BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỤC AN TOÀN THÔNG TIN

CẨM NANG

NHẬN DIỆN VÀ PHÒNG CHỐNG LỪA ĐẢO TRỰC TUYẾN

Hà Nội, 06/2023

MỤC LỤC

I. TÌNH HÌNH CHUNG

Lừa đảo trực tuyến là vấn đề đã và đang nhận được nhiều sự quan tâm của toàn xã hội. Các đối tượng xấu lợi dụng bối cảnh bùng nổ công nghệ thông tin để thực hiện nhiều vụ lừa đảo trực tuyến, chiếm đoạt tài sản có giá trị cao. Trong đó, có 3 nhóm lừa đảo chính (giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác) với **24 hình thức lừa đảo** đang diễn ra trên không gian mạng Việt Nam:

1. Lừa đảo "combo du lịch giá rẻ".
2. Lừa đảo cuộc gọi video Deepfake, Deepvoice.
3. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao.
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.
7. Thủ đoạn giả danh các công ty tài chính, ngân hàng.
8. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen,…
9. Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp (BHXH, ngân hàng…)
10. Lừa đảo SMS Brandname, phát tán tin nhắn giả mạo.
11. Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp.
12. Lừa đảo tuyển CTV online.
13. Đánh cắp tài khoản MXH, nhắn tin lừa đảo.
14. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo.
15. Rao bán hàng giả hàng nhái trên sàn thương mại điện tử.
16. Đánh cắp thông tin CCCD đi vay nợ tín dụng.
17. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng.
18. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa.
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, dẫn dụ đầu tư tài chính, gửi bưu kiện, trúng thưởng,…
23. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook.
24. Lừa đảo cho số đánh đề.

II. ĐỐI TƯỢNG MỤC TIÊU

Các hình thức lừa đảo trên không gian mạng được các đối tượng lừa đảo thực hiện bằng nhiều hình thức khác nhau và ngày càng tinh vi, trong đó nhắm vào nhiều

nhóm đối tượng, bao gồm: Người cao tuổi, trẻ em, sinh viên, đối tượng công nhân, nhân viên văn phòng…

Mỗi nhóm đối tượng ở độ tuổi khác nhau, kẻ xấu thực hiện những hình thức dẫn dụ khác nhau, mục tiêu chung là lấy lòng tin, đánh cắp thông tin người dùng, sau đó chiếm đoạt tài sản.

NHÓM ĐỐI TƯỢNG	CÁC HÌNH THỨC DẪN DỤ
Người cao tuổi	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 4. Giả mạo biên lai chuyển tiền thành công 5. Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp (BHXH, ngân hàng…) 6. Phát tán tin nhắn lừa đảo giả mạo Brandname 7. Giả danh công an, viện kiểm sát, tòa án gọi điện lừa đảo 8. Lừa đảo bán hàng kém chất lượng trên sàn thương mại điện tử 9. Đánh cắp thông tin CCCD đi vay tín dụng. 10. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng 11. Lừa đảo dịch vụ lấy lại Facebook 12. Lừa đảo tình cảm, dẫn dụ đầu tư, nhận bưu phẩm,… 13. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook 14. Lừa đảo cho số đánh đề 15. Lừa đảo tung tin giả về cuộc gọi mất tiền
Trẻ em	1. Lừa đảo cuộc gọi video Deepfake 2. Lừa đảo tình cảm, dẫn dụ chia sẻ hình ảnh nhạy cảm 3. Lừa đảo dịch vụ lấy lại Facebook
Sinh viên/ thanh niên	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 4. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen,… 5. Phát tán tin nhắn lừa đảo giả mạo Brandname 6. Lừa đảo đầu tư tài chính 7. Lừa đảo tuyển CTV online 8. Giả danh công an, viện kiểm sát, tòa án gọi điện lừa đảo 9. Lừa đảo bán hàng kém chất lượng trên các sàn thương mại điện tử. 10. Đánh cắp thông tin CCCD đi vay tín dụng. 11. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng 12. Lừa đảo dịch vụ lấy lại Facebook 13. Lừa đảo tình cảm, dẫn dụ đầu tư, nhận bưu phẩm,…
Nhân viên văn phòng	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 4. Giả danh các công ty tài chính, ngân hàng thu thập thông tin 5. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen,…

