BỘ CÔNG AN
CÔNG AN TỈNH TÂY NINH

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

Số: 10 /TB-CAT

Tây Ninh, ngày 12 tháng 4 năm 2022

THÔNG BÁO
Phương thức, thủ đoạn Lừa đảo chiếm đoạt tài sản trên không gian mạng

Thời gian sau Tết Nguyên đán Nhâm Dần năm 2022, tình hình tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng trên địa bàn tỉnh tiếp tục diễn biến phức tạp với nhiều phương thức, thủ đoạn đa dạng, tinh vi, số tiền chiếm đoạt lên đến hàng tỷ đồng.

Trong quý I năm 2022, trên địa bàn tỉnh Tây Ninh phát hiện rất nhiều trường hợp người dân bị lừa đảo chiếm đoạt tài sản trên không gian mạng, qua tiếp nhận 26 trường hợp bị lừa đảo chiếm đoạt tiền với các thủ đoạn: lôi kéo bị hại tham gia nhóm kín, rủ rê đầu tư trên các sàn tiền ảo, bị sập sàn; thông báo trúng thưởng, yêu cầu nộp thuế nhận thưởng; mua hàng qua mạng xã hội, chuyển tiền nhưng không giao hàng; kết bạn qua mạng xã hội facebook nhận chuyển tiền từ nước ngoài về Việt Nam với giá rẻ; chiếm quyền điều khiển mạng xã hội facebook nhắn tin cho người thân, bạn bè mượn tiền; nhắn tin qua mesenger facebook yêu cầu cung cấp số điện thoại để chuyển tiền vào ví điện tử, yêu cầu cung cấp mật khẩu ví điện tử để nhận thưởng thì bị chiếm đoạt tiền; vay tiền qua mạng, yêu cầu chuyển nhiều khoản phí hoặc báo lỗi chuyển tiền; giả danh nhân viên ngân hàng, công ty bảo hiểm, Công an, Viện kiểm sát, Toà án đe doạ; tuyển cộng tác viên bán hàng online;... Trong đó, thủ đoạn xảy ra nhiều và bị thiệt hại số tiền lớn, gồm có:

1. Tuyển cộng tác viên bán hành online: xảy ra 06 trường hợp với kịch bản tương tự, cụ thể như sau:

Bị hại tìm thấy các quảng cáo trên mạng xã hội (Facebook, Zalo) có nội dung về tuyển cộng tác viên (CTV) xử lý đơn hàng trên các trang thương mại điện tử uy tín (Shoppe, Lazada, Tiki,...) để hưởng hoa hồng từ 10 – 20% hoặc thu nhập từ 200.000đ – 700.000đ/ngày, không cần bằng cấp, kinh nghiệm, làm việc tại nhà, có sử dụng thẻ ATM, điện thoại, laptop... Bị hại nhấn vào đường link tham gia bằng cách để lại số điện thoại. Ngay lập tức, có người liên hệ lại và kết bạn qua zalo để hướng dẫn cách thức thực hiện. Đầu tiên, bị hại sẽ được làm nhiệm vụ đặt đơn hàng có giá trị nhỏ bằng cách chuyển tiền mua sản phẩm vào một tài khoản ngân hàng do đối tượng chỉ định và chụp hình chuyển tiền gửi lại cho đối tượng để xác thực, sau khi đối tượng xác nhận bị hại đã chuyển tiền mua đơn hàng thành công sẽ thanh toán lại tiền mua hàng kèm tiền hoa hồng như đã hứa để tạo lòng tin và đánh vào lòng tham vì việc kiếm tiền quá dễ dàng. Ví dụ món hàng có giá trị hơn 500.000 đồng thì bị hại sẽ chuyển tiền vào số tài khoản đó. Sau khi chuyển tiền xong từ 3 - 5 phút, các đối tượng hoàn tiền lại cho bị hại bao gồm tiền gốc và tiền hoa hồng. Tùy vào từng món hàng, có món thì được 8%, món 10%, món 20% hoa hồng. Sau 1 - 2 lần làm nhiệm vụ mua đơn hàng thành công và nhận được tiền

hoa hồng, bị hại sẽ được giao nhiều nhiệm vụ mua đơn hàng có giá trị lớn hơn, thực hiện rất nhiều nhiệm vụ để được thanh toán lại số tiền gốc và tiền hoa hồng. Tuy nhiên, khi đã nộp số tiền lớn để đặt mua hàng, thì các đối tượng liên tục đưa ra nhiều lý do khác nhau để yêu cầu bị hại mua thêm hàng. Bị hại vì muốn lấy lại số tiền mua sản phẩm ban đầu nên cứ làm theo và bị chiếm đoạt tiền nhiều lần.

2. Giả danh công ty bảo hiểm, Công an, Viện Kiểm sát... đe doạ vi phạm pháp luật yêu cầu chuyển tiền: xảy ra 03 trường hợp.

