BỘ CÔNG AN
CÔNG AN TỈNH LẠNG SƠN

THỦ ĐOẠN LỪA ĐẢO CỦA TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

SỬ DỤNG THÔNG TIN CÁ NHÂN CHIẾM QUYỀN SỬ DỤNG, GIẢ DANH TÀI KHOẢN MẠNG XÃ HỘI ĐỂ LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN

Lợi dụng việc người dân để lộ thông tin cá nhân trên mạng xã hội các đối tượng dùng các thông tin này để chiếm quyền sử dụng tài khoản mạng xã hội sau đó nhắn tin cho người thân, bạn bè của chủ tài khoản vay, mượn tiền rồi chiếm đoạt	Tạo tài khoản mạng xã hội có tên, hình đại diện và các thông tin cá nhân khác giống với tài khoản chính chủ sau đó nhắn tin cho người thân, bạn bè của chủ tài khoản để vay, mượn tiền rồi chiếm đoạt	Tạo tài khoản mạng xã hội có tên, hình ảnh và các thông tin cá nhân của nhà bán hàng trên mạng xã hội và đăng bán sản phẩm giống với nhà bán hàng. Yêu cầu người mua chuyển tiền đến tài khoản của nhà bán hàng thật rồi liên hệ với nhà bán hàng gửi sản phẩm cho đối tượng.

GIẢ DANH CÁN BỘ, CƠ QUAN, DOANH NGHIỆP ĐỂ LỪA ĐẢO

Giả danh cơ quan Công an, Tòa án, Viện kiểm sát gọi điện thông báo người dân bị xử phạt vi phạm giao thông hoặc liên quan đến các vụ án đang điều tra yêu cầu người dân phải cung cấp thông tin cá nhân, tài khoản ngân hàng và chuyển tiền để xác minh, chạy tội sau đó chiếm đoạt.

Giả làm nhân viên Ngân hàng thông báo tài khoản của người dân bị lỗi, bị khóa rồi yêu cầu cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng, mã OTP để xác minh, sửa lỗi, mở khóa tài khoản sau đó chiếm đoạt tiền trong tài khoản.

Giả làm nhân viên thu tiền điện, nước gọi điện thông báo và gửi kèm hóa đơn giả yêu cầu bị hại chuyển tiền thanh toán sau đó chiếm đoạt.

Giả làm giáo viên nhà trường, nhân viên ý tế gọi điện thoại thông báo cho người dân về việc con, em của họ bị tai nạn phải nhập viện và yêu cầu chuyển tiền để làm thủ tục cấp cứu nếu không sẽ nguy hiểm đến tính mạng.

Giả làm người nước ngoài kết bạn, làm quen và nói chuyện với người dân sau đó hứa hẹn sẽ tặng tiền, quà có giá trị cao và sẽ về Việt Nam thăm. Sau đó giả làm nhân viên sân bay, bưu điện, hải quan gọi điện yêu cầu nộp thuế, phí để làm thủ tục nhận quà.

Giả làm nhân viên nhà mạng viễn thông, gọi điện thông báo khóa sim vì chưa chuẩn hóa thuê bao yêu cầu cung cấp thông tin cá nhân, mã OTP… Sau đó dùng thông tin này để chiếm quyền sử dụng sim điện thoại. Sau đó sử dụng sim điện thoại để chiếm đoạt tiền trong các ứng dụng ngân hàng.

Giả làm nhân viên Ngân hàng gọi điện mời người dân rút tiền mặt trong thẻ tín dụng với chi phí thấp. Yêu cầu người dân cung cấp ảnh chụp hai mặt thẻ tín dụng hoặc thông tin in trên thẻ sau đó chiếm đoạt hạn mức tiền trong thẻ tín dụng.

