# THÔNG TIN TUYÊN TRUYỀN
## Các hình thức lừa đảo sử dụng công nghệ cao
## (Lừa đảo qua mạng xã hội)

Thời gian gần đây, tình hình tội phạm sử dụng công nghệ cao có chiều hướng phức tạp, gia tăng về quy mô, hậu quả với nhiều thủ đoạn mới, tinh vi. Nhiều người dân trong cả nước nói chung và tỉnh Quảng Ninh nói riêng đã bị lừa đảo hàng trăm, hàng tỷ đồng bởi loại tội phạm này. Qua theo dõi, nghiên cứu và điều tra xử lý về loại tội phạm này xác định một số phương thức, thủ đoạn mà đối tượng sử dụng để hoạt động phạm tội lừa đảo chiếm đoạt tài sản, cụ thể như sau:

**1./ Giả mạo hoặc chiếm quyền điều khiển tài khoản mạng xã hội của người dùng, sau đó nhắn tin lừa đảo bạn bè của họ.**

- Đối tượng giả mạo hoặc chiếm quyền điều khiển tài khoản mạng xã hội của người dùng (tấn công, hack nick Zalo, Facebook…). Có trường hợp chiếm tài khoản vĩnh viễn khiến người dùng không thể truy cập lại để sử dụng, có trường hợp chiếm tài khoản nhưng hoạt động song song, người dùng vẫn có thể sử dụng nên không phát hiện.

- Sau đó, đối tượng sẽ truy cập tài khoản để nghiên cứu, tìm hiểu sơ lược về các mối quan hệ, các thói quen sinh hoạt, thói quen viết tin nhắn của người dùng để bắt chước cách nhắn tin và tìm kiếm "con mồi".

- Tiếp đó, sẽ nhắn tin với người thân quen trong danh sách bạn bè của người dùng để nhờ thanh toán tiền, hoặc mua thẻ cào điện thoại, hoặc chuyển tiền vào một số tài khoản ngân hàng mà các đối tượng đã chuẩn bị sẵn từ trước hòng chiếm đoạt.

- Các tài khoản ngân hàng nhận tiền chiếm đoạt thường là các tài khoản không chính chủ, gồm: tài khoản mua của những người không có nhu cầu sử dụng; tài khoản ảo có sai sót trong việc đăng ký thông tin.

- Cá biệt, có nhiều trường hợp sau khi lừa xong, các đối tượng có thể hỏi mượn nhiều tài khoản của người bị mất tiền để thay đổi thông tin bảo mật tiếp tục hoạt động lừa đảo.

**2./ Lừa đảo qua dịch vụ VoIP mạo danh cơ quan thực thi pháp luật đề nghị cung cấp thông tin hỗ trợ điều tra. (Thủ đoạn được các đối tượng sử dụng nhiều trong thời gian dịch Covid - 19 diễn ra).**

- Thủ đoạn này thường do các đối tượng người nước ngoài như Trung Quốc, Đài Loan (Trung Quốc), Thái Lan… thực hiện.

- Các đối tượng tạo webite giả mạo Cục Cảnh sát giao thông, đồng thời gọi điện thoại cho nạn nhân để thông báo nạn nhân đã vi phạm Luật giao thông đường bộ thông qua việc tra cứu, giám sát từ hệ thống camera của Cục Cảnh sát giao thông, từ đó đã ra quyết định xử phạt hành chính. Với mục đích giúp các nạn nhân không tốn thời gian đi nộp phạt hoặc giảm uy tín cá nhân nên các đối tượng liên tục gọi điện và dẫn dắt nạn nhân gặp đồng bọn giả danh cán bộ cơ quan Công an, Viện kiểm sát, Tòa án yêu cầu cung cấp thông tin cá nhân, thông tin tài khoản tiết kiệm, thẻ ngân hàng, làm giả các hình ảnh giấy triệu tập, lệnh bắt,… đề nghị nạn nhân đăng ký mới tài khoản, chuyển mã OTP hoặc chuyển tiền vào tài khoản chỉ định trước của chúng để chiếm đoạt.

