BỘ CÔNG AN

CỤC AN NINH MẠNG VÀ PHÒNG CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

CẨM NANG

DẤU HIỆU NHẬN BIẾT VÀ PHÒNG TRÁNH LỪA ĐẢO TRỰC TUYẾN

Hà Nội, 04/2024

MỤC LỤC

I. TÌNH HÌNH CHUNG

Những năm vừa qua, lừa đảo trực tuyến đã và đang trở thành vấn nạn trên toàn thế giới, trong đó có Việt Nam. Các đối tượng lợi dụng bối cảnh bùng nổ công nghệ thông tin để thực hiện nhiều vụ lừa dảo trực tuyến, chiếm doạt tài sản có giá trị cao, gây bức xúc trong dư luận và quần chúng nhân dân, ảnh hưởng nghiêm trọng đến trật tự an toàn xã hội.

Nạn lừa đảo xảy ra ở hầu hết các địa phương trên cả nước, chiếm tỷ lệ cao trong cơ cấu tội phạm hình sự, đa dạng về hình thức, phạm vi hoạt động xuyên quốc gia. Các đối tượng liên tục thay đổi phương thức, sử dụng nhiều thủ đoạn phạm tội mới; hoạt động tinh vi, chuyên nghiệp hơn; có sự móc nối, học tập kinh nghiệm của các băng nhóm tội phạm trên thế giới.

Cục An ninh mạng và PCTP sử dụng công nghệ cao – Bộ Công an đã phối hợp các cơ quan quản lý nhà nước tuyên truyền nhiều phương thức, thủ đoạn hoạt động của các đối tượng. Tuy nhiên vẫn có nhiều người dân nhận thức chưa đầy đủ hoặc chưa nhận thức được phương thức thủ đoạn phạm tội của các đối tượng, thiếu cảnh giác và ý thức tự bảo vệ bản thân khi hoạt dộng trên môi trường mạng nên đã trở thành nạn nhân của các vụ lừa dảo.

Qua công tác nắm tình hình, phòng ngừa, đấu tranh với tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, Cục An ninh mạng và PCTP sử dụng công nghệ cao – Bộ Công an an xác định các đối tượng lừa đảo sử dụng nhiều hình thức khác nhau, nhắm đến mọi khía cạnh đời sống xã hội của người dân, với mỗi phương thức, các đối tượng đều xây dựng nhiều kịch bản tiếp cận khác nhau. Đặc điểm của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng là:

- Hoạt động trên không gian mạng hoặc sử dụng các thiết bị, phần mềm công nghệ có tính ẩn danh cao để thực hiện hành vi phạm tội.

- Khai thác lỗ hổng bảo mật trên các thiết bị điện tử hoặc sơ hở của người dùng khi tham gia môi trường mạng.

- Đánh vào lòng tham, tâm lý hoang mang, thiếu nhận thức, cảnh giác của người dân khi tham gia mạng xã hội.

- Hoạt động có tổ chức, phân công nhiệm vụ cụ thể cho từng nhóm khác nhau. Xây dựng kịch bản cho nhân viên trước từng tình huống cụ thể.

- Lợi dụng những sở hở trong công tác quản lý nhà nước về cung cấp dịch vụ viễn thông, internet, ngân hàng… để thực hiện hành vi phạm tội nhằm trốn tránh sự phát hiện của cơ quan chức năng.

Để nâng cao nhận thức, ý thức cảnh giác cho người dân khi tham gia hoạt động trên môi trường mạng, Cục An ninh mạng và PCTP sử dụng công nghệ cao – Bộ Công an đã xác định 11 phương thức lừa đảo phổ biến hiện nay và ban hành Cẩm nang về dấu hiệu nhận biết và biện pháp phòng tránh lừa đảo trực tuyến.

II. CÁC HÌNH THỨC LỪA ĐẢO TRỰC TUYẾN

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

- ***Dấu hiệu:***

- 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 tiền đặt cọc hoặc trả tiền trước, sau đó chiếm đoạt số tiền trên.

- Đăng bài viết quảng cáo dịch vụ làm thị thực (visa) 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 đặt cọc hoặc thanh toán trước chi phí, các đối tượng yêu cầu 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.

- Giả mạo 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 tiền để thanh toán dịch vụ du lịch các đối tượng sẽ chiếm đoạt tiền và chặn liên lạc.

- 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 vé 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.

