BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUY NHƠN

Số: 1932 /ĐHQN-CTCTSV
V/v tuyên truyền phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản bằng công nghệ cao

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Bình Định, ngày 17 tháng 4 năm 2024

Kính gửi: Các trưởng đơn vị.

Căn cứ Công văn số 1078/CATP-CSHS ngày 09/4/2024 của Công an thành phố Quy Nhơn về việc tuyên truyền phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao cho thấy tình hình tội phạm lừa đảo chiếm đoạt tài sản bằng cách sử dụng công nghệ cao hiện tại diễn biến phức tạp. Nhằm nâng cao hiểu biết về phương thức, thủ đoạn phạm tội của đối tượng lừa đảo chiếm đoạt tài sản để phòng ngừa hiệu quả loại tội phạm này, Nhà trường đề nghị các Trưởng đơn vị triển khai đến tất cả viên chức, người lao động và học viên, sinh viên một số nội dung sau:

- Tổ chức tuyên truyền hiệu quả đến viên chức, người lao động và học viên, sinh viên bằng nhiều hình thức như: tuyên truyền trong các buổi họp của đơn vị, trong các buổi sinh hoạt lớp của học viên, sinh viên, các nhóm zalo, facebook... về các phương thức, thủ đoạn lừa đảo qua mạng của các đối tượng tội phạm để nâng cao ý thức cảnh giác, phòng ngừa *(Kèm theo tài liệu về các phương thức, thủ đoạn lừa đảo bằng cách sử dụng công nghệ cao và các vụ án thực tế đã xảy ra của Công an TP. Quy Nhơn).*

- Trực tiếp, thường xuyên tiếp cận các bài tuyên truyền phòng ngừa lừa đảo chiếm đoạt tài sản, các khuyến cáo của lực lượng Công an, của Nhà trường nhằm nắm vững nguyên tắc "4 Không; 2 Phải" (Không sợ, không tham, không kết bạn với người lạ, không chuyển khoản và phải thường xuyên cảnh giác, phải tố giác ngay với Công an khi có nghi ngờ).

Đề nghị các Trưởng đơn vị thông tin đến toàn thể viên chức, người lao động và học viên, sinh viên để biết và nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- Hiệu trưởng (để b/c);
- Đăng website Trường;
- Đăng fanpage P. CTCTSV;
- Lưu: VT, CTCTSV.

KT. HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUY NHƠN

TS. Đinh Anh Tuấn

TÀI LIỆU
PHỤC VỤ TUYÊN TRUYỀN PHÒNG CHỐNG TỘI PHẠM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN SỬ DỤNG CÔNG NGHỆ CAO

I. CÁC PHƯƠNG THỨC, THỦ ĐOẠN LỪA ĐẢO CHỦ YẾU:

(1) Lừa đảo mua bán hàng hóa, dịch vụ (vé máy bay, du lịch...) giá rẻ

- Lợi dụng tâm lý ham rẻ của đa số người dân khi mua hàng hoặc tìm kiếm dịch vụ trên không gian mạng, các đối tượng đăng tải bài viết quảng cáo các loại hàng hóa, dịch vụ với mức giá rẻ hơn so với thị trường. Khi người dân liên hệ, các đối tượng tạo vỏ bọc uy tín, yêu cầu người dân chuyển khoản đặt cọc hoặc trả tiền trước, sau đó chiếm đoạt số tiền trên.

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

- Làm giả website/fanpage cửa hàng, công ty du tịch 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.

- 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, đăng tải nhiều bài viết thể hiện việc đặt vé máy bay cho nhiều đoàn khách khác nhau, Nếu khách hàng liên hệ, các đối tượng sẽ đặt chỗ vé máy bay, gửi mã đặt chỗ để làm tin hoặc sử dụng phần mềm chỉnh sửa ảnh để tạo về máy bay giả 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.

(2) Chiếm đoạt tài khoản mạng xã hội sau đó giả mạo người thân, quen nhắn tin, gọi điện vay tiền

Đây là hình thức lừa đảo khá phổ biến, các đối tượng sau khi đánh cắp được tài khoản mạng xã hội sẽ nghiên cứu cách thức nói chuyện của chủ tài khoản với bạn bè, người thân hoặc thu thập các video của chủ tài khoản còn lưu trên mạng xã hội, sử dụng căn cước công dân giả đăng ký tài khoản ngân hàng online trùng với tên của chủ tài khoản mạng xã hội bị đánh cắp, khiến cho nạn nhân lầm tưởng rằng đang chuyển tiền cho bạn bè, người thân của mình. Sau đó, nhắn tin hoặc gọi điện video cho người thân, quen hỏi vay tiền hoặc nhờ chuyển khoản hộ. *Dấu hiệu chủ yếu:*

- Tin nhắn hoặc email đáng ngờ: Nếu bạn nhận được một tin nhắn hoặc một email từ người bạn trong danh bạ 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 (http://), 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 01 tin nhắn hoặc email đáng ngờ từ một người bạn, hãy 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 có dấu hiệu lừa đảo nào, hãy báo cáo 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.

(3) Lừa đảo chuẩn hóa thông tin cá nhân (thuê bao di động, VneID, tài khoản ngân hàng...) để yêu cầu truy cập hoặc cài đặt ứng dụng độc hại.

Đây là hình thức lừa đảo giả danh quản lý nhà nước để yêu cầu người dân truy cập đường link chứa mã độc hoặc tải về ứng dụng giả mạo chứa mã độc. Sau khi người dân click vào đường dẫn hoặc tải về ứng dụng, cho phép truy cập thiết bị, các đối tượng sẽ thu thập được dữ liệu về thông tin cá nhân, tài khoản ngân hàng... nhằm mục đích chiếm đoạt tài sản. *Dấu hiệu chủ yếu:*

- Cuộc gọi từ số điện thoại cá nhân hoặc số điện thoại giả mạo thương hiệu (Brandname) như VneID, 113, Vinaphone, Viettel, ... các đối tượng giả danh cơ quan quản lý nhà nước (cảnh sát khu vực, cán bộ quản lý hộ tịch, nhà cung cấp dịch vụ viễn thông hoặc nhân viên ngân hàng...) thông báo đề nghị người dân bổ sung hoặc sửa đổi dữ liệu thông tin cá nhân để chuẩn hóa theo quy định.

- Các đối tượng yêu cầu người dân cung cấp thông tin cá nhân để chuẩn hóa, hoặc truy cập vào các đường dẫn giả mạo, tải ứng dụng chứa mã độc để chiếm quyền điều khiển thiết bị điện tử hoặc các tài khoản ngân hàng, thuê bao di động... Đối tượng gây áp lực bằng cách đe dọa nếu không làm theo hướng dẫn thì có thể sẽ bị khóa thuê bao di động, khóa tài khoản ngân hàng hoặc cơ quan công an sẽ đến nhà làm việc...

- Trong một số trường hợp, để tạo lòng tin, các đối tượng gọi video call cho người dân với trang phục công an hoặc giả mạo văn phòng làm việc của các cơ quan quản lý nhà nước.

(4) Giả mạo cơ quan, tổ chức, cá nhân tuyển người mẫu, cầu thủ nhí, người đại diện thương hiệu sau đó lôi kéo làm nhiệm vụ online hoặc đầu tư tài chính

Lợi dụng các sự kiện lớn sắp diễn ra hoặc thời gian nghỉ lễ của trẻ nhỏ, các đối tượng tạo lập các trang mạng xã hội đăng thông tin tuyển người mẫu, ca sĩ, cầu thủ nhí hoặc tuyển đại diện cho các thương hiệu lớn để quảng bá sản phẩm. Sau khi người dân đăng ký tham gia, chúng sẽ thu thập thông tin cá nhân của người dân và gia đình. Các đối tượng tiếp tục hướng dẫn người dân vào trang web của chương trình để làm nhiệm vụ tăng tương tác, tăng lượt bình chọn, sau đó yêu cầu chuyển tiền để hoàn thành nhiệm vụ. *Dấu hiệu chủ yếu:*

- Đối tượng chủ động tạo lập các trang web, trang Facebook..., lấy danh nghĩa các Công ty truyền thông, trung tâm đào tạo bóng đá... đăng tin quảng cáo trên mạng xã hội.

