MỘT SỐ PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM SỬ DỤNG TRÊN KHÔNG GIAN MẠNG NHẰM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN - DẤU HIỆU NHẬN BIẾT VÀ BIỆN PHÁP PHÒNG NGỪA

I. MỘT SỐ TÌNH HÌNH CHUNG VỀ TỘI PHẠM TRÊN KHÔNG GIAN MẠNG

Thời gian qua, tình hình tội phạm lợi dụng không gian mạng để thực hiện hành vi lừa đảo chiếm đoạt tài sản tiếp tục diễn biến phức tạp, số lượng các vụ án lừa đảo chiếm đoạt tài sản liên quan đến không gian mạng chưa có chiều hướng giảm. Các đối tượng lừa đảo giả danh cơ quan Công an, Viện kiểm sát và các cơ quan, ban ngành ... gọi điện thoại hướng dẫn người dân cài đặt, kích hoạt tài khoản điện thoại di động qua ứng dụng VneID, sau khi người dân cài đặt ứng dụng, đối tượng sẽ yêu cầu cung cấp tất cả các quyền truy cập danh bạ, vị trí, trợ năng trên điện thoại rồi thực hiện lệnh chuyển tiền và thực hiện hành vi chiếm đoạt tài sản, ngoài ra còn một số hành vi như "giả danh Công an điện thoại hướng dẫn sửa lỗi ứng dụng VneID", "cập nhật dữ liệu bị sai trên VneID" nhằm chiếm đoạt tài sản.

Thời gian gần đây, trong lĩnh vực tài chính, ngân hàng sau khi Ngân hàng Nhà nước Việt Nam ban hành Quyết định triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng, các đối tượng phạm tội sử dụng không gian mạng lừa đảo chiếm đoạt tài sản liên tục thay đổi về phương thức, thủ đoạn nhưng đều có điểm chung là sử dụng tài khoản ngân hàng không chính chủ để nhận, chuyển tiền vi phạm pháp luật, các đối tượng đã thay đổi phương thức hoạt động như: "*tuyển mộ người mở tài khoản, "nuôi nhốt", ăn ở tại chổ để xác thực tài khoản; dụ dỗ, lôi kéo trẻ vị thành niên từ đủ 14 tuổi, đang là học sinh, sinh viên mở tài khoản ngân hàng, yêu cầu chụp ảnh, quay phim khuôn mặt để thu thập dữ liệu sinh trắc học phục vụ xác thực khi cần thiết; sử dụng công nghệ trí tuệ nhân tạo AI (Deepfake) để vượt qua hàng rào bảo mật của ứng dụng eKYC ngân hàng, lập doanh nghiệp "Ma" để đăng ký mở tài khoản ngân hàng phục vụ hoạt động vi phạm pháp luật; dụ dỗ, lôi kéo đưa người ra nước ngoài để hoạt động lừa đảo, sử dụng tài khoản chính chủ đế nhận tiền, mua "tiền ảo " Bitcoin nhằm mục đích dịch chuyển dòng tiền đã chiếm đoạt.*

Ngoài ra, các đối tượng người nước ngoài còn cấu kết với một số đối tượng trong nước để thuê người lắp đặt tổng đài viễn thông đa SIM thông qua giải pháp thay đổi SIM từ xa. Hoạt động cài đặt hệ thống, nạp tiền vào SIM, điều hướng, thực hiện cuộc gọi lừa đảo từ xa thông qua môi trường Internet, toàn bộ các trao đổi, chỉ đạo giữa các đối tượng đều thông qua ứng dụng Telegram, có thể nhanh chóng xóa dữ liệu, tài liệu khi bị phát hiện. Đáng chú ý, khi triển khai biện pháp kiểm tra nghiệp vụ rà quét đối với các SIM thuê bao phát sinh cuộc gọi lừa đảo, cơ quan chức năng chỉ

xác định được khu vực lắp đặt thiết bị VoIP GSM Gateways, không phát hiện ra vị trí lắp đặt hệ thống SIMPool cũng như vị trí các đối tượng thực hiện cuộc gọi lừa đảo. Hoạt động này tiềm ẩn nguy cơ bị các thế lực thù địch lợi dụng, thực hiện hoạt động chống phá, xâm phạm an ninh quốc gia. Các tổ chức phản động lưu vong, số đối tượng chống đối trong và ngoài nước có thể lợi dụng hệ thống đa SIM tán phát tin nhắn, tuyên truyền chống Đảng, Nhà nước ... gây mất ổn định chính trị.