- ***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 mua sắm hàng hóa hoặc các gói dịch vụ trên mạng, nên lựa chọn mua hàng, dịch vụ đặt tour, đặt phòng, đặt vé máy bay... của những công ty uy tín. Để yên tâm hơn, người dân có thể đề nghị phía đối tác cho xem hóa đơn chứng từ, giấy phép hoạt động kinh doanh, giấy tờ, chứng chỉ hành nghề... của công ty lữ hành, du lịch; đề nghị thanh toán sau khi nhận và kiểm tra hàng đối với các giao dịch mua hàng trực tuyến.

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 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 (đã được xác thực) hoặc chọn các trang mạng xã hội uy tín mà mình biết rõ thông tin của người bán. Lưu lại thông tin

liên quan 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. Chiếm đoạt tài khoản mạng xã hội sau đó giả mạo người thân, quen nhắn tin, gọi điện yêu cầu chuyển 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 cho người thân, quen hỏi vay tiền hoặc nhờ chuyển khoản hộ.

- ***Dấu hiệu:***

- 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, cần thận hơn.

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

- ***Biện pháp phòng tránh:***

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

- 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.

- 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.

- Không click vào đường dẫn lạ do người thân, bạn bè gửi qua mạng xã hội; tìm cách liên lạc trực tiếp với người thân để kiểm tra thông tin.

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.

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 cơ quan 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:***

- Cuộc gọi đến 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.

- ***Biện pháp phòng tránh:***

- Cảnh giác khi nhận các cuộc gọi tự xưng là cán bộ cơ quan quản lý nhà nước, nhân viên ngân hàng, nhà mạng... đề nghị cung cấp thông tin cá nhân. Tuyệt đối không chia sẻ, cung cấp thông tin của bản thân cho người khác qua điện thoại hoặc mạng xã hội.

- Liên hệ trực tiếp đến Công an phường/xã nơi cư trú khi nhận được yêu cầu chỉnh sửa/ bổ sung thông tin cá nhân; Liên hệ đến số hotline của nhà mạng, ngân

hàng khi nhận được yêu cầu chuẩn hóa thông tin thuê bao hoặc tài khoản ngân hàng.

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.

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:***

- 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 dân 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.

- ***Biện pháp phòng tránh:***

- Tìm hiểu kỹ về các Công ty, Trung tâm trước khi đăng ký cho bản thân và người nhà tham gia các chương trình qua mạng xã hội. Chỉ chọn các Công ty, Trung tâm có uy tín, đã kiểm tra, xác thực chính xác thông tin (liên hệ hotline của các Công ty đăng tải trên trang web chính thống).

- Tuyệt đối không cung cấp thông tin cá nhân của bản thân và người thân cho các trang web, trang mạng xã hội khi chưa xác định chính xác mức độ uy tín để phòng tránh việc bị lừa đảo cũng như các mục đích xấu khác.

- Cảnh giác trước khi chuyển tiền phí tham dự chương trình, nếu có thể hãy đến trực tiếp văn phòng của Công ty/ Trung tâm để làm việc; không thực hiện các giao dịch chuyển tiền để làm nhiệm vụ online.

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 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:***

- 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 đảm bảo tài sản, sau đó các đối tượng sẽ chiếm đoạt số tiền này.

- Giả danh nhân viên ngân hàng quảng cáo dịch vụ mở thẻ tín dụng, nâng cấp hạn mức tín dụng tiêu dùng cho người dân. 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.

- ***Biện pháp phòng tránh:***

- Nên tìm hiểu kỹ và sử dụng dịch vụ của các cơ quan, doanh nghiệp uy tín trong lĩnh vực tài chính, ngân hàng.

- Cảnh giác khi thực hiện các giao dịch trong lĩnh vực tài chính, ngân hàng qua mạng. Liên hệ trực tiếp đến hotline trên trang chủ của các ngân hàng, công ty tài chính để kiểm tra thông tin.

- Không chuyển tiền đặt cọc, đảm bảo tài sản khi có nhu cầu vay tiền hoặc đăng ký dịch vụ tín dụng... qua mạng.

- Việc cài đặt ứng dụng qua mạng tiềm ẩn nhiều rủi ro liên quan đến lộ thông tin cá nhân, bị cài mã độc chiếm quyền điều khiển thiết bị điện tử.

6. Giả mạo danh nghĩa cơ quan, tổ chức phát tán tin nhắn SMS Brandname chứa đường dẫn truy cập vào các website giả mạo yêu cầu cung cấp thông tin cá nhân hoặc tải về 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 đang phát sóng 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. Ngoài ra, các đối tượng có thể sử dụng các phần mềm spam tin nhắn iMessage để phát tán tin nhắn giả mạo thương hiệu đến người dùng 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:***

- Nhận được tin nhắn mang tên các cơ quan, tổ chức doanh nghiệp chính thống (như: Bo Cong an, Bo Thong tin va 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 quyền 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.