- Khi người dân liên hệ sẽ được các đối tượng hướng dẫn cung cấp thông tin cá nhân của bản thân và gia đình: Sau đó, các đối tượng gửi đường dẫn để người dẫn truy cập vào đăng ký tài khoản, làm nhiệm vụ online, chuyển tiền đặt cọc để hoàn thành nhiệm vụ, nhận lại tiền sau khi hoàn thành nhiệm vụ.

- Được mời vào các nhóm kín trên mạng xã hội, trong đó có nhiều tài khoản *"vào vai"* các phụ huynh khác để thúc giục nạn nhân chuyển tiền hoàn thành nhiệm vụ.

(5) Giả danh công ty tài chính, ngân hàng để hỗ trợ cho vay, nâng hạn mức tín dụng... sau đó yêu cầu chuyển tiền để làm thủ tục

Những năm gần đây, nhu cầu vay tiền trực tuyến qua app hoặc nâng hạn mức tín dụng chi tiêu online của người dân tăng cao, các đối tượng đã giả danh công ty tài chính, ngân hàng đăng tải thông tin quảng cáo dịch vụ cho vay online lãi suất thấp, thủ tục đơn giản, giải ngân nhanh chóng hoặc hỗ trợ nâng hạn mức cho các tài khoản tín dụng. Để được giải quyết thủ tục, người dân cần nộp trước một số khoản phí để làm hồ sơ hoặc để bảo đảm tài sản... Số tiền này được hứa hẹn sẽ trả lại sau khi hoàn thành thủ tục. Thực tế, sau khi người dân chuyển tiền, các đối tượng sẽ cắt liên lạc hoặc lấy lý do khác nhau để không trả lại tiền. *Dấu hiệu chủ yếu:*

- Đối tượng sử dụng số điện thoại, tin nhắn hoặc email giả mạo gần giống với thông tin của nhân viên ngân hàng, liên hệ với người dân có nhu cầu.

- Các đối tượng lập nhiều trang mạng xã hội quảng cáo dịch vụ cho vay tiền online qua app. Khi người dân liên hệ sẽ được các đối tượng hướng dẫn cài ứng dụng nhằm mục đích thu thập thông tin cá nhân hoặc ứng dụng chứa mã độc nhằm chiếm quyền điều khiển thiết bị. Để được giải ngân khoản vay, người dân cần đóng khoản phí để đảm bảo tài sản, sau đó các đối tượng sẽ chiếm đoạt số tiền này.

- Giả danh nhân viên ngân hàng quản cáo dịch vụ mở thẻ tín dụng, nâng cấp hạn mức tín dụng tiêu dùng cho người thân. Để được đáp ứng dịch vụ, người dân cần cung cấp thông tin cá nhân, chuyển một khoản phí đảm bảo để được duyệt nâng hạn mức.

(6) Giả mạo danh nghĩa cơ quan, tổ chức phát tán tin nhắn SMS Brandname chứa đường dẫn lừa đảo, nội dung yêu cầu cung cấp thông tin cá nhân hoặc tải ứng dụng độc hại.

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 danh đang phát sóng ở gần. Các đối tượng đem thiết bị lên xe 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. Ngoài ra, các đối tượng có thể sử dụng các phần mềm spam tin nhắn Imessage để phán tán tin nhắn giả mạo thương hiệu đến người sử dụng thiết bị có hệ điều hành IOS. Bên cạnh đó, do tính năng tự động nhận diện thương hiệu trên điện thoại nên các tin nhắn giả mạo nhận được giống những tin nhắn chính thống đã nhận được trước đó.
Dấu hiệu chủ yếu:

- Nhận được tin nhắn mang tên cơ quan, tổ chức doanh nghiệp chính thống (như: Bo Cọng an, Bo Thong tin và Truyen thong, Vietcombank, Techcombank...), bên trong chứa nội dung như tin nhắn thông thường của các cơ quan, tổ chức, kèm theo đường dẫn giả mạo, đề nghị người dân truy cập, nhập thông tin tài khoản để chiếm đoạt hoặc cài đặt ứng dụng chứa mã độc để chiếm đoạt điều khiển thiết bị.

- Các trang web giả mạo thường chứa mã độc hoặc giả mạo trang web chính thống của cơ quan, tổ chức, yêu cầu đăng nhập tài khoản, nhập mã OTP nhằm mục đích chiếm đoạt tài sản.

(7) Lừa đảo đầu tư các sàn chứng khoán, tiền ảo, đa cấp... sau đó khóa, đánh cháy tài khoản hoặc đánh sập sàn

Trước xu thế đầu tư vào các hoạt động trực tuyến như chứng khoán, tiền ảo... của người dân tăng cao trong những năm gần đây, tội phạm lừa đảo qua mạng đẩy mạnh hoạt động thông qua hình thức này. Chúng tạo lập các sàn chứng khoán, đa cấp, tiền ảo... một cách dễ dàng, sử dụng mạng xã hội quảng cáo, tuyển người tham gia đầu tư với những lời hứa hẹn hấp dẫn như: cam kết có lãi, lợi nhuận cao, kiếm tiền dễ dàng... khiến cho không ít nạn nhân sập bẫy, mất số tiền lớn. Hầu hết nạn nhân khi tham gia đầu tư đều được tư vấn chi tiết cách thức mở tài khoản, đầu tư các khoản tiền nhỏ để thử và nhận lại khoản lãi suất tương ứng nhằm mục đích đánh vào lòng tham. Sau khi thấy có thể kiếm được tiền từ các sàn này, nạn nhân được mời gọi đầu tư số tiền lớn hơn và lấy nhiều lý do để không thể rút được tiền ra mà phải đóng thêm nhiều khoản phí với cam kết sẽ được nhận lại toàn bộ cả tiền phí và tiền lãi ban đầu (hệ thống thanh toán lỗi, nhập sai nội dung giao dịch, sai tài

khoản, cơ quan thuế nước ngoài điều tra...) hoặc khóa tài khoản, cho sập sàn giao dịch và cắt liên lạc với nạn nhân. *Dấu hiệu chủ yếu:*

- Các đối tượng thường chủ động tiếp cận với người dân để tìm cách giới thiệu, quảng cáo về trang web hoặc sàn giao dịch mà mình đang đầu tư và thu được lợi nhuận cao từ việc đầu tư này.

- Phương thức tiếp cận nạn nhân của các đối tượng rất đa dạng, có thể từ quảng cáo trên mạng xã hội, hoặc vào vai doanh nhân thành đạt kết bạn làm quen, trò chuyện tình cảm trong thời gian dài, dần dần lôi kéo đầu tư.

- Các đối tượng tìm nhiều cách để không gặp mặt nạn nhân, lấy lý do ở nước ngoài, đi công tác... giả mạo định vị để tạo lòng tin. Chúng luôn đóng vai là người đầu tư cùng khiến nhiều nạn nhân dù đã nghi ngờ bị lừa đảo nhưng vẫn tin tưởng vào "người bạn" của mình nên tiếp tục chuyển tiền.

- Nạn nhân thường được đưa vào các nhóm kín trên mạng xã hội (Zalo, Telegram...) có nhiều tài khoản ảo đóng vai "chuyên gia đọc lệnh", thành viên cùng tham gia đầu tư. Các tài khoản ảo thường xuyên đăng tin chuyển tiền thành công hoặc đã nhận được lãi suất từ sàn đầu tư sau khi làm theo hướng dẫn của các "chuyên gia". Khi nạn nhân có dấu hiệu nghi ngờ, cân nhắc chuyển tiền, các tài khoản ảo liên tục thúc giục việc chuyển tiền để nhóm tiếp tục hoạt động.

