ứng tiền, không chia sẻ thông tin nhạy cảm của bạn với bất kỳ ai nếu không tin tưởng hoặc không xác thực rõ mọi thông tin.

- Khi thực hiện nhiệm vụ mà phát hiện đối phương có dấu hiệu chần chừ trong việc thanh toán tiền thì cần dừng ngay việc mua hàng.

- Không thanh toán, đăng nhập tài khoản ngân hàng vào các trang web không an toàn.

- Khi tham gia làm cộng tác viên, hãy yêu cầu và đọc kỹ hợp đồng, thoả thuận. Nếu không có hợp đồng hoặc thoả thuận rõ ràng, có thể sẽ gặp rủi ro bị lừa đảo.

13. Chiếm đoạt (hack) hoặc mạo danh tài khoản mạng xã hội (Facebook, zalo...) nhắn tin lừa đảo người thân, bạn bè

**** Dấu hiệu nhận diện:***

- Tin nhắn hoặc email đáng ngờ: Nếu bạn nhận được một tin nhắn hoặc email từ một người bạn trong danh sách bạn bè yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu chuyển tiền hoặc thực hiện hành động khẩn cấp, hãy cảnh giác.

- Sự thay đổi đột ngột trong ngôn ngữ hoặc phong cách viết: Nếu tin nhắn từ bạn bè có sự thay đổi đột ngột trong cách viết, từ ngữ không giống với phong cách thông thường hoặc có chứa các lời lẽ lạ lùng, cần thận hơn.

- Đường link đáng ngờ: Kiểm tra đường link được chia sẻ trong tin nhắn. Nếu đường link có dấu hiệu đáng ngờ như URL không phổ biến, thiếu ký tự an toàn (https://), hoặc điều hướng đến các trang web không rõ nguồn gốc hoặc đáng ngờ.

- Yêu cầu cung cấp thông tin cá nhân hoặc thông tin đăng nhập: Đối tượng lừa đảo thường sử dụng chiêu này để chiếm quyền điều khiển tài khoản của bạn.

**** Biện pháp phòng tránh:***

- Xác minh thông tin: Nếu nhận được tin nhắn, email đáng ngờ từ một người bạn, có chứa các lời khẩn cấp, đe dọa, yêu cầu chuyển tiền hoặc yêu cầu không phù hợp, hãy kiểm tra lại xem có phải tin nhắn thực sự từ bạn bè hay không bằng cách liên hệ trực tiếp với họ thông qua các phương tiện khác (điện thoại, tin nhắn...); không sử dụng thông tin liên hệ được cung cấp trong tin nhắn đáng ngờ để xác minh.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn; không đăng nhập tài khoản cá nhân, tài khoản ngân hàng vào những địa chỉ này.

- Không cung cấp thông tin cá nhân nhạy cảm, thông tin đăng nhập (tên đăng nhập, mật khẩu) thông qua tin nhắn hoặc email.

- Báo cáo và cảnh báo: Nếu nhận thấy dấu hiệu lừa đảo, hãy thông báo ngay với người xung quanh.

- Luôn giữ cảnh giác và tuân thủ các biện pháp bảo mật cơ bản như không chia sẻ thông tin cá nhân và mật khẩu với bất kỳ ai, không bấm vào các liên kết không rõ nguồn gốc hoặc tin nhắn đáng ngờ, và cập nhật phần mềm bảo mật định kỳ để tránh các lỗ hổng bảo mật.

- Nếu gặp phải các dấu hiệu trên, hãy:

+ Thay đổi mật khẩu ngay lập tức của tài khoản MXH và sử dụng một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt.

+ Báo cáo sự cố thông qua MXH hoặc các liên hệ khác như điện thoại, email.

+ Thông báo cho bạn bè và người thân trong danh sách bạn bè của bạn về tình huống và cảnh báo họ không nên tin tưởng hoặc phản hồi vào những tin nhắn lừa đảo.

14. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo

**** Dấu hiệu nhận biết:***

- Đối tượng tự xưng là cơ quan công an, viện kiểm sát, tòa án...

- Sử dụng số điện thoại giả mạo: Đối tượng sẽ sử dụng số điện thoại giả mạo, thường có đầu số bất thường. Hãy lưu ý rằng cơ quan chức năng sẽ không làm việc chính thức qua điện thoại.

- Đe dọa và áp lực tâm lý: Đối tượng sẽ sử dụng các cách thức đe dọa, áp lực tâm lý như khống chế, hăm dọa, nói dối về việc có liên quan đến các vụ án đang điều tra để tạo áp lực và đánh vào sợ hãi của nạn nhân.

- Yêu cầu chuyển tiền hoặc thông tin cá nhân: Đối tượng sẽ yêu cầu bạn chuyển tiền vào một tài khoản cụ thể hoặc cung cấp thông tin cá nhân như số thẻ tín dụng, số căn cước công dân, mã số bảo mật và các thông tin nhạy cảm khác. Điều này nhằm mục đích chiếm đoạt tài sản của bạn.

- Yêu cầu nạn nhân không được tiết lộ nội dung mà đối tượng trao đổi cho bất kỳ ai.

- Tạo áp lực thời gian: Đối tượng thường tạo áp lực thời gian cho bạn, yêu cầu hành động phải được thực hiện ngay lập tức để tránh hậu quả nghiêm trọng. Đối tượng sẽ thuyết phục bạn rằng không có thời gian để suy nghĩ hay tham khảo người khác.

**** Biện pháp phòng tránh:***

- Giữ bình tĩnh và không bị đánh lừa bởi áp lực tâm lý và đe dọa.

- Xác minh thông tin: Hãy tự xác minh danh tính và thông tin của người gọi bằng cách gọi lại vào số điện thoại chính thức của cơ quan đó hoặc liên hệ trực tiếp với cơ quan Công an nơi cư trú.

- Không cung cấp thông tin cá nhân hay tiền bạc qua điện thoại, email hoặc các phương tiện truyền thông khác.

