BỘ CÔNG AN
CÔNG AN TỈNH TIỀN GIANG

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

Tiền Giang, ngày 25 tháng 12 năm 2023

Số: 6320 /CAT-ANM

Về việc tăng cường công tác tuyên truyền phòng, chống lừa đảo trên không gian mạng

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

Thời gian quan, công tác đấu tranh phòng, chống tội phạm trên không gian mạng có nhiều chuyển biến tích cực, các ngành, các cấp đã chung tay vào cuộc, thực hiện nhiều giải pháp để ngăn chặn, phòng ngừa tội phạm; các cơ quan truyền thông đẩy mạnh công tác tuyên truyền phổ biến thường xuyên các hành vi, thủ đoạn của tội phạm. Ngành Công an tăng cường thực hiện các mặt công tác nghiệp vụ, đẩy mạnh công tác điều tra xử lý các vụ việc đã xảy ra, làm rõ xử lý được nhiều vụ việc vi phạm pháp luật. Qua đó đã góp phần ngăn ngừa, phòng, chống tội phạm hoạt động trên không gian mạng từng bước mang lại hiệu quả tích cực hơn.

Tuy nhiên, từng lúc, từng nơi tội phạm hoạt động trên không gian mạng còn diễn biến phức tạp, đại đa số cán bộ, công chức và nhân dân đã biết được một số thủ đoạn hoạt động phổ biến của tội phạm, nhưng vẫn bị mắc bẫy, nhất là thủ đoạn lừa đảo chiếm đoạt tài sản qua không gian mạng.

Để góp phần nâng cao hiệu quả công tác phòng chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, Công an tỉnh Tiền Giang kính đề nghị lãnh đạo các sở, ban, ngành, đoàn thể, UBND các huyện, thành phố, thị xã:

1. Tổ chức tuyên truyền trong cán bộ, công chức viên chức và nhân dân các thủ đoạn lừa đảo qua không quan mạng (gởi kèm).

2. Tuyên truyền trong cán bộ, công chức viên chức và nhân dân

- Bảo vệ thông tin cá nhân bằng cách hạn chế chia sẻ thông tin (Chứng minh nhân dân/Căn cước công dân, địa chỉ, số điện thoại, hình ảnh nhận diện khuôn mặt, tài khoản ngân hàng…), hình ảnh con cái… trên mạng xã hội hoặc các nền tảng trực tuyến.

- Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ hoặc không rõ nguồn gốc. Không đăng nhập tài khoản cá nhân vào những địa chỉ này.

- Tuyệt đối không cung cấp tên đăng nhập, mật khẩu ứng dụng, mã xác thực OTP, email… cho bất kỳ ai kể cả khi người đó tự xưng là nhân viên ngân hàng, cơ quan nhà nước.

- Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại Cổng không gian mạng quốc gia (khonggianmang.vn). Nếu phát hiện bất kỳ ứng dụng, website có dấu hiệu lừa đảo nào, thông báo ngay cho Trung tâm giám sát an toàn không gian mạng quốc gia tại địa chỉ https://canhbao.khonggianmang.gov.vn để ngăn chặn, xử lý.

- Nhanh chóng trình báo cơ quan Công an nơi gần nhất khi phát hiện thủ đoạn mạo danh, lừa đảo chiếm đoạt tài sản hoặc bị mạo danh, lừa đảo chiếm đoạt tài sản.

Rất mong được sự phối hợp của các đồng chí./.

Nơi nhận:
- Như trên;
- Cục ANM và PCTP SDCNC;
- BGĐ Công an tỉnh;
- Các đơn vị, địa phương;
- Lưu: VT, Đội 1, An 85b

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Phan Văn Trắng

CÁC THỦ ĐOẠN LỪA ĐẢO QUA KHÔNG GIAN MẠNG

1. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao

Dấu hiệu nhận diện: Các đối tượng mạo danh là cán bộ của cơ quan quản lý Nhà nước hoặc nhà mạng gọi điện và thông báo số điện thoại sẽ bị khóa 2 chiều trong 2 tiếng với các lý do như "chưa nộp phạt", "thuê bao sai thông tin"...