(8) Lừa đảo tình cảm sau đó dẫn dụ đầu tư tài chính, làm nhiệm vụ online hoặc gửi tiền, quà có giá trị

Hình thức lừa đảo tình cảm hiện nay không còn mới, tuy nhiên vẫn có rất nhiều người dân dính phải bẫy lừa đảo của các đối tượng. Chúng lập ra nhiều tài khoản mạng xã hội ảo, lấy ảnh, thông tin của những người nổi tiếng hoặc có ngoại hình ưa nhìn, vỏ bọc đoanh nhân, nhắn tin trò chuyện trong thời gian dài với nạn nhân. Trong khi trò chuyện, các đối tượng chia sẻ việc mình kiếm được nhiều tiền thông qua công việc đầu tư, làm nhiệm vụ qua mạng, lôi kéo nạn nhân tham gia cùng nhằm chiếm đoạt tài sản. Ngoài ra, đối tượng có thể tự xưng mình là người nước ngoài, ngỏ ý muốn gửi quà tặng có giá trị cao cho nạn nhân, sau đó gia danh các cơ, quan chức năng (Công an, Thuế, Hải quan...) đề nghị nạn nhân đóng các khoản phí để nhận được quà. *Dấu hiệu chủ yếu:*

- Nhận được tin nhắn hỏi thăm từ các tài khoản mạng xã hội (khen tấm hình đẹp, hỏi thăm khung cảnh, khen ngoại hình...) với mục đích tiếp cận, làm quen. Những tài khoản này liên tục hỏi thăm trong một thời gian dài.

- Yêu cầu kết bạn thông qua các tài khoản mạng xã hội, đặc biệt là các ứng dụng hẹn hò (Facebook, Zalo, Tinder...). Các tài khoản kết bạn thường có vỏ bọc "hào nhoáng" như ngoại hình đẹp, cuộc sống giàu có, đi du lịch nhiều nơi...

- Trong thời gian nói chuyện với nạn nhân, các đối tượng thường xuyên chia sẻ về cuộc sống, sinh hoạt..., trong đó lồng ghép nội dung mình đang làm công việc online và kiếm được nhiều tiền từ công việc này. Trong một số trường hợp, các đối tượng nhờ nạn nhân đăng nhập tài khoản của mình trên sàn đầu tư để làm nhiệm vụ giúp vì lý do đang bận việc cá nhân, việc này nhằm mục đích cho nạn nhân làm quen trước khi rủ nạn nhân tham gia chung.

- Khi tham gia đầu tư theo lôi kéo của đối tượng, nạn nhân có thể nhận được tiền lãi sau một số lần đầu tư ban đầu với số tiền nhỏ. Dần dần hệ thống sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc lấy nhiều lý do để "giam tiền" như: cơ quan thuế nước ngoài phong tỏa, thao tác sai, lỗi giao dịch... và yêu cầu nạn nhân chuyển thêm tiền để có thể rút toàn bộ về.

- Hứa hẹn tặng quà có giá trị cao gửi từ nước ngoài về. Đối tượng sau thời gian trò chuyện qua mạng tỏ ý rất yêu mến nạn nhân, muốn tặng cho nạn nhân những món quà có giá trị cao. Tuy nhiên việc gửi quà về gặp nhiều trục trặc như: bị cơ quan chức năng tạm giữ do quà giá trị cao, cần các khoản phí để thông quan... Nhiều nạn nhân với tâm lý sẽ nhận được quà giá trị rất lớn nên chấp nhận ứng trước một số tiền để hoàn thiện thủ tục.

(9) Lừa đảo qua hình thức tuyển cộng tác viên cho các sàn thương mại điện tử, việc nhẹ lương cao

Những năm gần đây, hình thức lừa đảo tuyển cộng tác viên làm việc online cho các sàn thương tại điện tử rất phổ biến. Đánh trúng tâm lý muốn kiếm thêm thu nhập từ các công việc online, không mất thời gian đi làm, các đối tượng tạo lập các trạng thương mại điện từ giả mạo, lấy danh nghĩa các doanh nghiệp uy tín tuyển cộng tác viên làm viêc ngoài giờ, dụ dỗ nạn nhân tham gia đóng trước các khoản tiền tạm ứng để nhận nhiệm vụ hoặc mua các gói nhiệm vụ từ số tiền nhỏ đến số tiền lớn. *Dấu hiệu chủ yếu:*

- Các đối tượng thường sử dụng các tài khoản mạng xã hội giả mạo, đăng tin tuyển cộng tác viên làm việc online, chỉ cần máy tính kết nối mạng, làm nhiệm vụ đánh giá sản phẩm, thanh toán đơn hàng ảo, clíck quảng cáo... có thể kiếm về thu nhập cao.

- Nhận được lời mời từ các số điện thoại hoặc tài khoản mạng xã hội ảo. Các tài khoản này thường chủ động liên hệ nạn nhân, nhắn tin trò chuyện nhằm thu thập thông tin cá nhân, chiếm lòng tin và dụ dỗ nạn nhân tham gia hệ thống.

- Các công việc này thường yêu cầu nạn nhân đóng trước một khoản tiền nhỏ ban dầu và sẽ trả lương hoặc hoa hồng đầy đủ cho nạn nhân để tạo lòng tin. Dần dần, hệ thống sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc dùng nhiều cách khác nhau để không cho nạn nhân rút tiền về mà phải đóng nhiều khoản phí khác nhau.

(10) Giả danh cơ quan công quyền (công an, viện kiểm sát, tòa án, hải quan..), văn phòng luật sư, ngân hàng... gọi điện đe đọa yêu cầu chuyển tiền hoặc hỗ trợ lấy lại tiền đã bị lừa đảo

Đây là hình thức lừa đảo đã xuất hiện trong vài năm trở lại đây. Các đối tượng lợi dụng tâm lý hoang mạng, lo sợ của người dân khi bị cơ quan chức năng thông báo liên quan đến hành vi vì phạm pháp luật. Chúng sử dụng các ứng dụng gọi điện thoại giả mạo danh nghĩa cơ quan chức năng, tiến hành theo từng bước: thu thập thông tin cá nhân, đe dọa liên quan đến hành vi vi phạm pháp luật, yêu cầu chuyển tiền phục vụ công tác điều tra. Ngoài ra, chúng tạo nhiều trang mạng xã hội giả mạo cơ quan công quyền (công an, viện kiểm sát, tòa án, luật sư...) đăng

tin quảng cáo hoặc chủ động liên hệ các nạn nhân đã bị lừa đảo chiếm đoạt tài sản bởi các hình thức khác và tuyên bố có thể giúp lấy lại tiền bị lừa, yêu cầu chuyển khoản phí dịch vụ trước nhằm chiếm đoạt tài sản. *Dấu hiệu chủ yếu:*

- Nhận được cuộc gọi từ số điện thoại lạ hoặc tổng đài ảo (113, BOCONGAN...) thông báo về hành vi vi phạm pháp luật (vi phạm giao thông, liên quan vụ án đang điều tra...). Qua cuộc gọi này, các đối tượng sẽ thu thập thông tin cá nhân của người dân và đe dọa, gây áp lực tâm lý nhằm không cho người dân có cơ hội hỏi ý kiến người thân hoặc cơ quan chức năng. Sau khi thu thập được thông tin, chúng sẽ kết nối người dân đến cuộc gọi khác được giới thiệu là cơ quan kiểm sát, tòa án... để tiếp tục gây áp lực tâm lý, yêu cầu người dân chuyển tiền ngay đến tài khoản của chúng để phục vụ công tác điều tra hoặc xử lý vi phạm giao thông.

- Các đối tượng kết nối với người dân thông qua tài khoản mạng xã hội, tự xưng là cán bộ cơ quan công quyền, thông báo người dân liên quan đến vụ án hình sự đặc biệt nghiêm trọng. Sau khi gây áp lực tâm lý, chúng yêu cầu nạn nhân mở tài khoản ngân hàng mới theo số điện thoại do chúng cung cấp, sau đó chuyển toàn bộ tiền từ tài khoản của nạn nhân (tài khoản liên quan đến vụ án như đối tượng thông báo) đến tài khoản mới mở để niêm phong, tạm giữ nhằm chiếm đoạt số tiền này:

- Các đối tượng thường gợi ý về việc nếu không thể đến cơ quan chức năng làm việc thì chúng hỗ trợ làm việc thông qua điện thoại. Khi người dân đề nghị gặp mặt, chúng có thể sử dụng công nghệ giả mạo gương mặt (deepfake) với trang phục công an, kiểm sát, tòa án... để gọi điện video với người dân, tìm cách lẩn tránh không gặp mặt trực tiếp.