- Khi có người lạ gọi đến, tuyệt đối không chuyển tiền hay làm theo lời của đối tượng.

- Báo cáo sự việc: Nếu nhận được cuộc gọi đe dọa hoặc nghi ngờ có dấu hiệu lừa đảo, hãy thông báo ngay cho cơ quan Công an để được hỗ trợ và tư vấn.

- Lưu ý rằng, các cơ quan quản lý nhà nước sẽ không yêu cầu bạn chuyển tiền hoặc cung cấp thông tin nhạy cảm qua điện thoại một cách đột ngột mà không có văn bản thông báo trước; không làm việc, lấy lời khai qua điện thoại.

15. Lừa đảo trong mua bán hàng hóa trực tuyến

**** Cảnh báo:*** Thủ đoạn lừa đảo của người bán hàng là quảng cáo sản phẩm với lời mời chào hấp dẫn. Khi nhận được tiền cọc hoặc toàn bộ số tiền thanh toán của người mua thì đối tượng không giao hàng hoặc giao hàng giả, kém chất lượng, sai mẫu mã, sau đó cắt đứt liên lạc và chiếm đoạt tiền của người mua. Hoặc người mua hàng liên hệ người bán để mua hàng số lượng lớn, sau khi nhận được hàng thì cắt đứt liên lạc, chiếm đoạt hàng hóa hoặc tạo hóa đơn chuyển tiền giả để chiếm đoạt tài sản của người bán.

**** Dấu hiệu nhận diện:*** Các trang thương mại điện tử, tài khoản mạng xã hội (Zalo, Facebook, Tiktok...) rao bán hàng giả, hàng nhái trên mạng xã hội có dấu hiệu:

- Giá quá rẻ: Sản phẩm được rao bán với giá cực kỳ hấp dẫn, thường rẻ hơn rất nhiều so với giá thị trường.

- Thiếu thông tin sản phẩm: Người bán không cung cấp đủ thông tin chi tiết về sản phẩm, như thông số kỹ thuật, nguồn gốc, chất lượng, thông tin về nhà cung cấp và bảo hành.

- Số lượng giới hạn và áp lực mua hàng: Người bán áp đặt áp lực mua hàng nhanh chóng bằng cách khuyến khích mua hàng ngay lập tức với lý do rằng hàng chỉ có số lượng giới hạn hoặc đang có nguy cơ hết hàng.

- Đánh giá và nhận xét không tự nhiên: Sản phẩm nhận được đánh giá và nhận xét tích cực một cách quá mức, không tự nhiên hoặc không đáng tin cậy. Đây là một chiêu trò để tạo lòng tin và thuyết phục người mua.

- Phương thức thanh toán không an toàn: Người bán yêu cầu thanh toán bằng các phương thức không an toàn, như chuyển khoản trực tiếp qua ngân hàng, thanh toán bằng ví điện tử không rõ nguồn gốc, hoặc yêu cầu cung cấp thông tin thẻ tín dụng một cách đáng ngờ.

- Tài khoản người bán không đáng tin: Kiểm tra tài khoản của người bán trên mạng xã hội hoặc sàn thương mại điện tử, thường sẽ ít hoặc không có thông tin cá nhân, hoạt động mới hoặc không có đánh giá.

- Thiếu thông tin liên hệ và địa chỉ: Người bán không cung cấp thông tin liên hệ rõ ràng, như địa chỉ, số điện thoại hoặc email; điều này khiến việc theo dõi và giải quyết các vấn đề liên quan trở nên khó khăn.

- Thiếu uy tín và phản hồi tiêu cực: Người bán có lịch sử phản hồi tiêu cực, có nhiều khiếu nại từ người mua trước đó hoặc không có đủ đánh giá và phản hồi từ khách hàng.

**** Biện pháp phòng tránh:***

- Nghiên cứu và đánh giá kỹ thông tin đối tượng: Kiểm tra thông tin về người bán/người mua, bao gồm địa chỉ, số điện thoại, độ tin cậy của tài khoản đang liên hệ và nhận xét từ người mua khác trên các trang web đáng tin cậy.

- Kiểm tra thông tin sản phẩm: Đảm bảo bạn có đủ thông tin chi tiết về sản phẩm, hình ảnh chất lượng và mô tả chính xác.

- Tìm hiểu về chính sách bảo hành và hoàn tiền: Đảm bảo bạn hiểu rõ chính sách bảo hành và hoàn tiền của người bán, và có thể liên hệ với họ nếu cần thiết.

- Tìm kiếm phản hồi và đánh giá: Tìm hiểu ý kiến và đánh giá từ người mua khác về người bán và sản phẩm để có cái nhìn tổng quan.

- Luôn cảnh giác và nghĩ kỹ trước khi thao tác mua hàng trực tuyến trên sàn thương mại điện tử và mạng xã hội.

16. Đánh cắp thông tin Căn cước công dân đi vay tín dụng

*** Cảnh báo:**

- Cảnh báo về việc tiết lộ thông tin cá nhân: Sử dụng thông tin trên CCCD, chứng minh nhân dân để đăng ký mã số thuế ảo hoặc cung cấp thông tin cá nhân như số CMND, ngày sinh, địa chỉ trên mạng xã hội có thể rất nguy hiểm. Kẻ gian có thể lợi dụng thông tin này để thực hiện các hoạt động lừa đảo hoặc chiếm đoạt tài sản của bạn.

- Cảnh báo về vay tiền từ các tổ chức tín dụng trên mạng xã hội: Các tổ chức tín dụng trên mạng xã hội có thể cung cấp dịch vụ vay tiền nhanh chóng và dễ dàng. Tuy nhiên, hãy cẩn trọng với các khoản lãi suất cao và các điều khoản vay không rõ ràng. Nếu không thực hiện cẩn thận, bạn có thể rơi vào tình trạng nợ nần và mất tài sản.