	6. Phát tán tin nhắn lừa đảo giả mạo Brandname 7. Lừa đảo đầu tư tài chính 8. Lừa đảo tuyển CTV online 9. Giả danh công an, viện kiểm sát, tòa án gọi điện lừa đảo 10. Lừa đảo bán hàng kém chất lượng trên sàn thương mại điện tử. 11. Đánh cắp thông tin CCCD đi vay tín dụng. 12. Lừa đảo chuyển nhầm tiền vào tài khoản ngân 13. Lừa đảo dịch vụ lấy lại Facebook 14. Lừa đảo tình cảm, dẫn dụ đầu tư, nhận bưu phẩm,… 15. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook 16. Lừa đảo cho số đánh đề 17. Lừa đảo tung tin giả về cuộc gọi mất tiền 18. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa 19. Lừa đảo lấy cắp Telegram OTP
Công nhân/ Người lao động	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 4. Giả danh các công ty tài chính, ngân hàng thu thập thông tin 5. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen,… 6. Phát tán tin nhắn lừa đảo giả mạo Brandname 7. Lừa đảo đầu tư tài chính 8. Lừa đảo tuyển CTV online 9. Giả danh công an, viện kiểm sát, tòa án gọi điện lừa đảo 10. Lừa đảo bán hàng kém chất lượng trên sàn thương mại điện tử. 11. Đánh cắp thông tin CCCD đi vay tín dụng. 12. Lừa đảo chuyển nhầm tiền vào tài khoản ngân 13. Lừa đảo dịch vụ lấy lại Facebook 14. Lừa đảo tình cảm, dẫn dụ đầu tư, nhận bưu phẩm,… 15. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook 16. Lừa đảo cho số đánh đề 17. Lừa đảo tung tin giả về cuộc gọi mất tiền 18. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa 19. Lừa đảo lấy cắp Telegram OTP
Phụ huynh học sinh	1. Lừa đảo cuộc gọi video Deepfake 2. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao 3. Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu 4. Lừa đảo tuyển người mẫu nhí 5. Phát tán tin nhắn lừa đảo giả mạo Brandname 6. Giả danh công an, viện kiểm sát, tòa án gọi điện lừa đảo 7. Lừa đảo bán hàng kém chất lượng trên sàn thương mại điện tử 8. Đánh cắp thông tin CCCD đi vay tín dụng. 9. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng 10. Lừa đảo tung tin giả về cuộc gọi mất tiền

DẤU HIỆU NHẬN BIẾT VÀ CÁCH PHÒNG TRÁNH

1. Lừa đảo "combo du lịch giá rẻ"

- ***Dấu hiệu nhận diện:***

1. Đăng tải bài viết quảng cáo bán tour du lịch, phòng khách sạn giá rẻ trên mạng Internet và 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.

2. 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.

3. 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.

4. 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.

5. 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 chỉ biết được việc này khi đến sân bay.

- ***Biện pháp phòng tránh:***

Để tránh bị lừa đảo trước các thủ đoạn nêu trên, người dân 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.

Bên cạnh đó, 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, nếu có thể nên thực hiện giao dịch thanh toán trực tiếp.

Đồng thời, 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…

Đặc biệt, đối với các trang mạng xã hội (Fanpage) hoạt động mua bán, quảng bá các gói du lịch, nhất là gói du lịch giá rẻ, vé máy bay giá rẻ, người dân 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 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

Deepfake đang là một mối đe dọa đối với sự trung thực và tin cậy của video và hình ảnh. 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.

Phần lớn hình thức lừa đảo trực tuyến này nhắm tới việc lừa đảo tài chính. Nên khi người dân nhận được các cuộc gọi liên quan đến các nội dung về tài chính thì nên tỉnh táo xác nhận thêm.

- ***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 cũng là một vấn đề có thể xảy ra trong video. Âm thanh 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:***

Theo đó, nếu 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

- ***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".

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:***

Để phòng tránh, người dùng nên chủ động kiểm tra thông tin đã chuẩn hóa hay chưa thông qua các công cụ, hướng dẫn từ nhà mạng. Không thực hiện theo các yêu cầu khi nghe cuộc gọi từ số điện thoại lạ. 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.

Người dân 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. 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.

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.

Các 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 đã dùng một số 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. Cho đến khi các nạn nhân không thấy tài khoản báo có tiền và nhận ra mình đã bị lừa, thì các đối tượng đã "cao chạy xa bay".

- ***Cảnh báo:***

Để tránh bị lừa đảo, người dân nếu sử dụng giao dịch qua tài khoản ngân hàng cần lưu ý kỹ hóa đơn chuyển khoản, 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.

Với hệ thống công nghệ của các ngân hàng, việc chuyển khoản 24/7, khách hàng sẽ nhận được thông báo có tiền trong tài khoản. 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.

Ngoài ra, hình ảnh "giao dịch thành công" bị làm giả có một số đặc điểm khác với hình ảnh từ ngân hàng chính thống về màu sắc, phông chữ, thời gian...

Lưu ý, 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.

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.

Trong trường hợp này, các đối tượng sử dụng chiêu thức đánh vào tâm lý, tình cảm của nạn nhân, hình thành trạng thái bất an, lo sợ và hoảng loạn khi phụ huynh phải nghe tin người thân mình đang cấp cứu. Để hoàn toàn thao túng tâm lý nạn nhân trong thời gian ngắn, 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… Đáng nói, một số đối tượng còn thuộc lòng thông tin về trường, lớp học của con, tên giáo viên chủ nhiệm, thầy cô, hiệu trưởng khiến phụ huynh nhất thời tin tưởng.

Một số dấu hiệu đáng ngờ về đối tượng lừa đảo mà các phụ huynh cần lưu ý như cách xưng hô khác thường ngày, 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***

Việc tốt nhất bây giờ là hạn chế chia sẻ thông tin, hình ảnh cá nhân, con cái, danh tính của mình lên mạng xã hội. Cùng với đó, những dịch vụ mà mình đã đăng ký mà không còn nhu cầu nữa nên được hủy bỏ để hạn chế bớt việc các đơn vị giữ thông tin của mình.

Ngoài ra:

- 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 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.

- Các tổ chức, cá nhân có thể truy cập vào cổng thông tin khonggianmang.vn để tra cứu hoặc phản ánh tới cơ quan chức năng về những trường hợp nghi ngờ lừa đảo trực tuyến.

