HUYỆN ỦY ĐAK ĐOA
BAN TUYÊN GIÁO
*
Số 77 -HD/BTGHU

ĐẢNG CỘNG SẢN VIỆT NAM

Đak Đoa, ngày 16 tháng 6 năm 2023

HƯỚNG DẪN
tuyên truyền, phổ biến các biện pháp phòng ngừa và đấu tranh tội phạm lừa đảo, chiếm đoạt tài sản sử dụng mạng viễn thông, mạng Internet

---

Thời gian gần đây, tình hình tội phạm lừa đảo, chiếm đoạt tài sản thông qua mạng viễn thông, mạng Internet *(viết tắt là trên không gian mạng)* trên địa bàn tỉnh nói chung và huyện Đak Đoa nói riêng diễn biến phức tạp và có chiều hướng gia tăng; hoạt động của các đối tượng rất tinh vi, đa dạng về phương thức, gây thiệt hại lớn về tài sản, bức xúc trong xã hội, ảnh hưởng đến tình hình an ninh, trật tự xã hội tại địa phương. Mặc dù các cơ quan chức năng, cơ quan truyền thông thường xuyên thông báo phương thức, thủ đoạn hoạt động của các đối tượng sử dụng công nghệ cao để lừa đảo, chiếm đoạt tài sản, tuy nhiên vẫn có nhiều người dân do thiếu hiểu biết, nhẹ dạ, cả tin, mất cảnh giác nên để các đối tượng thực hiện các hành vi lừa đảo, chiếm đoạt tài sản.

Để tiếp tục nâng cao nhận thức cho cán bộ, đảng viên, quần chúng Nhân dân và tăng cường hiệu quả công tác phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng, Ban Tuyên giáo Huyện ủy hướng dẫn tuyên truyền, phổ biến các biện pháp phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng với các nội dung như sau:

I- MỤC ĐÍCH, YÊU CẦU

1. Đẩy mạnh công tác tuyên truyền nâng cao nhận thức của cán bộ, đảng viên và Nhân dân trên địa bàn huyện về các quy định của pháp luật trong phòng, chống tội phạm nói chung và tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng nói riêng; phương thức, thủ đoạn của các đối tượng lừa đảo chiếm đoạt tài sản trên không gian mạng. Từ đó, nâng cao chất lượng, hiệu quả công tác phòng ngừa xã hội, hạn chế các nguyên nhân, điều kiện mà các đối tượng có thể lợi dụng để thực hiện hành vi phạm tội trên không gian mạng.

2. Tổ chức các hình thức tuyên truyền phải phong phú, đa dạng, dễ tiếp cận; nội dung tuyên truyền phải bám sát quy định của pháp luật và phù hợp với đối tượng cũng như tình hình thực tế tại địa bàn.

3. Việc tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm phòng ngừa, chống vi phạm pháp luật và tội phạm trên không gian mạng phải được thực hiện thường xuyên, liên tục; đảm bảo có trọng tâm, trọng điểm với nội dung, hình thức

phù hợp; gắn với việc tuyên truyền các nhiệm vụ kinh tế - xã hội, đảm bảo quốc phòng - an ninh trên địa bàn huyện.

II- NỘI DUNG, HÌNH THỨC TUYÊN TRUYỀN

1. Nội dung tuyên truyền

Tuyên truyền, phổ biến các quy định của pháp luật về phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, nhất là: Luật An ninh mạng, Luật Hình sự,... .; một số phương thức, thủ đoạn lừa đảo, chiếm đoạt tài sản trên không gian mạng *(có phụ lục kèm theo).*

1.1. Phổ biến cho cán bộ, đảng viên, đoàn viên, hội viên và Nhân dân không lo lắng, hoảng sợ khi nhận được các cuộc điện thoại, tin nhắn, các thông tin mà người lạ mặt gửi đến có nội dung xấu liên quan đến cá nhân và người thân trong gia đình; khi có người lạ gọi điện hoặc gửi tin nhắn thông báo được trúng thưởng hoặc nhận được khoản tiền lớn không rõ nguồn gốc thì không được tin lời các đối tượng; khi có người lạ mặt trên mạng xã hội kết bạn làm quen không rõ là ai, mục đích là gì thì không nên kết bạn, nói chuyện, nhất là không được cung cấp các thông tin cá nhân để đối tượng có thể lợi dụng; 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 được làm theo. Phải thường xuyên cảnh giác, chủ động bảo mật các thông tin cá nhân, nhất là các thông tin quan trọng như: Thông tin thẻ căn cước công dân; thông tin tài khoản ngân hàng; thông tin tài khoản mạng xã hội. Chủ động, tự giác tố giác ngay với cơ quan pháp luật khi khi nhận được các cuộc gọi, tin nhắn hoặc các nội dung nghi ngờ là hoạt động lừa đảo,…. để được hướng dẫn xử lý.

