UBND XÃ THỐNG NHẤT
BAN CHỈ ĐẠO 138

Số: **55** /BCĐ

"V/v khuyến cáo thủ đoạn sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản"

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

Thống Nhất, ngày 12 tháng 7 năm 2022

Kính gửi:
- MTTQ và các đoàn thể xã;
- Các tổ chức Chính trị - Xã hội;
- Công chức Văn hóa - Xã hội xã;
- Trưởng các thôn trên địa bàn xã;
- Các cơ quan, đơn vị, doanh nghiệp, trường học trên địa bàn xã;
- Nhân dân trên địa bàn xã.

Theo thông báo của Công an thành phố, trong thời gian qua tình hình các đối tượng sử dụng công nghệ cao (không gian mạng) để thực hiện một số hành vi như kết bạn, làm quen trên mạng xã hội; Giả mạo hòm thư điện tử; Nhắn tin trúng thưởng; Giả danh người thân nhờ chuyển tiền rồi chiếm đoạt; Giả danh cán bộ Công an, Viện kiểm sát, Tòa án, cơ quan nhà nước...để thực hiện hành vi lừa đảo chiếm đoạt tài sản. Cá biệt có những vụ việc đối tượng là người nước ngoài kết bạn trên không gian mạng (facebook, zalo...) tán tỉnh, tạo niềm tin và đặt vấn đề tặng quà với giá trị lớn, người được tặng phải chuyển khoản một số tiền lớn cho đơn vị vận chuyển (là đồng bọn của đối tượng) thì mới nhận được quà, tiền. Qua đó đã có nhiều cá nhân tin tưởng đã chuyển số tiền lớn vào một số tài khoản do đối tượng yêu cầu.

Để chủ động phòng ngừa thủ đoạn sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản. Ban Chỉ đạo phòng chống tội phạm, tệ nạn xã hội và xây dựng phong trào toàn dân bảo vệ ANTQ (Ban Chỉ đạo 138/TN) khuyến cáo nhân dân một số biện pháp phòng ngừa như sau:

1. Kết bạn, làm quen trên mạng xã hội

- Đối tượng người nước ngoài (hoặc giả làm người nước ngoài) sử dụng mạng xã hội như Facebook, Zalo... kết bạn làm quen với người bị hại, dùng nhiều thời gian trò chuyện để tạo sự tin tưởng.

- Sau 1 thời gian thông báo gửi quà là tiền mặt hoặc tài sản có giá trị lớn.

- Đối tượng người Việt Nam giả danh nhân viên sân bay, hải quan, thuế... yêu cầu người bị hại nộp tiền để được nhận quà ->tạo nhiều lý do để bị hại nộp tiền nhiều lần. Cắt đứt liên lạc khi hết nguồn tiền hoặc bị nghi ngờ.

* **KHUYẾN CÁO:** Có thể quen biết, kết bạn với người nước ngoài qua mạng xã hội nhưng không nên gửi, chuyển tiền để đóng các loại phí vào tài khoản ngân hàng do đối tượng cung cấp với bất kỳ lý do gì.

2. Gọi điện thoại mời đổi sim 4G

- Đối tượng mạo danh nhân viên chăm sóc khách hàng, gợi ý và yêu cầu bị hại bấm dãy số: **21* số điện thoại hoặc nhắn tin theo cú pháp DSxxxx để được đổi sim 4G với ưu đãi hấp dẫn.

- Đây là cách chuyển cuộc gọi và đổi sim sang phôi trắng, nếu làm sẽ bị mất quyền kiểm soát số điện thoại. Đối tượng sử dụng số điện thoại chiếm đoạt được để thao tác chuyển tiền trong tài khoản, ví điện tử của bị hai

* **KHUYẾN CÁO:** Nếu có nhu cầu đổi sim 4G thì trực tiếp ra cửa hàng để thực hiện.

3. Giả mạo hòm thư điện tử

- Đối tượng lập các hộp thư điện tử tương tự hộp thư điện tử của các tổ chức, cá nhân kinh doanh, sản xuất có thực hiện giao dịch bằng thư điện tử.

- Mạo danh đối tác để đề nghị tổ chức, cá nhân chuyển tiền thanh toán hợp đồng vào tài khoản ngân hàng của đối tượng để chiếm đoạt.

* **KHUYẾN CÁO:** Nên kiểm tra trực tiếp với đối tác trước khi thực hiện việc chuyển tiền

4. Nhắn tin trúng thưởng

Đối tượng sử dụng Facebook để gửi tin nhắn cho bị hại thông báo trúng thưởng tài sản hoặc tiền mặt có giá trị lớn. Yêu cầu người bị hại nạp tiền qua thẻ điện thoại hoặc chuyển khoản qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Hoặc hướng dẫn truy cập vào các đường link gửi kèm để khai báo thông tin nhận thưởng.

* **KHUYẾN CÁO**

- Không thực hiện chuyển tiền hay nạp tiền qua thế điện thoại vì lý do nhận thưởng.

- Không truy cập vào các đường link được gắn kèm trong tin nhắn lạ, không thực hiện thao tác trên điện thoại theo cú pháp được hướng dẫn bởi người lạ.