- Một số nạn nhân sau khi bị lừa đảo bởi các hình thức khác có thể nhận được đề nghị giúp đỡ lấy lại tiền từ các tài khoản mạng xã hội giả mạo cơ quan chức năng (công an, viện kiểm sát, luật sư...). Các đối tượng thường tạo các trang mạng xã hội đăng nhiều thông tin cảnh báo lừa đảo, thêm người dân vào các nhóm chung với nhiều thành viên đóng vai nạn nhân trong các vụ lừa đảo khác đã lấy được tiền hoặc cũng đang nhờ sự trợ giúp để lấy lại tiền. Khi nại nhân đồng ý, chúng sẽ yêu cầu chuyển trước khoản phí dịch vụ và chiếm đoạt số tiền này.

(11) Một số phương thức lừa đảo khác (cho số lô đề, chuyển nhầm tiền, lấy lại tài khoản mạng xã hội).

Bên cạnh các phương thức lừa đảo phổ biến, còn xuất hiện nhiều hình thức khác như: cho số lô đề, chuyển nhầm tiền, lấy lại tài khoản mạng xã hội... *Dấu hiệu chủ yếu:*

- Các đối tượng thường sử dụng số điện thoại rác, nhiều tài khoản mạng xã hội giả mạo, không có thông tin chính thống, quảng cáo về các hình thức dịch vụ khác nhau, yêu cầu chuyển tiền phí hoặc đặt cọc trước.

- Bất ngờ nhận được một khoản tiền chuyển nhầm với các nội dung giao dịch nhạy cảm, sau đó có người liên hệ xin lại số tiền trên.

II. MỘT SỐ KHUYẾN CÁO, PHÒNG NGỪA:

1. Khi mua hàng online tìm hiểu kỹ thông tin về người bán, xem xét nguồn gốc rõ ràng, tuyệt đối không mua ở những trang mạng xã hội không có thông tin người bán và không có địa chỉ rõ ràng, hoặc khi hỏi thông tin thì cố tình giấu địa chỉ bán hàng, chỉ nhận đặt hàng qua tin nhắn, chỉ bán hàng Online chứ không có cửa hàng cụ thể.

2. Đề cao cảnh giác khi nhận các cuộc gọi đến bằng số điện thoại cố định, người gọi tự xưng là cán bộ các cơ quan Nhà nước, đặc biệt là lực lượng Công an để thông báo, yêu cầu điều tra vụ án qua điện thoại, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở... cho bất kỳ đối tượng nào khi chưa rõ nhân thân và lai lịch của người đó, đặc biệt không nghe lời của các đối tượng chuyển tiền vào các tài khoản được chỉ định. Lực lượng chức năng, nhất là lực lượng Công an, Viện kiểm sát, Tòa án nếu làm việc với người dân sẽ có giấy mời, giấy triệu tập gửi cho người đó và làm việc trực tiếp tại các trụ sở cơ quan, không làm việc Online qua mạng.

3. Không công khai các thông tin cá nhân như: ngày, tháng, năm sinh, số CMND/CCCD, số điện thoại, số tài khoản ngân hàng ... lên mạng xã hội để tránh bị các đối tượng lợi dụng khai thác, sử dụng vào mục đích lừa đảo; chọn lọc những thông tin cụ thể khi chia sẻ công khai lên mạng xã hội.

4. Thường xuyên kiểm tra và cập nhật các tính năng bảo mật, quyền riêng tư trên các tài khoản ngân hàng, tài khoản mạng xã hội và bảo mật tuyệt đối về thông tin của các tài khoản trên gồm: tên đăng nhập, mật khẩu, mã xác thực (OTP) hoặc số thẻ tín dụng,... không cung cấp cho bất kỳ cá nhân, tổ chức nào mà chưa xác định được nguồn gốc.

5. Không truy cập các đường link trong tin nhắn, email lạ không rõ nguồn gốc; không thực hiện giao dịch theo yêu cầu của các đối tượng lạ khi nhận được điện thoại, tin nhắn có nội dung liên quan đến giao dịch ngân hàng.

6. Cảnh giác khi tiếp cận website, ứng dụng (App) trong các tin nhắn mà người dùng nhận được, bao gồm các tin nhắn thương hiệu, tin nhắn từ các đầu số ngắn; tuyệt đối không truy cập vào các website, ứng dụng có nguồn gốc, nội dung không rõ ràng.

7. Cảnh giác, không tin tưởng vào những chiêu trò nhận thưởng qua mạng mà yêu cầu nạp thẻ điện thoại, hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Tìm hiểu kỹ thông tin khi kết bạn với những người lạ trên mạng xã hội, đặc biệt là những người hứa hẹn cho, tặng số tiền, tài sản lớn, không rõ lý do.

8. Cảnh giác với những trang web giả mạo dịch vụ chuyển tiền quốc tế, trang web ngân hàng... lưu ý chỉ nên nhập thông tin tài khoản ngân hàng trên trang web, ứng dụng chính thức của ngân hàng có uy tín.

9. Đối với các tin nhắn qua mạng xã hội, qua điện thoại người quen, bạn bè nhờ mua thẻ điện thoại, nhờ chuyển tiền hộ cần gọi điện trực tiếp (nếu có thể nên gọi video call) để xác nhận thông tin trước khi chuyển tiền theo yêu cầu của người đó.

10. Đối với các cá nhân có nhu cầu chuyển, nhận tiền từ nước ngoài về thì gửi nhận thông qua ngân hàng có uy tín, không sử dụng các dịch vụ chuyển tiền, đổi tiền quốc tế của các cá nhân, tổ chức không hợp pháp.

11. Không mở hộ, cho thuê, bán tài khoản ngân hàng cho người khác, đặc biệt là những đối tượng không quen biết. Khi phát hiện đối tượng có hành vi mua, thuê người khác mở tài khoản ngân hàng cần báo ngay cho Cơ quan Công an để có biện pháp xử lý theo quy định của pháp luật.

12. Không cài đặt lên điện thoại, máy tính các ứng dụng chưa được xác thực trên kho ứng dụng trước yêu cầu của đối tượng lạ.

13. Khi phát hiện sim điện thoại bị vô hiệu hóa, cần gọi ngay cho bộ phận chăm sóc khách hàng của nhà mạng để yêu cầu hỗ trợ, xác minh. Nếu bị mất điện thoại, cần khẩn trương báo nhà mạng khóa sim kịp thời.

14. Mọi người cần trang bị cho bản thân kiến thức cơ bản về công nghệ thông tin, phải biết phân biệt ứng dụng, trang web chính thông hay giả mạo. Không biết thì không dùng. Không cài đặt các ứng dụng lạ trên điện thoại khi chưa có đủ kiến thức, hiểu biết, cân nhắc việc cấp quyền cho ứng dụng truy cập vào các thông tin cá nhân như danh bạ, hình ảnh, màn hình, tin nhắn.

III. MỘT SỐ VỤ ÁN ĐIỂN HÌNH

1. Thủ đoạn lừa đảo chuẩn hóa thông tin cá nhân (thuê bao di động, VneID, tài khoản ngân hàng...) để yêu cầu truy cập hoặc cài đặt ứng dụng độc hại.