1.2. Những phương thức, thủ đoạn, đặc điểm nhận biết và cách phòng tránh đối với loại tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng. Trong đó, tập trung tuyên truyền về: Thủ đoạn gọi điện giả danh cán bộ Nhà nước, thầy cô giáo chủ nhiệm để lừa đảo chiếm đoạt tài sản; thủ đoạn lợi dụng lòng tham của các cá nhân thông báo trúng thưởng lớn để chiếm đoạt thông tin cá nhân, tài khoản ngân hàng, yêu cầu chuyển tiền; thủ đoạn chiếm quyền sử dụng tài khoản (mạng xã hội Facebook, Zalo...), lập tài khoản mạo danh người khác, tuyển cộng tác viên làm việc Online, thủ đoạn lợi dụng công nghệ Deepfake làm giả cuộc gọi video, các ứng dụng cho vay trực tuyến; hoạt động đầu tư tiền ảo, tiền điện tử... để thực hiện hành vi lừa đảo chiếm đoạt tài sản…

1.3. Tầm quan trọng của việc bảo vệ các thông tin dữ liệu cá nhân; nâng cao ý thức cảnh giác trong việc cung cấp các thông tin cá nhân cũng như việc xác thực con người trước khi thực hiện việc chuyển tiền bằng hình thức Internet banking; hậu quả, tác hại của việc: bán, cho thuê, cho mượn tài khoản ngân hàng, để các đối tượng xấu sử dụng tài khoản ngân hàng của mình phục vụ việc chuyển, nhận tiền, làm đầu ra cho tài sản chiếm đoạt được.

1.4. Kết quả công tác phòng ngừa, phát hiện, đấu tranh, ngăn chặn của lực lượng chức năng với tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng.

2. Hình thức tuyên truyền

- Các cơ quan tuyên truyền phải phối hợp thống nhất, chặt chẽ, sử dụng tối đa các phương tiện, điều kiện thông tin tuyên truyền hiện có và các hình thức tuyên truyền truyền thống, đa dạng về hình thức tuyên truyền và phù hợp với thực tế của đơn vị, địa phương. Chú trọng việc phát huy vai trò của người có uy tín, điển hình tiên tiến trong công tác tuyên truyền. Cụ thể:

2.1. *Tuyên truyền trên không gian mạng:* Thường xuyên tổng hợp thông tin, tạo các bài viết, phóng sự ngắn gọn, dễ hiểu... vận dụng các ứng dụng điện tử, các Fanpage, Zalo... nhanh chóng đưa thông tin về phương thức, thủ đoạn của các đối tượng, các phương pháp phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên một cách nhanh nhất đến với các cá nhân tham gia không gian mạng.

2.2. *Tuyên truyền miệng:* Tổ chức hội nghị tập huấn, tuyên truyền hoặc lồng ghép nội dung trong các hội nghị, lớp học, trong các buổi sinh hoạt của cơ quan, đơn vị, sinh hoạt chi bộ, sinh hoạt khu dân cư, sinh hoạt chi hội, tổ hội tại các thôn, làng, tổ dân phố... nhằm thông tin về phương thức, thủ đoạn của các đối tượng lừa đảo, chiếm đoạt tài sản trên không gian mạng và các biện pháp phòng, chống.

2.3. *Tuyên truyền qua phương tiện thông tin đại chúng:* Trang Thông tin điện tử huyện, xã, thị trấn; Đài truyền thanh - truyền hình huyện, trạm truyền thanh xã, thị trấn đăng tải, phát sóng các tin, bài, phóng sự, video clip...

3. Thời gian thực hiện: Nhiệm vụ thường xuyên.

III- TỔ CHỨC THỰC HIỆN

1. Đề nghị Công an huyện

- Phát huy vai trò là lực lượng nòng cốt trong thực hiện phong trào toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng, tham mưu Huyện ủy, Ủy ban nhân dân huyện chỉ đạo cả hệ thống chính trị thực hiện có hiệu quả phong trào "Toàn dân bảo vệ an ninh Tổ quốc", nhất là trong công tác phòng, chống tội phạm trên không gian mạng.