- Ngoài ra, chúng giả danh nhân viên bưu điện, các cơ quan Cảnh sát điều tra, Viện Kiểm Sát, Toà án gọi cho bị hại thông báo bị hại có liên quan đến các vụ án đặc biệt nghiêm trọng như: Buôn bán trái phép ma tuý; Rửa tiền; lừa đảo… đe doạ bị hại có thể bị khởi tố, bắt tạm giam hay phong toả các tài khoản ngân hàng. Yêu cầu nạn nhân chuyển tiền vào tài khoản tạm giữ của cơ quan chức năng để chúng kiểm tra hoặc để làm đảm bảo, trong vòng 1 đến 2 ngày sẽ hoàn trả. Sau khi có được tiền của bị hại, chúng nhanh chóng chuyển tiền đi và chiếm đoạt.

- Một số trường hợp còn giả làm cơ quan Cảnh sát phòng cháy chữa cháy để liên lạc các cơ sở kinh doanh trên địa bàn yêu cầu đóng tiền tập huấn, mua tài liệu tập huấn phòng cháy thông qua hình thức chuyển khoản ngân hàng.

- Thời gian qua ở nhiều địa phương trong cả nước, rất nhiều cá nhân đã bị lừa đảo bằng hình thức này với số tiền rất lớn.

**3./ Lừa đảo chiếm đoạt tài sản thông qua hình thức kinh doanh đa cấp hoặc thông qua các sàn giao dịch ảo** (sàn vàng, ngoại tệ, bất động sản, Forex, Wefinex, Deniex, Pocinex, Binaex, Remitex, Vista…).

- Xuất hiện nhiều doanh nghiệp hoạt động theo mô hình đa cấp có dấu hiệu chiếm đoạt tài sản dưới nhiều vỏ bọc khác nhau. Các doanh nghiệp này thường xây dựng đội ngũ duy trì hệ thống tại nhiều tỉnh, thành phố trên toàn quốc, thu hút hàng trăm nghìn người tham gia, gây thiệt hại ước tính hàng nghìn tỷ đồng.

- Lừa đảo chiếm đoạt tài sản thông qua các sàn giao dịch ảo (sàn vàng, ngoại tệ, bất động sản, Forex, Wefinex, Deniex, Pocinex, Binaex, Remitex, Vista): Đối tượng sử dụng những thủ đoạn phạm tội rất tinh vi, phức tạp gồm đội ngũ môi giới tiếp thị để lôi kéo khách hàng (các nhà đầu tư) mở tài khoản giao dịch: Chúng tự

lập sàn, website giả mạo sàn nước ngoài và điều chỉnh về kĩ thuật để chiếm đoạt tài sản.

- Với thủ đoạn mời, chào làm đại lý trên mạng, thời gian đầu bị hại có thể bán được hàng hoá (nhiều trường hợp thực chất là đối tượng cài người vào để mua hàng). Khi bị hại đã mắc bẫy, các đối tượng sẽ tiếp cận và đề nghị các nạn nhân nhập hàng với số lượng lớn để được hưởng chiết khấu cao. Với thủ đoạn trên, nhiều bị hại đã chi hàng tỷ đồng để nhập hàng về nhưng không bán được vì hàng hóa toàn là kém chất lượng, không rõ nguồn gốc xuất xứ.

- Riêng đối với các sàn giao dịch ảo "đầu tư tài chính" như: Forex, Wefinex, Deniex, Pocinex, Binaex, Remitex, Vista… là dạng phi vật chất, nên khi hệ thống dữ liệu bị xoá thì toàn bộ tài sản mà người dân nạp tiền vào sẽ bị mất, gây thiệt hại lớn.

