CÔNG AN QUẬN BÌNH TÂN

THÔNG TIN TUYÊN TRUYỀN

Phòng chống tội phạm sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản

Thời gian qua, xuất hiện ngày càng nhiều thủ đoạn lừa đảo, chiếm đoạt tài sản trên không gian mạng, người dân cần lưu ý để nhận biết, phòng tránh và chủ động phòng ngừa, không trở thành nạn nhân của tội phạm sử dụng công nghệ cao lừa đảo qua mạng, Công an quận Bình Tân cảnh báo một số thủ đoạn phạm tội để thông tin đến người dân:

*** Thủ đoạn thứ nhất**, các đối tượng giả mạo cơ quan công an, viện kiểm sát, toà án thông báo người bị hại liên quan đến vụ án hình sự và yêu cầu chuyển toàn bộ tiền có trong tài khoản với lý do để kiểm tra nguồn gốc, sẽ trả lại sau và đe dọa nếu không chuyển tiền sẽ bị bắt giam.

*** Thủ đoạn thứ 2**, đối tượng sử dụng SIM điện thoại đăng ký không chính chủ hoặc thông qua mạng xã hội Facebook, Zalo mạo danh các công ty viễn thông gửi tin nhắn thông báo khách hàng trúng các phần thưởng có giá trị; yêu cầu nạn nhân gửi tiền vào các tài khoản ngân hàng do chúng chuẩn bị trước hoặc mua các thẻ cào điện thoại để chuyển cho chúng làm thủ tục nhận thưởng, nhằm lừa đảo chiếm đoạt tài sản.

*** Thủ đoạn thứ 3,** đối tượng sử dụng Sim điện thoại đăng ký không chính chủ giả danh nhân viên ngân hàng gọi điện thông báo có chương trình tri ân khách hàng, đề nghị nạn nhân cung cấp số điện thoại đăng ký dịch vụ internet banking và mã xác thực OTP (là mã do ngân hàng cung cấp để thực hiện giao dịch chuyển nhận tiền) để nhận quà tặng là một khoản tiền có giá trị lớn từ ngân hàng. Sau khi nạn nhân cung cấp các thông tin này, chúng chiếm quyền sử dụng dịch vụ internet banking và chuyển toàn bộ số tiền có trong tài khoản ngân hàng của nạn nhân sang tài khoản chúng đã chuẩn bị trước để chiếm đoạt.

*** Thủ đoạn thứ 4,** các đối tượng sử dụng Sim đăng ký không chính chủ, mạo danh nhân viên nhà mạng gọi điện, nhắn tin cho chủ thuê bao, lấy lý do hỗ trợ khách hàng nâng cấp Sim từ 3G lên 4G, yêu cầu khách hàng làm theo cú pháp, truy cập đường link do chúng cung cấp. Nếu làm theo, Sim của chủ thuê bao sẽ bị khóa, thông tin của số thuê bao được chuyển sang SIM mới của đối tượng. Trong thời gian chiếm quyền kiểm soát Sim, đối tượng bẻ khóa, truy cập vào các tài khoản của chủ thuê bao gắn với số điện thoại cá nhân, nhất là tài khoản thẻ tín dụng; mục đích chiếm quyền sử dụng số điện thoại để phá bảo mật, nhận mã OTP từ nhà cung cấp dịch vụ hay ngân hàng để có thể bẻ khóa, xâm nhập chiếm đoạt tiền trong tài khoản.

*** Thủ đoạn thứ 5,** thông qua mạng xã hội Facebook, đối tượng giới thiệu là người nước ngoài kết bạn, làm quen với nạn nhân, nhằm tán tỉnh, yêu đương, rồi đề nghị chuyển quà như trang sức, mỹ phẩm và ngoại tệ số lượng lớn qua đường hàng không về Việt Nam để làm quà tặng; tiếp theo giả danh nhân viên sân bay yêu cầu nạn nhân chuyển tiền vào tài khoản ngân hàng cho chúng với lý do làm thủ tục nhận hàng, nhằm thực hiện hành vi lừa đảo chiếm đoạt tài sản.

*** Thủ đoạn thứ 6,** đối tượng đánh cắp quyền truy cập các tài khoản mạng xã hội, sử dụng mạo danh chủ tài khoản nhắn tin đề nghị chuyển hộ tiền, vay tiền hoặc mua thẻ cào điện thoại gửi cho chúng.