- 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

- ***Dấu hiệu nhận biết:***

Thủ đoạn của các đối tượng là thông qua mạng xã hội như Facebook, Zalo, Telegram…, các đối tượng lừa đảo sẽ kết bạn với phụ huynh và mời tham gia ứng tuyển người mẫu nhí cho hãng thời trang. 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 các phụ huynh khi muốn con mình tham gia vào ứng tuyển "người mẫu nhí" là chuyển khoản để mua sản phẩm hàng hiệu, sau đó 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

- ***Biện pháp phòng tránh:***

Tuy được đặt dưới cách thức hoạt động không mới nhưng những chiêu trò lừa đảo này vẫn ngang nhiên xuất hiện trên mạng xã hội gây tâm lí hoang mang cho phụ huynh. 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. Để phòng tránh lừa đảo và những hậu quả đáng tiếc xảy ra, người dân cần lưu ý:

+ 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. Đặc biệt không làm việc với nhà tuyển dụng nào mà yêu cầu ứng viên phải chuyển tiền, nộp tiền trước.

+ Nên kiểm tra tác giả, đọc kỹ nội dung để xác định thông tin thật hay giả; tin tức giả thường sẽ bị lỗi chính tả hoặc có bố cục lộn xộn, các hình ảnh, video trong tin giả thường bị chỉnh sửa, cắt ghép, thay đổi nội dung, ngày tháng của sự kiện thường bị thay đổi. 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.

+ 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. Ngoài ra, người dân nên cập nhật kiến thức thường xuyên về các phương thức thủ đoạn lừa đảo trực tuyến mới mà các loại tội phạm thực hiện và nên lưu ý rằng các cơ quan chức năng và nhà cung cấp dịch vụ không bao giờ gọi điện yêu cầu, hỗ trợ người dùng thực hiện các hướng dẫn trực tuyến trên mạng.

7. Giả danh các công ty tài chính, ngân hàng thu thập thông tin

- ***Dấu hiệu nhận biết:***

Thủ đoạn lừa đảo của các đối tượng là đánh vào tâm lý của những người đang cần tiền kinh doanh, tiêu xài, muốn được vay với số tiền lớn nhưng lại gặp khó do dính nợ xấu hoặc không đủ điều kiện vay vốn tại các tổ chức tài chính. Từ đó, các đối tượng mạo danh một số ngân hàng và các công ty tài chính có thật tại Việt Nam, tạo lập website, ứng dụng, chạy quảng cáo thông qua các nền tảng mạng xã hội để chào mời cho vay tín chấp với lãi suất đặc biệt thấp.

Các đối tượng lừa đảo tạo lập hàng nghìn tài khoản facebook với các nguồn thông tin giả, tham gia vào các hội nhóm, diễn đàn, đăng bài quảng cáo cho vay tín chấp với lãi suất thấp (chỉ 1%/ 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 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.

Sau khi dụ người vay chuyển tiền phục vụ hỗ trợ xác minh, duyệt khoản vay, các 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 các khoản tiền để bảo đảm khoản vay hoặc khắc phục lỗi hệ thống; hứa hẹn sẽ hoàn trả lại số tiền đã gửi cho khách hàng sau khi khoản vay được giải ngân. 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.

Với thủ đoạn lừa đảo tinh vi trên, bị hại không những bị mất tiền mà còn bị mất toàn bộ thông tin danh tính cá nhân, tiềm ẩn nguy cơ tiếp tục bị lợi dụng để phục vụ cho các hoạt động vi phạm pháp luật khác, ví dụ như: đăng kí SIM không chính chủ, đăng kí mở tài khoản ngân hàng, ví điện tử phục vụ các hoạt động lừa đảo, rửa tiền, cá độ trực tuyến…

- ***Biện pháp phòng tránh***

Trước thủ đoạn lừa đảo tinh vi, có nhiều diễn biến phức tạp trên không gian mạng, người dân cần:

- Chủ động nâng cao ý thức cảnh giác trước các thủ đoạn lừa đảo chiếm đoạt tài sản. 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 thoại đến các số 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 cá nhân mà các đối tượng lạ cung cấp, dụ dỗ.

- Nhanh chóng trình báo cơ quan Công an nơi gần nhất khi phát hiện thủ đoạn mạo danh, lừa đảo chiếm đoạt tài sản hoặc bị mạo danh, 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…

Thực tế, 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, nhắm đến những người nhẹ dạ cả tin, thiếu cảnh giác/hiểu biết đối với các tấn công lừa đảo qua mạng.

Ngoài ra, 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 nào, bạn cũng có thể báo cáo với NCSC tại địa chỉ https://canhbao.khonggianmang.gov.vn

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)

9. Giả mạo các trang thông tin điện tử cơ quan, doanh nghiệp (BHXH, ngân hàng…)

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin, các đối tượng xấu có thể thực hiện việc giả mạo một trang web khi có các kiến thức như một lập trình viên.

Các đối tượng này có thể 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, các đối tượng 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 và từ đó thực hiện hành vi đánh cắp, chiếm đoạt thông tin dữ liệu người dùng, lừa đảo. Một số địa chỉ đã từng được các đối tượng sử dụng đều có đường dẫn đến có định dạng bất thường như là vn-cbs.xyz. vn-ms.top…

- ***Dấu hiệu nhận biết website không an toàn***

- Đường dẫn URL trên thanh địa chỉ của trình duyệt phải được bắt đầu bằng "https://" và có một biểu tượng ổ khóa trên thanh địa chỉ (Lưu ý rằng, ổ khóa phải xuất hiện ở thanh địa chỉ trình duyệt chứ không phải trong nội dung của website). Điều này chứng tỏ website đã được bảo vệ bởi Secure Sockets Layer (SSL), một

giao thức mã hóa giúp đảm bảo thông tin được trao đổi một cách an toàn thông qua một chứng chỉ số SSL được tin cậy. Nên nhớ rằng, nếu cụm từ https:// chuyển sang màu đỏ và xuất hiện biểu tượng ổ khóa bị đánh dấu chéo, tức là có thể website mà người dùng truy cập vào đang sử dụng chứng chỉ số SSL hết hạn hoặc được cấp bởi một nguồn không đáng tin cậy.