- Tuyệt đối không cung cấp mã OTP cho người khác khi sử dụng tài khoản ngân hàng.

5. Tuyển cộng tác viên online

Đối tượng mạo danh nhân viên của các trang thương mại điện tử để lôi kéo cộng tác viên bản hàng online với hoa hồng hấp dẫn. Yêu cầu cộng tác viên phải thanh toán tiền đơn hàng trước mới được nhận tiền gốc và hoa hồng. Thanh toán cho cộng tác viên từ 1-3 đơn hàng có giá trị thấp. Dụ dỗ, mời cộng tác viên tham gia, chuyển khoản để mua các đơn hàng có giá trị cao rồi chiếm đoạt tiền.

* **KHUYẾN CÁO**: Nên kiểm tra kỹ các thông tin trước khi nhận làm cộng tác viên hoặc trước khi chuyển tiền.

6. Kinh doanh đa cấp qua các sàn giao dịch tiền ảo, sàn ngoại hối.. hoặc đầu tư đào tiền kỹ thuật số

Đối tượng lập ra các website tài chính, ứng dụng có giao diện tương tự sàn đầu tư tài chính quốc tế rồi lôi kéo người tham gia. Cam kết người chơi có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian, nếu kêu gọi được thêm người sẽ có hoa hồng. Sau 1 thời gian sàn thông báo dừng hoạt động để bảo trì hoặc lỗi không truy cập được. Khách hàng không đăng nhập được để rút tiền hoặc mất hết tiền kỹ thuật số trong tài khoản.

* **KHUYẾN CÁO:** Không tham gia vào các sàn giao dịch tiền ảo, tiền ngoại hối khi mình không hiểu rõ, không có kiến thức về loại hình này.

7. Bán hàng lừa đảo

- Đối tượng giả dạng nhân viên bán hàng chào mời mua các loại sản phẩm.

- Yêu cầu đặt cọc trước một nửa số tiền, hôm sau sẽ giao hàng. Sau đó chiếm đoạt số tiền trên, không còn liên lạc được nữa.

- Đối tượng quảng bá sản phẩm trên mạng, thu hút nhiều người theo dõi, nhiều lượt like, bình luận... nhưng khi chuyển hàng không đảm bảo chất lượng.

* **KHUYẾN CÁO:** Khi trao đổi, mua bán trực tuyến, qua các trang mạng xã hội phải tìm hiểu rõ nguồn gốc, hạn chế mua các đồ vật có giá trị lớn. Có thể dùng phương thức kiểm tra hàng xong mới trả tiền.

8. Giả danh người thân nhờ chuyển tiền rồi chiếm đoạt

Đối tượng lập tài khoản mạng xã hội, hoặc chiếm quyền quản trị tài khoản mạng xã hội (hack) của người khác. Nhắn tin cho người thân, bạn bè trong danh sách liên lạc hỏi vay tiền, hoặc nhờ chuyển tiền. Khi người thân gọi lại bằng video thì hình ảnh nhòa và nhiễu, sau đó bị tắt ngay do mất sóng.

* **KHUYẾN CÁO:** Gọi điện trực tiếp cho người thân để xác minh trước khi chuyển tiền (gọi số sim, không gọi qua các ứng dụng mạng).

9. Kiếm tiền online qua app

- Đối tượng lập ra các app kiếm tiền online (như: Pchome, Shopping Mall, Tailoc888) mời tham gia trò chơi, giật đơn hàng.Người chơi nạp tiền lần 1 và lần 2 (mỗi lần từ 500 nghìn đồng đến 1,5 triệu đồng) sẽ được chuyển lại tài khoản liên kết và lãi ngay 20%. Từ lần 3 trở đi sẽ được báo trúng đơn hàng từ 20 triệu trở lên và chuyển tài khoản lần nào mất tiền lần đó.

- Hoặc người chơi đăng ký tài khoản trên trang web, nạp tiền theo 9 mức từ 180.000đ đến 99.000.000đ. Sau đó mua các gói đầu tư từ 180.000đ đến 540.000đ để hưởng lãi suất từ 20 - 55% mỗi ngày. Một thời gian sau đối tượng đánh sập hệ thống và chiếm đoạt tiền.

* **KHUYẾN CÁO:** Không tham gia vào các app kiếm tiền online.

10. Vay tiền qua app

Mạo danh ngân hàng, nhân viên ngân hàng, công ty tài chính đăng tải thông tin hỗ trợ vay tiền trực tuyến, giải ngân nhanh trên mạng xã hội với thủ tục nhanh gọn, không cần chấp nhận tài sản. Hướng dẫn người dùng truy cập vào trang web hoặc ứng dụng điện thoại để làm thủ tục. Thông báo người dân cung cấp sai thông tin

nên hệ thống báo lỗi không thể giải ngân. Đề nghị bị hại nộp các khoản tiền để làm thủ tục vay và dùng số tiền

* **KHUYẾN CÁO:** Không vay tiền trực tuyến từ các ứng dụng không rõ nguồn gốc. Nếu có nhu cầu vay tiền thì liên hệ và đến trực tiếp ngân hàng, tổ chức tín dụng gần nhất để được hỗ trợ.Tuyệt đối không cung cấp OTP mã hóa cho người khác khi sử dụng hàng ngân khoản.