Trên địa bàn tỉnh Bình Dương, trong thời gian qua tình hình tội phạm lừa đảo sử dụng công nghệ cao diễn ra khá phức tạp với nhiều hình thức, một trong các phương thức, thủ đoạn nổi lên gần đây là: các đối tượng chiếm tài khoản mạng xã hội của người dùng, lợi dụng uy tín của người dùng gửi tin nhắn đến người thân, bạn bè để dụ dỗ tham gia trò chơi có thưởng, hướng dẫn làm nhiệm vụ cộng tác viên đơn hàng, đầu tư tiền ảo với hoa hồng và lợi nhuận cao... nhằm lừa đảo, chiếm đoạt tài sản. Do là tin nhắn từ tài khoản của bạn bè, người thân nên nạn nhân rất dễ mất cảnh giác và mắc bẫy các đối tượng.

Điển hình, thời gian gần đây Công an tỉnh Bình Dương tiếp nhận nhiều đơn trình báo của người dân, tố cáo bị các đối tượng sử dụng số điện thoại hoặc tài khoản mạng xã hội giả mạo các cơ quan, tổ chức liên hệ với các cơ sở kinh doanh để đặt hàng, sau đó nhờ mua các loại hàng hóa khác để chiếm đoạt tài sản.

II. MỘT SỐ PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

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

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

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.

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.

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

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 về ứng dụng độc hại.

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

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

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

10. Giả danh cơ quan công quyền (Công an, Viện kiểm sát, Tòa án, Hải quan...). Giả danh văn phòng luật sư, ngân hàng... gọi điện đe dọa yêu cầu chuyển tiền hoặc lấy lại tiền đã bị lừa đảo.

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

III. NHẬN BIẾT MỘT SỐ PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

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.

**** Dấu hiệu chủ yếu:***

- 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 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 đo khác nhau để không trả lại tiền.

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

- 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 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.

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 đào 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 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 đấu 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 đề 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 bị ảnh hường 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 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 chủ yếu:

- 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 địch 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 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 cùa 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 tỉn 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 chuyên tiền hoàn thành nhiệm vụ.

5. Giả danh công ty tài chính, ngân hàng để hỗ trợ cho vay, nâng 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 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 nhiêu trang mạng xã hội quảng cáo dịch yụ 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 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 bào 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 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 chủ yếu:

- 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.

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 về 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 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 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 mại điện từ 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 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, clip 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.

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 giúp 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 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, Kiểm sát, Luật sư...). Các đối tượng thường tạo các trang mạng xã hội đăng nhiều thông tin cảnh báo lừa đảo, thêm người khác 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.

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.

III. BIỆN PHÁP PHÒNG NGỪA TỘI PHẠM LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

Để phòng ngừa, đấu tranh với các loại tội phạm nói chung và tội phạm lừa đảo trên không gian mạng nói riêng, mọi người dân cần nâng cao cảnh giác, chủ động phòng ngừa, đấu tranh với các loại tội phạm, trong đó phòng ngừa là chính, thực hiện phương châm "Tự quản, tự phòng, tự bảo vệ". Ngoài ra mỗi người cần nhận biết những dấu hiệu, phương thức, thủ đoạn của tội phạm để cùng tham gia tuyên truyền cho gia đình, người thân, bạn bè và mọi người biết để cùng tham gia phòng ngừa, đấu tranh, tố giác tội phạm góp phần đảm bảo và giữ gìn an ninh, trật tự.

Với những dấu hiệu nhận biết về tội phạm lừa đảo trên không gian mạng, mỗi người chúng ta tùy vào từng trường hợp cụ thể mà có cách xử lý phù hợp, trong đó cần chú ý:

**** Cảnh báo và khuyến cáo của cơ quan Công an:***

1. Khi nhận tin nhắn từ mạng xã hội, kể cả của bạn bè, người thân trong gia đình yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu chuyển mượn tiền hoặc thực hiện hành động khẩn cấp, ***hãy cảnh giác - lừa đảo.***

2. Nếu tin nhắn 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, ***hãy cảnh giác - lừa đảo.***

3. Kiểm tra đường Link được chia sẻ trong tin nhắn. Nếu đường link có chèn thêm 01 hoặc vài ký tự khác so với đường link gốc chính thống, hay đường link điều hướng đến các trang web không rõ nguồn gốc hoặc đáng ngờ, ***hãy cảnh giác - lừa đảo.***

4. Khi được hứa hẹn thực hiện công việc với mức hoa hồng rất cao, nhất là chuyển tiền sau đó nhận lại, ***hãy cảnh giác - lừa đảo.***

**** Biện pháp phòng tránh:***

1. Xác minh thông tin: Nếu bạn nhận được một tin nhắn hoặc email đáng ngờ từ một người bạn, dừng ngay việc sử dụng thông tin đáng ngờ được cung cấp qua email hoặc tài khoản mạng xã hội. 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.