*** Thủ đoạn thứ 7,** đối tượng gọi điện đến các thuê bao di động, hoặc qua mạng xã hội giới thiệu là có người nhà làm trong các công ty xổ số có khả năng biết trước kết quả, sau đó đối tượng gửi số lô, số đề; hứa cung cấp tiền để nạn nhân mua số lô, số đề, chia phần trăm hoa hồng cho đối tượng; sau đó đối tượng thông tin hết tiền, đề nghị nạn nhân ứng tiền mua số lô, số đề. Nếu may mắn trúng số lô, số đề, nạn nhân gửi tiền hoa hồng cho đối tượng và bị chiếm đoạt.

*** Thủ đoạn thứ 8,** đối tượng tạo ra các ứng dụng, website cho vay tiền, quảng cáo trên mạng xã hội (Facebook, Zalo) với mục đích tìm người muốn vay tiền để thực hiện hành vi lừa đảo. Sau khi người muốn vay tiền tải ứng dụng về điện thoại; đăng nhập thông tin theo yêu cầu, thì hệ thống website gửi tin nhắn qua Facebook, Zalo trực tuyến tại bộ phận xét duyệt và thông báo nếu muốn vay tiền thì người vay phải đóng lãi số tiền vay trước thì mới được gửi mã mật khẩu để rút tiền.

Sau khi người vay tiền chuyển tiền vào tài khoản do các đối tượng cung cấp thì hệ thống thông báo người chuyển tiền nhập sai số tài khoản nên bị đóng băng và yêu cầu người vay phải chuyển thêm tiền để kích hoạt lại tài khoản, số lần yêu cầu người vay tiền chuyển khoản thường không có giới hạn; toàn bộ số tiền người vay chuyển khoản vào tài khoản của các đối tượng chuẩn bị trước bị chiếm đoạt.

*** Thủ đoạn thứ 9,** đối tượng tạo lập các trang, tài khoản mạng xã hội (chủ yếu trên Zalo, Facebook), sau đó đăng tải các bài viết, tạo dựng, cung cấp những nội dung không có thật về cơ quan, tổ chức, cá nhân đang gặp hoàn cảnh khó khăn cần sự hỗ trợ, giúp đỡ; cung cấp tài khoản ngân hàng, đề nghị, kêu gọi chuyển tiền trợ giúp. Nếu người muốn trợ giúp chuyển tiền thì bị đối tượng chiếm đoạt.

*** Thủ đoạn thứ 10,** đối tượng lập công ty, website tổ chức kinh doanh sàn ngoại hối (forex), tiền điện tử (altcoin). Để thu hút "nhà đầu tư", đối tượng đưa những người tự xưng là chuyên gia về lĩnh vực tài chính, làm quen rồi chia sẻ kinh nghiệm, gọi điện thoại trực tiếp hoặc thông qua mạng xã hội mời người dân tham gia. Các đối tượng khẳng định lợi nhuận rất cao, khi người dân tham gia, nộp tiền để "đầu tư" thì bị chiếm đoạt.

*** Thủ đoạn thứ 11,** các đối tượng kết nối, giao tiếp với nạn nhân với nội dung tuyển dụng việc làm online. Sau khi nạn nhân liên lạc, đồng ý thì đối tượng giao việc ứng tiền của nạn nhân để chuyển đến các tài khoản do đối tượng chỉ định, sau khi thực hiện thành công, các đối tượng chuyển khoản trả cả tiền gốc và tiền công cho nạn nhân (với số tiền công lớn để tạo lòng tin của nạn nhân). Sau một vài giao dịch thành công, do được hưởng lợi lớn và tin tưởng đối tượng sẽ chuyển trả lại tiền nên các nạn nhân đã thực hiện chuyển số tiền lớn đến các tài khoản ngân hàng theo yêu cầu của đối tượng. Sau đó, đối tượng không chuyển trả tiền như đã hứa hẹn và cắt liên lạc với nạn nhân.

*** Thủ đoạn thứ 12,** đối tượng sử dụng thông tin cá nhân giả mạo đăng ký các tài khoản mạng xã hội (Facebook, Zalo), sau đó, tìm kiếm những người bán hàng trực tuyến trên mạng xã hội để kết bạn và nhắn tin mua hàng. Sau khi người bán hàng đồng ý, thì các đối tượng sẽ yêu cầu người bán hàng gửi thông tin tài khoản ngân hàng có đăng ký dịch vụ Internet banking, số điện thoại của mình cho đối tượng.Sau khi nhận được thông tin, đối tượng sẽ tạo cớ chuyển tiền mua hàng không thành công, đề nghị người bán hàng truy cập vào trang web

giả mạo của ngân hàng để nhập đầy đủ thông tin như: Tên tài khoản, số tài khoản và mã OTP để hoàn tất thủ tục nhận tiền. Khi nạn nhân nhập thông tin và mã OTP thì các đối tượng chiếm quyền sử dụng dịch vụ Internet banking của tài khoản ngân hàng đó và ngay lập tức sẽ rút toàn bộ số tiền trong tài khoản của nạn nhân chuyển tới tài khoản khác để chiếm đoạt.

