BỘ CÔNG AN
CÔNG AN TỈNH TRÀ VINH

Số: 7361 CAT-PCSHS
V/v thông báo một số thủ đoạn đối tượng sử dụng mạng viễn thông, mạng xã hội để lừa đảo chiếm đoạt tài sản

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

Trà Vinh, ngày 31 tháng 3 năm 2023

Kính gửi:
- Các Sở, ban ngành, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố.

Từ đầu năm 2023 đến nay, qua công tác phòng ngừa, đấu tranh tình hình tội phạm sử dụng mạng viễn thông, mạng xã hội để lừa đảo chiếm đoạt tài sản trên cả nước tiếp tục diễn biến phức tạp, đã xảy ra một số vụ lừa đảo với số lượng lớn *(Cục Cảnh sát hình sự phối hợp với Công an Tây Ninh và các đơn vị liên quan phá vụ lừa đảo xuyên quốc gia do người Trung quốc cầm đầu bắt 23 đối tượng lừa 100 người với số tiền 400 tỷ đồng; phát hiện nhóm 22 đối tượng sử dụng công nghệ cao, móc nối với các đối tượng người Đài Loan hoạt động tại Campuchia thực hiện hành vi chiếm đoạt tài sản với số tiền hơn 29 tỷ đồng).*

Riêng trên địa bàn tỉnh Trà Vinh từ đầu năm 2023 đến nay, Công an tỉnh đã tiếp nhận tổng số 24 vụ trình báo bị lừa đảo chiếm đoạt tài sản do đối tượng sử dụng mạng viễn thông, mạng xã hội (*Tiểu Cần: 06; Cầu Ngang: 04; Trà Cú: 04; Càng Long: 04; Châu Thành: 02; TPTV: 02; TXDH: 01; huyện Duyên Hải: 01)*, tổng thiệt hại là **hơn 4,765 tỷ đồng.**

Qua tổng hợp, phân tích các vụ sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản trên địa bàn tỉnh, nổi lên một số phương thức, thủ đoạn như sau: (1) chiếm quyền sử dụng mạng xã hội; (2) tạo ra trang web, app vay tiền để chiếm đoạt tài sản; (3) hoạt động trao đổi, mua bán qua mạng, thanh toán hóa đơn trên sàn thương mại điện tử, Tik Tok; (4) giả danh cơ quan thực thi pháp luật qua mạng Zalo để lừa đảo. **Cụ thể:**

(1) Chiếm quyền điều khiển tài khoản mạng xã hội của người dùng (người đang sinh sống ở nước ngoài), sau đó nhắn tin cho những người trong danh sách bạn bè của tài khoản đó (hiện sinh sống tại Việt Nam) để nhờ chuyển tiền dùm cho người thân (số tài khoản do đối tượng cung cấp) để chiếm đoạt tài sản.

Thủ đoạn phổ biến là các đối tượng sử dụng tài khoản facebook, zalo,... với *"hồ sơ cá nhân"* thu hút như: Là người nước ngoài (Mỹ, Anh) đang tham chiến ở chiến trường Syria, Afganistan,... để kết bạn với bị hại, rồi nói với bị hại sẽ chuyển quà, tiền về Việt Nam nhờ bị hại nhận và giữ giùm. Để tạo niềm tin cho bị hại, các đối tượng còn gửi ảnh bưu phẩm và các giấy tờ liên quan đến việc chuyển quà, tiền cho bị hại và yêu cầu người dân phải nộp tiền đóng phí nhận quà.

Đặc biệt thời gian gần đây, nắm được tâm lý người dùng mạng xã hội hiện nay đã cảnh giác với thủ đoạn lừa đảo bằng tin nhắn nhờ chuyển tiền, các đối

tượng đã sử dụng thủ đoạn tinh vi hơn, lợi dụng **công nghệ Deepfake**[1] để làm giả cuộc gọi video nhằm chiếm đoạt tài sản, trong đó:

- Thông qua mạng Internet, các đối tượng đã thu thập hình ảnh, giọng nói của người dùng trên mạng xã hội, sử dụng công nghệ Deepfake *(thông qua các phần mềm: Avatarify, MyHeritage, Morphin, DeepFakeLab, Faceswap... được chia sẻ trên internet)* tạo ảnh động, video giả mạo người dùng đang nói chuyện trực tuyến với cùng khuôn mặt, âm điệu giọng nói và cách xưng hô.