11. Giả danh cán bộ Công an, Viện kiểm sát, Tòa án, cơ quan nhà nước

- Đối tượng thông báo bị hại liên quan đến vụ án đang điều tra, rồi nối máy đến đối tượng khác giả danh người của cơ quan tư pháp để khai thác thông tin cá nhân và tài khoản ngân hàng.

- Đối tượng tự xưng là nhân viên bưu điện thông báo bị hại đang nợ tiền cước điện thoại hoặc có bưu phẩm lâu ngày không đến nhận.

- Đối tượng thông báo bị hại thiếu nợ tiền ngân hàng do người khác lấy CMND đăng ký mở tài khoản ngân hàng.

- Điện thoại thông báo có giao dịch chuyển tiền vào tài khoản nhưng bị treo, yêu cầu cung cấp thông tin đăng nhập, mật khẩu và mã OTP để nhận tiền. Yêu cầu bị hại chuyển tiền vào tài khoản chỉ định để kiểm tra nguồn gốc rồi sẽ trả lại hoặc đe dọa nếu không chuyển tiền sẽ bắt tạm giam. Hướng dẫn bị hại tải phần mềm "Bộ Công an" giả mạo để cung cấp thông tin sau đó chiếm quyền sử dụng tài khoản.

* **KHUYẾN CÁO**: Cơ quan Công an, Viện kiểm sát, Tòa án không yêu cầu phải chuyển tiền vào tài khoản cá nhân vì bất cứ lý do gì. Mọi trường hợp đều làm việc tại trụ sở cơ quan nhà nước. Khi có số điện thoại lạ liên lạc, thông báo có liên quan đến tội phạm và yêu cầu cung cấp thông tin cá nhân hoặc chuyển tiền, thì tuyệt đối không chuyển tiền, thông báo cho người thân trong gia đình và nhanh chóng trình báo với cơ quan công an gần nhất để kịp thời phối hợp xử lý. Không cung cấp thông tin cá nhân cho người không quen biết, yêu cầu được làm việc trực tiếp."

12. Hành vi giả chuyển tiền vào tài khoản của cá nhân rồi gọi điện xin lại

- Dấu hiệu hành vi: Đối tượng dùng một số tài khoản X để chuyển một số tiền nhất định với giá trị lớn (thường khoảng 20 triệu đến 40 triệu) với nội dung chuyển khoản "Cho anh (chị) A vay; Trả nợ anh (chị) B.... rồi cho một đối tượng khác (đồng bọn) gọi điện cho bị hại báo chuyển nhầm và xin lại số tiền trên vào tài khoản Y. Sau khi bị hại chuyển trả số tiền thì đối tượng chủ tài khoản X gọi điện thông báo chuyển nhầm và yêu cầu chuyển tiền trả lại vào tài khoản X, nếu không chuyển sẽ khởi kiện ra Tòa án.

* **KHUYẾN CÁO:** Khi có một số tiền nhất định chuyển vào tài khoản cá nhân mà không rõ nguồn gốc, lý do. Khẩn trương đến đơn vị Ngân hàng gần nhất để thông tin về số tiền trong tài khoản và nhờ sự trợ giúp của Ngân hàng trong việc quản lý, giao dịch đối với số tiền trên. Không tự ý chuyển cho bất kỳ số tài khoản nào khi không biết rõ là ai.

Mọi người dân khi phát hiện các dấu hiệu hành vi, thủ đoạn nêu trên, chủ động liên hệ Công an nơi gần nhất hoặc đồng chí Trung tá Đàm Quang Toàn, Đội trưởng Đội Cảnh sát Hình sự, Công an thành phố Hạ Long (SĐT 0936871999) để được hướng dẫn xử lý.

Để làm tốt công tác phòng ngừa tội phạm sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản và đảm bảo mọi người dân nắm được nội dung trên, Ban Chỉ đạo 138/TN đề nghị MTTQ, các đoàn thể, tổ chức Chính trị - Xã hội, công chức Văn hóa - Xã hội, các cơ quan, đơn vị, doanh nghiệp, trường học, Trưởng các thôn trên địa bàn xã tăng cường công tác tuyên truyền trên hệ thống loa phát thanh, lồng ghép các cuộc họp, sinh hoạt, giao ban cơ quan đơn vị, đồng thời tổ chức in ấn Khuyến cáo này phát cho các hộ gia đình trên địa bàn biết, nâng cao tinh thần cảnh giác và phòng ngừa./.

Nơi nhận:
- Như kính gửi;
- Đ/c Trưởng Ban Chỉ đạo 138/TN;
- Lưu VT.

TM. BAN CHỈ ĐẠO
KT. TRƯỞNG BAN
PHÓ BAN THƯỜNG TRỰC

CÔNG AN THÀNH PHỐ HẠ LONG - T. QUẢNG NINH
CÔNG AN XÃ THỐNG NHẤT

TRƯỞNG CÔNG AN XÃ
Thiếu tá Nguyễn Tiến Hưng