Vụ 1: Lúc 14h40 ngày 28/5/2023, đối tượng (chưa rõ lai lịch) dùng số điện thoại "0568.825.049" gọi đến số điện thoại "0563017777" của chị Huỳnh Ngọc Châu (Sinh năm: 1985; Nơi thường trú: phường Nguyễn Văn Cừ, thành phố Quy Nhơn, tỉnh Bình Định), mạo danh nhân viên chi cục thuế, hướng dẫn chị Châu truy cập vào trang web "d.gdtgov.cfd" để tải và cài đặt ứng dụng "TỔNG CỤC THUẾ" trên điện thoại di động hiệu Samsung Z Fold 3 của chị Châu để kê khai thuế kinh doanh. Chị Châu tưởng thật nên đã thực hiện theo hướng dẫn của đối tượng. Trong khi cài đặt, chị Châu đã cấp quyền cho ứng dụng trên truy cập vào dữ liệu cá nhân, tin nhắn, hình ảnh, màn hình, cho phép ứng dụng điều khiển từ xa điện thoại di động của chị Châu. Lúc 14h56 ngày 03/6/2023, đối tượng thông qua ứng dụng trên truy cập trái phép vào điện thoại có kết nối mạng internet của chị Châu. Sau đó truy cập vào ứng dụng VPBank trên điện thoại của chị Châu, thực hiện giao dịch chuyển khoản số tiền 174.850.000 đồng trong tài khoản VPBank số 0563017777 của chị Châu đến tài khoản Ngân hàng TMCP Tiên Phong (TPBank) số 00002506304 - Nguyen Duy Duc, chiếm đoạt của chị Châu số tiền trên. Lúc 02h54 ngày 09/6/2023, đối tượng tiếp tục truy cập trái phép vào tài khoản internetbanking BIDV số 58010000404770 của chị Châu chuyển khoản số tiền 43.300.000 đồng cũng đến tài khoản Ngân hàng TPBank số 00002506304 - Nguyen Duy Duc. Đối tượng chiếm đoạt tổng cộng 218.150.000 đồng *(Hai trăm mười tám triệu một trăm năm mười nghìn đồng)* trong 02 tài khoản ngân hàng của chị Châu.

Vụ 2: Lúc 08h38 ngày 05/3/2024, có người nói giọng nam miền Bắc, sử dụng số điện thoại 0859190402, tự xưng nhân viên cục thuế, gọi điện yêu cầu gọi điện

cho anh Lê Trần Sang (Sinh năm: 1996; Trú: P. Đống Đa, TP. Quy Nhơn) tải, cài đặt ứng dụng "Chính phủ" trên điện thoại di động của anh Sang để kê khai thuế kinh doanh. Anh Sang mới đăng ký doanh nghiệp vào ngày 04/3/2024 (thông tin công ty, số điện thoại, địa chỉ của anh Sang được công khai trên các trang web doanh nghiệp). Anh Sang tưởng thật nên đã thực hiện theo yêu cầu của đối tượng. Đối tượng hướng dẫn anh Sang truy cập vào trang web "vitegov.com" để tải ứng dụng có tên "Chính phủ". Khi cài đặt ứng dụng, anh Sang không đọc kỹ mà nhấn "Next" liên tục, vô tình đã cấp quyền cho ứng dụng này truy cập vào dữ cá nhân, tin nhắn, hình ảnh, điều khiển từ xa điện thoại di động của anh Sang. Sau khi cài ứng dụng này, anh Sang phát hiện điện thoại của anh Sang rất nóng, các ứng dụng tài khoản ngân hàng trên điện thoại của anh Sang đều bị xóa. Ngay sau đó, anh Sang gọi cho ngân hàng thì phát hiện có người đã truy cập trái phép vào tài khoản Sacombank của anh Sang chuyển khoản 3.000.000 đồng đến tài khoản EximBank số 0907037684 - Pham Thi Thuy Huynh lúc 08h56 ngày 05/3/2024, truy cập vào tài khoản Techcombank của anh Sang chuyển khoản 244.000.000 đồng cùng đến tài khoản Agribank 5700205893671 - Tran Vinh Thanh lúc 10h16 ngày 05/3/2024. Anh Sang bị chiếm đoạt tổng cộng 247.000.000 đồng trong 02 tài khoản ngân hàng.

2. Thủ đoạn lừa đảo đầu tư các sàn chứng khoán, tiền ảo, đa cấp... sau đó khóa, đánh cháy tài khoản hoặc đánh sập sàn

Vụ 1: Vào ngày 05/9/2023, bà Lê Hồng Ngọc (Sinh năm: 1972; Nơi cư trú: phường Đống Đa, TP. Quy Nhơn, tỉnh Bình Định) đọc được một quảng cáo trên Facebook với nội dung "Câu lạc bộ kết nối bí mật" nên nhắn tin tìm hiểu thì được tài khoản facebook tên "Thảo Wendy" (chưa rõ lai lịch người sử dụng) nhắn tin tư vấn. Đến ngày 17/9/2023, tài khoản facebook "Thảo Wendy" thêm bà Ngọc vào nhóm Telegram "Phòng Quay Thưởng" để tham gia chương trình quay thưởng nhận tiền của "Câu lạc bộ kết nối bí mật" nêu trên. Bà Ngọc đọc tin nhắn trong nhóm telegram trên thấy nhiều người tham gia đặt lệnh "Trên - Dưới", "Lớn - Nhỏ" (có kết quả ngay sau đó) trên trang web "g.tl510.cn" theo hướng dẫn của thầy trên nhóm đều thắng được tiền, nhiều người gửi ảnh chụp màn hình đã nhận được số tiền lớn do thắng lệnh, bà Ngọc thấy ham nên đồng ý tham gia theo lời mời của các đối tượng trong nhóm. Bà Ngọc được các tài khoản telegram tên "Quốc Huy" (@huynguyen_ceo), "Trợ lý _ Thanh Vân" (@TL_ThanhVan), "CSKH - Online" (@CSKHONLINE_247) (chưa rõ lai lịch người sử dụng) nhắn tin, hướng dẫn cách thức tạo tài khoản, đặt lệnh, nạp, rút tiền trên trang web "g.tl510.cn". Chiều 17/9/2023, bà Ngọc sử dụng tài khoản Techcombank số 19020877160019 chuyển khoản số tiền 99.000 đồng và 1.000.000 đồng đến tài khoản Vietcombank số 1030723536 - Nguyen Huu Cong để nạp tiền, đặt lệnh trên trang "g.tl510.cn" theo hướng dẫn của đối tượng. Bà Ngọc dễ dàng thắng lệnh, nhanh chóng được đối tượng chuyển khoản lại số tiền 150.000 đồng và 1.297.000 đồng. Sau đó, đối tượng yêu cầu bà Ngọc nạp số tiền lớn hơn, đặt lệnh lớn hơn để thu được nhiều lợi nhuận hơn. Bà Ngọc tin tưởng nên trong ngày 17/9/2023, bà Ngọc tiếp tục sử dụng tài khoản Techcombank số 19020877160019 chuyển khoản nhiều lần với tổng số tiền số tiền 260.165.000 đồng đến tài khoản Vietcombank số 1030723536 - Nguyen Huu Cong

và ACB số 36172487 - Hoang Van Lich, do đối tượng cung cấp để nạp tiền đặt lệnh, đóng phí rút tiền thắng lệnh. Đối tượng yêu cầu bà Ngọc chuyển khoản số tiền ngày càng lớn, đóng hết phí này đến phí khác nhưng vẫn không cho phép bà Ngọc rút tiền, bà Ngọc nghi ngờ bị lừa nên nhắn tin hỏi những người trong nhóm telegram "Phòng Quay Thưởng" thì được những người này trấn an rằng họ cũng chuyển khoản đóng phí như bà Ngọc và đều đã nhận được tiền nên bà Ngọc tin tưởng, tiếp tục chuyển khoản cho đối tượng. Sáng 18/9/2023, bà Ngọc sử dụng tài khoản SHB số 0109831332 chuyển khoản thêm 283.322.000 đồng đến tài khoản Vietinbank số 108878757665 - Nguyen Thi My Y theo yêu cầu của đối tượng để đóng thuế thu nhập cá nhân rồi đối tượng sẽ cho phép bà Ngọc rút tiền. Tuy nhiên, sau khi chuyển khoản, bà Ngọc vẫn không thể rút được số tiền hơn 1,2 tỷ đồng hiển thị trong tài khoản của bà Ngọc trên trang web "g.tl510.cn". Đối tượng yêu cầu bà Ngọc chuyển thêm 369 triệu đồng, bà Ngọc nghi ngờ bị lừa nên không đồng ý. Chiều 20/9/2023, bà Ngọc đến Công an thành phố Quy Nhơn trình báo bị chiếm đoạt số tiền 543.487.000 đồng đã chuyển khoản cho đối tượng.