- Cảnh báo về lừa đảo chiếm đoạt tài sản: Trên mạng xã hội, có rất nhiều hình thức lừa đảo nhằm chiếm đoạt tài sản của người khác. Họ có thể sử dụng các chiêu thức như làm quen, tạo dựng lòng tin và yêu cầu chuyển khoản tiền hoặc cung cấp thông tin cá nhân. Hãy cẩn trọng với các tin nhắn, cuộc gọi hoặc thông tin từ người không rõ danh tính.

**** Biện pháp phòng tránh:***

- Bảo vệ thông tin cá nhân: Không tiết lộ thông tin cá nhân quan trọng như số CCCD, số CMND, số tài khoản ngân hàng hoặc mật khẩu cho bất kỳ ai trên mạng xã hội hay qua các tin nhắn không xác định nguồn gốc.

- Kiểm tra danh tính: Nếu nhận được cuộc gọi, tin nhắn hoặc email từ các tổ chức tài chính, hãy xác minh danh tính của họ bằng cách liên hệ trực tiếp với tổ chức đó qua số điện thoại hoặc địa chỉ email đã được công bố chính thức.

- Kiểm tra mức uy tín của sàn giao dịch: Trước khi tham gia vào giao dịch trực tuyến, hãy kiểm tra sự đáng tin cậy của sàn giao dịch bằng cách tìm hiểu về sàn giao dịch, đọc đánh giá từ người dùng khác và xem xét các chứng chỉ, giấy phép hoạt động.

- Giữ cảnh giác và kiên nhẫn: Luôn luôn giữ cảnh giác với các cơ hội kiếm tiền nhanh chóng, và đừng để bị lừa bởi những lời hứa quá mức hấp dẫn. Hãy kiên nhẫn và tỉnh táo khi đưa ra quyết định về giao dịch tài chính.

- Sử dụng hệ thống bảo mật mạnh mẽ: Đảm bảo rằng bạn sử dụng phần mềm bảo mật mạnh mẽ và luôn cập nhật phiên bản mới nhất để bảo vệ thiết bị của mình khỏi các mối đe dọa trực tuyến.

17. Lừa đảo "chuyển nhầm tiền" vào tài khoản ngân hàng

**** Dấu hiệu nhận biết:***

- Người dân nhận được một khoản tiền chuyển đến trong tài khoản không rõ nguồn gốc.

- Đối tượng mạo danh ngân hàng gọi điện hoặc gửi tin nhắn tin thông báo về việc có người chuyển nhầm tiền và yêu cầu khách hàng truy cập đường link website mạo danh nhằm lấy cắp thông tin như tên truy cập, mật khẩu, mã OTP để chiếm đoạt tiền trong tài khoản.

- Đối tượng giả danh là người thu hồi nợ của một công ty tài chính nào đó để liên hệ với nạn nhân và yêu cầu người này trả lại số tiền kia như một khoản vay cùng với khoản lãi suất cao.

- Đối tượng đe dọa, khủng bố tin nhắn, điện thoại của nạn nhân khiến họ hoảng sợ và lo lắng mà thực hiện theo yêu cầu.

**** Biện pháp phòng tránh:***

- Không tiêu tiền chuyển nhầm: Khi nhận được tiền chuyển khoản nhầm, dù chưa có ai liên hệ cũng tuyệt đối không được tiêu số tiền này; người nhận phải có nghĩa vụ trả lại tiền theo quy định của pháp luật.

- Không vội chuyển tiền trả cho bên kia: Hãy luôn kiểm tra và xác nhận rõ ràng nguồn gốc và mục đích của giao dịch chuyển tiền trước khi thực hiện. Không chuyển tiền dựa trên các yêu cầu đột xuất, không xác định hoặc không rõ ràng.

- Kiểm tra thông tin chuyển khoản: Kiểm tra kỹ các thông tin liên quan đến người gửi, người nhận và số tài khoản trước khi thực hiện giao dịch chuyển tiền. So sánh thông tin với nguồn tin chính thức hoặc thông qua ngân hàng chủ quản để đảm bảo tính xác thực.

- Xác minh bằng nhiều cách khác nhau: Nếu nhận được yêu cầu chuyển tiền hoặc trả lại số tiền từ một người hoặc tổ chức, không nên tiêu hoặc động đến số tiền đó mà hãy xác minh thông qua kênh liên lạc độc lập khác như ngân hàng, số điện thoại được công bố chính thức hoặc email chính thức của họ. Đừng dựa vào thông tin được cung cấp bởi người yêu cầu.

- Thận trọng với các khoản vay không rõ ràng: Nếu bạn nhận được yêu cầu trả lại số tiền như một khoản vay, hãy xem xét cẩn thận trước khi đồng ý. Đảm bảo rằng điều khoản và lãi suất được đề xuất là rõ ràng và hợp lý. Nếu có bất kỳ nghi ngờ nào, hãy tìm kiếm lời khuyên từ cơ quan ngân hàng hoặc chuyên gia tài chính độc lập.

- Báo cáo sự việc: Nếu bạn nghi ngờ hoặc trở thành nạn nhân của lừa đảo chuyển nhầm tiền, giả danh thu hồi nợ, hãy ngay lập tức báo cáo sự việc cho cơ quan chức năng, như cảnh sát hoặc ngân hàng, để họ tiến hành điều tra và cung cấp sự hỗ trợ.

- Luôn luôn giữ cảnh giác và không đồng ý thực hiện bất kỳ giao dịch tài chính nào mà không có đầy đủ thông tin và xác minh. Bảo vệ thông tin tài chính cá nhân của bạn và tìm hiểu thêm về các hình thức lừa đảo phổ biến để tránh trở thành nạn nhân.

18. Lừa đảo dịch vụ lấy lại tiền

**** Dấu hiệu nhận biết:***

- Đối tượng thường tự giới thiệu mình là luật sư, kiểm sát viên, nhân viên ngân hàng... có trình độ, quan hệ để tiếp cận nhận nhân. Thường sử dụng các nick Facebook ảo, không chính chủ, thông tin không chính xác, sim rác... để liên hệ.