Biện pháp phòng tránh: Người dùng không thực hiện theo các yêu cầu khi nghe cuộc gọi từ số điện thoại lạ; kiểm tra lại thông tin sim thông qua các công cụ, hướng dẫn từ nhà mạng hoặc các điểm giao dịch nhà mạng.

2. Lừa đảo tuyển dụng CTV online "việc nhẹ lương cao"

Dấu hiệu nhận diện: Giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn quảng cáo công việc quá hấp dẫn và dễ dàng, mà không yêu cầu kỹ năng hay kinh nghiệm đặc biệt; yêu cầu bị hại tạm ứng tiền trước khi bắt đầu công việc.

Biện pháp phòng tránh: Không nghe, thực hiện theo "quảng cáo" của đối tượng. Không thực hiện khi thiếu thông tin công ty hoặc không có thông tin liên hệ; thiếu hợp đồng hoặc thoả thuận rõ ràng được ký kết hợp pháp.

3. Giả danh Giáo viên/Nhân viên y tế báo người thân đang cấp cứu

Dấu hiệu nhận biết: Số điện thoại lạ gọi đến tự xưng là Giáo viên/ Nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con em/ người thân họ đang cấp cứu trong tình trạng nguy kịch. Một số đối tượng còn thuộc lòng thông tin về trường, lớp học của con, tên giáo viên chủ nhiệm, thầy cô, hiệu trưởng khiến phụ huynh nhất thời tin tưởng.

Biện pháp phòng tránh: Khi nhận các cuộc điện thoại, tin nhắn, người dân hỏi thông tin con em/ người thân nằm viện ở đâu; không trả lời câu hỏi đối tượng tìm hiểu về con em/ người thân. **Tuyệt đối không làm theo yêu cầu của đối tượng về chuyển tiền**. Tiếp theo cần điện thoại ngay cho giáo viên chủ nhiệm lớp; người thân; đến bệnh viện tìm hiểu.

4. Đánh cắp tài khoản mạng xã hội, nhắn tin lừa đảo

Dấu hiệu nhận diện: Khi nhận được một tin nhắn hoặc email từ một người bạn trong danh sách bạn bè yêu cầu chuyển tiền. Tin nhắn có sự thay đổi đột ngột trong cách xưng hô, cách viết.

Biện pháp phòng tránh: Thay đổi mật khẩu ngay lập tức của tài khoản mạng xã hội và sử dụng một mật khẩu có độ bảo mật cao, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. 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.

5. Giả danh cơ quan Công an, Viện kiểm sát, Tòa án gọi điện lừa đảo

Dấu hiệu nhận biết: Đối tượng giả danh cơ quan Công an, Viện kiểm sát, Tòa án để gọi điện thông báo nạn nhân gây tai nạn giao thông bỏ trốn, có quyết định khởi tố của Tòa án, có liên quan đến các vụ án đang điều tra … Sử dụng các cách thức đe dọa, áp lực tâm lý như khống chế, hăm dọa. Đối tượng yêu cầu nạn nhân chuyển tiền vào một tài khoản cụ thể hoặc cung cấp thông tin cá nhân như số thẻ tín dụng, số căn cước công dân, mã số bảo mật và các thông tin nhạy cảm khác. Điều này nhằm mục đích chiếm đoạt tài sản của nạn nhân. Yêu cầu nạn nhân phải thực hiện ngay lập tức để tránh hậu quả nghiêm trọng. Đối tượng thuyết phục nạn nhân, liên tục thúc giục nạn nhân không có thời gian để suy nghĩ hay tham khảo người khác.

Biện pháp phòng tránh: **Không thực hiện theo yêu cầu của đối tượng vì** cơ quan quản lý nhà nước sẽ không yêu cầu tổ chưc, cá nhân chuyển tiền hoặc cung cấp thông tin nhạy cảm qua điện thoại một cách đột ngột mà không có văn bản thông báo trước.

