**BÀI TUYÊN TRUYỀN**

# Cảnh báo một số thủ đoạn lừa đảo

# chiếm đoạt tài sản sử dụng công nghệ cao và cách phòng ngừa

--------------------

#  Trong thời gian gần đây, trên địa bàn cả nước nói chung và trên địa bàn thành phố Kon Tum nói riêng, xuất hiện một số thủ đoạn lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao như thông qua nhiều cuộc gọi, tin nhắn, thư điện tử giả mạo, lừa đảo với mục đích chiếm đoạt tài sản với nhiều phương thức, thủ đoạn hoạt động mới tinh vi, gây thiệt hại tài sản nghiêm trọng, ảnh hưởng tâm lý người dân, gây bức xúc trong dư luận xã hội. Trước tình hình trên, Ủy ban nhân dân thành phố đề nghị các cơ quan, ban ngành thành phố, Ủy ban Mặt trận Tổ quốc Việt Nam, các đoàn thể thành phố và Ủy ban nhân dân xã, phường tăng cường tuyên truyền, cảnh báo một số phương thức, thủ đoạn phổ biến qua mạng internet, mạng viễn thông và các dịch vụ bưu chính để người dân kịp thời nhận diện, cảnh giác và phòng ngừa.

**1.** Giả mạo tài khoản mạng xã hội (Facebook, Zalo,…), hộp thư điện tử của các đồng chí lãnh đạo, nguyên lãnh đạo Đảng, Nhà nước các cấp bằng cách thiết lập tài khoản mạng xã hội, hộp thư điện tử với tên tương tự, hình ảnh đại diện là hình ảnh của các đồng chí lãnh đạo Đảng, Nhà nước, kết bạn với cán bộ, nhân viên cấp dưới sau đó mạo danh chỉ đạo chuyển tiền phục vụ công việc cơ quan hoặc vay mượn xử lý công việc và đề nghị chuyển tiền đến tài khoản ngân hàng được chỉ định sẵn để chiếm đoạt.

 **\* Cách phòng ngừa:** Nếu thấy có tin nhắn từ tên của lãnh đạo, người thân, bạn bè yêu cầu chuyển tiền, vay mượn tiền qua các mạng xã hội, hộp thư điện tử thì gọi điện thoại trực tiếp (nếu có thể thì gọi video trực tiếp) cho người đó để xác minh thông tin chính xác trước khi chuyển tiền, 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, giả mạo tài khoản mạng xã hội.

**2.** Giả mạo lực lượng Công an, Viện kiểm sát, Tòa án gọi điện thông báo nạn nhân đang liên quan đến một vụ việc nghiêm trọng như mua bán, tàng trữ, sử dụng ma túy, gây tai nạn bỏ trốn, lừa đảo xuyên quốc gia; giả danh nhân viên bưu điện thông báo nhận bưu phẩm, nhân viên viễn thông thông báo nợ cước, nhân viên điện lực thông báo nợ tiền điện... Khi nạn nhân trả lời mình không liên quan hoặc không phải là tội phạm được nói đến, các đối tượng lừa đảo sẽ khai thác thông tin cá nhân hoặc nói rằng có thể thông tin cá nhân của nạn nhân bị lợi dụng để thực hiện các hành vi vi phạm pháp luật, từ đó dẫn dụ nạn nhân làm theo những yêu cầu của đối tượng.

**\* Cách phòng ngừa:** Khi nghe điện thoại, người dân cần nêu cao cảnh giác nguy cơ bị lừa đảo chiếm đoạt tài sản đối với các cuộc điện thoại tự nhận là cơ quan chức năng đang điều tra, giải quyết vụ án, vụ việc qua điện thoại, yêu cầu chuyển tiền vào tài khoản. Theo quy định của pháp luật, người dân chỉ làm việc với cán bộ các cơ quan pháp luật tại trụ sở, không làm việc qua điện thoại, qua mạng xã hội; khi làm việc với người dân thì các cơ quan chức năng (Công an, Viện kiểm sát, Tòa án, Thi hành án, Thuế,...) đều có giấy giới thiệu, giấy mời hoặc trực tiếp gặp mặt để trao đổi công việc và không có quy định gọi điện thoại yêu cầu chuyển tiền.

**3.** Đánh cắp thông tin tài khoản ngân hàng với một số phương thức, thủ đoạn:

- Giả mạo nhân viên của sàn thương mại điện tử, trung tâm mua sắm, đài truyền hình, công ty xổ số... gọi điện hoặc nhắn tin cho nạn nhân thông báo họ may mắn nhận được phần thưởng giá trị cao của một chương trình nào đó, thúc giục nạn nhân nếu không thực hiện ngay những yêu cầu đưa ra thì sẽ không có cơ hội nhận được phần thưởng giá trị nữa. Từ đó, các đối tượng yêu cầu nạn nhân cung cấp mã OTP gửi về điện thoại hay đưa ra bất kỳ lý do nào khác để yêu cầu nạn nhân cung cấp thông tin về thẻ hoặc tài khoản ngân hàng điện tử nhằm trộm tiền trong tài khoản.