- Chúng đưa ra thông tin là số tiền của nạn nhân "bị treo" trên mạng, trên sàn đầu tư, sàn thương mại điện tử; sử dụng nhiều kỹ thuật thao túng tâm lý, xây dựng lòng tin để nạn nhân tin đối tượng có khả năng liên kết với ngân hàng, cơ quan bảo vệ pháp luật để cung cấp "dịch vụ lấy lại tiền".

- Yêu cầu nạn nhân chuyển trước tiền phí dịch vụ; sau đó đưa ra các lý do khác nhau để yêu cầu người dân tiếp tục chuyển thêm tiền, sau đó cắt liên lạc. Các tài khoản nhận tiền thường là tài khoản không chính chủ.

- Ngoài ra, đối tượng có thể yêu cầu nạn nhân cung cấp các thông tin cá nhân (số tiền bị treo, số tài khoản ngân hàng, căn cước công dân...) tạo điều kiện cho các đối tượng thực hiện hành vi lừa đảo tiếp theo.

**** Biện pháp phòng tránh:***

- Khi đã mất tiền hay là nạn nhân của các vụ lừa đảo, trước tiên người dân phải bình tĩnh và hết sức tỉnh táo; chỉ có thể dựa vào lực lượng chức năng để tìm ra đối tượng lừa đảo và đòi lại tài sản. Việc nhờ vào các dịch vụ "lấy lại tiền" là nguy cơ tiếp tục bị lừa đảo.

- Đề cao cảnh giác, kiểm tra, xác minh kỹ các thông tin trên các trang mạng xã hội; không chuyển tiền cho bất kỳ an khi chưa xác thực thông tin.

- Báo ngay cho cơ quan Công an khi phát hiện dấu hiệu lừa đảo.

19. Lừa đảo lấy cắp Telegram OTP

**** Dấu hiệu nhận biết:***

- Đối tượng lừa đảo tạo một profile giả mạo, đánh cắp hình ảnh của những người uy tín có liên quan đến nạn nhân để tạo sự tin cậy: thường dùng sự kiện đáng tin cậy và hấp dẫn để đảm bảo người khác tin tưởng và tham gia vào quá trình.

- Gửi thông báo giả từ tài khoản Telegram được giả danh như một cơ quan chính phủ, tổ chức tài chính, hoặc một người có uy tín cao. Bảo rằng đang nghi ngờ có 2 tài khoản giả mạo nạn nhân, nên cần nạn nhân chụp hình screenshot để xác minh coi có đúng không, nhưng đồng thời kẻ lừa đảo đã dùng số điện thoại của nạn nhân và chọn chức năng quên mật khẩu của Telegram, khi chụp hình screenshot thì vô tình chụp luôn mã OTP từ Telegram mới gửi về.

- Nhận thông tin OTP: Khi người khác chụp màn hình và cung cấp cho kẻ lừa đảo, lúc đó có thể nhận được mã OTP thông qua hình ảnh đó; đối tượng sẽ sử dụng mã OTP để truy cập vào tài khoản Telegram của họ.

**** Các biện pháp phòng tránh:***

- Tăng cường kiến thức và nhận thức: Hãy cảnh giác với các hình thức lừa đảo thông qua việc tìm hiểu về các chiêu trò phổ biến mà lừa đảo tổ chức sử dụng. Điều này giúp bạn nhận ra các tín hiệu đáng ngờ và tránh rơi vào bẫy.

- Xác minh danh tính: Khi bạn nhận được cuộc gọi, tin nhắn hoặc yêu cầu thông tin cá nhân qua điện thoại, hãy xác minh danh tính của người gọi bằng cách yêu cầu thông tin địa chỉ, số điện thoại liên hệ hoặc liên lạc lại qua một kênh tin cậy khác.

- Bảo vệ thông tin cá nhân: Không chia sẻ thông tin cá nhân nhạy cảm, như số OTP, mật khẩu hoặc thông tin tài khoản, với bất kỳ ai nếu chưa xác thực độ tin cậy.

- Xác thực nguồn tin: Luôn xác minh nguồn tin trước khi tin tưởng và cung cấp thông tin nhạy cảm. Đảm bảo rằng bạn đang giao tiếp với người hoặc tổ chức đáng tin cậy bằng cách kiểm tra thông tin liên lạc và xác minh danh tiếng của họ.

- Sử dụng phần mềm bảo mật: Cài đặt và cập nhật các phần mềm bảo mật, chống virus và chống phishing để giảm khả năng bị tấn công và lừa đảo qua Internet.

- Báo cáo hành vi đáng ngờ: Nếu bạn phát hiện hoạt động lừa đảo hoặc nghi ngờ một ai đó đang cố gắng lừa bạn, hãy báo cáo ngay lập tức cho các cơ quan chức năng để giúp ngăn chặn hành vi xấu.

20. Lừa đảo tung tin giả về cuộc gọi mất tiền như FlashAI

- Thông tin rằng chỉ bằng việc nhận cuộc gọi voicecall bạn có thể bị mất tiền như FlashAI hoặc tương tự là KHÔNG chính xác.

- Không có cách nào để người dùng bị trừ tiền chỉ bằng việc nhận cuộc gọi voicecall thông thường trên điện thoại di động. Việc các đối tượng làm vậy nhằm mục đích câu views, likes và gây hoang mang dư luận xã hội.

- Bạn nên cảnh giác và tránh tiếp nhận các cuộc gọi không mong muốn từ các số điện thoại lạ, đặc biệt là từ các số không rõ nguồn gốc. Có một số hình thức lừa đảo, như "cướp cuộc gọi" (call spoofing) hay "vishing", trong đó kẻ gian sẽ giả mạo số điện thoại hoặc sử dụng các công nghệ để hiển thị số điện thoại khác khi gọi đến. Mục đích của chúng là lừa đảo người dùng bằng cách thuyết phục họ THAO TÁC theo hướng dẫn của kẻ lừa đảo để tiết lộ thông tin cá nhân, mật khẩu hoặc thực hiện các giao dịch tài chính. Vì vậy, nếu bạn nhận được cuộc gọi không mong muốn, hãy cẩn thận và không tiết lộ thông tin cá nhân hay tài khoản của mình.