- Đối tượng tạo lập tài khoản giả mạo trên mạng xã hội trùng thông tin và ảnh đại diện với người dùng, kết bạn với nạn nhân trong danh sách bạn bè và nhắn tin vay mượn tiền theo kịch bản sẵn có. Trong một số trường hợp, đối tượng chiếm đoạt tài khoản mạng xã hội của người dùng để trực tiếp nhắn tin cho các nạn nhân trong danh sách bạn bè. Để tạo lòng tin với nạn nhân, đối tượng truyền tải Deepfake video có sẵn lên kênh video call, khiến nạn nhân nhận ra hình ảnh và giọng nói của người quen và nhanh chóng chuyển tiền theo yêu cầu của đối tượng.

(2) Giả danh cơ quan thực thi pháp luật *(Cảnh sát giao thông, Cơ quan điều tra, Viện kiểm sát...),* nhân viên bưu điện, điện lực, sử dụng mạng viễn thông (VoIP) yêu cầu người dân phải nộp tiền vào các tài khoản để đóng tiền phạt, kiểm tra, nhất là hiện nay lợi dụng việc cập nhật thông tin thuê bao di động, các đối tượng đã giả danh các nhà mạng viễn thông liên lạc người dân để thu thập thông tin cá nhân, thông tin tài khoản ngân hàng, mã OTP… để chiếm đoạt tài sản.

(3) Lừa đảo qua hoạt động trao đổi, mua bán qua mạng:

- Đối tượng thông qua mạng Internet đăng bài tuyển cộng tác viên tương tác làm việc online trên các sàn thương mại điện tử giả mạo Shopee, Lazada, Tiki,...để được hưởng hoa hồng từ 10 đến 30% giá trị mỗi đơn hàng. Sau khi bị hại liên hệ được đối tượng gửi link web giả mạo Shopeemall để lập tài khoản, chuyển tiền đến các tài khoản ngân hàng đối tượng cung cấp để thực hiện tạo mua đơn hàng có sẵn để được hưởng hoa hồng thì các đối tượng khóa trang mạng, bỏ số điện thoại liên lạc để xóa dấu vết và chiếm đoạt tài sản của bị hại.

- Đối tượng gọi điện lôi kéo, dụ dỗ bị hại tham gia theo dõi tiktok, nghe nhạc MP3 để được trả công từ 10.000 đồng đến 50.000 đồng/1 lần, lập tài khoản trên một trong các trang web Corona, Goruurl.com, SX38.com, ua8wglfq.com (các trang web này có giao diện giống với các trang web đánh bạc), đặt các lệnh tài/xỉu hoặc chẵn/lẻ để được hưởng hoa hồng từ 30% đến 65% trên tổng số tiền mỗi lần đặt cược; sau mỗi lần bị hại chuyển tiền đến tài khoản ngân hàng đối tượng cung cấp sẽ

[1] Là công nghệ ứng dụng trí tuệ nhân tạo (AI) tạo ra các sản phẩm công nghệ âm thanh, hình ảnh và video làm giả các đối tượng ngoài đời thực với độ chính xác rất cao. Dựa trên tệp tin hình ảnh khuôn mặt, giọng nói của một người ngoài đời thực, Deepfake sẽ sử dụng thuật toán để tái tạo khuôn mặt và giọng nói phù hợp với nét mặt, biểu cảm của một người khác, sau đó tạo ra video giả mạo hoàn toàn đối tượng ngoài đời thực. Với công nghệ Deepfake, video giả mạo có độ chính xác cao, rất khó phân biệt thật giả. Tuy nhiên, video do đối tượng tạo sẵn thường có nội dung chung chung, không phù hợp hoàn toàn với ngữ cảnh thực tế giao tiếp với nạn nhân, có thể khiến nạn nhân nghi ngờ, phát hiện. Để che lấp khuyết điểm trên, các đối tượng thường tạo ra video với âm thanh khó nghe, hình ảnh không rõ nét giống cuộc gọi video có tín hiệu chập chờn được thực hiện trong khu vực phủ sóng di động/wifi yếu.