6. Giả mạo biên lai chuyển tiền thành công

Dấu hiệu nhận diện: Thủ đoạn của các đối tượng lừa đảo là mua hàng số lượng lớn, sau đó vay thêm tiền mặt của nạn nhân rồi chuyển khoản trả.

Biện pháp phòng tránh: Người dân nếu sử dụng giao dịch qua tài khoản ngân hàng cần lưu ý kỹ hóa đơn chuyển khoản, không giao hàng hóa cho bất kỳ ai khi chưa nhận được tiền trong tài khoản ngân hàng, kể cả khi kẻ gian cung cấp hình ảnh đã chuyển khoản thành công.

7. Giả danh các Công ty tài chính, Ngân hàng thu thập thông tin

Dấu hiệu nhận biết: Đánh vào tâm lý của những người đang cần tiền kinh doanh, tiêu xài, muốn được vay với số tiền lớn nhưng lại gặp khó do dính nợ xấu hoặc không đủ điều kiện vay vốn tại các tổ chức tài chính. Hình thức cho vay tín chấp với lãi suất thấp (chỉ 1%/ tháng), thủ tục vay đơn giản, không cần gặp trực tiếp; nợ xấu vẫn vay được; không thế chấp, không thẩm định, chỉ cần Chứng minh nhân dân hoặc Căn cước công dân và có tài khoản ngân hàng/thẻ ATM là có thể vay được tiền... Các ứng dụng vay tiền trực tuyến hay các link quảng cáo cờ bạc, cá độ thường được quảng cáo rộng rãi trên các trang web với những tiêu đề thu hút như "*Không cần thế chấp, lãi suất không đồng", "Vay siêu tốc, nhận tiền sau 30 phút, lãi suất thấp, nhận tiền ngay*"… hoặc nhắn tin qua số điện thoại kèm theo đường link đến ứng dụng…Tuy nhiên, khi xong thủ tục thì tài khoản thấy có tiền

chuyển đến nhưng không thể rút được, đối tượng sẽ yêu cầu đóng thuế, chứng minh tài khoản… ***vừa không vay được tiền ngược lại còn bị mất tiền.***

Biện pháp phòng tránh: Khi có nhu cầu vay tiền, cần liên hệ trực tiếp với các tổ chức tín dụng, chi nhánh ngân hàng để được tư vấn, hướng dẫn làm thủ tục vay vốn. Tuyệt đối không vay qua các trang này.

8. Lừa đảo đầu tư chứng khoán quốc tế, tiền ảo

Dấu hiệu để nhận diện: Sàn đầu tư lừa đảo thường hứa lợi nhuận vượt trội, không thể tin được và quá cao so với thị trường thực tế; Không cung cấp đầy đủ thông tin về công ty, giấy phép hoạt động, lịch sử giao dịch và nhân sự quản lý; Yêu cầu người tham gia chuyển khoản tiền trước khi bắt đầu giao dịch, thường là dưới hình thức phí đăng ký, phí tham gia hoặc tiền ký quỹ; Không có sự kiểm soát từ các cơ quan quản lý hoặc không được cấp phép hoạt động đúng quy định.

Biện pháp phòng tránh: Chỉ tin tưởng vào các nền tảng và sàn giao dịch có uy tín và được xác thực. Đối với các sàn giao dịch và công ty trực tuyến, hãy tìm hiểu về hệ thống bảo mật và cơ chế bảo vệ thông tin cá nhân và tài sản của người dùng. Hãy cẩn trọng với các khoản phí và chi phí không rõ ràng hoặc quá cao so với thị trường thông thường.

9. Lừa đảo "chuyển nhầm tiền" vào tài khoản ngân hàng

Dấu hiệu để nhận diện: Tài khoản nạn nhân sẽ nhận một số tiền lớn nhưng không biết người gửi. Đối tượng giả danh người chuyển nhầm tiền yêu cầu nạn nhân chuyển trả lại số tiền trên; khi nạn nhân chuyển trả lại, sẽ có đối tượng khác điện thoại đến là báo là thu hồi nợ.