- Giả danh ngân hàng để gọi điện, gửi tin nhắn, email,... mời chào, cung cấp các khoản vay online từ ngân hàng. Các đối tượng thường tiếp cận với nạn nhân bằng cách gọi điện thoại, gửi tin nhắn, email qua các ứng dụng nhắn tin miễn phí. Sau đó hướng dẫn nạn nhân làm thủ tục vay hoặc mở thẻ tín dụng qua trang web giả mạo ngân hàng; gửi các văn bản giả “xác nhận phê duyệt khoản vay” cho nạn nhân để tạo niềm tin và yêu cầu nạn nhân nộp tiền lệ phí hoặc tiền trả góp đợt đầu vào tài khoản chỉ định rồi chiếm đoạt.

- Lừa đảo bằng cách gửi tin nhắn rác vào tài khoản người dùng với nội dung tuyển dụng cộng tác viên, nhân viên làm việc trực tuyến tại nhà với thu nhập cao. Khi nạn nhân làm theo hướng dẫn trong tin nhắn, các đối tượng sẽ tự xưng là nhân viên tư vấn, tuyển dụng của một công ty nào đó hay giả mạo là nhân viên của sàn thương mại điện tử để yêu cầu nạn nhân cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng sau đó chiếm đoạt tiền

**\* Cách phòng ngừa:** Không tin vào những chiêu trò nhận thưởng qua mạng với yêu cầu cung cấp thông tin về thẻ hoặc tài khoản ngân hàng điện tử để làm thủ tục nhận thưởng; Theo quy định, các ngân hàng không yêu cầu khách hàng cung cấp thông tin tài khoản, thẻ ngân hàng, ví điện tử, mã OTP hoặc bất kỳ thông tin cá nhân của khách hàng qua mail/tin nhắn hay gọi điện thoại; không tò mò nhấn vào các đường link lạ, tuyệt đối không cung cấp các thông tin tài khoản ngân hàng cho bất kỳ cá nhân, tổ chức nào thông qua các cuộc gọi, đường link gửi bằng mail/tin nhắn.

**4.** Tự giới thiệu là người nước ngoài, liên lạc để tạo mối quan hệ với nạn nhân, sau đó đối tượng lừa đảo sẽ thông báo muốn gửi tiền, quà từ nước ngoài về Việt Nam; đề nghị nạn nhân nộp các khoản tiền như thuế, phí, cước vận chuyển,... vào tài khoản ngân hàng do các đối tượng cung cấp để nhận quà.

**\* Cách phòng ngừa:** Cảnh giác với các cuộc điện thoại từ số máy lạ, nhất là các số máy có đầu số nước ngoài; tuyệt đối không cung cấp thông tin cho tổ chức, cá nhân nào khi chưa biết họ là ai và sử dụng vào mục đích gì. Giữ bí mật, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở, thông tin về tài khoản ngân hàng, tài khoản các dịch vụ trên internet... cho bất kỳ người lạ nào gọi đến.

**5.** Thông qua các ứng dụng trên nền tảng mạng xã hội, các đối tượng lừa đảo lập các trang thông tin tuyển dụng để đưa thông tin quảng cáo về công việc nhẹ, phù hợp với mọi trình độ, hưởng lương cao, kèm theo chế độ đãi ngộ hấp dẫn. Sau khi nạn nhân đồng ý làm việc, các nhóm tội phạm sẽ liên hệ và tổ chức xuất cảnh trái phép ra nước ngoài làm việc. Sau khi sang nước ngoài, nạn nhân sẽ bị bán vào các sòng bạc, bị cưỡng bức lao động từ 15 - 16 giờ/ngày và bị ngược đãi về mặc tinh thần lẫn thể chất. Khi muốn thôi việc và quay về Việt Nam buộc phải “bồi thường hợp đồng lao động” với số tiền lớn.

**\* Cách phòng ngừa:** Cảnh giác với các trang thông tin tuyển dụng với thông tin quảng cáo “việc nhẹ, lương cao” trên mạng. Cần gọi ngay Trung tâm tư vấn việc làm tại địa phương để được hỗ trợ.

 **6.** Các đối tượng lừa đảo, tội phạm công nghệ cao thực hiện thủ đoạn giả danh nhân viên chăm sóc khách hàng của các nhà mạng, ngân hàng, ví điện tử để hỗ trợ giải quyết sự cố. Sau đó, kẻ xấu yêu cầu khách hàng nhắn tin theo cú pháp \*\*21\*#.

Tuy nhiên, cú pháp \*\*21\*# thực chất là cú pháp chuyển hướng cuộc gọi (Call Forward) - dịch vụ của các nhà mạng như Mobifone, Vinaphone, Vietnamobile cho phép thuê bao di động chuyển hướng cuộc gọi đến một số điện thoại nội mạng hoặc ngoại mạng. Sau đó, các đối tượng sẽ thao tác đăng nhập ứng dụng ví Momo của nạn nhân từ xa. Tổng đài Momo sẽ gọi để cung cấp mã OTP, tuy nhiên cuộc gọi này chuyển hướng đến số điện thoại của đối tượng. Từ đó kẻ xấu chiếm đoạt tiền trong ví, tài khoản ngân hàng liên kết với ví.