- Kịp thời phát hiện, ngăn chặn, đấu tranh, xử lý đối với các hành vi vi phạm pháp luật về bảo đảm an toàn, an ninh mạng; đồng thời cung cấp thông tin đến các cơ quan, đơn vị biết, tuyên truyền, phổ biến rộng rãi cho cán bộ, đảng viên và các tầng lớp Nhân dân biết, nêu cao cảnh giác và tích cực đấu tranh phòng, ngừa.

- Chỉ đạo lực lượng Công an xã, thị trấn làm tốt công tác tham mưu cho Ủy ban nhân dân các xã, thị trấn làm tốt công tác tuyên truyền, nâng cao nhận thức, ý thức cảnh giác của quần chung Nhân dân; tiếp tục phát huy vai trò của các Tổ tự quản, nhất là sử dụng các nhóm zalo để tuyên truyền về các phương thức, thủ đoạn của các

đối tượng lừa đảo, chiếm đoạt tài sản trên không gian mạng; chủ động tiếp nhận thông tin, cảnh báo và hướng dẫn quần chúng Nhân dân xử lý tình huống khi các đối tượng liên lạc đến thực hiện hành vi lừa đảo.

2. Phòng Văn hóa và Thông tin; Trung tâm Văn hóa - Thông tin và Thể thao huyện phối hợp với các cơ quan, ban, ngành liên quan triển khai các nội dung tuyên truyền; thường xuyên đăng tải các thông tin liên quan đến: Luật An ninh mạng; các phương thức thủ đoạn lừa đảo, chiếm đoạt tài sản của các đối tượng trên không gian mạng; kết quả công tác đấu tranh với các đối tượng phạm tội trên không gian mạng trên Cổng thông tin điện tử huyện và phát trên sóng Đài Truyền thanh - Truyền hình huyện.

3. Phòng Giáo dục và Đào tạo huyện: Chỉ đạo các cơ sở giáo dục trên địa bàn huyện tăng cường tuyên truyền về các phương thức, thủ đoạn của các đối tượng lừa đảo, chiếm đoạt tài sản trên không gian mạng; hướng dẫn giáo viên, cán bộ, học sinh xử lý tình huống khi các đối tượng liên lạc đến thực hiện hành vi lừa đảo.

4. Mặt trận Tổ quốc và các tổ chức thành viên: Đẩy mạnh tuyên truyền, vận động hội viên, đoàn viên và các tầng lớp Nhân dân tự trang bị kiến thức, nâng cao ý thức cảnh giác trước các thủ đoạn của đối tượng vi phạm pháp luật trên không gian mạng; các biện pháp phòng, tránh không để bị các đối tượng lừa đảo, chiếm đoạt tài sản.

5. Các tổ chức cơ sở Đảng trực thuộc Huyện ủy

- Chủ động triển khai thực hiện ở địa phương, đơn vị mình. Phải xác định, công tác tuyên truyền là công tác quan trọng, then chốt trong nâng cao nhận thức, ý thức cảnh giác để phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng.

- Đảng ủy các xã, thị trấn cần đa dạng hoá các hình thức tuyên truyền, trong đó cần chú ý đến các trường hợp ít được tiếp cận thông tin, các trường hợp nhẹ dạ, người có hoàn cảnh khó khăn, người cao tuổi, người có trình độ nhận thức chưa cao... để tổ chức tuyên truyền. Chú trọng đến các cá nhân là người có uy tín trong đồng bào dân tộc thiểu số, chức sắc, chức việc trong các tôn giáo để tuyên truyền một cách hiệu quả.

Ban Tuyên giáo Huyện ủy đề nghị Mặt trận Tổ quốc và các tổ chức chính trị - xã hội, các tổ chức cơ sở Đảng trực thuộc Huyện ủy, các địa phương, cơ quan, đơn vị quan tâm phối hợp, triển khai thực hiện; báo cáo kết quả về Ban Tuyên giáo Huyện ủy tổng hợp báo cáo Thường trực Huyên ủy biết và chỉ đạo.

TRƯỞNG BAN

BAN TUYÊN GIÁO

Lê Thị Huệ

Nơi nhận:
- Thường trực Huyện ủy (b/c),
- Ủy ban nhân dân huyện,
- Các tổ chức cơ sở Đảng trực thuộc Huyện ủy,
- Mặt trận Tổ quốc và các đoàn thể chính trị - xã hội huyện,
- Lưu Ban Tuyên giáo Huyện ủy.