Biện pháp phòng tránh: Khi tài khoản nhận số tiền lớn không rõ nguồn gốc thì nạn nhân nên báo ngay với Ngân hàng nơi mở tài khoản về số tiền trên. Giữ nguyên số tiền trong tài khoản, không chuyển cho bất kỳ ai điện thoại đến yêu cầu, trừ khi cá nhân chuyển nhầm yêu cầu Ngân hàng chuyển lại và nạn nhân giao dịch trực tiếp với Ngân hàng.

10. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa; lấy lại Facebook

Dấu hiệu nhận biết: Kẻ lừa đảo sẽ đăng quảng cáo, nhắn tin trên các mạng xã hội về **"dịch vụ lấy lại tiền khi đã bị lừa", "lấy lại Facebook"** với thông tin số điện thoại, mạng xã hội. Tuy nhiên, khi nhắn tin hoặc điện thoại lại thì kẻ lừa đảo sẽ yêu cầu đóng phí, các khoảng thuế… nạn nhân sẽ tiếp tục bị mất tiền.

Biện pháp phòng tránh: Chỉ có cơ quan pháp luật mới có quyền phong tỏa tài khoản để lấy lại tiền đã bị lừa đảo chuyển đến tài khoản; các tổ chức, cá nhân khác không thực hiện được. Facbook có chế độ bảo mật do cá nhân thiết lập từ

ban đầu; Facebook không bao giờ yêu cầu bạn cung cấp thông tin đăng nhập của mình thông qua email, tin nhắn hoặc các hình thức liên lạc khác.

11. Lừa đảo tình cảm

Dấu hiệu nhận diện: Kẻ lừa đảo tạo một hồ sơ giả mạo, sử dụng hình ảnh đánh cắp của người khác với ngoại hình đẹp và lôi cuốn, sau đó sử dụng các chiêu trò như tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa. Dẫn dụ nạn nhân gửi hình ảnh video nhạy cảm (sau đó dùng những hình ảnh này để đe dọa, tống tiền nạn nhân). Thuyết phục nạn nhân tham gia đầu tư vào thị trường tài chính Forex thông qua một sàn giao dịch giả mạo mà kẻ lừa đảo kiểm soát sau đó chiếm đoạt số tiền đầu tư. Hứa gửi hàng bưu kiện có giá trị và bắt đóng tiền thuế bằng cách gửi tiền vào tài khoản kẻ lừa đảo. Kẻ lừa đảo có thể đe dọa hoặc lừa đảo nếu nạn nhân không tuân thủ yêu cầu.

Biện pháp phòng tránh: Không tin tưởng vào một người mới gặp qua mạng xã hội hoặc các nền tảng trực tuyến khác. Cần xác minh danh tính của họ bằng cách tìm hiểu về họ, yêu cầu thông tin địa chỉ nhà, số điện thoại liên hệ hoặc thậm chí gặp gỡ trực tiếp nếu có thể. Cảnh giác với những yêu cầu gửi tiền, đầu tư vào Forex hoặc tham gia các giao dịch tài chính không rõ nguồn gốc. Trước khi nhận hàng bưu kiện của một người không quen biết, hãy kiểm tra và xác minh thông tin về địa chỉ, tên và các chi tiết khác.

12. Lừa đảo trúng thưởng

Dấu hiệu nhận diện: Nếu nhận được một cuộc gọi thông báo trúng thưởng một giải thưởng lớn và yêu cầu cung cấp thông tin cá nhân nhạy cảm hoặc chuyển khoản tiền để nhận giải thưởng.

Biện pháp phòng tránh: Hãy luôn nhớ rằng không có ai trúng thưởng mà không tham gia hoặc không có cách để trúng thưởng mà không phải trả phí. Tuyệt đối không cung cấp thông tin cá nhân, chuyển tiền theo yêu cầu của đối tượng dẫn đến bị lừa./.