- Các tên miền cấp cao nhất (Top Level Domain – TLD) phổ biến mà người dùng thường quen thuộc, ví dụ như tên miền cấp cao nhất dùng chung (gTLD): .com, .net…; hay tên miền cấp cao nhất của quốc gia (ccTLD): .vn, .cn… thường sẽ an toàn hơn các URL có TLD lạ, tuy nhiên đây chỉ là một dấu hiệu và người dùng không thể chỉ dựa vào mỗi chi tiết này để đánh giá về trang web là có an toàn hay không.

- Những website không đáng tin cậy và kém 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,… Nguyên nhân do các website lừa đảo thường không có thời gian kỹ càng để kiểm duyệt và chỉnh sửa các nội dung.

- Các website lừa đảo thường sẽ xuất hiện những cảnh báo, đe dọa hoặc các chương trình trúng thưởng hấp dẫn với nhiều phần quà có giá trị ngay khi người dùng truy cập trang, mục đích là để đánh lừa và dụ dỗ người dùng truy cập vào các thông tin quan trọng nhằm đánh cắp dữ liệu cá nhân, hoặc điều hướng truy cập đến những website không an toàn khác có chứa mã độc hại.

- Doanh nghiệp muốn kinh doanh hợp pháp trên website bắt buộc phải khai báo tên miền và trang web với Bộ Công Thương (các website bán hàng hay sàn thương mại điện tử, ví dụ như sendo.com, tiki.vn hay shoppee.vn,…). Vì thế, nếu cuối trang chưa có logo của Bộ Công Thương thì đây là một website mới được tạo ra và chưa có độ an toàn hay đáng tin cậy.

- 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 thì nên cảnh giác và không thực hiện theo yêu cầu.

- ***Biện pháp phòng tránh***

- Kiểm tra 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.

- 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: Khi truy cập vào các trang web yêu cầu cung cấp thông tin nhạy cảm, hãy đảm bảo rằng kết nối là an toàn bằng cách kiểm tra xem trang web có chứng chỉ SSL hợp lệ hay không. Biểu tượng ổ khóa và "https" ở đầu URL là một dấu hiệu của kết nối an toàn.

- Cẩn thận với email và liên kết: Tránh nhấp vào liên kết trong email không xác định hoặc không mong muốn. Kiểm tra nguồn gốc của email và đảm bảo rằng nó là đáng tin cậy trước khi tiếp tục. Nếu có liên kết, hãy kiểm tra xem địa chỉ URL có khớp với trang web mục tiêu hay không.

- Hạn chế cung cấp thông tin cá nhân: Chỉ cung cấp thông tin cá nhân nhạy cảm trên các trang web đáng tin cậy và an toàn. Tránh cung cấp thông tin cá nhân như 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. Cập nhật chúng thường xuyên để bảo vệ chống lại các mối đe dọa mới nhất.

- Đào tạo và nhận biết: Hãy tự trang bị kiến thức về các phương pháp tấn công phishing và nhận biết các dấu hiệu nhận biết trang web lừa đảo qua tinnhiemmang.vn hoặc ncsc.gov.vn. 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)

- Giữ tỉnh táo và cảnh giác: Luôn giữ một tinh thần cảnh giác khi truy cập vào các trang web và giao dịch trực tuyến. Hãy tin vào cảm giác của bạn và không bao giờ cung cấp thông tin cá nhân nếu bạn có bất kỳ nghi ngờ nào về tính xác thực của trang web đó.

- 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, hãy tránh truy cập vào trang web đó.

- Sử dụng các phương pháp xác thực bổ sung: Nếu có sẵn, hãy sử dụng các phương pháp xác thực bổ sung như xác thực hai yếu tố hoặc sử dụng mã OTP (One-Time Password) để bảo vệ tài khoản của bạn. Điều này làm tăng cường bảo mật và khó khăn hơn đối với kẻ tấn công phishing.

- 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. Kẻ tấn công phishing

thường sử dụng chiêu này để lừa đảo người dùng. 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.

- Báo cáo các trang web phishing: Nếu bạn phát hiện một trang web phishing, hãy báo cáo cho nhà cung cấp dịch vụ trực tuyến hoặc cơ quan chức năng có thẩm quyền để họ có thể đối phó với tình huống đó và ngăn chặn người khác trở thành nạn nhân tiếp theo.

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

- ***Dấu hiệu nhận biết:***

Tình trạng tin nhắn SMS Brandname giả mạo phần lớn xuất phát từ việc các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới người dùng với mục đích nhằm chiếm đoạt tài sản.

Các điện thoại với tính năng tự động kết nối vào các trạm BTS có cường độ sóng mạnh, do cơ chế này nên các máy điện thoại tự động kết nối vào trạm BTS giả đang phát 2G ở gần. Các đối tượng đem thiết bị lên ô tô hoặc xe máy để di chuyển đến những nơi đông người, phát tán tin nhắn tới những thuê bao kết nối vào trạm BTS giả.

