1.7. Giả mạo tài khoản mạng xã hội

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.

1.8. Một số thủ đoạn lừa đảo khác

- Đăng các tin, bài bán hàng trên mạng xã hội… 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 người bị hại nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ 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.

BIỆN PHÁP PHÒNG NGỪA TỘI PHẠM LỪA ĐẢO, CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG

A. Luôn cảnh giác

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

- Tuyệt đối không cung cấp thông tin cá nhân, mã OTP, CMND, CCCD, giấy tờ tùy thân khác… cho bất kỳ tổ chức, cá nhân nào khi chưa biết họ là ai và sử dụng vào mục đích gì.

- 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.

- Không chuyển tiền cho người lạ quen biết trên mạng. Với người quen nhờ chuyển tiền, cần gọi điện thoại 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 chiếm đoạt tài khoản mạng xã hội.

- Cảnh giác với những thông tin tuyển dụng, kiếm tiền qua mạng, đầu tư các sàn giao dịch tiền ảo, ngoại hối…

- Khi tài khoản bỗng dưng nhận được một khoản tiền "chuyển nhầm" thì không được sử dụng số tiền ấy vào việc chi tiêu cá nhân. Đồng thời, chỉ làm việc và liên lạc với ngân hàng để giải quyết vấn đề.

A. Bảo vệ tài khoản an toàn

- Mật khẩu các tài khoản cá nhân, tài khoản mạng xã hội phải có chữ hoa, chữ thường, các ký tự đặc biệt và số.

- Không dùng chung mật khẩu cho tất cả các tài khoản.

- Không dùng thông tin cá nhân (họ tên, ngày sinh, địa chỉ, số điện thoại, số chứng minh nhân dân…) để đặt mật khẩu.

- Định kỳ thay đổi mật khẩu.

- Xác thực 2 bước (liên kết với số điện thoại hoặc tài khoản email đã được xác thực 2 bước).

In 8.000 bản, khổ 20,5 cm x 29cm
tại Công ty TNHH Tính toán, In & Thương mại Bắc Giang
Giấy phép xuất bản số: 67/GP-STTTT,
cấp ngày 12 tháng 9 năm 2023
In xong và nộp lưu chiểu quý III năm 2023.

(XUẤT BẢN PHẨM KHÔNG BÁN)

SỞ TƯ PHÁP TỈNH BẮC GIANG

PHÒNG CHỐNG TỘI PHẠM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG

Bắc Giang, năm 2023

THỦ ĐOẠN LỪA ĐẢO, CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG

1.1. Giả danh nhân viên nhà mạng, ngân hàng, điện lực

- Giả danh cán bộ Ngân hàng gọi điện cho bị hại thông báo bị hại có người chuyển 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 viễn thông gọi điện thoại hoặc nhắn tin cho nạn nhân đề nghị hỗ trợ nâng cấp, chuyển đổi sim 4G/5G miễn phí. Khi nạn nhân kích hoạt esim (sim điện tử) trên điện thoại, đối tượng lừa đảo có thể chiếm được quyền kiểm soát sim điện thoại, đánh cắp các thông tin thẻ tín dụng, lấy mã OTP.

- 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.

1.2. Giả danh cán bộ Công an, Viện kiểm sát, Tòa án

- Đối tượng lừa đảo gọi điện thông báo người dân có liên quan đến vụ án nghiêm trọng 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.

1.3. Tuyển cộng tác viên kiếm tiền Online, tuyển nhân viên làm việc tại nhà

* Hình thức nhận nguyên liệu làm việc tại nhà

- Đối tượng thường đăng các bài tuyển nhân viên, cộng tác viên trên các hội, nhóm Facebook với nội dung như: 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; 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.

** Thủ đoạn mua các nhiệm vụ ăn hoa hồng*

- Chúng tạo Facebook giả mạo các nhãn hàng, trang thương mại điện tử như: Tiki, Lazada, Tokyolife, Shopee…. 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 trên các ứng dụng nhắn tin Facebook, Zalo, Telegram 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.

1.4. Cho vay Online với lãi suất thấp

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, Chạy quảng cáo để tiếp cận các bị hại. Sau khi tiếp cận được nạn nhân, các đối tượng sẽ gửi các đường link, tải các ứng dụng lừa đảo 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… 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.

1.5. Đầu tư tài chính Online (sàn vàng, sàn nhị phân…)

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.

1.6. Chiếm đoạt tài khoản mạng xã hội

Đối tượng gửi các đường link lạ vào tài khoản mạng xã hội như Facebook, Zalo, … của các nạn nhân nhờ chia sẻ, like giúp. Khi bị hại nhấn vào đường link lạ trên thì sẽ bị các đối tượng chiếm đoạt tài khoản mạng xã hội, sau đó chúng sẽ sử dụng để 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.