- ***Biện pháp phòng tránh:***

- Kiểm tra kỹ nội dung khi nhận được tin nhắn từ các cơ quan, tổ chức, đặc biệt là các tin nhắn gây chú ý (trúng thưởng, cảnh báo, khuyến mãi…). Không click vào các đường dẫn có dấu hiệu đáng ngờ, kiểm tra kỹ tên miền trang web trước khi đăng nhập thông tin tài khoản.

- Tuyệt đối không chia sẻ thông tin cá nhân, tài khoản ngân hàng, mã OTP với bất kỳ ai.

- 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. Gọi điện thoại đến cơ quan, tổ chức liên quan để xác thực xem có phải trang web, ứng dụng là của họ hay không.

7. Lừa đảo tham gia đầu tư sàn chứng khoán ảo, 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:***

- 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.

- ***Biện pháp phòng tránh:***

- Cảnh giác khi tham gia đầu tư chứng khoán, đa cấp, tiền ảo... vào các sàn giao dịch trực tuyến trên mạng không rõ thông tin hoặc thông tin có dấu hiệu bị giả mạo. Tìm hiểu kỹ thông tin về sàn giao dịch trước khi đầu tư, đặc biệt là các sàn đầu tư đăng tải địa chỉ ảo, không có thật, hoặc giả mạo của sàn đầu tư chính thống.

- Nâng cao cảnh giác khi giao tiếp với người lạ trên mạng xã hội, tuyệt đối không chia sẻ thông tin cá nhân, làm theo hướng dẫn khi chưa xác định chính xác nhân thân, lai lịch của người đó.

- Chỉ đầu tư vào các sàn giao dịch chính thống đã được cơ quan quản lý nhà nước cấp phép hoạt động. Trước khi đầu tư, nên đến trực tiếp văn phòng của các sàn giao dịch để được tư vấn, hỗ trợ và kiểm chứng thông tin.

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 doanh 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 giả 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:***

- 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.

- ***Biện pháp phòng tránh:***

- Cẩn trọng khi tiếp xúc với người lạ trên mạng, đặc biệt là các tài khoản lạ, không có bạn chung, từ nước ngoài... Tuyệt đối không tin tưởng vào những "bạn bè" qua mạng khi chưa gặp mặt và nắm rõ thông tin cá nhân.

- Cần tìm hiểu kỹ về các hoạt động kiếm tiền online như: sàn thương mại điện tử, làm nhiệm vụ hưởng hoa hồng, đầu tư online...

- Cảnh giác khi được mời tham gia các hệ thống đầu tư online, công việc đơn giản nhưng có thu nhập "khủng".

- Kiểm tra kỹ thông tin khi có đề nghị nhận quà tặng từ người lạ. Cần xác minh thông tin qua đơn vị vận chuyển chính thống, không chuyển tiền trả các khoản phí trước khi nhận và kiểm tra hàng.

- Việc tìm kiếm bạn bè, kết bạn qua mạng xã hội tiềm ẩn nhiều nguy cơ rủi ro trở thành nạn nhân lừa đảo hoặc bị xâm hại bởi các hành vi khác. Vì vậy cần tìm hiểu thật kỹ thông tin, gặp mặt trực tiếp và xác định chính xác danh tính trước khi đi đến một mối quan hệ với bạn quen qua mạng xã hội.

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 mại 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 trang thương mại điện tử giả mạo, lấy danh nghĩa các doanh nghiệp uy tín tuyển cộng tác viên làm việc 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:***

- 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, click 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 đầu 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.

- ***Biện pháp phòng tránh:***

- Cẩn trọng khi tìm kiếm việc làm thông qua mạng xã hội. Khi có nhu cầu tìm việc làm online, cần tìm hiểu kỹ về các đơn vị tuyển dụng, đặc biệt là các thông tin tuyển dụng việc nhẹ lương cao, cộng tác viên đánh giá sản phẩm trên các sàn thương mại điện tử, công việc yêu cầu ứng tiền trước để làm nhiệm vụ...

- Cảnh giác khi nhận được lời mời tham gia làm cộng tác viên online từ các tài khoản hoặc bạn bè ảo trên mạng xã hội. Các tài khoản này thường không có danh tính rõ ràng hoặc giả mạo, khi đề nghị gặp mặt trực tiếp sẽ tìm nhiều cách lẩn tránh.

- Tuyệt đối không chuyển tiền trước để thực hiện các nhiệm vụ, công việc tìm kiếm qua mạng khi chưa xác thực chính xác danh tính của công ty chủ quản. Liên hệ đến công ty chính thống để xác thực thông tin trước khi tham gia làm cộng tác viên.