Mỗi thiết bị BTS giả có thể phát tán tới mấy chục nghìn tin nhắn/1 ngày. Đây là thủ đoạn tấn công khai thác điểm yếu xác thực của mạng 2G. Đến nay vẫn chưa có giải pháp kỹ thuật nào để ngăn chặn triệt để được nguy cơ này. Theo thông tin ghi nhận, các thiết bị được sử dụng để tạo trạm BTS giả là các thiết bị trôi nổi vào Việt Nam không qua thị trường chính ngạch.

- ***Biện pháp phòng tránh***

Để chủ động ngăn chặn tình trạng này, bản thân mỗi người dùng cũng phải trang bị đầy đủ các kiến thức, thông tin liên quan đến các hình thức mạo danh thương hiệu. đồng thời tham khảo các khuyến cáo từ Cục An toàn thông tin để phòng tránh sập bẫy lừa đảo.

1. Lưu ý rằng các ngân hàng, đơn vị cung cấp dịch vụ, nhà sản xuất,... thường sẽ không yêu cầu khách hàng cung cấp thông tin cá nhân thông qua SMS, email, phần mềm chat,... Bởi vậy, việc xuất hiện các tin nhắn có nội dung yêu cầu cung cấp thông tin cá nhân là điều bất thường. Hãy 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.

2. 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.

3. 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. Các website chính thức của các tổ chức ngân hàng thường sử dụng giao thức https và kết thúc bằng đuôi .vn.

4. 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 kiểm chứng lên công ty, tổ chức, ngân hàng có liên quan, bằng cách tìm thông tin liên hệ phòng chăm sóc khách hàng của hô để hỏi họ xem có phải trang web, ứng dụng là của họ hay không!

5. Ngoài ra, trong trường hợp phát hiện lừa đảo, người dùng cũng cần lưu lại các bằng chứng, thực hiện phản ánh tới Doanh nghiệp viễn thông quản lý thuê bao để yêu cầu xử lý; bên cạnh đó cung cấp các bằng chứng đã có tới các cơ quan chức năng của Bộ Công an nơi gần nhất đề nghị xử lý vi phạm theo đúng quy định của pháp luật.

6. 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). Nếu phát hiện dấu hiệu lừa đảo, hãy gửi phản ánh về địa chỉ của Trang cảnh báo an toàn thông tin Việt Nam https://canhbao.khonggianmang.gov.vn.

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

Nhận diện sàn đầu tư chứng khoán quốc tế, giao dịch vàng, ngoại hối, tiền ảo, bất động sản, kinh doanh đa cấp có mục tiêu quảng cáo, lôi kéo số lượng lớn người tham gia đầu tư và có nguy cơ lừa đảo chiếm đoạt tài sản là rất quan trọng để bảo vệ mình và tránh rơi vào các cạm bẫy tài chính.

Dưới đây là một số **dấu hiệu để nhận diện**:

- 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.

- ***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.

- Đánh giá từ người dùng khác: Tìm hiểu và đánh giá từ người dùng khác về trải nghiệm của họ 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.

- Nếu có nghi ngờ, hãy tìm kiếm sự tư vấn chuyên gia: Nếu bạn không chắc chắn về một sàn giao dịch hoặc công ty, hãy tìm sự tư vấn từ chuyên gia tài chính hoặc luật sư để đảm bảo rằng bạn đưa ra quyết định thông minh và an toàn.

Lưu ý rằng việc nhận diện và phòng ngừa lừa đảo là rất quan trọng. Hãy luôn giữ cảnh giác và chỉ tin tưởng vào các nền tảng và sàn giao dịch có uy tín và được xác thực.

12. Lừa đảo tuyển dụng CTV online

Hiện nay, hình thức lừa đảo phổ biến nhất vẫn là lừa tuyển cộng tác viên "việc nhẹ lương cao" - giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn để chiếm đoạt tài sản của các nạn nhân. Khoản tiền các đối tượng lừa chiếm đoạt được từ hình thức này thường từ vài triệu đến vài trăm triệu đồng.

- ***Dấu hiệu nhận diện và biện pháp phòng tránh:***

- Yêu cầu tạm ứng tiền: Nếu bạn được yêu cầu nộp một khoản tiền tạm ứng trước khi bắt đầu công việc, hãy cảnh giác. Lừa đảo thường sử dụng chiêu này để chiếm đoạt số tiền của bạn mà không cung cấp công việc thực tế.

- Yêu cầu thông tin tài khoản cá nhân: Lừa đảo có thể yêu cầu bạn 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. Hãy luôn cảnh giác và không chia sẻ thông tin nhạy cảm của bạn với bất kỳ ai mà bạn không tin tưởng hoặc không biết rõ.

- Trang thanh toán đơn hàng không an toàn: Kiểm tra xem trang thanh toán đơn hàng có đủ các biểu tượng bảo mật như khóa SSL hay "https://" trước URL không. Nếu trang không có các biểu tượng này, đó có thể là dấu hiệu của một trang web giả mạo và thông tin của bạn có thể bị đánh cắp.

- Quảng cáo công việc quá hấp dẫn và dễ dàng: Lừa đảo thường hứa hẹn công việc có thu nhập cao và dễ dàng, mà không yêu cầu kỹ năng hay kinh nghiệm đặc biệt. Hãy cẩn thận với những đề nghị quá mức hấp dẫn và đánh giá kỹ trình độ của bạn trước khi tham gia.