được đối tượng gửi qua Telegram cho bị hại một hợp đồng cam kết khách hàng tên Công ty Cổ phần Tài chính HANDICO hoặc Công ty tài chính TNHH MB SHINSEL cam kết bảo hiểm an toàn 100% vốn cho bị hại. Sau đó, đối tượng hướng dẫn bị hại liên hệ qua Telegram gặp chuyên gia để được hướng dẫn đặt cược. Ban đầu với số tiền ít, đối tượng cho bị hại rút tiền về tài khoản ngân hàng, khi bị hại chuyển số tiền lớn và yêu cầu rút tiền thì đối tượng tạo ra nhiều lý do như sai số tài khoản ngân hàng, bị hại đặt cược sai lệch...để không cho bị hại rút tiền. Đối tượng dụ dỗ bị hại chuyển thêm tiền thì chặn liên lạc, xóa tài khoản của bị hại.

- Đối tượng tạo các tin nhắn giả mạo các ngân hàng thương mại (SMS Brandname) với nội dung thông báo khách hàng đã đăng ký, kích hoạt dịch vụ *(nhiều dịch vụ khác nhau do các đối tượng nghĩ ra như: quảng cáo trên Tiktok, dịch vụ tài chính toàn cầu...)* có mức phí sử dụng mỗi tháng từ 3.000.000đ – 6.000.000đ, nếu muốn hủy thì truy cập vào các đường dẫn *(đối tượng sử dụng rất nhiều đường dẫn giả mạo trang web của ngân hàng như: http://vietinbank.com.vn-vb.top, http://vpbank.com.vn-vb.top, http://scb.com.vn-as.life, http://msb.com.vn-sx.top...)*, mục đích là dụ dỗ khách hàng truy cập vào trang web giả mạo ngân hàng. Rất nhiều người do nhầm tưởng là tin nhắn thông báo của ngân hàng nên đã thực hiện theo, dẫn đến bị chiếm quyền truy cập tài khoản ngân hàng và bị chiếm đoạt toàn bộ số tiền có trong tài khoản.

(4) Các đối tượng thành lập Công ty bình phong, tạo các ứng dụng giả, tuyển dụng nhân viên giao cho nhiệm vụ gọi điện, mạo danh nhân viên của các ngân hàng, đưa ra thông tin gian dối về việc ngân hàng cho vay hạn mức từ 10 – 100 triệu đồng với lãi suất 0%, khách hàng chỉ phải đóng phí bảo hiểm tiền vay từ 1.700.000 đồng – 3.895.000 đồng, tùy vào số tiền vay. Sau khi "khách hàng" đồng ý và lựa chọn mức vay, sẽ cung cấp thông tin để làm hợp đồng vay tiền. Sau đó, đối tượng yêu cầu bị hại phải chuyển lại phần trăm số tiền vay, tiền phí để kiểm tra rồi mới giải ngân số tiền vay. Sau khi người dân chuyển tiền vào thì đối tượng khóa trang mạng và chiếm đoạt tài sản.

(5) Một số đối tượng sử dụng không gian mạng (qua email, mạng xã hội Facebook, Zalo, tin nhắn...) mạo danh lấy tên, năm sinh của các đồng chí Lãnh đạo tỉnh, Lãnh đạo các Sở, Ban, Ngành (cấp tỉnh), các địa phương (cấp huyện) trong tỉnh tạo ra các tài khoản giả, thư điện tử giả mạo gửi đến một số tổ chức, cá nhân trong và ngoài tỉnh để thực hiện hành vi lừa đảo, trục lợi, chiếm đoạt tài sản.