PHỤ LỤC
MỘT SỐ PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN SỬ DỤNG CÔNG NGHỆ CAO, THÔNG QUA MẠNG VIỄN THÔNG, MẠNG INTERNET

(Kèm theo Hướng dẫn số -HD/BTGHU của Ban Tuyên giáo Huyện ủy ngày tháng 6 năm 2023)

---

1. Thủ đoạn sử dụng phần mềm độc hại, mã độc để tấn công chiếm đoạt thông tin

- *Cài sẵn phần mềm gián điệp* trong các thiết bị viễn thông, tin học như các thiết bị lưu trữ ngoài (USB), điện thoại thông minh, máy ảnh số, máy in… để làm quà tặng cho đối tác; một số công ty, tập đoàn điện tử, viễn thông của nước ngoài cài đặt sẵn các phần mềm gián điệp vào các sản phẩm, thiết bị điện tử trước khi tung ra thị trường. Khi các thiết bị này kết nối với máy tính, phần mềm gián điệp sẽ tự kích hoạt, lây nhiễm vào hệ thống máy tính, tạo kết nối để các cơ quan đặc biệt nước ngoài thu thập tình báo.

- *Sử dụng các kỹ năng xã hội để tấn công vào sự chủ quan, bất cẩn, hiểu biết hạn chế hay tình trạng thiếu kiểm soát của người dùng máy tính để đánh cắp thông tin cá nhân hay lây nhiễm phần mềm gián điệp*. Chúng có thể thực hiện nhiều phương thức khác nhau như: Gửi các email, tin nhắn có nội dung, hình thức hấp dẫn, tin cậy để dẫn dụ, thuyết phục người dùng khai báo thông tin cá nhân hoặc tải về và mở các tập tin đính kèm đã được nhúng mã độc; tạo ra các trang web giả mạo có nội dung hấp dẫn nhưng chứa mã độc rồi dẫn dụ người dùng truy cập hoặc yêu cầu cài đặt các gói cập nhật quan trọng cho hệ thống, trong đó đính kèm mã độc…

- *Phần mềm độc hại*

Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

- *Mã độc Mustang Panda*

Mã độc Mustang Panda là một loại mã độc gián điệp do nhóm tin tặc Mustang Panda của Trung Quốc phát tán. Nhóm mã độc này thường lây lan qua các thiết bị lưu trữ ngoại vi để tấn công vào các máy tính không có kết nối mạng.

Mã độc Mustang Panda đã phát triển thành 5 biến thể. Mã độc Mustang Panda có tính năng lây nhiễm sang thiết bị lưu trữ ngoài (gồm: USB, ổ cứng di động, đĩa quang để định dạng USB...) và sao chép, mã hóa dữ liệu từ máy tính sang thư mục ẩn trong thiết bị lưu trữ ngoài.

2. Thủ đoạn lợi dụng lòng tham của người dân để lừa đảo chiếm đoạt tài sản

a. Lừa đảo nhận quà từ nước ngoài

Thông qua các ứng dụng mạng xã hội như Facebook, Zalo… Các đối tượng lợi dụng lòng tin của một số phụ nữ, đặc biệt hướng tới phụ nữ độc thân, thiếu thốn tình cảm để chủ động kết bạn giới thiệu là người nước ngoài có chức danh, địa vị hoặc có điều kiện kinh tế đang còn độc thân để làm quen, xây dựng mối quan hệ thân thiện với bị hại, hứa hẹn chuyển về cho bị hại một món hàng, quà có giá trị lớn. Sau khi có được lòng tin từ bị hại, các đối tượng giả danh nhân viên sân bay, hải quan, bưu điện, thuế... liên lạc với bị hại thông báo tiền, hàng đã chuyển về Việt Nam, phải nộp các loại thuế, lệ phí, cước phí… để có thể nhận tiền, hàng hóa từ nước ngoài gửi về, Vì nghĩ món hàng, quà có giá trị cao nên bị hại đã chuyển tiền vào tài khoản tại ngân hàng do chúng cung cấp, đến khi bị hại không còn khả năng cung cấp tiền hoặc phát hiện ra bị lừa thì bọn chúng ngắt liên lạc, chiếm đoạt tài sản.

b. Lừa tuyển cộng tác viên các sàn thương mại điện tử (Shopee, Sen Đỏ, Lazada, ...) hoặc ứng dụng Tiktok

