UBND TỈNH CÀ MAU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 73 /STTTT-TTBCXB

V/v tuyên truyền nâng cao cảnh giác trước những thủ đoạn lừa đảo trên không gian mạng

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

Cà Mau, ngày 10 tháng 01 năm 2025

Kính gửi:
- Báo Cà Mau;
- Đài Phát thanh - Truyền hình Cà Mau;
- Các cơ quan báo chí thường trú tại tỉnh Cà Mau;
- Cổng Thông tin điện tử tỉnh;
- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, TP Cà Mau.

Hiện nay, các quy định về dịch vụ internet, mạng viễn thông khuyến khích và tạo thuận lợi cho nhân dân đăng ký, sử dụng các giao dịch tài chính, ngân hàng, thương mại điện tử để phát triển kinh tế - xã hội của đất nước, nhưng đây cũng là điều kiện để tội phạm lợi dụng lừa đảo chiếm đoạt tài sản... Đối tượng xấu khai thác điểm yếu về dân trí và sự thiếu thông tin, tâm lý chủ quan, cả tin, nhẹ dạ của người dân để thực hiện hành vi lừa đảo, giả danh cơ quan pháp luật, cán bộ nhà nước, giả danh khách hàng mua bán hàng trực tuyến, hack tài khoản, kết bạn làm quen trên mạng xã hội, tuyển cộng tác viên qua mạng. Các đối tượng còn tinh vi hơn khi sử dụng công nghệ để làm giả hình ảnh, giọng nói người quen của bị hại tham gia mạng xã hội để lừa đảo chiếm đoạt tài sản. Không chỉ riêng đồng bào ở những nơi khó khăn, kể cả những người có nhận thức nhất định cũng vẫn có thể bị lừa.

Sở Thông tin và Truyền thông đề nghị các cơ quan báo chí, Cổng/Trang thông tin điện tử các sở ngành, địa phương và hệ thống thông tin cơ sở trong tỉnh đẩy mạnh thông tin tuyên truyền để mọi người đề cao cảnh giác, tránh bị lừa khi gặp các thủ đoạn dưới đây:

(1) Giả danh các nhà mạng gọi điện thông báo số thuê bao điện thoại của bạn đã trúng thưởng tài sản có giá trị lớn; để nhận được tài sản đó phải mất phí, nếu đồng ý thì mua thẻ cào nạp vào số tài khoản mà các đối tượng lừa đảo cung cấp. Khi người dân đóng tiền để nhận thưởng thì chặn liên lạc và chiếm đoạt số tiền đó.

(2) Giả danh là cán bộ Ngân hàng gọi điện thông báo có người chuyển tiền vào tải khoản nhưng do bị lỗi nên chưa chuyển được hoặc thông báo phần mềm chuyển tiền của khách hàng bị lỗi... và yêu cầu khách hàng cung cấp mã số thẻ, mã OTP để kiểm tra. Qua đó các đối tượng sử dụng thông tin bị hại cung cấp để truy cập vào tài khoản và rút tiền.

(3) Giả danh Công an, Tòa án… gọi điện thông báo có liên quan đến vụ án hoặc xử phạt nguội vi phạm giao thông, yêu cầu chuyển tiền vào tài khoản mà chúng đưa ra để phục vụ công tác điều tra, xử lý. Khi người dân lo sợ và chuyển tiền vào tài khoản được yêu cầu thì các đối tượng chuyển tiếp số tiền đó vào nhiều tài khoản khác và chiếm đoạt.

(4) Giả mạo tuyển cộng tác viên, bằng thủ đoạn lập các trang facebook giả mạo các nhãn hàng, trang thương mại điện tử như Tiki.vn, Lazada, TokyoLive, Shopee… và chạy quảng cáo, khi bị hại nhắn tin hỏi cách thức làm cộng tác viên, các đối tượng sẽ gửi các thông tin về công ty, nhân viên chăm sóc khách hàng... đồng thời, yêu cầu gửi thông tin cá nhân, kết bạn zalo để tư vấn. Ban đầu, đối tượng gửi đường dẫn các sản phẩm có giá trị nhỏ khoảng vài trăm ngàn đồng để bị hại chọn và xác thực đơn, chụp ảnh đơn hàng gửi cho đối tượng qua Zalo, Facebook chuyển tiền vào các tài khoản do đối tượng cung cấp và được đối tượng chuyển lại toàn bộ số tiền đã bỏ ra mua hàng cùng với hoa hồng từ 3-20%. Sau vài lần tạo niềm tin bằng cách trả gốc và hoa hồng như cam kết ban đầu, đối tượng viện lý do là "bạn đã được công ty nâng hạng", gửi các đường dẫn sản phẩm trên sàn Lazada, Shopee... có giá trị lớn hơn và tiếp tục yêu cầu bị hại chụp lại hình ảnh sản phẩm đồng thời chuyển tiền. Khi đã nhận được, đối tượng không chuyển tiền mà thông báo cho cộng tác viên phải tiếp tục thực hiện nhiệm vụ khác thì mới được chuyển lại tiền và hoa hồng (thực chất là tiếp tục chuyển tiền vào tài khoản đối tượng). Sau đó, các đối tượng chiếm đoạt tiền của bị hại.