21. Lừa đảo dịch vụ lấy lại Facebook

**** Dấu hiệu nhận biết:***

- Tìm thông tin tài khoản Facebook: Đối tượng lừa đảo tìm cách thu thập thông tin tài khoản Facebook mục tiêu mà họ muốn lừa đảo. Kẻ lừa đảo có thể sử dụng các phương pháp như lừa đảo thông qua email, trang web giả mạo hoặc sử dụng các phần mềm mã độc đánh cắp thông tin.

- Giả mạo dịch vụ lấy lại tài khoản: Tạo ra một trang web giả mạo hoặc gửi email giả mạo cho người dùng Facebook, hoặc chủ động nhắn tin cho người dùng Facebook, tuyên bố rằng họ là dịch vụ lấy lại tài khoản và có thể giúp nạn nhân khôi phục tài khoản bị mất.

- Yêu cầu thông tin cá nhân nhạy cảm như tên đăng nhập, mật khẩu, số điện thoại, địa chỉ email, mã OTP, hoặc thông tin thẻ tín dụng để xác minh danh tính và thực hiện việc lấy lại tài khoản. Hoặc bắt nạn nhân phải đóng một khoản tiền cọc trước và khi đã đạt được mục đích, kẻ lừa đảo khóa chặn cuộc trò chuyện với nạn nhân hoặc xóa luôn tất cả các dấu vết.

**** Biện pháp phòng tránh:***

- Không chia sẻ thông tin đăng nhập: Không chia sẻ thông tin đăng nhập của tài khoản Facebook với bất kỳ ai hoặc bất kỳ dịch vụ nào. Facebook không bao giờ yêu cầu bạn cung cấp thông tin đăng nhập của mình thông qua email, tin nhắn hoặc các hình thức liên lạc khác.

- Sử dụng kênh liên lạc chính thức: Nếu bạn gặp vấn đề với tài khoản Facebook của mình, hãy sử dụng kênh liên lạc chính thức của Facebook để được hỗ trợ. Điều này có thể bao gồm việc sử dụng trang Trợ giúp và Hỗ trợ của Facebook hoặc liên hệ với Facebook qua kênh liên lạc mà họ cung cấp trên trang web chính thức.

- Kiểm tra URL và trang web: Khi bạn cần truy cập vào trang web của Facebook hoặc bất kỳ trang web nào liên quan, hãy chắc chắn kiểm tra URL để đảm bảo rằng bạn đang truy cập vào trang web chính thức của Facebook. Lưu ý rằng các trang web giả mạo có thể có URL tương tự nhưng có thể dẫn đến việc lừa đảo.

- Đặt mật khẩu mạnh và đổi thường xuyên: Sử dụng mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Đảm bảo rằng bạn đổi mật khẩu thường xuyên và không sử dụng mật khẩu giống nhau cho nhiều tài khoản khác nhau.

- Kích hoạt xác minh hai yếu tố: Sử dụng tính năng xác minh hai yếu tố trên tài khoản Facebook của bạn. Điều này đòi hỏi bạn phải cung cấp thông tin bổ sung (thông dụng như mã xác minh gửi qua điện thoại di động hoặc email khi đăng nhập vào tài khoản từ một thiết bị mới. Kích hoạt xác minh hai yếu tố sẽ làm tăng bảo mật và giảm khả năng bị lừa đảo.)

- Cảnh giác với các tin nhắn và email đáng ngờ: Hãy luôn cảnh giác với các tin nhắn hoặc email mà bạn nhận được với nội dung liên quan đến việc lấy lại tài khoản Facebook. Lừa đảo thường sử dụng các phương pháp xâm nhập và chiếm đoạt thông tin cá nhân bằng cách giả mạo các thông báo từ Facebook. Nếu có bất kỳ nghi ngờ nào, hãy kiểm tra kỹ thông tin và xác minh từ các nguồn tin cậy trước khi tiếp tục.

- Sử dụng phần mềm diệt malware và bảo mật: Đảm bảo rằng bạn cài đặt và cập nhật phần mềm diệt malware và bảo mật trên thiết bị của mình. Điều này sẽ giúp phát hiện và ngăn chặn các phần mềm độc hại và công cụ lừa đảo có thể tấn công vào tài khoản Facebook của bạn.

- Hạn chế công khai thông tin cá nhân trên mạng xã hội: Các thông tin cá nhân có thể bị sử dụng để tấn công và lừa đảo bạn.

- Cập nhật và nắm bắt thông tin bảo mật từ Facebook: Luôn theo dõi các thông báo và cập nhật bảo mật từ Facebook. Facebook thường cung cấp thông tin về các biện pháp bảo mật mới và cách ngăn chặn lừa đảo. Bằng cách nắm bắt những thông tin này, bạn có thể tăng cường an ninh cho tài khoản của mình.

22. Lừa đảo tình cảm, lừa gửi quà

**** Dấu hiệu nhận diện:***

- Xác định và tiếp cận nạn nhân: Đối tượng tìm và tiếp cận người mục tiêu thông qua các kênh trực tuyến như mạng xã hội, trang web hẹn hò hoặc diễn đàn. Kẻ lừa đảo tạo một hồ sơ giả mạo, sử dụng hình ảnh đánh cắp của người khác với ngoại hình đẹp và lôi cuốn, sau đó sử dụng các chiêu trò lừa đảo để thu hút sự quan tâm của nạn nhân.

- Xây dựng mối quan hệ: Đối tượng lừa đảo tạo một mối quan hệ tình cảm giả với nạn nhân bằng cách sử dụng các chiêu trò như tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa.