*** Thủ đoạn thứ 13,** các đối tượng giả danh là nhân viên của đơn vị phát hành thẻ tín dụng, gọi điện thoại tư vấn các chủ thẻ tín dụng rút tiền mặt qua phần mềm; sau khi nạn nhân đồng ý, các đối tượng yêu cầu chụp hình 2 mặt thẻ tín dụng và cung cấp mã OTP; sau đó chúng thực hiện quẹt thẻ thông qua các gian hàng trên 1 website để chuyển đổi tiền từ thẻ của nạn nhân sang tài khoản ví điện tử của các đối tượng để chiếm đoạt.

*** Thủ đoạn thứ 14,** dụ phụ huynh nộp tiền "làm nhiệm vụ" để con thành người mẫu nhí. Các đối tượng lừa đảo thông qua các trang mạng xã hội đăng tải thông tin: "Tuyển người mẫu nhí từ 2 - 15 tuổi. Thu nhập tại gia cùng bé từ 7 - 15 triệu đồng/tháng, hoa hồng hấp dẫn". Phụ huynh chỉ cần có Zalo, thẻ ngân hàng để đăng ký làm việc, nhận lương và được yêu cầu kết bạn Zalo với đối tượng xưng là nhân viên bộ phận nhân sự, để đăng ký hồ sơ cho con và tham gia nhóm Telegram là đủ điều kiện tham gia. Nhóm do các nghi can lập ra, chỉ có 1 - 2 người (nạn nhân) là thật, còn lại đều là nick ảo do chính các nghi can lập để dẫn dắt câu chuyện, nhằm lừa đảo. Để bé được xét tuyển chính thức, các đối tượng sẽ yêu cầu nạn nhân lần lượt hoàn thành 5 "nhiệm vụ mua sản phẩm" với hứa hẹn sẽ được hoàn lại tiền gốc và lãi theo phần trăm hoa hồng từ giá trị sản phẩm. Sau nhiệm vụ 1, nhiệm vụ 2 với sản phẩm phải thanh toán có mệnh giá thấp, bị hại sẽ được hoàn trả tiền gốc và lãi 10%. Đến nhiệm vụ thứ 3, sản phẩm sẽ có giá hàng triệu đồng. Khi nạn nhân chuyển khoản thì sẽ được thông báo sai số lượng, số tiền bị đóng băng và yêu cầu nạn nhân phải chuyển lại từ đầu nhiệm vụ 3, với số tiền gấp đôi thì mới được xem là hoàn thành nhiệm vụ. Các đối tượng sẽ tiếp tục dẫn dụ "Nhiệm vụ 5 cũng là nhiệm vụ cuối cùng, phụ huynh được hoàn tiền kèm lãi suất và bé nhà sẽ được chính thức thành mẫu ảnh nhí" để nạn nhân tin và tiếp tục chuyển tiền.

*** Thủ đoạn thứ 15,** hiện nay đa phần người dân đã chuyển sang sử dụng CCCD gắn chip, so với CMND và CCCD mã vạch thì CCCD gắn chip chứa đựng được nhiều thông tin hơn qua việc quét mã QR và chip điện tử gắn trên thẻ. Điều này đã vô tình tạo cơ hội cho kẻ xấu lợi dụng để sử dụng vào mục đích vi phạm pháp luật, nhất là các tội phạm công nghệ cao. Người dân không nên chia sẻ hình ảnh CMND/CCCD không làm mờ thông tin ra ngoài, bởi các đối tượng có thể lấy thông tin, ảnh chụp và thực hiện các giao dịch vay tiền trên app chỉ thông qua ảnh chụp CMND/CCCD và thông tin cá nhân nhằm mục đích chiếm đoạt; Bị sử dụng thông tin để đăng ký thuê bao trả sau của các nhà mạng, sau đó, chúng thực hiện những cuộc gọi quốc tế, hoặc thực hiện các cuộc gọi trong nước một cách vô tội vạ và chủ thẻ có thể phải chịu các khoản phí nợ cước...; Bị các công ty ảo sử dụng thông tin cá nhân, ảnh chụp CMND/CCCD để đăng ký mã số thuế nhằm qua mặt các cơ quan chức năng…