Vụ 2: Vào ngày 22/11/2023, có người (không rõ lai lịch) nói giọng nữ miền Nam, xưng tên Thanh Trúc dùng số điện thoại 0917066666 gọi đến số điện thoại 0935002700 của anh Hồ Minh Vương, giới thiệu với anh Vương về lớp học đầu tư chứng khoán trên Zalo hoàn toàn miễn phí. Anh Vương đang có nhu cầu đầu tư chứng khoán nên đồng ý tham gia. Ngay sau đó, tài khoản zalo tên Nguyễn Thanh Trúc (zalo.me/84566960323) kết bạn với tài khoản tên "Vuong Ho" của anh Vương, thêm anh Vương vào nhóm Zalo tên "ADVANTAGE A1136 ĐIỄN ĐÀN TTCK". Sau một thời gian đọc tin nhắn trên nhóm zalo trên, anh Vương thấy có nhiều người tham gia đầu tư bằng cách đặt lệnh "tăng - giảm" để mua cổ phiếu trên ứng dụng có tên "ADVANTAGE" (APCK) có kết quả ngay sau đó, thắng được tiền ngay sau đó, nhiều người rút được số tiền lớn, gửi lên nhóm ảnh chụp màn hình nhận được tiền. Anh Vương thấy ham nên vào ngày 05/01/2024, anh Vương đã tham gia đầu tư theo lời mời của các đối tượng trên nhóm zalo trên. Tài khoản zalo Nguyễn Thanh Trúc hướng dẫn cho anh Vương cách tải ứng dụng, nạp tiền, đặt lệnh trên ứng dụng. Từ ngày 05/01/2024 đến ngày 10/01/2024, anh Vương đã sử dụng tài khoản PVCombank số 107000234295 của anh Vương chuyển khoản nhiều lần với tổng số tiền 495.000.000 đồng đến tài khoản Ngân hàng TMCP Kỹ Thương Việt Nam số 19039928978014 đứng tên Công ty TNHH Quản lý Đầu tư ADVANTAGE để nạp tiền đặt lệnh, cụ thể: chuyển 35.000.000 đồng lúc 14h01 ngày 05/01/2024, chuyển 100.000.000 đồng lúc 14h16 ngày 08/01/2024, chuyển 120.000.000 đồng lúc 11h09 ngày 09/01/2024 và chuyển 240.000.000 đồng lúc 09h58 ngày 10/01/2024. Anh Vương đặt lệnh theo hướng dẫn của tài khoản zalo tên "Chuyên gia Hoàng Minh Quân" (không rõ số điện thoại đăng ký) trên nhóm "ADVANTAGE A1136 ĐIỄN ĐÀN TTCK". Anh Vương nhanh chóng thắng được số tiền 1.200.649.075 đồng *(Một tỷ hai trăm triệu sáu trăm chín mươi bốn nghìn không trăm bảy mươi lăm đồng)*, tiền đã hiển thị trên tài khoản của anh Vương trên ứng dụng ADVANTAGE. Tuy nhiên, anh Vương không thể nào rút số tiền trên về, các đối tượng yêu cầu anh Vương muốn rút tiền phải chờ công ty duyệt lệnh, phải đóng phí. Hiện anh Vương không đăng nhập được vào lại ứng dụng "ADVANTAGE", nhóm zalo trên đã bị

xóa, anh Vương nghi ngờ bị lừa nên anh Vương đến Công an thành phố Quy Nhơn trình báo sự việc.

3. Thủ đoạn chiếm đoạt tài khoản mạng xã hội sau đó giả mạo người thân, quen nhắn tin, gọi điện vay tiền

Lúc 08h16 ngày 13/3/2024, có người nói giọng nam miền Nam dùng số điện thoại 0948191044 gọi đến số điện thoại 0913662236 của bà Trần Thị Thanh Thảo. Người này mạo danh ông Lê Minh Châu, Viện phó Viện kiểm sát nhân dân tỉnh Ninh Thuận, bạn của bà Thảo, đã lâu không liên lạc. Đối tượng nói rằng ngày 14/3/2024 sẽ ra Bình Định có công việc nên gọi trước cho bà Thảo. Bà Thảo dặn đối tượng ghé nhà bà Thảo chơi và bảo đối tượng đến khách sạn của người quen bà Thảo tại đường Chương Dương ở. Lúc khoảng 09h30 ngày 14/3/2024, người này gọi lại cho bà Thảo, nói với bà Thảo là đang trên xe khách ra Bình Định, nhờ bà Thảo chuyển khoản giúp số tiền 6.000.000 đồng đến tài khoản Sacombank số 060285431681 - Le Lam Viet do đang trên xe không có mạng internet. Bà Thảo tưởng thật nên bà Thảo dùng tài khoản BIDV số 58000347468 của bà Thảo chuyển khoản số tiền 6.000.000 đồng đến tài khoản trên theo yêu cầu của đối tượng. Sau đó, đối tượng gọi lại cho bà Thảo, nhờ chuyển thêm 20.000.000 đồng đến tài khoản trên. Bà Thảo tin tưởng, tiếp tục dùng tài khoản BIDV trên chuyển 20.000.000 đồng đến tài khoản trên cho đối tượng. Chiều ngày 14/3/2024, bà Thảo gọi lại đến số điện thoại 0948191044 thì không liên lạc được. Bà Thảo gọi lại số điện thoại của ông Châu mà bà Thảo đã lưu trước đây thì phát hiện bị lừa. Đối tượng trên đã mạo danh ông Châu, lừa bà Thảo chuyển khoản 26.000.000 đồng, chiếm đoạt của bà Thảo số tiền trên. Chiều 14/3/2024, bà Thảo đến Công an thành phố Quy Nhơn trình báo bị chiếm đoạt số tiền trên.

4. Thủ đoạn giả danh cơ quan công quyền (công an, viện kiểm sát, tòa án, hải quan..), văn phòng luật sư, ngân hàng... gọi điện đe dọa yêu cầu chuyển tiền hoặc hỗ trợ lấy lại tiền đã bị lừa đảo

Vụ 1: Lúc 08h30 ngày 02/8/2023, 03 đối tượng (gồm 1 nữ và 2 nam đều nói giọng miền Bắc, chưa rõ lai lịch), sử dụng số điện thoại "0916.381.321", tài khoản Zalo tên "Vũ Xuân Đăng" (không rõ số điện thoại đăng ký) gọi điện, nhắn tin cho bà Nguyễn Thị Vinh (Sinh năm: 1964; Nơi cư trú: phường Lý Thường Kiệt, TP. Quy Nhơn, tỉnh Bình Định). Các đối tượng trên giả danh nhân viên công ty viễn thông, cán bộ công an thông báo bà Vinh có liên quan đến vụ án mua bán ma túy, rửa tiền, đã có lệnh bắt tạm giam bà Vinh. Các đối tượng yêu cầu bà Vinh muốn chứng minh vô tội, bị oan, để không bị bắt giam thì phải cung cấp thông tin đăng nhập tài khoản LPBank số 0979178187 của bà Vinh để chúng phong tỏa, phục vụ điều tra, làm tin không bắt giam bà Vinh. Bà Vinh tưởng thật nên đã làm theo yêu cầu của đối tượng. Lúc 10h10 ngày 02/8/2023, đối tượng đã truy cập trái phép vào tài khoản LPBank số 0979178187 của bà Vinh, chuyển khoản số tiền 69.999.000 đồng trong tài khoản này đến tài khoản Vietcombank số 0051000147914 - Le Van The, chiếm đoạt của bà Vinh toàn bộ số tiền trên.