- Dẫn dụ nạn nhân gửi hình ảnh video nhạy cảm (sau đó dùng những hình ảnh này để đe dọa, tống tiền nạn nhân). Một số kẻ lừa đảo tinh vi thì sử dụng nhiều cách khác nhau để thuyết phục nạn nhân tham gia đầu tư vào thị trường tài chính Forex thông qua một sàn giao dịch giả mạo mà kẻ lừa đảo kiểm soát.

- Kẻ lừa đảo gửi hàng bưu kiện có giá trị và sau đó giả danh làm nhân viên sân bay, thuế, hải quan... gọi điện yêu cầu nộp các khoản thuế, phí... để chiếm đoạt tiền của nạn nhân. Kẻ lừa đảo có thể đe dọa hoặc lừa đảo nếu nạn nhân không tuân thủ yêu cầu.

- Chiếm đoạt tài sản hoặc tống tiền: Khi tham gia đầu tư tài chính Forex, nạn nhân sẽ bị dẫn dụ thắng vài lần tạo niềm tin và lòng tham, sau đó khi thắng số tiền lớn hơn thì nạn nhân sẽ không rút ra được, bắt phải đóng phí giao dịch, đóng thuế hoặc thông báo tài khoản bị sai thông tin, phải đóng tiền để xác minh chứng thực... từ đó chiếm đoạt tiền của nạn nhân.

**** Biện pháp phòng tránh:***

- Cảnh giác và không quá nhanh tin tưởng vào một người mà bạn mới gặp qua mạng xã hội hoặc các nền tảng trực tuyến khác. Lừa đảo tình cảm thường bắt đầu bằng việc xây dựng một mối quan hệ tình cảm nhanh chóng để lấy lòng và đánh lừa nạn nhân. Hãy tự đặt câu hỏi và xem xét cẩn thận trước khi thực hiện bất kỳ hành động nào.

- Không tin tưởng vào các lời hứa và cam kết không rõ ràng hoặc quá hấp dẫn. Lừa đảo thường sử dụng các chiêu trò để tạo ra sự tin tưởng và dụ dỗ nạn nhân. Hãy luôn kiểm tra và xác minh thông tin trước khi thực hiện bất kỳ hành động nào liên quan đến tài chính hoặc gửi thông tin cá nhân.

- Xác minh danh tính: Khi gặp một người mới trên mạng xã hội hoặc các nền tảng trực tuyến, hãy xác minh danh tính của họ bằng cách tìm hiểu về họ, yêu cầu thông tin địa chỉ, số điện thoại liên hệ hoặc thậm chí gặp gỡ trực tiếp nếu có thể. Đừng chia sẻ thông tin cá nhân quá nhanh chóng.

- Cẩn trọng với yêu cầu tài chính: Hãy cảnh giác với những yêu cầu gửi tiền, đầu tư vào Forex hoặc tham gia các giao dịch tài chính không rõ nguồn gốc. Lừa đảo thường sử dụng chiêu trò hứa hẹn lợi nhuận cao hoặc cơ hội đầu tư hấp dẫn để chiếm đoạt tài sản của nạn nhân.

- Kiểm tra thông tin trước khi nhận hàng bưu kiện: Trước khi nhận hàng bưu kiện của một người mà bạn không quen biết, hãy kiểm tra và xác minh thông tin về địa chỉ, tên và các chi tiết khác. Hãy lưu ý rằng, không có món quà nào là "ngẫu nhiên"

- Cẩn trọng khi chia sẻ hình ảnh và video nhạy cảm: Không chia sẻ hình ảnh hoặc video nhạy cảm của bạn với người mà bạn không quen biết hoặc không tin tưởng. Lừa đảo có thể sử dụng các hình ảnh và video nhạy cảm này để tống tiền hoặc tống khứ đối với bạn sau đó. Luôn nhớ rằng hình ảnh và video cá nhân của bạn là riêng tư và chỉ nên được chia sẻ với người mà bạn tin tưởng thực sự.

- Bình tĩnh và đặt sự an toàn cá nhân lên hàng đầu: Trong trường hợp bạn bị mắc kẹt trong một cuộc lừa đảo và đối mặt với yêu cầu tống tiền hoặc chiếm đoạt tài sản, hãy giữ bình tĩnh và đặt sự an toàn cá nhân lên hàng đầu. Không bao giờ đồng ý chuyển khoản tiền, gửi hàng hoặc cung cấp thông tin cá nhân nhạy cảm. Báo cáo sự việc cho cơ quan chức năng và yêu cầu hỗ trợ từ họ.

- Bảo vệ thông tin cá nhân riêng tư và an toàn: Không chia sẻ quá nhiều thông tin trên mạng xã hội hoặc các nền tảng trực tuyến. Đặc biệt, hãy cẩn thận với việc cung cấp số điện thoại, địa chỉ nhà, tài khoản ngân hàng hoặc bất kỳ thông tin nhạy cảm nào cho người mà bạn không tin tưởng hoặc không biết.

- Nghiên cứu kỹ kiến thức trước khi tham gia đầu tư: Nếu bạn quan tâm đến đầu tư tài chính, hãy đảm bảo rằng bạn có đủ kiến thức và hiểu rõ về cách hoạt động của thị trường và các rủi ro liên quan. Tìm hiểu về các công ty và nhà môi giới đáng tin cậy và luôn tìm lời khuyên từ chuyên gia tài chính trước khi tham gia bất kỳ giao dịch nào.

23. Lừa thông báo trúng thưởng

**** Dấu hiệu nhận biết:***

- Đối tượng tự xưng là nhân viên của doanh nghiệp gọi điện, nhắn tin (qua điện thoại, Facebook...) thông báo "bạn đã trúng thưởng một giải thưởng lớn", yêu cầu nạn nhân cung cấp thông tin cá nhân nhạy cảm, chuyển tiền trả các loại thuế, phí, hay yêu cầu mua thêm các sản phẩm để được nhận thưởng, tăng giá trị tiền thưởng.

- Sau khi nạn nhân chuyển tiền, tiếp tục lấy nhiều lý do khác nhau để yêu cầu nạn nhân chuyển thêm tiền.