- Thiếu thông tin công ty hoặc không có thông tin liên hệ: Kiểm tra thông tin về công ty hoặc người tuyển dụng. Nếu không có thông tin rõ ràng hoặc không có thông tin liên hệ, đó có thể là dấu hiệu của một hoạt động lừa đảo.

- Thiếu hợp đồng hoặc thoả thuận rõ ràng: Khi tham gia vào một chương trình tuyển cộng tác viên, hãy yêu cầu và đọc kỹ hợp đồng hoặc thoả thuận liên quan. Nếu không có hợp đồng hoặc thoả thuận rõ ràng, bạn có thể gặp rủi ro bị lừa đảo.

- Kiểm tra về đánh giá và phản hồi tiêu cực: Trao đổi với người dùng khác và tìm hiểu về kinh nghiệm của họ với chương trình tuyển cộng tác viên mà bạn quan tâm. Nếu có nhiều phản hồi tiêu cực hoặc đánh giá không tốt, hãy cân nhắc trước khi tham gia.

13. Đánh cắp tài khoản MXH, nhắn tin lừa đảo

- ***Dấu hiệu nhận diện và biện pháp phòng tránh:***

- 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. Đặc biệt, nếu tin nhắn có chứa các lời khẩn cấp, đe dọa hoặc yêu cầu không phù hợp, hãy kiểm tra lại xem có phải tin nhắn thực sự từ bạn bè của bạn hay không.

- 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, cẩn 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, hãy tránh nhấp chuột hoặc truy cập vào đường link đó.

- Yêu cầu cung cấp thông tin cá nhân hoặc thông tin đăng nhập: Lưu ý rằng bạn không nên cung cấp thông tin cá nhân nhạy cảm hoặc thông tin đăng nhập (tên đăng nhập, mật khẩu) thông qua tin nhắn hoặc email. Lừa đảo thường sử dụng chiêu này để chiếm quyền điều khiển tài khoản của bạn.

- Xác minh thông tin: Nếu bạn nhận được một tin nhắn hoặc email đáng ngờ từ một người bạn, hãy thử liên hệ trực tiếp với họ thông qua các phương tiện khác (điện thoại, tin nhắn, email) để xác minh xem tin nhắn đó có phải từ họ hay không. Đừng sử dụng thông tin liên hệ được cung cấp trong tin nhắn đáng ngờ để xác minh.

- Báo cáo và cảnh báo: Nếu bạn nhận thấy bất kỳ dấu hiệu lừa đảo nào, hãy báo cáo ngay lập tức cho người bạn bè bị ảnh hưởng và thông báo vụ việc cho nền tảng mạng xã hội hoặc dịch vụ email để họ có thể thực hiện biện pháp cần thiết.

Nếu bạn/ người thân gặp phải bất kỳ dấu hiệu nào như trên, hãy thực hiện các biện pháp sau:

- 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.

Ngoài ra, hãy 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.

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

- ***Dấu hiệu nhận biết:***

Đối tượng giả danh cơ quan công an, viện kiểm sát, tòa án để gọi điện hăm dọa và lừa đảo thường sử dụng các chiêu trò và phương pháp nhằm lừa đảo và chiếm đoạt tài sản của nạn nhân. Dưới đây là một số dấu hiệu nhận diện:

- Sử dụng số điện thoại giả mạo: Đối tượng sẽ sử dụng số điện thoại giả mạo, có thể hiển thị số điện thoại của cơ quan công an, viện kiểm sát hoặc tòa án trên màn hình điện thoại của bạn. Hãy lưu ý rằng cơ quan chính thức sẽ không sử dụng số điện thoại giả mạo hoặc giả danh.

- 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.

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

- ***Biện pháp phòng tránh:***

Để phòng chống và bảo vệ mình khỏi các hình thức lừa đảo như trên, hãy áp dụng các biện pháp sau:

- 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 qua các kênh chính thức.

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

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

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.

15. Rao bán hàng giả hàng nhái qua sàn thương mại điện tử

- ***Dấu hiệu nhận diện:***

Dấu hiệu nhận biết các hoạt động thương mại điện tử, rao bán hàng giả và hàng nhái trên mạng xã hội và các sàn thương mại điện tử có thể bao gồm:

- Giá quá rẻ: Sản phẩm được rao bán với giá cực kỳ hấp dẫn, thường rẻ hơn rất nhiều so với giá thị trường. Đây có thể là dấu hiệu của hàng giả, hàng nhái hoặc gian lận.

- 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 có đáng tin cậy. Đây có thể 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, chẳng hạn 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. Nếu tài khoản không đáng tin, với ít hoặc không có thông tin cá nhân, hoạt động mới hoặc không có đánh giá, đó có thể là một dấu hiệu cho thấy người bán không đáng tin cậy.

- 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:***

Để phòng chống và tránh bị lừa đảo khi mua hàng trực tuyến, hãy áp dụng các biện pháp sau:

- Nghiên cứu và đánh giá nguồn gốc người bán: Kiểm tra thông tin về người bán, bao gồm địa chỉ, số điện thoại 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.

Hãy luôn cảnh giác và nghĩ kỹ trước khi thao tác mua hàng trực tuyến trên sàn thương mại điện tử và mạng xã hội. Đồng thời, thường xuyên cập nhật thông tin mới nhất về các biện pháp bảo vệ thông tin và quyền lợi cá nhân trên báo chí và các website chính thống.