Lợi dụng chức năng quảng cáo của các ứng dụng trên, các đối tượng đăng hàng loạt các bài tuyển cộng tác viên các sàn thương mại điện tử (Shopee, Tiki, Sendo, Lazada…), Tiktok. Làm các nhiệm vụ chuyển tiền thanh toán các đơn hàng tăng tương tác, doanh số… theo các đơn hàng bất kỳ mà chúng gửi, hứa hẹn trả tiền công và lợi nhuận cao từ 10% đến 30%. Sau khi tạo dựng niềm tin cho bị hại bằng một số đơn hàng giá trị nhỏ thanh toán hoa hồng đầy đủ, chúng yêu cầu bị hại thanh toán đơn hàng giá trị lớn hơn, sau đó đưa ra các lý do người cộng tác vi phạm quy định như lỗi sai cú pháp, vượt quá định mức số tiền thanh toán trong ngày, quá hạn… dẫn đến bị khóa tài khoản và yêu cầu bị hại chuyển thêm nhiều lần tiền để bảo lãnh, xác minh tài khoản… thì mới cho rút lại tiền gốc và lãi. Đối tượng đưa bị hại vào tình trạng muốn lấy lại tiền, tiếc tiền nên phải theo cho đến khi hết khả năng thanh toán thì mới biết bị lừa. Nguy hiểm hơn là một số đối tượng hướng dẫn bị hại thực hiện các nhiệm vụ trên các trang web đánh bạc mà bị hại hoàn toàn không nhận thức được.

c. Lừa đảo kêu gọi đầu tư tài chính, tiền ảo

Lừa đảo qua kêu gọi người dân bỏ tiền tham gia đầu tư, mua - bán, giao dịch các loại "tiền ảo", "tiền kỹ thuật số", "tiền mã hóa" (Bitcoin, Etherum, USDT…) trên các sàn giao dịch quyền chọn nhị phân (Binary Option - BO), sàn đầu tư ngoại hối… gắn mác giấy phép hoạt động của nước ngoài, kèm theo các lời cam đoan, hứa hẹn lợi nhuận lớn, bảo hiểm vốn…

Khi huy động được lượng tiền đủ lớn, các đối tượng chủ sàn sẽ can thiệp làm mất giá trị của đồng tiền ảo, điều chỉnh kết quả giao dịch thắng thua một cách tinh vi hoặc đánh sập hệ thống để chiếm đoạt toàn bộ số tiền của nhà đầu tư.

Đối tượng dùng thủ đoạn bằng hình thức làm quen qua mạng xã hội, đánh vào tâm lý muốn kiếm tiền nhanh chóng bằng hình thức đầu tư vào các sàn giao dịch tiền ảo bởi các trang giao dịch không có nguồn gốc, xuất xứ rõ ràng. Đối tượng lừa đảo dẫn dắt, hướng dẫn bị hại tham gia chơi sàn giao dịch ảo, đầu tư bằng cách bỏ tiền thật ra mua đổi tiền ảo. Tải ứng dụng sàn giao dịch và lập tài khoản để nạp tiền USDT, từ đó chuyển sang sàn để giao dịch. Người chơi tưởng thật đã nạp tiền để tham gia. Nhưng sau đó các đối tượng đã chiếm đoạt tiền, đánh sập sàn giao dịch mà người chơi tham gia, nên không thể xác minh làm rõ để xử lý theo pháp luật.

3. Thủ đoạn lợi dụng lòng tin của người dân để chiếm đoạt tài sản

a. Chiếm đoạt quyền sử dụng tài khoản cá nhân (zalo, facebook...), mạo danh người thân, người quen để lừa vay tiền, chuyển tiền

Bằng một số hình thức như gửi link tham gia các cuộc bình chọn, khi nạn nhân click và đường link trên thì sẽ hiện lên giao diện đăng nhập giống như các trang mạng xã hội. Khi nạn nhân nhập các thông tin tài khoản của mình vào thì ngay lúc đó các đối tượng liền chiếm quyền sử dụng tài khoản Facebook, Zalo của người sử dụng, giả danh chủ tài khoản nhắn tin cho người thân, bạn bè hoặc các mối quan hệ uy tín để vay tiền hoặc nhờ chuyển tiền vào tài khoản ngân hàng (do chúng cung cấp) sau đó chiếm đoạt tài sản.

Đối tượng sử dụng thông tin cá nhân, hình ảnh của các đồng chí Lãnh đạo các cơ quan chính quyền, đoàn thể, … để thiết lập tài khoản mạng xã hội (zalo, facebook, …) mạo danh. Sau đó, các đối tượng dùng tài khoản mạo danh để kết bạn, nhắn tin trao đổi vay, mượn tiền của bạn bè, người thân, đồng nghiệp, cấp dưới, … và chiếm đoạt tiền của các bị hại chuyển đến.