(5) Mời chào, lôi kéo tham gia đầu tư vào các sàn giao dịch tiền ảo… tự thiết lập, cam kết sẽ hưởng lợi nhuận cao khi tham gia hệ thống. Các đối tượng thường quảng bá, đánh bóng tên tuổi bằng cách đăng tin, bài trên mạng xã hội, tổ chức các buổi hội thảo, gặp mặt offline, tự nhận là chuyên gia đầu tư, người truyền cảm hứng, người dẫn đường... để lừa đảo, kêu gọi đầu tư vào hệ thống. Khi huy động được lượng tiền đủ lớn, các đối tượng sẽ can thiệp vào các giao dịch báo lỗi, ngừng hoạt động (sập sàn) để chiếm đoạt tiền của người tham gia.

(6) Mạo danh lãnh đạo các cơ quan chính quyền, đoàn thể... để thiết lập tài khoản mạng xã hội (Zalo, Facebook...). Sau đó, 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. Đối tượng lừa đảo sử dụng hack (chiếm đoạt quyền điều khiển) tài khoản mạng xã hội, tạo ra kịch bản nhắn tin lừa đảo đến bạn bè của chủ tài khoản mạng xã hội và chiếm đoạt tiền của các bị hại chuyển đến tài khoản ngân hàng do các đối tượng chỉ định.

(7) Lập ra các trang trên mạng xã hội chạy quảng cáo để tiếp cận. Sau khi tiếp cận được nạn nhân, các đối tượng sẽ gửi các đường link kết nối với CH Play để các bị hại cài đặt ứng dụng vào điện thoại và làm theo ứng dụng (app). Khi bị hại đăng nhập app để vay tiền thì app sẽ báo lỗi, các đối tượng yêu cầu bị hại phải chuyển tiền đặt cọc để mở lại app thì mới giải ngân được (sau khi giải ngân thì sẽ trả lại tiền cọc và tiền cho vay) hoặc yêu cầu nạn nhân mua bảo hiểm khoản vay, đóng tiền phí giải ngân... Nhiều bị hại thực hiện chuyển nhiều lần để được vay cho đến khi nghi ngờ bị lừa không chuyển nữa thì các đối tượng lừa đảo thông báo nếu không chuyển tiếp sẽ không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

(8) Lập các tài khoản mạng xã hội giả để đăng tin trên các trang, hội nhóm... đăng bán vé máy bay cho người dân có nhu cầu từ nước ngoài về nước. Khi bị hại hỏi mua, thỏa thuận xong giá cả thì các đối tượng yêu cầu thanh toán và đồng

thời gửi cho khách hàng các hình ảnh giả về vé máy bay do các đối tượng tự tạo ra, sau đó chiếm đoạt số tiền bị hại thanh toán.

Để không bị lừa qua mạng xã hội, người dùng cần cảnh giác đối với những trường hợp sau:

(1) Cảnh giác với số máy lạ nhất là các số máy có đầu số nước ngoài. Tuyệt đối không cung cấp số điện thoại cá nhân, thông tin cá nhân cho bất kỳ tổ chức, cá nhân nào khi chưa biết họ là ai và sử dụng vào mục đích gì. Ngoài ra, khi nghe những câu mời chào bạn đã trúng thưởng, yêu cầu chuyển khoản,v.v. Hãy kiểm tra kỹ số điện thoại đó thuộc tổ chức nào trước khi cung cấp thông tin.

(2) Không tiết lộ thông tin cá nhân để tránh lừa đảo trên mạng xã hội: Tuyệt đối không cung cấp chứng minh thư/căn cước công dân, tài khoản cá nhân, tài khoản ngân hàng. Không chuyển, nộp tiền vào bất kỳ tài khoản cá nhân, tổ chức nào khi chưa biết rõ họ là ai. Việc cung cấp bừa bãi thông tin cá nhân chính là miếng mồi ngon để hành vi lừa đảo qua mạng xã hội diễn ra.