*** Thủ đoạn thứ 16,** đối tượng tham gia vào các nhóm phụ huynh có con em đang học tại các trường điểm trên địa bàn thành phố, tội phạm lừa đảo sẽ lập các group dạy thêm, học thêm, đăng thông tin của những thầy cô nổi tiếng, có uy tín trong trường; sau đó đưa ra các khoá học, chương trình dạy học, khoá luyện thi vào các trường nổi tiếng, trường điểm; đánh vào tâm lý muốn con theo học của phụ huynh, để phụ huynh đăng ký, sau khi đăng ký chúng yêu cầu phụ huynh chuyển một số tiền nhất định để đóng tiền cọc khoá học, đóng tiền học phí, từ đó chiếm đoạt.

*** Thủ đoạn thứ 17,** đối tượng lừa mua xe gắn máy, laptop, đồ dung công nghệ… giá rẻ: tội phạm sử dụng mạng Zalo, Facebook, sim không chính chủ lập trang mạng bán xe máy, laptop rẻ, hàng trốn thuế, đánh vào tâm lý ham rẻ của người dân, khi người dân liên hệ đăng ký mua, chúng sẽ yêu cầu chuyển một số tiền nhất định để làm tin, sau đó thông báo, thời gian giao hàng; gần đến thời gian giao hàng chúng sẽ lấy lý do thuyết phục yêu cầu bị hại chuyển thêm tiền để làm thủ tục, giấy tờ, sau khi nạn nhân chuyển tiền xong sẽ chiếm đoạt và chặn số lien lạc. Các đối tượng thường sẽ có một kịch bản rất thuyết phục như gửi giấy tờ xe đăng ký tên khách hàng trước, hóa đơn mua bán, giấy tờ này cũng là giấy tờ giả, khiến nạn nhân tin tưởng và tiếp tục chuyển tiền cho chúng. Bằng thủ đoạn này, tội phạm có thể lừa bán nhiều loại hàng hoá khác nhau, khi mua khách hàng phải cọc một số tiền nhất định và tội phạm tiến hành chiếm đoạt.

*** Thủ đoạn thứ 18,** gọi điện cho phụ huynh học sinh, thông báo con em học sinh bị tai nạn, đang phối hợp với cô giáo, nhà trường đưa học sinh đi cấp cứu, cần phụ huynh chuyển tiền gấp vào tài khoản để làm thủ tục nhập viện, đóng viện phí, đóng chi phí khác. Bằng cách đánh vào tâm lý lo lắng cho con em, tội phạm đã yêu cầu phụ huynh phải chuyển tiền, sau đó chiếm đoạt.

***Thủ đoạn thứ 19,** gọi điện thông báo cho nạn nhân, nội dung thông báo là nạn nhân ‘‘đã mở tài khoản dịch vụ tại công ty tài chính toàn cầu”, hoặc một công ty khác cụ thể, thực tế nạn nhân không mở; chúng đối tượng sẽ yêu cầu nạn nhân để huỷ dịch vụ phải thực hiện một số thao tác nhấn vào đường link do chúng gửi đến, sau đó điền các thông tin cá nhân vào, trong đó có cả thông tin tài khoản ngân hàng, lúc này tài khoản ngân hàng của nạn nhân sẽ bị chúng rút tiền và chiếm đoạt.

*** Thủ đoạn thứ 20,** gửi thông báo cho người dân may mắn đã trúng thưởng chương trình quay thưởng, yêu cầu người dân liên kết thẻ ngân hàng, đăng nhập vào đường link, nhập số tài khoản, mã OTP để nhận tiền; qua đó rút tiền trong tài khoản của người dân chiếm đoạt tài sản.

Công an quận Bình Tân đề nghị cán bộ, công nhân viên chức, đoàn viên, hội viên, người lao động, học sinh, sinh viên và Nhân dân cần nâng cao ý thức cảnh giác, thường xuyên cập nhật thông tin về các vụ lừa đảo sử dụng công nghệ cao để có thông tin đầy đủ về phương thức thủ đoạn của tội phạm; cần chủ động bảo vệ thông tin cá nhân của mình cũng như người thân, coi đó là tài sản riêng hợp pháp, không khai báo thông tin cá nhân trong những trường hợp không cần thiết; thực hành thói quen sử dụng mạng an toàn, ngay khi phát hiện những dấu hiệu bất thường phải có ý thức tự bảo vệ như thực hiện đổi mật khẩu tài khoản, thông báo cho bạn bè, người thân biết việc tài khoản riêng của mình có thể bị xâm nhập trái phép để tránh bị lừa đảo; Nhanh chóng đến cơ quan Công an gần nhất để trình báo trong trường hợp bị chiếm đoạt tài sản (Các số điện thoại trình báo). /.