16. Đánh cắp thông tin CCCD đi vay tín dụng

Sự nguy hiểm của việc sử dụng thông tin trên CCCD đăng ký mã số thuế ảo, vay tiền từ các tổ chức tín dụng trên mạng xã hội và lừa đảo chiếm đoạt tài sản là rất nghiêm trọng. Dưới đây là các **cảnh báo** bạn nên lưu ý:

- 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***

Để phòng ngừa các nguy cơ trên, hãy áp dụng các biện pháp sau:

- 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

Cảnh báo: Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng và giả danh người thu hồi nợ để yêu cầu trả lại số tiền là một hình thức lừa đảo nguy hiểm. Dưới đây là các **điểm cần lưu ý và biện pháp phòng ngừa** để bảo vệ bản thân:

- Không chuyển tiền ngay lập tức: 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 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 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 khi đã bị lừa

- ***Dấu hiệu nhận biết:***

- Nghiên cứu mục tiêu: kẻ lừa đảo xác định những cá nhân hoặc tổ chức có danh tiếng chân thật và đáng tin cậy. Điều này sẽ giúp kẻ lừa đảo chọn đúng mục tiêu để giả mạo.

- Tạo một danh tính giả: kẻ lừa đảo xây dựng một nhân vật xuất hiện có thể tin tưởng và đáng tin cậy. Điều này có thể liên quan đến việc tạo các hồ sơ giả, trang web giả hoặc tài liệu để ủng hộ sự lừa dối của bạn.

- Thiết lập liên lạc: Tiếp cận nạn nhân hoặc những người liên quan đến mục tiêu dưới cái giả của một cá nhân, tổ chức hoặc nhân viên đáng tin cậy. Sử dụng ngôn ngữ thuyết phục và các chiến thuật để xây dựng lòng tin của họ.

- Trình bày cơ hội: Thuyết phục nạn nhân rằng họ có khả năng khôi phục lại số tiền đã mất. Tôn vinh khả năng chuyên môn, mối quan hệ hoặc phương pháp độc quyền mà bạn là ứng cử viên lý tưởng cho nhiệm vụ này.

- Yêu cầu thanh toán hoặc thông tin nhạy cảm: Sau khi nạn nhân tin tưởng vào khả năng của kẻ lừa đảo, yêu cầu thanh toán hoặc thông tin cá nhân dưới giả danh phí xử lý, yêu cầu pháp lý hoặc bất kỳ lý do hợp lý nào khác.

- Tiếp tục giả mạo, cung cấp thông tin cập nhật và sự đảm bảo để giữ cho nạn nhân tham gia và ngăn họ nghi ngờ ý đồ thật sự của kẻ lừa đảo.

- ***Biện pháp phòng tránh:***

- Không chuyển tiền ngay lập tức: 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 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 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.

- 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.

19. Lừa đảo lấy cắp Telegram OTP

- ***Dấu hiệu nhận biết:***

Thường kẻ lừa đảo, tạo một profile giả mạo, đánh cắp hình ảnh của 1 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 trong lúc này kẻ lừa đảo đã dùng số điện thoại của nạn nhân và chọn chức năng quên mật khẩu của Telegram, lúc này khi chụp hình screenshot thì vô tình để nạn nhân thấy 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. 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 không có lý do hợp lý và 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 hoặc tổ chức có thẩm quyền 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: Kẻ 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:***

- Tránh 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 thông tin cá nhân trên mạng xã hội: Để giảm khả năng bị lừa đảo, hạn chế việc tiết lộ thông tin cá nhân quá nhiều trên mạng xã hội, bao gồm cả Facebook. Thông tin cá nhân quá chi tiết có thể được 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

- ***Dấu hiệu nhận diện:***

- Xác định và tiếp cận nạn nhân: 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: Kẻ 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. (Vì kẻ lừa đảo nắm bắt được tâm lý và tình hình tài chính của nạn nhân)

- Kẻ lừa đảo gửi hàng bưu kiện có giá trị và bắt đóng tiền thuế bằng cách gửi tiền vào tài khoản kẻ lừa đảo. 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 bảo là tài khoản bị sai thông tin, phải đóng tiền để xác minh chứng thực... Cứ thế cho đến khi nạn nhân hết sạch tiền, phá sản.

- ***Biện pháp phòng tránh:***

- Nên chậm lại: Hãy giữ 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.

- 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.

- Cảnh giác với cuộc gọi trúng thưởng: Nếu bạn nhận được một cuộc gọi thông báo rằng bạn đã trúng thưởng một giải thưởng lớn, hãy cẩn thận và xác minh thông tin từ nguồn tin cậy. Lừa đảo thường sử dụng các cuộc gọi trúng thưởng để lừa đảo nạn nhân để yêu cầu họ cung cấp thông tin cá nhân nhạy cảm hoặc chuyển khoản tiền để nhận giải thưởng. Hãy luôn nhớ rằng không có ai trúng thưởng mà không tham gia hoặc không có cách để trúng thưởng mà không phải trả phí.

- Cẩn trọng khi chia sẻ hình ảnh và video nhạy cảm: Tránh 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.

- Tìm hiểu về các hình thức lừa đảo: Nắm vững kiến thức về các hình thức lừa đảo phổ biến và cách nhận diện các dấu hiệu đáng ngờ. Điều này giúp bạn nhận biết được khi một tình huống có thể là một hình thức lừa đảo và cảnh báo kịp thời.

- Luôn giữ cảnh giác và không tin tưởng quá nhanh: 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.