Tháng 03/2022, Công an tỉnh Gia Lai đã điều tra, xác minh và làm rõ nhóm đối tượng (Lê Trung; Dương Công Khánh; Phạm Bá Huy đều là học sinh THPT trên địa bàn tỉnh Quảng Trị) có hành vi Hack tài khoản Facebook và thực hiện hành vi lừa đảo nhắn tin mượn tiền đối với nhiều bị hại ở các địa phương khác trên cả nước (trong đó chị Hoàng Thị Hạnh, trú tại: phường Đống Đa, TP. Pleiku, tỉnh Gia Lai).

b. Lừa đặt cọc mua hàng nhằm chiếm đoạt tài sản

Đối tượng lập các trang mạng xã hội giả mạo các doanh nghiệp, công ty có hoạt động trên thực tế và giới thiệu, quảng cáo bán hàng và đưa ra các chương trình khuyến mại, giảm giá, hỗ trợ chi phí vận chuyển sau đó ác đối tượng đăng tin bán ô tô, xe máy, thiết bị điện tử, sắt thép… trên các trang mạng xã hội (Facebook, zalo,…) với số tiền thấp hơn giá trị thực rất nhiều và yêu cầu bị hại đặt cọc trước. Sau khi nhận được tiền đặt cọc bằng hình thức chuyển khoản trước từ người đặt mua hàng, đối tượng không giao hàng hoặc giao hàng giả, sau đó khóa trang mạng, cắt liên lạc, chiếm đoạt tài sản. Do tâm lý hám lợi, người dân đã gửi tiền vào tài khoản do đối

tượng cung cấp để nhận hàng. Ngay sau khi chiếm đoạt các đối tượng lập tức chuyển tiền vào các tài khoản ngân hàng có được do mua bán (tài khoản rác).

Công an tỉnh Gia Lai đã bắt giữu khởi tố 01 đối tượng trú tại huyện Đô Lương - tỉnh Nghệ An về tội "Lừa đảo chiếm đoạt tài sản" theo Điều 174, BLHS 2015(Bị hại trên địa bàn huyện Chư Pưh).

c. Lừa cho vay tiền qua mạng

Lợi dụng tâm lý muốn được vay vốn với số tiền lớn, lãi suất thấp, không cần thế chấp tài sản, thủ tục nhanh gọn, các đối tượng đã đăng tin cho vay vốn thông qua các ứng dụng, mạng xã hội như (Zalo, Facebook…). Sau khi tiếp cận được nạn nhân, các đối tượng yêu cầu nạn nhân tải các ứng dụng (app) vay tiền của chúng vào điện thoại của nạn nhân để thu thập thông tin cá nhân, danh bạ điện thoại. Tiếp theo, chúng yêu cầu nạn nhân chuyển tiền nhiều lần vào các tài khoản mà chúng cung cấp với các lý do như chuyển tiền để chứng minh tài chính, nộp tiền thuế khoản vay, chuyển tiền để bảo đảm hồ sơ vay, tài khoản yêu cầu vay bị sai hoặc thiếu thông tin; số tiền vay vượt quá định mức vay… Sau khi nạn nhân chuyển tiền thì các đối tượng nhanh chóng rút tiền khỏi tài khoản, khóa sim, cắt đứt liên lạc nhằm chiếm đoạt tài sản.

d. Giả danh cơ quan chức năng và sử dụng mạng xã hội để lừa đảo, chiếm đoạt tài sản.

Thủ đoạn gọi điện qua giao thức Internet (VoIP) đến số điện thoại của các bị hại tự xưng là nhân viên của công ty viễn thông để báo nợ tiền cước điện thoại; tự xưng là cán bộ Công an, cán bộ Viện kiểm sát thông báo bị hại có liên quan đến đường dây rửa tiền, buôn lậu ma túy mà Bộ Công an đang tiến hành điều tra; tham gia đầu tư APP; tuyển cộng tác viên....Sau đó đề nghị bị hại kê khai tài chính, tài sản, tiền mặt hiện có, tiền trong tài khoản ngân hàng đồng thời đe dọa yêu cầu cung cấp thông tin liên quan tài khoản ngân hàng để phục vụ cho công tác điều tra, xác minh, hoặc nộp thêm tiền để chứng minh thu nhập. Nhiều bị hại do tâm lý lo sợ dẫn đến lầm tưởng các đối tượng là cán bộ Công an, Viện kiểm sát thật và sợ ảnh hưởng đến uy tín, danh dự của cá nhân và gia đình nên đã cung cấp các thông tin theo yêu cầu của đối tượng, nộp tiền vào tài khoản theo yêu cầu của đối tượng và bị các đối tượng chiếm đoạt.