Kẻ xấu cũng có thể yêu cầu khách hàng nhắn tin theo cú pháp DS gửi 901. Đây là cú pháp đổi sim điện thoại qua phôi sim trắng theo phương thức nhắn tin (SMS). Sau đó, kẻ xấu sẽ nhắn tin lừa đảo rằng giúp người dùng nâng cấp sim điện thoại thành SIM 4G, 5G.

Các đối tượng này yêu cầu người dùng nhắn tin theo cú pháp trên. Khi thao tác thành công, người dùng sẽ mất quyền kiểm soát sim vì sim của đối tượng lừa đảo trở thành sim “chính chủ" và truy cập vào ứng dụng ví điện tử, ứng dụng thanh toán online để chiếm đoạt tiền.

**\* Cách phòng ngừa:** không cung cấp mật khẩu và mã xác thực (OTP) của ví điện tử cho bất kỳ ai bên ngoài ứng dụng. Người dân không bấm vào đường link lạ để nhập mật khẩu và mã xác thực (OTP); đồng thời luôn tra cứu, tìm hiểu thông tin để nắm chắc mục đích, ý nghĩa của các cú pháp tin nhắn trước khi thực hiện.

**7.** Tuyển nhân viên bán hàng online: Theo đó, cá nạn nhân bị các đối tượng mạo danh nhân viên của Shopee, Lazada, Tiki… lôi kéo tham gia cộng tác viên bán hàng online với hoa hồng từ 10-20% hoặc thu nhập từ 200.000 đồng đến 700.000 đồng/ngày, không cần bằng cấp, kinh nghiệp, làm việc tại nhà, có sử dụng thẻ ATM, điện thoại, laptop… rồi yêu cầu đăng nhập vào đường link tham gia bằng cách để lại số điện thoại. Sau khi người bị hại để lại số điện thoại thì 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 hướng dẫn đặt đơn hàng có giá trị nhỏ bằng cách chuyển tiền mua sản phẩm vào tài khoản ngân hàng do đối tượng chỉ định và chụp hình chuyển tiền gửi lại cho đối tượng để xác thực. Sau đó, bị hại được thanh toán lại tiền mua hàng kèm tiền hoa hồng như đã hứa để tạo lòng tin. Tuy nhiên, khi bị hại nộp số tiền lớn để mua hàng, lúc này các đối tượng liên tục đưa ra nhiều lý do khác nhau để yêu cầu mua thêm hàng. Nạn nhân vì muốn lấy lại số tiền mua sản phẩm ban đầu nên cứ làm theo và bị chiếm đoạt tiền nhiều lần.

Chiếm quyền quản lý tài khoản mạng xã hội người khác rồi mạo danh nhắn tin mượn tiền: Các đói tượng tạo ra các website giải mạo có dạng: Bình chọn siêu nhí, giọng hát Việt nhí, bình chọn hoa khôi… có chứa các ô nhập thông tin tài khoản Facebook rồi nhắn tin gửi đường link trang web này có chứa mã độc đến các tài khoản Facebook. Khi có người đăng nhập vào đường link chứa mã độc, đối tượng xấu dễ dàng đánh cắp mật khẩu, chiếm đoạt tài khoản mạng xã hội. Sau khi chiếm đoạt tài khản Facebook hoặc Zalo, chúng xem kỹ lịch sử giao dịch, tin nhắn trao đổi giữa bạn bè hoặc người thân với chủ tài khoản, từ đó lựa chọn tài khoản để dàn dựng kịch bản từ đảo nhờ chuyển tiền hoặc mượn tiền.

**\* Những việc cần làm ngay sau khi trở thành nạn nhân của tội phạm lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao**, bao gồm:

- Không lấy lại tài sản bị mất bằng cách chuyển thêm tiền theo yêu cầu của đối tượng.

- Liên hệ ngay với ngân hàng chủ quản hoặc công ty nơi mở tài khoản ví điện tử để yêu cầu khóa thẻ, ví điện tử, dựng mọi giao dịch liên quan đến tài khoản ngân hàng, ví điện tử.

- Thông báo ngay cho người thân, bạn bè, đối tác kinh doanh biết việc tìa khoản mạng xã hội của mình sử dụng đã bị kẻ xấu chiếm quyền quản lý, đồng thời lấy lại quyền quản lý tài khoản.

- Đến cơ quan Công quan để trình báo vụ việc.

Dự báo thời gian tới, hoạt động của tội phạm lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao sẽ vẫn tiếp diễn, với phương thức, thủ đoạn ngày càng tinh vi, có khả năng gây thiệt hại lớn cho người dân, ảnh hưởng đến uy tín của cá nhân, cơ quan, doanh nghiệp. Đề nghị các tầng lớp nhân dân trên địa bàn thành phố đề cao cảnh giác, chủ động, tăng cường các biện pháp tự phòng ngừa, bảo vệ tài sản; kịp thời thông báo cho cơ quan Công an nơi gần nhất để được tiếp nhận và hướng dẫn giải quyết theo quy định khi có vụ việc xảy ra./.