Vụ 2: Vào ngày 27/3/2024, bà Trần Thúy Hằng (Sinh năm: 1972; Trú: Phường Trần Quang Diệu, thành phố Quy Nhơn) nhận được một cuộc gọi từ số điện thoại 0565145218. Đầu dây bên kia có giọng nói giống như giọng của tổng đài

tự động, nội dung "Bộ thông tin truyền thông thông báo số thuê bao của Quý khác sẽ bị khóa 2 chiều trong vòng 02 giờ nữa, để biết thêm chi tiết, vui lòng bấm phím 0". Khi bà Hằng bấm phím 0 thì có một người xưng là cán bộ bộ Thông tin truyền thông, hỏi bà Hằng liên hệ tổng đài có việc gì, bà Hằng trình bày rằng bà Hằng mới được thông báo số thuê bao của bà Hằng sắp bị khóa, không rõ lý do. Đối tượng trên yêu cầu bà Hằng cung cấp họ tên, năm sinh, số CCCD, địa chỉ để tra cứu thông tin. Bà Hằng không nghi ngờ gì, thản nhiên cung cấp các thông tin cá nhân của chị cho đối tượng.

Đối tượng thông báo rằng vào tháng 01/2024, bà Hằng có dùng CCCD đăng ký 01 số điện thoại tại TP. Đà Nẵng, số điện thoại này thực hiện nhiều vụ lừa đảo chiếm đoạt tài sản, người dân phản ánh nên tất cả các số điện thoại đăng ký bằng thông tin của bà Hằng sẽ bị khóa. Bà Hằng trả lời rằng bà Hằng không đăng ký số điện thoại trên, trong khoảng thời gian trên, bà Hằng cũng không đến TP. Đà Nẵng, bà Hằng không liên quan gì hết các đối tượng lừa đảo. Lúc này, đối tượng nói rằng sẽ kết nối bà Hằng với Công an thành phố Đà Nẵng để bà Hằng "báo án, khi công an xác nhận thì tổng đài sẽ hủy bỏ việc khóa số điện thoại của bà Hằng". Bà Hằng tưởng thật nên đồng ý. Ngay sau đó, cuộc gọi được chuyển tiếp, bà Hằng gặp một người nói giọng nam miền Trung tự xưng Nguyễn Minh Hải - Điều tra viên, Công an thành phố Đà Nẵng. Đối tượng Hải nói rằng, thông tin cá nhân của bà Hằng đã được đưa vào hồ sơ vụ án, ngoài việc đăng ký số điện thoại lừa đảo trên, bà Hằng còn mở nhiều tài khoản ngân hàng rồi giao cho đồng bọn sử dụng để mua bán ma túy, rửa tiền. Các đồng phạm đã khai nhận bà Hằng, cơ quan công an đã có đủ chứng cứ để buộc tội bà Hằng, đã khởi tố bị can đối với bà Hằng, đã có lệnh bắt giam bà Hằng. Đối tượng mặc trang phục Cảnh sát gọi video cho bà Hằng, gửi cho bà Hằng ảnh chụp lệnh bắt bị can để tạm giam, quyết định phê chuẩn của Viện kiểm sát, bà Hằng thấy rằng thông tin trên lệnh bắt đều trùng khớp với thông tin của bà Hằng, các lệnh đều có dấu đỏ, đối tượng mặc trang phục công an nên bà Hằng hoảng hốt, tưởng rằng mình bị oan. Bà Hằng quên mất rằng, chính mình đã cung cấp thông tin cá nhân của chị cho đối tượng tự xưng nhân viên tổng đài. Các đối tượng thay phiên gọi điện, dọa bắt bà Hằng, yêu cầu bà Hằng cài đặt ứng dụng "lạ" có giao diện bộ công an trên điện thoại di động của bà Hằng để phục vụ điều tra. Sau đó, đối tượng nói rằng sẽ tạo điều kiện cho bà Hằng, không bắt giam bà Hằng, sẽ thay lệnh giam bằng lệnh phong tỏa tài khoản, yêu cầu bà Hằng phải kê khai tài sản, phải chuyển hết tài sản vào một tài khoản ngân hàng đứng tên của bà Hằng để cơ quan công an phong tỏa, thì sẽ không bắt giam bà Hằng, để làm tin, đảm bảo bà Hằng không bỏ trốn.

Bà Hằng nói rằng có một sổ tiết kiệm 550.000.000 đồng, tiền vợ chồng bà Hằng giành dụm để dưỡng già. Đối tượng yêu cầu bà Hằng phải tất toán sổ tiết kiệm, chuyển toàn bộ tiền vào tài khoản ngân hàng đang được đăng nhập trên điện thoại của bà Hằng. Đối tượng căn dặn bà Hằng rằng nếu nhân viên ngân hàng có hỏi việc tất toán sổ tiết kiệm trước hạn thì trả lời rằng dùng tiền để mua nhà cho con. Bà Hằng thực hiện theo các yêu cầu của đối tượng để chứng minh mình bị oan, vô tội, bị đối tượng xâm nhập vào tài khoản ngân hàng bằng ứng dụng "lạ",

chiếm đoạt toàn bộ số tiền 550.000.000 đồng mà vợ chồng bà Hằng tích cóp cả đời.

5. Thủ đoạn giả mạo danh nghĩa cơ quan, tổ chức phát tán tin nhắn SMS Brandname chứa đường dẫn lừa đảo, nội dung yêu cầu cung cấp thông tin cá nhân hoặc tải ứng dụng độc hại.

Lúc khoảng 09h00 ngày 01/10/2022, đối tượng (chưa rõ lai lịch) gửi 01 tin nhắn tên "SCB" trùng với tin nhắn của Ngân hàng SCB đến số điện thoại "0399.991.989" của chị Nguyễn Trần Thanh Phương (Sinh năm: 1989; Nơi cư trú: phường Thị Nại, thành phố Quy Nhơn, tỉnh Bình Định), với nội dung "Tai khoan cua ban dang duoc dang nhap tren thiet bi khac, neu khong phai ban dang nhap vui long vao https://scb.com.vn-us.club de sua doi mat khau hoac thoat khoi thiet bi". Chị Phương đọc tin nhắn trên, tưởng rằng Ngân hàng SCB thông báo có người đã truy cập trái phép vào tài khoản SCB của chị nên chị Phương đã thực hiện theo hướng dẫn trong tin nhắn. Chị Phương truy cập nhập số điện thoại, mật khẩu, mã xác thực (OTP) của tài khoản SCB số 0600110665100001 đứng tên Lê Thị Lan Phương vào trang web https://scb.com.vn-us.club để đổi mật khẩu. Ngay khi chị Phương thực hiện, có người (chưa rõ lai lịch) đã sử dụng các thông tin mà chị Phương nhập vào trang web https://scb.com.vn-us.club, truy cập trái phép vào tài khoản SCB số 0600110665100001, chuyển khoản 99.999.999 đồng đến tài khoản Techcombank số 19038913599010 - Nguyen Van Huong, chiếm đoạt của chị Phương số tiền trên.

6. Thủ đoạn lừa đảo qua hình thức tuyển cộng tác viên cho các sàn thương mại điện tử, việc nhẹ lương cao

Vào ngày 18/10/2023, tài khoản facebook tên "Ngọc Yến" (facebook.com/ ngocyenyen.xinhxinh; 100077593488398) kết bạn, nhắn tin làm quen với ông Võ Thanh Quang (Sinh năm: 1969; Nơi ĐKHKTT: TX. Chơn Thành, tỉnh Bình Phước). Ông Quang và Yến thường xuyên nhắn tin, gọi điện nói chuyện với nhau qua tài khoản facebook tên "Ngọc Yến", tài khoản viber tên "Chi sáu gấu" (+84865234384) và số điện thoại 0865234384 của Yến. Yến nói giọng nữ miền Bắc, xưng tên là Ngọc Yến, 28 tuổi, quê ở tỉnh Bắc Ninh, đang làm kế toán tại TP. Hà Nội. Sáng 27/10/2023, Yến rủ ông Quang tham gia công việc chuyển khoản mua đơn hàng ảo để tăng tương tác cho các trang bán hàng trên Lazada, Yến đã làm công việc này được 03 năm, lợi nhuận ổn định. Yến hướng dẫn ông Quang nhắn tin với tài khoản Viber tên "Lazada CSKH" (+84973726513) để tham gia công việc mua đơn hàng ảo, hưởng hoa hồng khoảng 10% giá trị đơn hàng. Ông Quang tin tưởng nên đồng ý tham gia công việc chuyển khoản mua đơn hàng ảo cùng với Yến. Công việc cụ thể là chuyển khoản đến các tài khoản ngân hàng do tài khoản Viber tên "Lazada CSKH" cung cấp để giả vờ mua hàng nhưng không nhận hàng, số tiền chuyển khoản cùng hoa hồng sẽ được chuyển khoản lại cho ông Quang ngay sau đó.