**** Biện pháp phòng tránh:***

- Nếu bạn nhận được một cuộc gọi thông báo rằng bạn đã trúng thưởng một giải thưởng lớn, hãy cảnh giác vì không có ai trúng thưởng mà trước đó không chủ động tham gia các chương trình quay thưởng, dự thưởng; không có giải thưởng nào mà bạn có thể trúng một cách dễ dàng.

- Khi nhận được cuộc gọi từ người lạ, yêu cầu họ cung cấp đầy đủ thông tin họ tên, chức vụ, nơi công tác, địa chỉ, số điện thoại, tên công ty... để tìm hiểu, tra cứu, xác minh kỹ thông tin từ nhiều nguồn khác nhau.

- Không cung cấp thông tin cá nhân cho người lạ.

- Không chuyển tiền trước, hay mua hàng để nhận tiền thưởng, vì đây gần như là dấu hiệu của đối tượng lừa đảo.

- Liên hệ ngay với cơ quan chức năng để được hướng dẫn.

24. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook

**** Dấu hiệu nhận biết:***

- Kẻ lừa đảo tạo một trang web giả mạo có giao diện tương tự như một trang web đáng tin cậy như ngân hàng hoặc dịch vụ trực tuyến. Trang web này được thiết kế để thu thập thông tin cá nhân và đăng nhập của người dùng khi họ nhập vào.

- Tạo một đường link hấp dẫn: Tạo một đường link hấp dẫn sử dụng một tiêu đề hoặc mô tả mà người dùng có thể quan tâm, chẳng hạn như "Nhận ngay ưu đãi đặc biệt" hoặc "Kiểm tra tài khoản của bạn" hoặc "Bạn bị bóc phốt" hoặc các sự kiện đang hot trending xu hướng trên mạng xã hội. Đảm bảo đường link này giống như một đường link đáng tin cậy để gây thiện cảm và khó phát hiện.

- Rải link và seeding quảng cáo bẩn trên Facebook: Kẻ lừa đảo sử dụng các tài khoản giả mạo hoặc các tài khoản đã bị xâm nhập để rải link và seeding quảng cáo bẩn trên Facebook. Đăng bài viết, nhận xét, bình luận hoặc quảng cáo với đường link đã được tạo, hấp dẫn người dùng để nhấn vào.

- Lừa đảo và đánh cắp thông tin, tài sản: Khi người dùng nhấn vào đường link lừa đảo, họ sẽ được chuyển hướng đến trang web phishing mà kẻ lừa đảo đã tạo. Từ đó, kẻ lừa đảo có thể thu thập thông tin cá nhân, tài khoản hoặc đăng nhập của họ và sử dụng để lừa đảo hoặc đánh cắp tài sản.

**** Biện pháp phòng tránh:***

- Cẩn thận với các đường link không rõ nguồn gốc: Khi bạn nhận được một đường link từ nguồn không rõ hoặc không quen thuộc, hãy cẩn thận và không nhấp vào ngay. Kiểm tra xem link có xuất phát từ một nguồn đáng tin cậy hay không. Các đường link rút gọn cũng cần được kiểm tra trước khi nhấp vào.

- Kiểm tra địa chỉ URL trước khi nhấp vào: Trước khi nhấp vào một đường link trên Facebook hoặc bất kỳ nền tảng nào, hãy kiểm tra địa chỉ URL trên thanh địa chỉ của trình duyệt. Đảm bảo rằng nó khớp với trang web bạn định truy cập và không có các ký tự hoặc chuỗi lạ.

- Đánh giá tính xác thực của quảng cáo, tin nhắn, bình luận: Khi bạn thấy một quảng cáo trên Facebook, hãy đánh giá tính xác thực của nó trước khi tương tác. Kiểm tra chính xác nguồn gốc của quảng cáo, tìm hiểu về công ty hoặc sản phẩm được quảng cáo và đảm bảo rằng nó không có dấu hiệu lừa đảo hoặc đánh cắp thông tin.

- Tăng cường bảo mật tài khoản: Đảm bảo rằng bạn sử dụng mật khẩu mạnh và kích hoạt các biện pháp bảo mật bổ sung như xác thực hai yếu tố cho tài khoản Facebook của bạn. Điều này giúp ngăn chặn kẻ xấu truy cập vào tài khoản và tránh việc rải link phishing từ tài khoản của bạn.

- Tìm hiểu về các hình thức lừa đảo và phishing: Để trở nên cảnh giác hơn, tìm hiểu về các hình thức lừa đảo và phishing phổ biến, cùng với các dấu hiệu nhận biết và kỹ thuật lừa đảo. Điều này giúp bạn nhận ra các quảng cáo hoặc đường link đáng ngờ và tránh nhấp vào chúng.

- Cài đặt phần mềm chống phishing và bảo mật: Sử dụng phần mềm chống malware và chống phishing để bảo vệ thiết bị của bạn

- Hạn chế chia sẻ thông tin cá nhân trên Facebook và các nền tảng trực tuyến khác, nhất là thông tin nhạy cảm như số thẻ tín dụng, số bảo hiểm xã hội hoặc bất kỳ thông tin cá nhân khác cho các đường link hoặc quảng cáo không rõ nguồn gốc.

- Kiểm tra đánh giá và phản hồi của người dùng khác: Trước khi tương tác với một đường link hoặc quảng cáo, hãy đọc các đánh giá và phản hồi từ người dùng khác. Nếu có những báo cáo về lừa đảo hoặc đánh cắp thông tin, hãy cân nhắc và tránh tương tác với nội dung đó.

- Luôn cập nhật và sử dụng phiên bản mới nhất của trình duyệt và phần mềm bảo mật: Đảm bảo rằng bạn luôn cập nhật phiên bản mới nhất của trình duyệt web và phần mềm bảo mật trên thiết bị của bạn. Các bản vá bảo mật thường cung cấp bảo vệ chống lại các lỗ hổng bảo mật và các cuộc tấn công phishing.