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 dọa 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 mang, lo sợ của người dân khi bị cơ quan chức năng thông báo liên quan đến hành vi vi 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:***

- 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, 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 nạn nhân đồng ý, chúng sẽ yêu cầu chuyển trước khoản phí dịch vụ và chiếm đoạt số tiền này.

- ***Biện pháp phòng tránh:***

- Cảnh giác khi nhận được cuộc gọi tự xưng là cán bộ cơ quan công quyền, liên hệ cơ quan chức năng nơi gần nhất hoặc số điện thoại của cơ quan công quyền đăng tải trên các trang chính thống để xác thực thông tin trước khi làm theo yêu cầu của người kết nối. Lưu ý: cơ quan chức năng không làm việc qua điện thoại, chỉ làm việc tại trụ sở cơ quan.

- Không cung cấp thông tin cá nhân cho bất kỳ ai thông qua điện thoại khi chưa xác thực chính xác danh tính của người liên hệ với mình.

- Không tin vào các lời quảng cáo hỗ trợ lấy lại tiền đã bị lừa đảo. Cơ quan chức năng cần xác minh làm rõ vụ việc, làm việc trực tiếp với nạn nhân, không hỗ trợ lấy lại tiền qua mạng.

- Luôn luôn giữ tâm lý bình tĩnh khi nhận được cuộc gọi thông báo liên quan đến hành vi vi phạm pháp luật hoặc sau khi bị lừa đảo chiếm đoạt tài sản. Trình báo đến cơ quan Công an nơi sinh sống, làm việc để được hướng dẫn cụ thể, không làm theo đề nghị của các cá nhân, tổ chức khi chưa xác thực danh tính.

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

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, gọi video nhạy cảm nhằm tống tiền nạn nhân...

- ***Dấu hiệu:***

- 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.

- Các đối tượng chủ động nhắn tin làm quen qua mạng xã hội hoặc các ứng dụng kết bạn, gạ gẫm gọi điện video với các hình ảnh nhạy cảm, kích dục sau đó lưu lại video và tống tiền nạn nhân.

- ***Biện pháp phòng tránh:***

- Cẩn trọng khi tìm kiếm dịch vụ trên không gian mạng, đặc biệt là các giao dịch yêu cầu chuyển tiền đặt cọc hoặc phí dịch vụ trước khi thực hiện.

- Không chuyển lại tiền theo đề nghị của các cá nhân qua điện thoại. Nếu nhận được tiền chuyển nhầm hay trình báo cơ quan Công an nơi gần nhất hoặc liên hệ thông báo với ngân hàng chủ quản. Trường hợp có người lạ liên hệ xin lại tiền chuyển nhầm, hãy yêu cầu đến cơ quan Công an nơi gần nhất hoặc trụ sở ngân hàng làm việc trực tiếp thông qua nhân viên ngân hàng.

- Luôn luôn đề phòng khi kết bạn với người lạ qua mạng xã hội, không để lộ thông tin cá nhân, hình ảnh nhạy cảm khi hoạt động trên mạng xã hội.

III. NGƯỜI DÂN CẦN LÀM GÌ SAU KHI BỊ LỪA ĐẢO TRỰC TUYẾN

- Khi nghi ngờ bản thân có biểu hiện đang bị lừa đảo qua mạng, hãy tìm kiếm thông tin về các hình thức lừa đảo trên mạng internet hoặc xin sự tư vấn từ bạn bè, người thân. Đừng ngại ngùng chia sẻ câu chuyện mình đang gặp phải, người bên ngoài sẽ luôn có tâm lý bình tĩnh, tỉnh táo hơn.

- Trình báo ngay sự việc đến cơ quan Công an nơi gần nhất để nhận được tư vấn và hỗ trợ kịp thời.

- Liên hệ với Ngân hàng chủ quản để báo cáo sự việc và đề nghị hỗ trợ.

- Lưu lại tất cả thông tin như lịch sử trò chuyện, các số điện thoại, tài khoản mạng xã hội liên quan, sao kê giao dịch ngân hàng và cung cấp cho cơ quan Công an khi trình báo.

- Cài đặt lại mật khẩu các tài khoản cá nhân trong trường hợp bị đánh cắp thông tin cá nhân hoặc bị tấn công chiếm quyền điều khiển thiết bị điện tử.

- Cảnh báo cho bạn bè, người thân về hình thức lừa đảo mình đã hoặc đang gặp phải nhằm chủ động phòng ngừa.