ĐỀ CƯƠNG TUYÊN TRUYỀN

Tuyên truyền về phương thức, thủ đoạn của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng và biện pháp phòng tránh

(Kèm theo công văn số 94/TBATANM ngày 27/3/2023)

1. Các phương thức, thủ đoạn lừa đảo chiếm đoạt tài sản

+ Giả danh cán bộ Công an, Viện Kiên sát, Tòa án gọi điện thông báo người dân có liên quan đến vụ án hoặc xử phạt nguội vi phạm giao thông, yêu cầu bị hại chuyển tiền vào tài khoản mà các đối tượng lừa đảo đưa ra để phục vụ công tác điều tra, xử lý... Sau đó, người dân lo sợ, chuyển tiền vào tài khoản mà đối tượng yêu cầu thì sẽ bị đối tượng chiếm đoạt.

+ Giả danh cán bộ Ngân hàng gọi điện cho bị hại thông báo bị hại có người chuyên tiền vào tài khoản nhưng do bị lỗi nên chưa chuyển được hoặc thông báo phần mềm chuyển tiền Internet banking của khách hàng bị lỗi ... nên yêu cầu khách hàng cung cấp mã số thẻ và mã OTP để kiểm tra. Các đối tượng sử dụng thông tin bị hại cung cấp để truy cập vào tài khoản và chiếm đoạt tiền của bị hại.

+ Giả danh nhân viên nhà mạng gọi điện thông báo số thuê bao 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 nạp tiền vào tài khoản theo yêu cầu để nhận thưởng thì các đối tượng chặn liên lạc và chiếm đoạt tiền. Gần đây, các đối tượng thông báo thuê bao của người dùng bị khóa do có liên quan đến vụ án hình sự, …yêu cầu người dùng gửi thông tin bao gồm họ tên, địa chỉ, số căn cước công dân, thậm chí yêu cầu chụp ảnh. Mục tiêu những kẻ này nhằm đánh cắp thông tin cá nhân của người dùng hoặc chiếm đoạt tiền thông qua giao dịch chuyển khoản. Với thông tin của nạn nhân, chúng có thể tạo hồ sơ, căn cước giả để liên hệ nhà mạng, sau đó lấy cắp số điện thoại gắn với thẻ SIM bằng thủ tục đăng ký eSIM.

+ Mạo danh là giáo viên, nhân viên y tế nhà trường hoặc nhân viên y tế bệnh viện liên hệ trực tiếp với phụ huynh học sinh báo tin về việc học sinh, người nhà bị tai nạn, đang nhập viện cấp cứu, yêu cầu phải nhanh chóng chuyển tiền để đóng viện phí, cấp cứu bệnh nhân, từ đó chiếm đoạt tài sản.

+ Giả danh nhân viên điện lực gọi điện thông báo nộp tiền điện dưới hình thức chuyển khoản với nội dung: "Bạn đang sử dụng điện cao bất thường, chúng tôi sẽ cắt điện trong thời gian tới, vui lòng bấm số 9 gặp nhân viên tư vấn". Với các thông báo đó, khách hàng rất dễ bị lừa, chuyển khoản nộp tiền điện và bị đối tượng chiếm đoạt.

+ Thủ đoạn giả mạo, chiếm đoạt tài khoản Zalo, Facebook

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, 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.

Đối tượng chiếm quyền điều khiển tài khoản mạng xã hội (Facebook, Zalo) của người dùng, sau đó nhắn tin lừa đảo, mượn tiền mọi người trong danh sách bạn bè của nạn nhân.

+ Thủ đoạn lừa đảo thông qua hình thức tuyển cộng tác viên online, tuyển nhân viên làm việc tại nhà.

* Trường hợp 1:

Đối tượng thường đăng các bài tuyển nhân viên, cộng tác viên trên các hội, nhóm Facebook: "tuyển nhân viên xâu vòng tại nhà, không yêu cầu về trình độ, độ tuổi, nguyên liệu có người giao tận nơi...với tiền công hấp dẫn "xâu 1 kg hạt được 350.000 đồng"; hay gia công lì xì, túi đựng hạt giống, làm tranh đá tại nhà...

Để làm những công việc này, người làm phải đặt cọc số tiền là từ vài trăm nghìn đến hàng triệu đồng tiền nguyên liệu. Tuy vậy, khi hoàn thành, bị hại gửi sản phẩm cho bên thuê dịch vụ thì bị trả lời sản phẩm không đạt yêu cầu nên không nhận và chiếm đoạt tiền của bị hại.

* Trường hợp 2:

Lợi dụng sự nhẹ dạ cả tin và nhu cầu kiếm tiền nhanh của bị hại, các đối tượng giả mạo tuyển cộng tác viên xử lý đơn hàng cho các sàn thương mại điện tử để thực hiện hành vi chiếm đoạt tài sản. Bằng thủ đoạn lập các trang Facebook giả mạo các nhãn hàng, trang thương mại điện tử như: Tiki.vn, Lazada, Tokyolife, 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... yêu cầu gửi thông tin cá nhân, kết bạn Zalo để tư vấn.