4. Thủ đoạn khác

a. Giả danh nhân viên ngân hàng tư vấn mở, huỷ thẻ tín dụng để chiếm đoạt tài sản trong tài khoản

Đối tượng giả danh là nhân viên các ngân hàng gọi điện đến cho nạn nhân có mở thẻ tín dụng tại các ngân hàng để tư vấn thủ tục hủy thẻ và bằng các thủ đoạn gian dối, các đối tượng yêu cầu nạn nhân cung cấp thông tin: họ tên, số thẻ tín dụng, mã xác thực OTP. Sau đó thực hiện các giao dịch rút tiền trong thẻ tín dụng của nạn nhân và chiếm đoạt.

Tháng 6/2022 Công an tỉnh Gia Lai đã điều tra làm rõ và khởi tố 01 vụ/03 bị can (trú tại TPHCM, BR-VT) về tội "Sử dụng mạng máy tính, mạng viễn thông, PTĐT thực hiện hành vi chiếm đoạt tài sản" theo Điều 290, BLHS 2015. Các đối tượng thực hiện hành vi lừa đảo với nhiều nạn nhân trên cả nước với số tiền chiếm đoạt lên đến hàng tỷ đồng (anh Lâm Tường Bảo Duy trú tại phường Hội thương). Trong vụ này phát hiện trên 1,4 triệu thông tin cá nhân bị lộ lọt, trong đó Gia Lai có trên 1.300 thông tin.

b. Giả mạo tin nhắn thương hiệu (SMS Brandname) của các ngân hàng thương mại để chiếm đoạt tài sản.

Đối tượng đã tạo tin nhắn SMS Brandname trùng với tên thương hiệu của các ngân hàng thương mại và chèn tin nhắn vào trong luồng tin nhắn chính thức làm cho khách hàng nhầm tưởng đây là tin nhắn chính thức của ngân hàng mà mình mở tài khoản. Nội dung tin nhắn mang tính chất cảnh báo như trừ tiền, cảnh báo mất tiền, đóng tài khoản... và đề nghị khách hàng truy cập vào đường link có sẵn trong tin nhắn để xử lý, khắc phục tránh hậu quả bị thiệt hại.

Sau đó nếu khách hàng click vào đường link giả mạo thì sẽ xuất hiện màn hình giao diện đăng nhập có hình thức tương tự như của trang web chính của ngân hàng mình đăng ký mở tài khoản, từ đó nhập thông tin tài khoản, mật khẩu đăng nhập Online, mã OTP xác thực giao dịch đăng nhập, mã OTP kích hoạt tính năng Smart OTP… Chính lúc này, đối tượng đã chiếm quyền kiểm soát tài khoản ngân hàng của khách hàng và thực hiện lệnh chuyển tiền đến các tài khoản ngân hàng khác và chiếm đoạt tài sản.

c. Lừa sang Campuchia lao động, làm "việc nhẹ, lương cao" nhưng thực chất là bị cưỡng bức lao động, cưỡng đoạt tài sản, nguy hiểm đến tính mạng.

Thông qua tìm kiếm việc làm trên mạng xã hội (Zalo, Facebook...) hoặc từ bạn bè, người quen rủ rê, giới thiệu sang Campuchia làm việc nhẹ nhàng, lương cao. Các nạn nhân bị lừa sang Campuchia làm việc chủ yếu trong độ tuổi từ 18-35 tuổi, đa số sau khi nhập cảnh trái phép qua Campuchia, nạn nhân bị đưa vào làm việc tại các cơ sở tổ chức hoạt động các hành vi lừa đảo trên không gian mạng; bị nhốt, cưỡng ép lao động từ 12-16 tiếng/ngày, không cho ra khỏi cơ sở, bị bán sang các chủ sử dụng lao động khác hoặc bắt gọi điện về cho gia đình, người thân tại Việt Nam để nộp tiền chuộc mới cho về nước với số tiền từ rất lớn. Nhiều trường hợp bỏ trốn khi chưa có tiền chuộc, đã bị các đối tượng sử dụng lao động đánh đập, ngược đãi, bán sang cơ sở khác nhau. Đối tượng cầm đầu hoạt động cưỡng bức lao động và đòi tiền chuộc, cưỡng đoạt tài sản là các đối tượng người Trung Quốc, có sự tham gia, giúp sức của các đối tượng người Việt hiện đang hoạt động tại Campuchia.

d. Mua bán thẻ ngân hàng để thực hiện việc chuyển tiền qua lại để chiếm đoạt tiền của các trang Web đánh bạc và tiền quảng cáo trên Google

Đối tượng lợi dụng sự thiếu hiểu biết về pháp luật của một bộ phận người dân, để yêu cầu lập và bán các thông tin tài khoản ngân hàng để đối tượng mua sử dụng vào các hành vi phạm tội..