Lừa đảo theo một kịch bản đã xây dựng với nhiều đối tượng tham gia nhằm đánh lạc hướng bị hại tin tưởng và làm theo mà không kịp suy nghĩ đúng sai. Đầu tiên, giả danh Công ty bảo hiểm gọi điện thoại thông báo bị hại đã làm giả hồ sơ bệnh án để chiếm đoạt tiền bảo hiểm tại Đà Nẵng, bị hại phủ nhận. Tiếp theo, đối tượng chuyển máy điện thoại cho đối tượng khác giả danh Công an để xác nhận tên của bị hại đã làm giả hồ sơ bảo hiểm và cũng liên quan trong vụ án lớn (buôn bán ma tuý, rửa tiền, lừa đảo xuyên quốc gia) do bị hại có tham gia mở tài khoản ngân hàng phục vụ cho việc rửa tiền phạm pháp, bị hại đã có Lệnh bắt giam của Viện kiểm sát, Toà án. Tiếp đó, đối tượng chuyển máy cho đối tượng khác giả danh Viện kiểm sát, Toà án và yêu cầu bị hại kết bạn Zalo để gửi Lệnh bắt bị can tạm giam có thông tin đúng như bị hại.

Nếu bị hại không muốn ra Toà hoặc bị bắt tạm giam thì phải mở một tài khoản ngân hàng cá nhân và chuyển tất cả tiền có được vào tài khoản này để "nộp Kho bạc Nhà nước". Nhưng trên thực tế, sau khi bị hại mở tài khoản Ngân hàng đứng tên mình thì bị hại đã cung cấp toàn bộ số tài khoản, mật khẩu Internet Banking, mã OTP,... cho đối tượng. Đối tượng đã chiếm quyền điều khiển tài khoản ngân hàng của bị hại và chiếm đoạt toàn bộ số tiền trong tài khoản.

3. Lừa với hình thức tham gia vay tiền qua ứng dụng trên điện thoại: xảy ra 05 trường hợp

Các đối tượng lừa đảo thường đánh vào tâm lý muốn được vay vốn với số tiền lớn, thủ tục nhanh gọn ở những người đang cần tiền để tiêu dùng. Sau khi tiếp cận được "con mồi", các đối tượng sử dụng sim, tài khoản thuộc các trang mạng xã hội như Zalo, Messenger để hướng dẫn việc thực hiện thủ tục vay thông qua các ứng dụng tài chính online như "FC Credit", "CE Credit", "Mirae Asset"... do các đối tượng cung cấp và hướng dẫn bị hại cài đặt trên điện thoại.

Sau khi cài đặt ứng dụng thì điền thông tin cá nhân, các thông tin về gói vay. Đối tượng yêu cầu nộp tiền bảo hiểm khoản vay qua tài khoản ngân hàng do đối tượng hướng dẫn. Sau khi bị hại nộp tiền thì đối tượng chiếm đoạt và thông báo chưa nhận được tiền với nhiều lý do như sai tài khoản, sai cú pháp,... hoặc thông báo nhận được tiền nhưng đưa ra nhiều lý do khác để yêu cầu nộp thêm tiền như tài khoản yêu cầu vay bị sai hoặc thiếu thông tin, nộp phạt số tiền vay vượt quá định mức vay, trả trước một khoản lãi suất sau khi giải ngân sẽ chuyển đủ tiền cho vay... để chiếm đoạt số tiền lớn, có khi lớn gấp nhiều lần số tiền cần vay.

Hầu hết số tiền thiệt hại qua các thủ đoạn lừa đảo đều chuyển vào tài khoản ngân hàng do đối tượng chỉ định. Số tiền chiếm đoạt được chuyển qua nhiều tài khoản ngân hàng khác nhau và sau cùng là chuyển vào các tài khoản ngân hàng

của các đại lý game, sàn giao dịch tiền ảo… để xoá dấu vết, gây khó khăn cho Cơ quan Công an trong quá trình điều tra.

*** Biện pháp phòng ngừa:**

- Luôn nâng cao cảnh giác với các thủ đoạn lừa đảo chiếm đoạt tài sản qua mạng.

- Không chuyển tiền vào các tài khoản ngân hàng lạ.

- Cơ quan thực thi pháp luật như Công an, Viện kiểm sát, Toà án,… gặp gỡ, làm việc với người dân thông qua công an cơ sở, không làm việc, gửi lệnh bắt, giam giữ qua điện thoại, mạng xã hội.

- Không vay tiền qua các trang web, ứng dụng điện thoại không rõ nguồn gốc.

Công an tỉnh Tây Ninh thông báo đến các sở, ban, ngành, đoàn thể và UBND các huyện, thành phố tổ chức quán triệt cho cán bộ, người thân trong gia đình và người dân xung quanh nâng cao ý thức cảnh giác với tội phạm nhằm bảo vệ tài sản cho cá nhân, người thân, bạn bè, hàng xóm.

Công an các đơn vị, huyện, thị xã, thành phố thông báo phương thức thủ đoạn hoạt động phạm tội này đến Nhân dân để nâng cao tinh thần cảnh giác, phòng ngừa tội phạm./.

Nơi nhận:
- Các sở, ban, ngành và UBND huyện, tp (nắm);
- Đài Truyền hình, Báo Tây Ninh (t/truyền);
- Đ/c Giám đốc (thay b/cáo);
- Đ/c Đại tá Lý Hồng Sinh -PGĐ (c/đạo)
- Phòng PX03, PV05 (t/hiện);
- Công an các huyện, thị xã, thành phố (t/hiện);
- Lưu: VT, PV01, PC02.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Lý Hồng Sinh