SỬ DỤNG CUỘC GỌI DEEP FAKE, DEEP VOICE ĐỂ LỪA ĐẢO

Thu thập thông tin giọng nói, hình ảnh của người muốn giả mạo. Sử dụng trí tuệ nhân tạo để tạo video, cuộc gọi giả. Khi các đối tượng gọi điện cho người dân sẽ có hình ảnh, giọng nói như người chúng muốn giả mạo. Hình thức này các đối tượng dùng để phục vụ hoạt động lừa đảo giả danh hoặc chiếm quyền sử dụng, giả tài khoản mạng xã hội

TUYỂN CỘNG TÁC VIÊN, LÀM NHIỆM VỤ NHẬN THƯỞNG ĐỂ LỪA ĐẢO

Quảng cáo trên các mạng xã hội, gọi điện thoại trực tiếp cho người dân với nội dung tuyển cộng tác viên của các trang thương mại điện tử, các nhãn hiệu nổi tiếng làm nhiệm vụ nhận thưởng. Ban đầu nhiệm vụ sẽ là thích, chia sẻ video, đánh giá sản phẩm và được nhận phần thưởng giá trị thấp. Sau khi lấy được lòng tin của người dân các đối tượng yêu cầu người dân làm nhiệm vụ có số tiền thưởng lớn hơn chuyển tiền cho đối tượng để thực hiện nhiệm vụ sau đó sẽ nhận được tiền hoa hồng theo số tiền đã chuyển. Các nhiệm vụ sẽ tăng dần số tiền cần chuyển và xuất hiện các lỗi yêu cầu người dân phải nộp thêm tiền nếu không sẽ mất số tiền đã chuyển trước đó. Khi người dân không còn khả năng chuyển tiền thì các đối tượng sẽ chiếm đoạt toàn bộ số tiền.

Quảng cáo trên các mạng xã hội tuyển cộng tác viên Online làm việc tại nhà với các công việc đơn giản như lắp bút bi, sâu vòng tay, dán tranh đá… với mức lương hấp dẫn. Các đối tượng yêu cầu nạn nhân chuyển trước một khoản tiền cọc để nhận sản phẩm về làm tại nhà. Số tiền này sau đó sẽ bị chiếm đoạt.

Quảng cáo dịch vụ hẹn hò qua mạng, gái gọi trực tuyến. gửi hình ảnh những phụ nữ có ngoại hình đẹp cho người dân chọn rồi yêu cầu làm nhiệm vụ để mở thẻ hẹn hò. Yêu cầu người dân làm nhiệm vụ chuyển tiền và nhận hoa hồng, số tiền để thực hiện nhiệm vụ sẽ tăng dần và xuất hiện các lỗi yêu cầu người dân phải nộp thêm tiền nếu không sẽ mất số tiền đã chuyển trước đó. Khi người dân không còn khả năng chuyển tiền thì các đối tượng sẽ chiếm đoạt toàn bộ số tiền đã chuyển.

MỜI VAY TIỀN TRỰC TUYẾN ĐỂ LỪA ĐẢO

Quảng cáo cho vay tiền trên các mạng xã hội, gọi điện trực tiếp cho người dân mời vay tiền với lãi suất thấp hơn lãi suất ngân hàng, thủ tục đơn giản không cần thế chấp tài sản... Gửi liên kết đến website giả có giao diện giống với ngân hàng hoặc các tổ chức tín dụng và yêu cầu người vay nhập các thông tin cá nhân và khởi tạo khoản vay. Lúc này trên website sẽ hiển thị người dân có khoản tiền chờ rút, tuy nhiên khi nạn nhân thực hiện rút tiền sẽ xuất hiện lỗi và không thể rút về được. Sau đó các đối tượng sẽ đưa ra các lý do là người vay cung cấp sai thông tin cá nhân, thông tin tài khoản ngân hàng hoặc thực hiện không đúng thao tác rồi yêu cầu người dân phải chuyển tiền để xác minh, thay đổi thông tin mới rút được tiền. Nếu người vay không chuyển tiền các đối tượng sẽ đe dọa khoản vay đã được khởi tạo nếu không chuyển tiền để rút về người vay vẫn phải thanh toán khoản vay và bị ngân hàng thu hồi nợ.

ĐĂNG TẢI THÔNG TIN SAI SỰ THẬT ĐỂ LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN

Lợi dụng các hoạt động từ thiện nhân đạo các đối tượng kêu gọi ủng hộ, quyên góp tiền cho các gia đình có hoàn cảnh khó khăn, hiểm nghèo thông qua các mạng xã hội. Sau khi các nhà hảo tâm chuyển tiền từ thiện các đối tượng sẽ chiếm đoạt số tiền này.