Công an tỉnh Gia Lai đã tổ chức công tác điều tra, xác minh làm rõ nhóm đối tượng có hành vi mua, bán 23 thông tin tài khoản ngân hàng của các cá nhân cư trú tại Gia Lai và trong cả nước để thực hiện các giao dịch chuyển tiền bất thường (gần 20 tỷ đồng) trong thời gian ngắn. Đã khởi tố 01 vụ/02 bị can về tội "Thu thập, trao đổi, mua bán trái phép thông tin tài khoản ngân hàng" và "Tội trốn thuế" theo Điều 291 và Điều 200 BLHS 2015.

Nhóm đối tượng gồm 40 người đa phần là học sinh các trường phổ thông trên địa bàn thị xã An Khê có hành vi mua, bán thông tin tài khoản ngân hàng. Các đối tượng mua để chuyển tiền trong các trang Web đánh bạc.

MỘT SỐ BIỆN PHÁP PHÒNG NGỪA

Thứ nhất, tăng cường trau dồi kiến thức về pháp luật, chính sách, thường xuyên theo dõi các thông báo phương thức thủ đoạn phạm tội của cơ quan chức năng trên các phương tiện, thông tin đại chúng. Nghiên cứu, kiểm tra kỹ trước khi thực hiện các giao dịch về tài chính, đề phòng trước những khoản đầu tư mang lại "lợi nhuận cao". Đồng thời tích cực tuyên truyền về thủ đoạn lừa đảo của đối tượng để người thân, bạn bè, nhân dân biết phòng tránh.

Thứ hai, 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 biết rõ nhân thân và lai lịch của người đó, đặc biệt không nghe lời của các đối tượng chuyển tiền vào các tài khoản do các đối tượng 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.

Thứ ba, điện thoại di động, máy tính cá nhân cần sử dụng chế độ bảo mật nhiều lớp; thường xuyên kiểm tra và cập nhật các tính năng bảo mật, quyền riêng tư trên các tài khoản mạng xã hội, thường xuyên thay đổi để đảm bảo tính an toàn của mật khẩu, không truy cập các đường link lạ, tải và sử dụng các ứng dụng không rõ nguồn gốc. Chuyên viên các công ty tài chính, chứng khoán, phòng giao dịch ngân hàng cần có ý thức bảo mật thông tin trong quá trình thực hiện các giao dịch.

Thứ tư, người dân khi mua hàng qua mạng cần sàng lọc, kiểm tra kỹ thông tin

quảng cáo, rao bán về hàng hóa, danh tính người bán hàng, lựa chọn địa chỉ uy tín, hình thức thanh toán minh bạch. Không chia sẻ quá nhiều thông tin cá nhân trên mạng xã hội; không cho mượn, cho thuê các giấy tờ cá nhân có liên quan như: Căn cước công dân, giấy chứng minh nhân dân, sổ hộ khẩu, thẻ ngân hàng, không nhận chuyển khoản ngân hàng hoặc nhận tiền chuyển khoản của các ngân hàng cho người không quen biết.

Thứ năm, cảnh giác, không tin tưởng vào những chiêu trò nhận thưởng qua mạng mà yêu cầu nạp tiền 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 lớn, những món quà đắt tiền. Đối với các tin nhắn qua mạng xã hội, qua điện thoại người quen, bạn bè nhờ mua thẻ cào điện thoại, nhờ chuyển tiền hộ cần gọi điện trực tiếp để xác nhận thông tin với người nhờ, không nói chuyện qua tin nhắn.

Trường hợp có nghi ngờ về hoạt động lừa đảo chiếm đoạt tài sản, cần giữ tinh thần bình tĩnh, không thực hiện theo yêu cầu chuyển tiền do đối tượng đưa ra. Duy trì liên lạc với đối tượng, lưu giữ các thông tin liên quan như: Tin nhắn, hình ảnh, ghi âm đàm thoại, thông tin số điện thoại, tài khoản ngân hàng, tài khoản mạng xã hội, thông tin địa chỉ… của đối tượng liên quan. Nhanh chóng đến cơ quan Công an nơi gần nhất để trình báo để được tiếp nhận và hướng giải quyết.