- Hãy giữ 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.

- Giữ thông tin cá nhân riêng tư và an toàn: Bảo vệ thông tin cá nhân của bạn bằng cách 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.

- Đào sâu kiến thức về đầu tư tài chính: Nếu bạn quan tâm đến đầu tư tài chính như Forex, 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.

- Luôn cảnh giác và tin tưởng vào trực giác của bạn: Nếu bạn cảm thấy có điều gì đó không đúng hoặc không thoải mái trong một tình huống, hãy tin tưởng vào trực giác của bạn. Đừng bị lừa bởi lời hứa hoặc áp lực từ người khác. Luôn tự đặt câu hỏi và xem xét cẩn thận trước khi thực hiện bất kỳ hành động nào.

23. 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

- Cẩn trọng với việc chia sẻ thông tin cá nhân: Hạn chế việc chia sẻ thông tin cá nhân trên Facebook và các nền tảng trực tuyến khác. Tránh việc cung cấp 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 của bạn để giúp họ tránh trở thành nạn nhân và cùng nhau tạo một môi trường trực tuyến an toàn hơn. 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)

24. Lừa đảo cho số đánh lô đề

Cảnh báo: 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 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 mánh khóe để lôi kéo người dùng.

- 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.

- Kiểm tra tính xác thực của nguồn tin: Xác minh thông tin từ nguồn tin đáng tin cậy và có uy tín. Nếu có người liên hệ với bạn trên mạng xã hội và đề nghị đánh số lô, số đề, hãy kiểm tra kỹ thông tin về họ, đảm bảo tính xác thực và đáng tin cậy của họ trước khi tham gia.

- Tránh chia hoa hồng khi trúng: Nếu người liên hệ yêu cầu bạn chia hoa hồng khi trúng số, đây là một dấu hiệu rõ ràng của lừa đảo. Không đồng ý chia hoa hồng hoặc chuyển bất kỳ số tiền nào cho người khác, đặc biệt là nếu bạn không có hợp đồng hoặc thoả thuận rõ ràng với họ.

- 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, như cảnh sát hoặc cơ quan quản lý mạng xã hội, để họ tiến hành điều tra và cung cấp sự hỗ trợ.

Cảnh báo: Việc tham gia vào các hoạt động không rõ nguồn gốc và không đáng tin cậy như đánh số lô, số đề trên mạng xã hội có thể gây mất tiền bạc và hậu quả pháp lý nghiêm trọng. Hãy cẩn thận, cân nhắc và tìm hiểu kỹ trước khi quyết định tham gia bất kỳ hoạt động tài chính nào để bảo vệ tài sản và tránh trở thành nạn nhân của lừa đảo trực tuyến.

IV: PHẢI LÀM GÌ KHI ĐÃ BỊ LỪA ĐẢO TUYẾN

*** Hành động nhanh nếu đã bị lừa đảo:**

Nếu bạn đã bị lừa đảo, hãy làm theo các bước sau:

- Đừng 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, làm đơn tố giác gửi tới cơ quan công an nơi lưu 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)

*** 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 nơi lưu trú.

- 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)

*** 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. Đây là những việc 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:**

Một kẻ lừa đảo giả vờ là người từ nhà cung cấp Internet hoặc điện thoại của bạn. Họ nói rằng bạn gặp sự cố kỹ thuật và yêu cầu quyền truy cập vào thiết bị của bạn. Sau đó, những kẻ lừa đảo sẽ lây nhiễm vi-rút vào đó để đánh cắp mật khẩu và thông tin tài chính của bạn. Đây là những việc cần làm:

- 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.

Bạn cũng có thể nhờ chuyên gia công nghệ thông tin kiểm tra trực tiếp thiết bị của mình.

*** Liên hệ đến các cơ quan, tổ chức, doanh nghiệp về an ninh mạng, an toàn thông tin:**

1. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05),

Bộ Công an; hoặc Cục Cảnh sát hình sự (C02) trực thuộc Bộ Công An.

Tại mỗi địa phương, liên hệ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (PA05).

2. Cục An toàn thông tin (AIS), trực thuộc Bộ Thông tin và Truyền thông. Cục An toàn thông tin là cơ quan quản lý nhà nước và thực thi pháp luật về an toàn thông tin, điện thoại 024 3209 6789; email ais@mic.gov.vn.

3. Bộ Tư lệnh Tác chiến không gian mạng (Bộ Tư lệnh 86), Bộ Quốc phòng Việt Nam.

Bên cạnh đó Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc trung ương tại 63 tỉnh/thành phố là cánh tay nối dài của Bộ Thông tin và Truyền thông tại các tỉnh, thành phố.

5. Hiệp hội an toàn thông tin Việt Nam (VNISA), số điện thoại: 024 62901028; email info@vnisa.org.vn.

6. Các doanh nghiệp an toàn thông tin của Việt Nam: Bkav, VNPT Cyber Immunity, Viettel Cyber Security, CMC Cyber Security, FPT IS, HPT, MISOFT và VNCS...

7. Liên minh tuyên truyền nâng cao nhận thức, kỹ năng bảo đảm an toàn thông tin cho người dân trên không gian mạng do Cục An toàn thông tin (AIS) và Hiệp hội An toàn thông tin Việt Nam (VNISA) chủ trì điều phối cùng 8 đơn vị sáng lập VNPT, Viettel, MobiFone, CMC, Bkav, VNG, TikTok và Cốc Cốc.