Chiều ngày 27/10/2023, theo sự hướng dẫn của Yến và tài khoản viber "Lazada CSKH", ông Quang sử dụng tài khoản Sacombank số 9998889999 đứng tên Võ Thanh Quang chuyển khoản nhiều lần với tổng số tiền là 1.332.510.000 đồng và nhờ

Lê Thanh Hùng (Sinh năm: 1984; Nơi thường trú: PTX. Chơn Thành, tỉnh Bình Phước) sử dụng tài khoản ACB số 609848888 của Hùng chuyển khoản số tiền 800.000.000 đồng cùng đến tài khoản KienlongBank số 0587962869 - Le Duc Viet và 0588421305 - Luu Hai Duong do đối tượng cung cấp để mua đơn hàng ảo, đóng phí để được rút tiền. Tổng số tiền ông Quang chuyển cho đối tượng là 2.135.510.000 đồng, tuy nhiên, ông Quang chỉ được chuyển khoản lại 59.171.000 đồng.

Chiều 28/10/2023, ông Quang đến Công an thành phố Quy Nhơn trình báo bị chiếm đoạt 2.076.339.000 đồng *(Hai tỷ bảy mươi sáu triệu ba trăm ba mươi chín nghìn đồng).*

7. Thủ đoạn lừa đảo đầu tư các sàn chứng khoán, tiền ảo, đa cấp... sau đó khóa, đánh cháy tài khoản hoặc đánh sập sàn

Vào ngày 25/12/2023, anh Võ Văn Linh (Sinh năm: 1987; Trú: TP. Quy Nhơn, tỉnh Bình Định) nhân viên một ngân hàng tại phường Lý Thường Kiệt, TP. Quy Nhơn được một đối tượng nữ gọi điện mời tham gia lớp học chứng khoán trên zalo. Anh Linh đã kinh nghiệm trong việc đầu tư chứng khoán. Nghĩ rằng lừa đảo, lừa gà, vì hiếu kỳ nên anh Linh đã tham gia, xem thử các đối tượng lừa đảo như thế nào. Tuy nhiên, sau một thời gian dài đọc tin nhắn trên nhóm zalo, thấy nhiều người tham gia, nhiều người thu được số tiền cao, nhiều người gửi ảnh chụp lên nhóm thắng được tiền, anh Linh bắt đầu tin tưởng. Vào ngày 02/3/2024, anh Linh quyết định xuống tiền đầu tư, nghĩ rằng sẽ nhanh chóng nhận được tiền, thu được lợi nhuận như những người trên nhóm nên anh Linh đã mạnh dạn vay mượn tiền của nhiều người, bạn bè, khách hàng. Từ ngày 02/3/2024 đến ngày 05/3/2023, anh Linh đã chuyển khoản số tiền 495.000.000 đồng đến tài khoản Ngân hàng TMCP Kỹ Thương Việt Nam số 19039928978014 đứng tên Công ty TNHH Quản lý Đầu tư ADVANTAGE. Tuy nhiên, do không thu được lợi nhuận như cam kết nên ngày 10/3/2024, anh Linh đến Công an thành phố Quy Nhơn trình báo bị chiếm đoạt toàn bộ số tiền trên.

Trước đó, vào cuối tháng 01/2024 đến ngày 01/3/2024, chị Võ Thúy Hằng, 43 tuổi, trú phường Trần Quang Diệu, thành phố Quy Nhơn bị chiếm đoạt số tiền 1,6 tỷ đồng bằng thủ đoạn như trên.

8. Thủ đoạn giả danh công ty tài chính, ngân hàng để hỗ trợ cho vay, nâng hạn mức tín dụng... sau đó yêu cầu chuyển tiền để làm thủ tục

Vào ngày 01/11/2022, đối tượng (chưa rõ lai lịch) sử dụng số điện thoại "0979.750.846", tài khoản zalo tên "Tạ Văn Uyên" (số điện thoại 0862.826.050), "Lê Trọng Việt" (số điện thoại 0367.514.200) và "Vila Nguyễn" gọi điện, nhắn tin với chị Phạm Thị Thanh Thảo (Sinh năm: 1999; Nơi cư trú: phường Trần Quang Diệu, thành phố Quy Nhơn), đưa ra thông tin gian dối về việc chuyển tiền đóng các khoản phí sẽ được chuyển khoản tiền vay trên ứng dụng "Viet Credit". Chị Thảo tưởng thật nên trong ngày 01/11/2022, tại xã Phước Mỹ, thành phố Quy Nhơn, chị Thảo sử dụng tài khoản BIDV số 58110001558385 mang tên Phạm Thị Thanh Thảo chuyển khoản nhiều lần với tổng số tiền 320.000.000 đồng đến tài khoản BIDV số 17910000318200 - Thai Minh Khiem do đối tượng cung cấp. Tuy nhiên,

chị Thảo không nhận được tiền vay, không được hoàn lại số tiền đã chuyển nên đến sáng ngày 02/11/2022, chị Thảo đến Công an thành phố Quy Nhơn trình báo bị chiếm đoạt 320.000.000 đồng nêu trên. Sau khi chị Thảo chuyển khoản 320.000.000 đồng vào tài khoản BIDV số trên 17910000318200 - Thai Minh Khiem, số tiền này tiếp tục được chuyển đến tài khoản TPBank số 00000100862 và VIB số 027761774 cùng đứng tên Thái Minh Khiêm.

CATP QUY NHƠN

"4 KHÔNG" "2 PHẢI" ĐỂ PHÒNG CHỐNG LỪA ĐẢO

"4 KHÔNG"

KHÔNG SỢ:

KHÔNG HOẢNG SỢ khi nhận được điện thoại, tin nhắn người lạ gửi đến có **NỘI DUNG XẤU** liên quan đến cá nhân và người thân, thông báo liên quan đến vụ việc, vụ án

KHÔNG THAM:

Không tham lam những tài sản, món **QUÀ KHÔNG RÕ NGUỒN GỐC** được nhận dễ dàng, những lợi nhuận "**PHI THỰC TẾ**", không tốn sức lao động, những lời mời chào, dụ dỗ "**VIỆC NHẸ, LƯƠNG CAO**"

KHÔNG KẾT BẠN VỚI NGƯỜI LẠ:

Khi người lạ trên **MXH** kết bạn làm quen, mời tham gia các hội nhóm mà không rõ mục đích thì **KHÔNG KẾT BẠN**, bắt chuyện, tham gia; **KHÔNG CUNG CẤP** thông tin cá nhân cho người lạ

KHÔNG CHUYỂN KHOẢN:

Khi các cá nhân không quen biết yêu cầu cung cấp thông tin cá nhân hoặc yêu cầu chuyển tiền hay làm một số việc thì **TUYỆT ĐỐI KHÔNG LÀM THEO**

"2 PHẢI"

PHẢI THƯỜNG XUYÊN CẢNH GIÁC:

Chủ động **BẢO MẬT** thông tin cá nhân, nhất là các thông tin quan trọng, nhạy cảm như: Thông tin thẻ **CCCD**; thông tin tài khoản Ngân hàng, thông tin tài khoản mạng xã hội...

TỐ GIÁC NGAY VỚI CÔNG AN 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 các cá nhân phải **BÁO NGAY** cho cơ quan công an để được hướng dẫn xử lý

HOT LINE 0256.3546114
TRỰC BAN CATP QUY NHƠN

ZALO CATP QUY NHƠN

HOT LINE 0256 3847 660
CÔNG AN PHƯỜNG Nguyễn Văn Cừ