(6) Một số thủ đoạn mới xuất hiện thời gian gần đây:

- Đối tượng giả danh nhân viên Bệnh viện, giáo viên để liên hệ với người dân, thông báo người thân bị tai nạn, cần tiền để phẫu thuật gấp và yêu cầu người dân phải chuyển tiền vào tài khoản do đối tượng cung cấp để đóng tiền viện phí. Sau khi người dân chuyển tiền thì đối tượng chiếm đoạt.

- Đối tượng tạo giả các giấy tờ nhập viện của các Bệnh viện, sau đó đưa lên các trang mạng xã hội thông báo người thân bị tai nạn, bị bệnh nặng cần tiền để đóng viện phí, phẫu thuật gấp và kêu gọi từ thiện. Khi các nhà hảo tâm chuyển tiền vào tài khoản do đối tượng cung cấp thì đối tượng chiếm đoạt.

Công an tỉnh nhận định: Những thủ đoạn chiếm đoạt tài sản đã nêu trên rất tinh vi, đối tượng câu kết thành băng nhóm, có cơ cấu tổ chức chặt chẽ hoạt động liên tỉnh, xuyên quốc gia; có sự phân công vai trò rất cụ thể nên khó đấu tranh, xử lý, vẫn có nhiều người bị hại. Thời gian qua, Công an tỉnh đã có thông báo rộng rãi thủ đoạn tương tự, thực hiện định kỳ hằng tháng. Tuy nhiên, một số người dân trên địa bàn vẫn còn bị lừa, thiếu ý thức cảnh giác tội phạm, trong đó đáng lưu ý một số trường hợp bị hại là cán bộ, đảng viên, công chức trên địa bàn tỉnh.

Để chủ động phòng ngừa, ngăn chặn có hiệu quả loại tội phạm này trên địa bàn, Công an tỉnh Trà Vinh thông báo một số thủ đoạn nêu trên đến các Sở, ban ngành, đoàn thể tỉnh và UBND các huyện, thị xã, thành phố biết, đồng thời phối hợp thực hiện một số nội dung sau:

1. Tổ chức quán triệt, phổ biến các phương thức thủ đoạn nêu trên đến cán bộ, đảng viên, công chức, viên chức và người lao động tại đơn vị nắm, chủ động áp dụng các biện pháp phòng ngừa, đấu tranh. Theo chức năng, nhiệm vụ được giao đẩy mạnh tuyên truyền cho người dân, doanh nghiệp nắm các phương thức, thủ đoạn nêu trên biết, chủ động phòng, chống, trong đó tập trung tuyên truyền một số nội dung sau:

- Khi sử dụng mạng Internet, mạng viễn thông cần hết sức chú ý khi làm quen, kết bạn trên mạng cũng như các hoạt động chuyển tiền, tránh trở thành bị hại của các đối tượng lừa đảo.

- Khi nhận được các cuộc gọi lạ, nhất là các đối tượng giả danh nhân viên bưu điện, nhà mạng viễn thông, giả danh cán bộ Công an, Viện kiểm sát, Tòa án,... có dấu hiệu nghi vấn, phải bình tĩnh, không làm theo yêu cầu hoặc làm theo dẫn dụ bấm các phím số trên máy điện thoại. Tuyệt đối không được cung cấp thông tin cá nhân, thông tin tài khoản, mã OTP, thẻ tín dụng… trong các trường hợp không quen biết đối tượng, nhất là các đối tượng yêu cầu cung cấp thông tin qua điện thoại; Không chuyển tiền vào các tài khoản theo yêu cầu của người lạ.

- Đối với thủ đoạn đối tượng chiếm quyền điều khiển tài khoản mạng xã hội, sử dụng công nghệ Deepfake giả danh bạn bè, người thân,… khi nhận được bất kỳ tin nhắn vay mượn tiền, nạp thẻ điện thoại thông qua mạng xã hội, cần có biện pháp kiểm tra, gọi điện trực tiếp qua số điện thoại người nhận để xác thực thông tin trước khi thực hiện việc chuyển tiền, nạp thẻ điện thoại.

- Trước các tin tức giật gân, những trang mạng không rõ nguồn gốc trên mạng Internet và mạng xã hội, tuyệt đối không truy cập vào xem. Trong trường hợp lỡ tay truy cập vào đường link, cần nhanh chóng thay đổi mật khẩu của trang cá nhân để tránh mất tài khoản.