- Báo cáo các trường hợp đáng ngờ: Nếu bạn phát hiện một đường link phishing hoặc quảng cáo lừa đảo trên Facebook, hãy báo cáo cho Facebook bằng cách sử dụng tính năng báo cáo hoặc liên hệ trực tiếp với họ để thông báo về tình huống. Bằng cách báo cáo, bạn giúp ngăn chặn sự lan truyền của lừa đảo và bảo vệ cộng đồng trực tuyến.

- Giáo dục và nâng cao nhận thức: Nắm vững kiến thức về các hình thức lừa đảo và phishing trên mạng xã hội. Hãy chia sẻ thông tin và nhận thức này với gia đình, bạn bè và cộng đồng để giúp họ tránh trở thành nạn nhân.

25. Lừa đảo cho số đánh lô đề

**** Cảnh báo:***

- Lô, đề là một hình thức đánh bạc trái phép; chơi lô, đề là hành vi vi phạm pháp luật, có thể bị xử phạt hành chính hoặc xử lý hình sự.

- Đánh số lô, số đề trên mạng xã hội với các dấu hiệu như phải đóng phí trước, rủi ro mất phí khi không trúng và phải chia hoa hồng khi trúng là một hình thức lừa đảo nguy hiểm.

**** Dấu hiệu nhận biết:***

- Tiếp cận và quảng cáo: Kẻ lừa đảo tiếp cận người khác thông qua các phương tiện như điện thoại, email, tin nhắn hoặc mạng xã hội. Họ quảng cáo về việc cung cấp số lô, số đề may mắn có khả năng trúng thưởng lớn.

- Tạo niềm tin: Kẻ lừa đảo sử dụng các câu chuyện thành công, chứng cứ giả và những lời tán tụng để tạo niềm tin và thuyết phục người khác rằng họ có khả năng đưa ra các số lô, số đề chính xác.

- Yêu cầu đóng phí trước: Kẻ lừa đảo yêu cầu người khác đóng một khoản phí trước để nhận được các số lô, số đề may mắn. Họ thường đưa ra lý do như phí dịch vụ, phí tiên tri hoặc phí đăng ký.

- Đánh số lô, số đề: Sau khi người khác đã đóng phí, kẻ lừa đảo cung cấp các số lô, số đề cho người đó đánh. Họ tạo ra cảm giác rằng những số này sẽ mang lại kết quả trúng thưởng lớn.

- Mất phí nếu không trúng: Trong trường hợp người khác không trúng thưởng, kẻ lừa đảo không trả lại số tiền phí mà người khác đã đóng trước đó. Họ sử dụng lý do rằng đó là một khoản phí không hoàn lại hoặc chi phí liên quan đến việc cung cấp các số lô, số đề.

- Chia hoa hồng nếu trúng: Nếu người khác trúng thưởng, kẻ lừa đảo yêu cầu người đó chia hoa hồng hoặc trả một phần tiền thưởng cho mình dưới danh nghĩa đã cung cấp các số lô, số đề may mắn.

**** Biện pháp phòng tránh:***

- Không tham gia chơi lô, đề dưới mọi hình thức vì đây là hành vi vi phạm pháp luật

- Không tin vào lời hứa dễ dàng kiếm tiền: Hãy luôn giữ cảnh giác với những lời hứa kiếm tiền nhanh chóng và dễ dàng từ việc đánh số lô, số đề trên mạng xã hội. Các lời quảng cáo hấp dẫn có thể là cá bẫy để dụ dỗ người dân.

- Không đóng phí trước: Lưu ý rằng việc yêu cầu đóng phí trước khi nhận được số lô, số đề là một dấu hiệu đáng ngờ. Hãy từ chối đóng bất kỳ khoản phí nào trước khi xác minh tính xác thực và đáng tin cậy của dịch vụ.

- Báo cáo sự việc: Nếu bạn nghi ngờ hoặc trở thành nạn nhân của lừa đảo đánh số lô, số đề trên mạng xã hội, hãy ngay lập tức báo cáo sự việc cho cơ quan chức năng để điều tra, xử lý.

26. Lừa đảo chuyển tiền từ thiện

**** Dấu hiệu nhận biết:***

Đối tượng lừa đảo tạo lập các trang mạng xã hội (chủ yếu là Facebook), sau đó đăng tải các bài viết, tạo dựng những nội dung không đúng sự thật về một số hoàn cảnh khó khăn, hoạn nạn, cần được giúp đỡ; hoặc giả mạo các trang mạng xã hội chuyên làm từ thiện được Nhà nước cho phép, rồi đăng tải các bài viết kêu gọi cộng đồng mạng giúp đỡ. Đối tượng có thể sử dụng các bài báo viết về các hoàn cảnh khó khăn đã được đăng tải trên các phương tiện thông tin đại chúng để dẫn nguồn trên Facebook, rồi xen vào đó số tài khoản ngân hàng tiếp nhận từ thiện do các đối tượng tự tạo lập quản lý để tiếp nhận tiền ủng hộ. Sau khi tiếp nhận tiền do các nhà hảo tâm ủng hộ, các đối tượng không bàn giao tiền từ thiện cho các hoàn cảnh khó khăn mà sẽ chiếm đoạt.

**** Biện pháp phòng tránh:***

- Thận trọng tìm hiểu, kiểm chứng kỹ các thông tin đăng tải kêu gọi ủng hộ trên không gian mạng; kiểm tra kỹ thông tin, uy tín của người kêu gọi từ thiện; yêu cầu công khai, minh bạch thông tin về người cần giúp đỡ hoặc liên hệ với chính quyền địa phương, bệnh viện nơi họ điều trị để kiểm chứng thông tin.

- Nên lựa chọn các quỹ, chương trình từ thiện do Nhà nước, đoàn thể, quỹ xã hội, quỹ từ thiện được Nhà nước cấp phép đứng ra tổ chức.

- Trường hợp có nghi ngờ về lừa đảo, cần báo ngay với cơ quan chức năng.