(3) Cảnh giác với các tin nhắn yêu cầu chuyển/ nhận tiền: Không thực hiện yêu cầu chuyển tiền qua tin nhắn từ mạng xã hội như: Facebook, zalo, viber,… Kể cả là của người thân, bạn bè. Cần gọi điện xác nhận nếu người nhận không nghe máy hoặc viện lý do không tiện nói chuyện thì kiên quyết không chuyển khoản. Để tránh trường hợp người thân, bạn bè bị hack tài khoản.

(4) Xác minh kỹ thông tin khi thực hiện chuyển tiền trên mạng xã hội: Chỉ thực hiện giao dịch trên các website chính thức của các tổ chức tài chính, ngân hàng. Tuyệt đối không cung cấp mã OTP cho người khác. Hạn chế việc công khai số căn cước công dân, số điện thoại, số tài khoản ngân hàng trên mạng xã hội. Các tài khoản công khai dùng để giao dịch online cần hạn chế số tiền dư quá lớn.

Để phòng ngừa, đấu tranh hiệu quả với loại tội phạm lừa đảo trên không gian mạng, Sở Thông tin và Truyền thông khuyến cáo:

1. Không chuyển tiền, cung cấp thông tin cá nhân, mã OTP, tài khoản E-Banking theo yêu cầu từ người lạ. Cài đặt bảo vệ các tài khoản mạng xã hội bằng xác thực 2 lớp.

2. Nếu tài khoản mạng xã hội (Facebook, Zalo, ...) bị hack, chiếm quyền sử dụng, nên công bố ngay cho những người thân quen, bạn bè có trong danh bạ biết để phòng ngừa loại tội phạm lừa đảo chiếm đoạt tài sản.

3. Nếu nhận được tin nhắn từ người thân hỏi vay mượn tiền, chuyển khoản, nạp thẻ điện thoại... nên gọi điện thoại hoặc gặp trực tiếp để hỏi chính xác trước khi chuyển tiền.

4. Không vay tiền online từ các ứng dụng không rõ nguồn gốc. Không nộp các loại phí, thuế do đối tượng yêu cầu để được nhận khoản vay; đây là hình thức lừa đảo hoặc cho vay lãi nặng qua các ứng dụng điện thoại di động.

5. Cảnh giác khi làm quen, kết bạn hẹn hò qua mạng xã hội, các web và ứng dụng hẹn hò.

6. Cảnh giác với tất cả các e-mail và đường link lạ, tuyệt đối không nhập và gửi thông tin cá nhân vào các cửa sổ trong các trang web mà chưa kiểm chứng về sự an toàn và nguồn gốc của nó. Không cài đặt các ứng dụng lạ mà có yêu cầu cấp quyền truy cập vào danh bạ, tin nhắn, camera...

7. Tìm hiểu rõ nguồn gốc, hạn chế mua sản phẩm không rõ nguồn gốc, xuất xứ, giá trị lớn qua mạng xã hội. Hãy lựa chọn cách mua hàng trên các sàn thương mại điện tử được cấp phép, có uy tín, có lượng đánh giá tích cực lớn.

8. Cảnh giác với các lời mời tham gia đầu tư tài chính trên không gian mạng, tuyệt đối không đầu tư khi chưa tìm hiểu rõ ràng.

9. Cảnh giác trước các lời mời, quảng cáo tuyển cộng tác viên làm nhiệm vụ hưởng tiền hoa hồng trên các trang mạng xã hội. Khi làm cộng tác viên cho các công ty, doanh nghiệp, đơn vị cung ứng hàng hóa, dịch vụ, cần kiểm tra rõ các thông tin về hàng hóa và đơn vị cung cấp thông qua nhiều nguồn khác nhau để kiểm chứng tính chính xác.

10. Thường xuyên cập nhật các phương thức, thủ đoạn hoạt động của tội phạm lừa đảo trên không gian mạng qua các phương tiện thông tin truyền thông.

11. Kịp thời thông báo cho Cơ quan Công an gần nhất để được tiếp nhận, giải quyết nếu nghi ngờ có hành vi lừa đảo chiếm đoạt tài sản hoặc các hành vi vi phạm pháp luật khác.

Sở Thông tin và Truyền thông rất mong quý cơ quan báo chí trong ngoài tỉnh, quý cơ quan, đơn vị, địa phương trong tỉnh phối hợp triển khai nội dung nêu trên./.

Nơi nhận:
- Như trên;
- UBND tỉnh (b/c);
- Lưu: VT, TTBCXB (MP).

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH CÀ MAU

Trần Văn Trung