* Số điện thoại trực ban của Công an TP. Hồ Chí Minh: **069.3187.344,** hoặc số điện thoại của trực ban Phòng Cảnh sát Hình sự - CATP. Hồ Chí Minh**:** **069.3187.200** để cung cấp thông tin, phối hợp điều tra, xử lý khi nhận được cuộc gọi lừa đảo.

* Số điện thoại trực ban Công an quận Bình Tân: **028.37560.128**; hoặc số điện thoại của trực ban Đội CSĐTTP về TTXH số điện thoại: **028.3756.0136** để cung cấp thông tin, phối hợp điều tra, xử lý khi nhận được cuộc gọi lừa đảo.

CÔNG AN QUẬN BÌNH TÂN

HƯỚNG DẪN

HAI CÁCH ĐỂ NGƯỜI DÂN XỬ LÝ HIỆU QUẢ NHỮNG CUỘC GỌI LỪA ĐẢO

Khi nhận cuộc gọi rác, cuộc gọi có dấu hiệu lừa đảo, người dân có thể thực hiện phản ánh tới đầu số 156 thông qua 02 hình thức gửi Tin nhắn hoặc gọi điện thoại.

CÁCH 1

+ VỚI TIN NHẮN RÁC:

S [số ĐT - nguồn phát tán] [nội dung phản ánh]

gửi 156 (hoặc 5656)

+VỚI CUỘC GỌI CÓ DẤU HIỆU GỌI RÁC:

V [Số điện thoại - nguồn phát tán] [Nội dung phản ánh]

gửi 156 (5656)

Hoặc

V [nguồn phát tán] [nội dung cuộc gọi rác]

gửi 156

+ VỚI CUỘC GỌI CÓ DẤU HIỆU LỪA ĐẢO:

LD [Số điện toại - Nguồn phát tán] [nội dung phản ánh]

gửi 156 (hoặc 5656)

CÁCH 2

Người dân gọi tới đầu số 156

Các doanh nghiệp viễn thông sẽ áp dụng việc miễn phí cước cuộc gọi

24/7

Các nhà mạng sẽ sàng lọc, xác minh, phản hồi khách hàng đồng thời tổng hợp, thông báo tới cơ quan quản lý nhà nước.

NẾU THÔNG TIN THUÊ BAO KHÔNG ĐÚNG QUY ĐỊNH SẼ XỬ LÝ VI PHẠM

(tạm dừng cung cấp dịch vụ viễn thông một chiều, tiếp theo tạm dừng cung cấp dịch vụ viên thông 2 chiều nếu không thực hiện và tiếp theo là thanh lý hợp đồng, chấm dứt cung cấp dịch vụ viễn thông)

BỘ CÔNG AN CÔNG KHAI 18 TÀI KHOẢN NGÂN HÀNG CỦA CÁC ĐỐI TƯỢNG LỪA ĐẢO

Nơi nhận đơn tố giác: Phòng 9, Cục Cảnh sát hình sự
(497 Nguyễn Trãi, quận Thanh Xuân, Hà Nội)

1021730962	Trần Nguyễn Kỳ Duyên	Vietcombank
1026773428	Nguyễn Thị Anh Thư	Vietcombank
0949244275	Đào Minh Hưng	Eximbank
100015677	Nguyễn Thị Linh	Eximbank
100015941	Cao Vũ Minh Hiếu	Eximbank
04201016995715	Cao Vũ Minh Hiếu	MSB
04301013956240	Nguyễn Thị Linh	MSB
29086013567777	Trần Anh Phương	MSB
1020563830	Đào Minh Hưng	SHB
1020537138	Nguyễn Huy Vũ	SHB
1020623712	Trần Anh Phương	SHB
8017041054066	Đào Thị Nhật Trinh	Bản Việt
05670015101	Đào Thị Nhật Trinh	TPBank
0927015933	Đào Thị Nhật Trinh	MB
104000969563	Đào Thị Nhật Trinh	PVcomBank
49864542950	Nguyễn Thị Linh	SCB
19035803064015	Nguyễn Tiến Sang	Techcombank
121704070008027	Nguyễn Huy Vũ	HDBank