Thông qua mạng xã hội đăng bài rao bán các mặt hàng, sản phẩm đang được ưa chuộng, combo du lịch… với giá thấp hơn giá thị trường tuy nhiên để mua được sản phẩm phải chuyển một phần hoặc toàn bộ số tiền hàng cho đối tượng. Số tiền này sau đó sẽ bị chiếm đoạt.

Đăng tải các thông tin tuyển người mẫu nhí, cầu thủ nhí trên các mạng xã hội để tiếp cận, dụ dỗ các bậc phụ huynh cho con trẻ đăng ký ứng tuyển sau đó yêu cầu nạn nhân đóng nhiều loại phí để chiếm đoạt.

MỜI CHÀO ĐẦU TƯ CHỨNG KHOÁN, TIỀN ẢO, ĐA CẤP ĐỂ LỪA ĐẢO

Quảng cáo trên các mạng xã hội, gọi điện, nhắn tin trực tiếp cho người dân mời người dân tham gia vào các nhóm trên các mạng xã hội để tham gia cùng đầu tư chứng khoán, tiền ảo. Những nhóm này sẽ có các tài khoản ảo do các đối tượng lập nên và đăng các hình ảnh, nội dung đầu tư thắng số tiền lớn. Sau đó các đối tượng gửi đường link, hướng dẫn người dân tham gia vào các sàn chứng khoán, tiền ảo giả do các đối tượng tự tạo nên có giao diện website, ứng dụng giống với các sàn chứng khoán, tiền ảo uy tín. Khi người dân tin tưởng, đầu tư vào các sàn chứng khoán, tiền ảo này sẽ bị chiếm đoạt toàn bộ số tiền.

Quảng cáo trên các mạng xã hội, gọi điện, nhắn tin trực tiếp cho người dân hoặc tổ chức các cuộc hội thảo, tuyên truyền ở nhiều nơi trên cả nước để mời người dân góp vốn tham gia vào các dự án ảo, mua cổ phần của các công ty nước ngoài do chúng dựng lên để được hưởng lợi nhuận khủng. Ngoài ra khi người dân rủ thêm được người khác đầu tư sẽ được chiết khấu hoa hồng từ khoản đầu tư của người đến sau. Bằng cách dùng tiền của người đến sau trả lãi cho người đến trước các đối tượng lôi kéo được rất nhiều người tham gia thu được số tiền cực kỳ lớn lúc này các đối tượng sẽ chiếm đoạt toàn bộ số tiền và cắt đứt liên lạc với người dân.

LỪA ĐẢO DỊCH VỤ TRÊN MẠNG INTERNET ĐỂ CHIẾM ĐOẠT TÀI SẢN

Quảng cáo trên các mạng xã hội đăng bán các loại tài khoản có tính phí như Google drive, Onedrive, Youtube Premium, Canva, Netflix… với giá rẻ hơn giá của nhà cung cấp dịch vụ. Khi có người đăng ký các đối tượng tư vấn mua các gói thời gian dài từ 06, 12 tháng trở lên để được hưởng ưu đãi giá rẻ, những tài khoản này sau đó chỉ sử dụng được khoảng 01 tháng người mua sẽ bị chiếm đoạt số tiền đóng trước cho các tháng tiếp theo.

Quảng cáo trên các mạng xã hội dịch vụ lấy lại tài khoản Facebook bị mất, mở khóa Facebook vi phạm chính sách của nhà phát hành, đăng ký tick xanh Facebook, tăng like, tăng share, tăng tương tác bán hàng… Khi người dân có nhu cầu các đối tượng yêu cầu người dân thanh toán trước phí dịch vụ rồi chiếm đoạt.

Quảng cáo trên các mạng xã hội dịch vụ cho số đánh đề. Khi người dân nhắn tin mua số các đối tượng sẽ cho các số ngẫu nhiên nếu trúng sẽ yêu cầu người dân chi trả tiền hoa hồng.

GIẢ MẠO TRANG THÔNG TIN ĐIỆN TỬ CỦA CƠ QUAN, DOANH NGHIỆP, NGÂN HÀNG

Tạo website giả mạo có giao diện giống với website của các cơ quan, doanh nghiệp, ngân hàng. Người dân khi thực hiện khai báo thông tin trên các website này sẽ bị đánh cắp thông tin cá nhân và chiếm đoạt tiền trong tài khoản ngân hàng.