- Đề cao cảnh giác trước các thủ đoạn cho vay lãi nặng qua các ứng dụng (App); Không vay tiền qua các App hoạt động trái phép trên không gian mạng, không cung cấp các thông tin của bản thân và người thân, bạn bè cho các đối tượng.

2. Đề nghị Sở Thông tin và Truyền thông phối hợp với các Công ty Viễn thông trên địa bàn (Vinaphone, Mobifone, Viettel,...) có biện pháp tuyên truyền phổ biến rộng rãi thủ đoạn của loại tội phạm này đến các thuê bao di động trả

trước, trả sau trên địa bàn để biết phòng ngừa. Đồng thời, phối hợp với Công an tỉnh và các cơ quan liên quan đẩy mạnh công tác nắm tình hình, điều tra, phát hiện và xử lý nghiêm theo quy định của pháp luật đối với các đối tượng có hành vi mua bán sim không chính chủ (sim rác), hành vi lừa đảo, trục lợi, chiếm đoạt tài sản trên không gian mạng.

3. Đề nghị Ngân hàng Nhà nước Việt Nam chi nhánh tỉnh Trà Vinh chỉ đạo các Ngân hàng thương mại, Tổ chức tín dụng trên địa bàn tuyên truyền đến cán bộ, công nhân viên chức tránh trường hợp bị đối tượng lừa đảo chiếm đoạt tài sản. Đặc biệt, cần tuyên truyền đến các nhân viên giao dịch tại các quầy của ngân hàng, tổ chức tín dụng… để nắm các trường hợp rút tiền, chuyển tiền của người dân và tích cực giải thích, thông báo cho người dân biết được thủ đoạn phạm tội của đối tượng sử dụng công nghệ cao, nhất là các hành vi lừa đảo chiếm đoạt tài sản. Đồng thời, cần chú ý giám sát, kiểm tra các tài khoản có các dấu hiệu nghi vấn như: Các tài khoản do người ở khu vực nông thôn, vùng sâu, vùng xa đăng ký mở và mở dịch vụ Internet banking, ngay sau khi mở đã có các khoản tiền lớn (hàng trăm triệu đồng) chuyển đến, các tài khoản này bị rút tiền tại các ATM nước ngoài,... để có biện pháp xử lý và cung cấp cho cơ quan Công an. Ngoài ra, tăng cường kiểm tra, rà soát quy trình, giám sát chặt việc mở tài khoản, phát hành thẻ cho khách hàng để phát hiện, xử lý các trường hợp sử dụng Giấy Chứng minh nhân dân giả, Giấy Chứng minh nhân dân của người khác mở tài khoản, hành vi thu thập, mua bán tài khoản ngân hàng… nhằm kịp thời ngăn chặn thiệt hại về tài sản của nhân dân.

Mọi người dân khi phát hiện có dấu hiệu nghi vấn đối tượng sử dụng mạng viễn thông, mạng xã hội lừa đảo chiếm đoạt tài sản phải kịp thời báo ngay với cơ quan Công an nơi gần nhất hoặc Phòng Cảnh sát hình sự Công an tỉnh Trà Vinh (số điện thoại ***0294.3842.974)*** để tiếp nhận, kịp thời điều tra xử lý.

Công an tỉnh Trà Vinh rất mong được sự quan tâm, phối hợp của quý cơ quan./.

Nơi nhận:
- Như trên (để phối hợp tuyên truyền);
- TT. Tỉnh ủy, UBND tỉnh (để báo cáo);
- Đ/c Giám đốc (báo cáo);
- Các Đ/c Phó Giám đốc (phối hợp chỉ đạo);
- Tiểu đoàn Cảnh sát cơ động (để biết);
- Trại giam Bến Giá (để biết);
- Công an các đơn vị, huyện, TX, TP (th/dõi);
- Lưu: VT – PTM, CSHS (Đội 5).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH TRÀ VINH

Đại tá Lê Văn Tư