Ban đầu, đối tượng gửi link (đường dẫn) các sản phẩm có giá trị nhỏ khoảng vài trăm nghìn 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 một số lần tạo niềm tin bằng cách trả gốc và hoa hồng như cam kết ban đầu, tiếp theo đối tượng viện lý do là "bạn đã được công ty nâng hạng" và 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 tiếp tục thông báo cho cộng tác viên phải tiếp tục thực hiện nhiệm vụ khác thì mới được chuyển lại tiền và hoa hồng. Sau đó các đối tượng chiếm đoạt toàn bộ số tiền của bị hại.

+ Thủ đoạn lừa đảo thông qua các sàn giao dịch trên mạng.

Các đối tượng mời chào, lôi kéo bị hại tham gia đầu tư vào các sàn giao dịch tiền ảo do đối tượng 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, tự nhận là chuyên gia đầu tư, người truyền cảm hứng, người dẫn đường... để lừa đảo, kêu gọi đầu tư vào hệ thống do chúng thiết lập. Khi huy động được lượng tiền đủ lớn, các đối tượng sẽ can thiệp vào các giao dịch, điều chỉnh thắng thua hoặc báo lỗi, ngừng hoạt động (sập sàn) để chiếm đoạt tiền của người tham gia.

+ Thu đoạn cho vay tiền qua ứng dụng (vay tiền online qua app).

Lợi dụng tâm lý vay tiền online thuận lợi, nhanh chóng, không phải ra ngân hàng làm thủ tục, các đối tượng lập ra các trang trên mạng xã hội (Zalo, Facebook...) chạy quảng cáo để tiếp cận các bị hại. Sau khi tiếp cận được nạn nhân, các đối tượng sẽ gửi các đường link kết nối với CH Play hoặc App Store để các bị hại cài đặt ứng dụng vào điện thoại và làm theo hướng dẫn. Sau đó, khi bị

hại đăng nhập vào ứng dụng vay tiền thì ứng dụng sẽ báo lỗi, các đối tượng yêu cầu bị hại phải chuyển tiền đặt cọc để mở lại tài khoản thì mới giải ngân được, hoặc các đối tượng yêu cầu nạn nhân mua bảo hiểm khoản vay, đóng tiền phí giải ngân, làm sai dữ liệu, giải băng khoản vay... 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 nữa thì không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

+ Một số thủ đoạn lừa đảo khác

* Đăng các tin, bài bán hàng trên mạng xã hội với giá rẻ hơn thị trường... Khi bị hại kết nối và đặt cọc hoặc thanh toán số tiền theo thỏa thuận thì các đối tượng chặn liên hệ, đổi số điện thoại... và chiếm đoạt số tiền đã nhận được.

* Thông báo trúng thưởng tiền, tài sản có giá trị lớn như xe máy, điện thoại, đồng hồ hoặc tiền mặt... Sau đó, đối tượng yêu cầu bị hại nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thù tục nhận thưởng và chiếm đoạt.

* Gửi tin nhắn SMS giả mạo của Ngân hàng để lừa khách hàng truy cập vào đường link giả, sau đó yêu cầu cung cấp các thông tin bảo mật như tên, mật khẩu đăng nhập, mã OTP, thông tin thẻ... Khi có được các thông tin này, đối tượng sẽ rút tiền trong tài khoản của nạn nhân.

* Các đối tượng lừa đảo cố ý "chuyển nhầm " một khoản tiền đến tài khoản ngân hàng. Tiếp đó, chúng yêu cầu người dùng trả lại số tiền kia như một khoản vay cùng với khoản lãi rất cao. Nếu không trả, các đối tượng sẽ nhắn tin đe dọa, gây phiền hà, ghép hình ảnh bôi nhọ danh dự, nhân phẩm, làm mất uy tín và làm ảnh hưởng đến cuộc sống của bị hại và người thân.

2. Biện pháp phòng ngừa

(1) Cảnh giác với các cuộc điện thoại từ số máy lạ, đặc biệt là các số máy có đầu số nước ngoài.

(2) Tuyệt đối không cung cấp 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.

(3) Không truy cập vào các đường link gắn kèm trong nội dung tin nhắn lạ; không thực hiện thao tác trên điện thoại theo các cú pháp được hướng dẫn bởi người lạ.

(4) Không mua, bán, cho mượn Giấy chứng minh thư nhân dân/Căn cước công dân, tài khoản cá nhân, tài khoản ngân hàng, các loại thẻ tín dụng; Không đăng ảnh CMND/CCCD hoặc thông tin cá nhân lên mạng xã hội.

(5) Giữ bí mật, không cung cấp thông tin cá nhân, số điện thoại, thông tin về tài khoản ngân hàng, mã OTP... cho bất kỳ người lạ nào gọi đến.

(6) Không tham gia hoặc không chuyển bất cứ khoản tiền nào khi làm cộng tác viên bán hàng online.

(7) Không tham gia việc vay tiền qua ứng dụng di động, đầu tư tiền ảo không rõ thông tin.

(8) Không thực hiện các yêu cầu chuyển tiền thông qua tin nhắn của các trang mạng xã hội, kể là của người thân, bạn bè khi chưa xác thực lại qua điện thoại, liên hệ trực tiếp.