2. 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.

3. Thay đổi mật khẩu ngay lập tức tài khoản mạng xã hội và sử dụng một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt.

4. Báo cáo sự cố thông qua mạng xã hội hoặc các liên hệ khác như điện thoại, email.

5. Thông báo cho bạn bè và người thân trong danh sách bạn bè của bạn về tình huống và đưa ra cảnh báo để mọi người cảnh giác.

6. Nếu đã lỡ bị lừa đảo thì dừng ngay việc chuyên tiền cho các đối tượng, thực hiện các biện pháp cần thiết, thông báo cho ngân hàng của mình để hạn chế thiệt hại, tố giác tội phạm cho Công an nơi gần nhất để được hướng dẫn, giải quyết.

IV. BIỆN PHÁP PHÒNG NGỪA MỘT SỐ TỘI PHẠM LỪA ĐẢO MỚI TRÊN KHÔNG GIAN MẠNG HIỆN NAY

*** Phòng ngừa lừa đảo qua cài đặt ứng dụng VneID:**

1. Tuyệt đối không nhập, cung cấp thông tin cá nhân hoặc cung cấp các quyền truy cập cho bất cứ người nào thông qua điện thoại. Khi sử dụng ứng dụng VneID, mỗi người dân nâng cao cảnh giác, khi thấy có bất cứ điều gì bất thường hoặc nhận cuộc gọi điện thoại tự xưng là Bộ công an, Viện kiểm sát, yêu cầu cung cấp thông tin cập nhật dữ liệu bị sai trên VneID, hướng dẫn sửa lỗi ứng dụng VneID thì chấm dứt cuộc gọi và báo ngay cơ quan Công an nơi gần nhất.

2. Tuyệt đối không chuyển tiền, đóng các loại phí như phí sửa lỗi thông tin, phí giải quyết sự cố, khi bị đối tượng yêu cầu.

3. Hiện tại định danh điện tử mức độ 2 làm tại Công an các phường và công an các huyện, thành phố trên địa bàn tỉnh Bình Dương.

Việc sử dụng ứng dụng định danh mức độ 2 trên App VneID mang lại nhiều thuận lợi cho công dân trong giải quyết nhu cầu hành chính của công dân như đăng ký thường trú, xác nhận thông tin cư trú, đăng ký tạm trú, khai báo lưu trú, sử dụng giấy tờ điện tử như sổ hộ khẩu, CCCD, Bảo hiểm y tế, giấy phép lái xe ... Do vậy mỗi công dân phải hiểu biết về ứng dụng App VneID, sử dụng và bảo mật thông tin cá nhân một cách thông minh tránh bị kẻ xấu lợi dụng gây hậu quả cho cá nhân và xã hội.

*** Phòng ngừa, cảnh giác với thủ đoạn quảng cáo dịch vụ "Lấy lại tiền bị lừa đảo", "Lấy lại tiền bị treo"…**

1. Cần trực tiếp đến các cơ quan Công an để trình báo hoặc gửi đơn, thư theo đường bưu chính về các vụ việc lừa đảo mà mình là nạn nhân để được tiếp nhận, giải quyết. Hiện nay, các đơn vị Công an và các cơ quan liên quan không phối hợp, ủy quyền cho bất cứ đơn vị nào để hướng dẫn, nhận hồ sơ của người dân về các vụ việc lừa đảo chiếm đoạt tài sản qua các trang mạng xã hội, cũng như không có đơn vị, cơ quan Công an nào đăng tin, chạy quảng cáo qua các trang mạng xã hội về nội dung công việc của tổ chức, đơn vị mình.

2. Tuyệt đối không nghe theo, không liên hệ với các website, Fanpage, tài khoản mạng xã hội quảng cáo dịch vụ "Tiếp nhận hồ sơ", "Hỗ trợ lấy lại tiền bị treo", "Thu hồi tiền lừa đảo"... trên không gian mạng.

3. Cần cảnh giác đối với các trang mạng xã hội mạo danh cá nhân, tổ chức hành nghề luật sư, cơ quan chức năng; mọi giao dịch chuyển tiền cần xác thực đầy đủ thông tin để tránh bị lừa đảo. Khi phát hiện các vụ việc nghi ngờ có dấu hiệu tội phạm, hãy liên hệ ngay với Công an nơi gần nhất để được hướng dẫn, xử lý kịp thời.

*** Phòng ngừa, cảnh giác với thủ đoạn tạo lập các trang fanpage giả mạo các giải chạy "Marathon kid 2024"**

1. Kiểm tra kỹ các thông tin quảng cáo của các Fanpage trên mạng xã hội. Liên hệ trực tiếp với các đơn vị tổ chức, yêu cầu đơn vị tổ chức cung cấp giấy tờ tài liệu chứng minh.