GIẢ MẠO DỊCH VỤ LẤY LẠI TIỀN CHUYỂN NHẦM, TIỀN BỊ LỪA ĐẢO QUA MẠNG

Sau khi các đối tượng lừa đảo chiếm đoạt tài sản của người dân, các đối tượng gọi điện cho nạn nhân tự xưng là Công an, Ngân hàng thông báo các đối tượng lừa đảo đã bị bắt để được nhận lại tiền bị chiếm đoạt người dân cần cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng hoặc chuyển tiền để xác minh danh tính sau đó tiếp tục chiếm đoạt số tiền.

Tạo trang cá nhân, Fanpage, Nhóm trên mạng xã hội quảng cáo là luật sư, nhân viên ngân hàng có thể giúp người dân lấy lại tiền đã bị lừa qua mạng, lấy lại tiền chuyển khoản nhầm. Yêu cầu người dân thanh toán phí hoặc cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng, mã OTP để chiếm đoạt tài sản.

LỪA ĐẢO CHUYỂN TIỀN

Gửi tin nhắn giả nội dung chuyển tiền giống với tin nhắn thông báo giao dịch được cộng tiền vào tài khoản của ngân hàng gửi đến số điện thoại của người dân sau đó liên lạc báo bị chuyển nhầm tiền và yêu cầu người dân chuyển trả tiền vào tài khoản do chúng cung cấp.	Chuyển tiền đến tài khoản của người dân kèm theo tin nhắn xác nhận vay tiền thành công. Sau khoảng 01 tuần sẽ liên lạc đòi tiền kèm theo lãi suất cao. Các đối tượng sẽ dọa nạt, bôi nhọ, uy hiếp tinh thần nếu bị hại không trả tiền.

SỬ DỤNG ỨNG DỤNG GIẢ MẠO CHIẾM QUYỀN ĐIỀU KHIỂN ĐIỆN THOẠI DI ĐỘNG

Giả làm Công an, Cơ quan nhà nước gọi điện hướng dẫn người dân cài đặt ứng dụng để kích hoạt tài khoản định danh điện tử VNeID, khai báo nộp thuế… Khi người dân cài đặt ứng dụng do đối tượng cung cấp sẽ bị chiếm quyền điều khiển điện thoại và chiếm đoạt tiền trong tài khoản ngân hàng.

Làm giả các trò chơi, ứng dụng điện thoại có tính phí trên cửa hàng ứng dụng của điện thoại đăng tải miễn phí lên các website, mạng xã hội (Zalo, Facebook…) Khi người dân cài đặt ứng dụng này sẽ bị chiếm quyền điều khiển điện thoại và chiếm đoạt tiền trong tài khoản ngân hàng.

CƠ QUAN CÔNG AN KHUYẾN CÁO VÀ ĐỀ NGHỊ

- **KHÔNG** đăng tải, chia sẻ thông tin cá nhân lên mạng Internet.
- **KHÔNG** truy cập vào các website mà trình duyệt web cảnh báo nguy hiểm, **KHÔNG** nhấn vào các đường link lạ.
- **KHÔNG** chuyển tiền cho bất kỳ ai thông qua điện thoại, internet mà chưa biết rõ về họ. Khi người quen, người thân hỏi mượn tiền, nhờ chuyển tiền hãy gọi điện để xác nhận lại thông qua kênh liên lạc khác.
- Cơ quan nhà nước **KHÔNG** làm việc qua điện thoại, nếu cần sẽ mời đến trụ sở làm việc.
- Tuyệt đối **KHÔNG** cung cấp mã **OTP**, tài khoản, mật khẩu Internet Banking, Mobile Banking cho bất kỳ ai.
- Đa số các cách kiếm tiền dễ dàng trên mạng xã hội, mạng Internet đều là các hành vi lừa đảo chiếm đoạt tài sản **HÃY CẢNH GIÁC.**

Cập nhật các thông tin mới nhất về thủ đoạn của tội phạm sử dụng công nghệ cao tại Fanpage "Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an Lạng Sơn"

https://www.facebook.com/anninhmanglangson