2. Không tham gia các hội, nhóm Zalo, Telegram để thực hiện nhiệm vụ, không chuyển tiền cho đối tượng.

3. Khi nghi ngờ các hoạt động lừa đảo chiếm đoạt tài sản, đề nghị người dân đến cơ quan Công an nơi gần nhất để được tư vấn, hướng dẫn.

*** Phòng ngừa, cảnh giác với thủ đoạn giả danh cán bộ cơ quan nhà nước (Công an, Thuế...) để yêu cầu người dân, nhân viên doanh nghiệp tải, cài đặt các phần mềm trên thiết bị di động**

1. Cảnh giác với các cuộc gọi, tin nhắn từ người người lạ tự xưng là cán bộ cơ quan chức năng hướng dẫn thực hiện các thủ tục dịch vụ công trực tuyến, không cung cấp thông tin cá nhân và cũng không làm theo các hướng dẫn cài đặt các phần mềm thông thông qua các ứng dụng mạng xã hội. Liên hệ với cơ quan chức năng để xác minh về người gọi điện.

2. Cảnh giác với các yêu cầu cài đặt phần mềm được gửi từ các nền tảng mạng xã hội và chỉ cài đặt các phần mềm được cung cấp trực tiếp tại cơ quan chức năng hoặc được tải về trực tiếp trên trang điện tử chính thống của cơ quan chức năng.

3. Tuyệt đối không bấm vào các đường Link nhận được qua tin nhắn SMS, mạng xã hội, không cài đặt ứng dụng không rõ nguồn gốc qua link hoặc file Apk được gửi qua nền tảng mạng xã hội.

4. Khi cần thiết phải cài đặt bất kỳ phần mềm nào, người dân nên chậm lại xác định ai là người đang gửi link phần mềm cho mình, đọc kỹ thông tin, cảnh báo trước khi xác nhận đồng ý tất cả các điều khoản. *Hãy chắc chắn và hiểu rõ, bản thân đang cho phép phần mềm kiểm soát, làm gì trên thiết bị cá nhân của mình trước khi cài đặt.* Chỉ truy cập, tải và cài đặt ứng dụng chính thức thông qua Google Play và Apple Store, kiểm tra thông tin tác giả (nhà phát triển)

* *Điều quan trọng:* 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. Không liên hệ với các web quảng cáo "hỗ trợ lấy lại tiền bị treo, bị lừa đảo..." trên Internet.

*** Phòng ngừa, cảnh giác với hiểm họa từ việc đăng tải, chia sẻ giấy khen, bảng thành tích học tập của trẻ em trên các nền tảng mạng xã hội**

Trước những phương thức, thủ đoạn lừa đảo ngày càng tinh vi của tội phạm trên không gian mạng, Công an tỉnh Bình Dương khuyến cáo người dân, đặc biệt là phụ huynh học sinh cần tỉnh táo, đề cao cảnh giác trước các chiêu trò lừa đảo của tội phạm, tuyệt đối không được chuyển tiền cho người lạ và cung cấp thông tin cá nhân cho bất kỳ đối tượng nào khi chưa rõ nhân thân, lai lịch của người đó. Khi nhận được cuộc gọi nghi lừa đảo cần xác minh lại với giáo viên chủ nhiệm, ban phụ huynh. Trường hợp nghi vấn đối tượng lừa đảo chiếm đoạt tài sản, báo ngay cho cơ quan công an gần nhất để được hỗ trợ, xử lý kịp thời.

Trong mọi trường hợp cần hướng dẫn và giải quyết, tố cáo, tố giác tội phạm trên không gian mạng, tất cả người dân cần liên hệ Công an nơi gần nhất hoặc liên hệ:

- Phòng Cảnh sát hình sự - SĐT: 0274.382.40.87
- Phòng An ninh mạng và PCTP sử dụng Công nghệ cao - SĐT: 0274.381.55.05
- Công an thành phố Thủ Dầu Một – SĐT: 0274. 382.20.39
- Công an thành phố Thuận An – SĐT: 0274.224.11.81
- Công an thành phố Dĩ An – SĐT: 0274.247.35.79
- Công an thành phố Tân Uyên – SĐT: 0274.365.62.54
- Công an thành phố Bến Cát – SĐT: 0274.356.42.68
- Công an huyện Bắc Tân Uyên – SĐT: 0274.36.83.113
- Công an huyện Phú Giáo – SĐT: 0274.22.00.444
- Công an huyện Bàu Bàng – SĐT: 0274.355.23.68
- Công an huyện Dầu Tiếng – SĐT: 0274.356.10.22