- Ngoài ra, các đối tượng còn câu dụ người dân tham gia đầu tư vào các sàn ngoại hối ảo để nhận tiền hoa hồng, sau đó thông báo cháy tài khoản hoặc sập sàn, chiếm đoạt tiền đầu tư từ các bị hại.

Đối với sàn giao dịch trực tuyến dưới hình thức tạo tài khoản chỉ là các "sàn giao dịch ngoại hối" tự xưng. Trong nhiều trường hợp, đó chỉ là vỏ bọc để che đậy hoạt động huy động tiền. Bản chất của hoạt động này là lấy tiền của người vào mạng lưới sau (nhà đầu tư sau) trả cho người vào mạng lưới trước. Khi không còn người đóng tiền vào hệ thống thì hệ thống sẽ sụp đổ. Biểu hiện của mô hình này là các tổ chức hứa hẹn trả hoa hồng, tiền thưởng cao bất thường so với số tiền bỏ ra ban đầu hoặc hứa hẹn với người tham gia chỉ cần đầu tư tiền vào các dự án, sau đó không làm gì nhưng vẫn hưởng được tiền hoa hồng, tiền thù lao và các lợi ích kinh tế khác.

**4./ Lừa đảo chiếm đoạt tài sản thông qua mạng xã hội kết bạn, xây dựng tình cảm và hứa hẹn gửi quà có giá trị.**

- Các đối tượng lừa đảo bằng hình thức này thường là người ngước ngoài (Nigieria, Châu Phi…). Thủ đoạn của các đối tượng là:

+ Thông qua mạng xã hội như Zalo, Facebook, Twiter, Instagram… các đối tượng làm quen và kết bạn với các nạn nhân.

+ Đối tượng tự giới thiệu mình là kĩ sư, quân nhân, doanh nhân… đang sinh sống và làm việc tại nước ngoài và tâm sự những chuyện riêng tư nhằm tạo niềm tin rồi hứa hẹn tặng quà, hứa kết hôn và bảo lãnh nạn nhân đi nước ngoài hoặc ngỏ ý muốn giúp đỡ tạo điều kiện để nạn nhân kinh doanh.

+ Sau khi nạn nhân tin tưởng thì các đối tượng thông báo sẽ chuyển tiền hoặc đồ vật có giá trị từ nước ngoài về Việt Nam.

+ Tiếp đến, các đối tượng cho người đóng giả làm nhân viên Hải quan, thuế hoặc Công an… gọi điện thoại thông báo với nạn nhân là quà tặng bị giam giữ khi về đến sân bay, bến cảng do có giá trị lớn nên buộc các nạn nhân phải chuyển tiền để nộp thuế hoặc "hối lộ" cho cán bộ Hải quan, Công an…

+ Sau đó các đối tượng cung cấp số tài khoản cho các nạn nhân, yêu cầu chuyển tiền và chiếm đoạt tiền của nạn nhân. Các đối tượng này thường chia làm 3 nhóm:

(1) Nhóm các đối tượng ở nước ngoài kết bạn làm quen, nhắn tin tâm sự để lừa nạn nhân chuyển tiền.

(2) Nhóm đối tượng ở Việt Nam làm quen với người ở Việt Nam, nhờ mở tài khoản hoặc nhận làm cán bộ Hải quan, Công an Việt Nam để gọi điện cho nạn nhân.

(3) Nhóm các đối tượng rút tiền sử dụng các thẻ Visa, Master của ngân hàng như VPbank, Sacombank… mở tại Việt Nam nhưng có thể rút tiền mặt tại nước ngoài.

**5./ Lừa đảo chiếm đoạt tài sản thông qua tấn công hộp thư Email.**

- Chủ yếu do các đối tượng người nước ngoài thực hiện như: Nigeria, Nam Phi… Chúng sử dụng các biện pháp kĩ thuật giả mạo, xâm nhập, chiếm quyền điều khiển email của các doanh nghiệp, các nhân hệ kinh doanh, thanh toán tiền với các đối tác nước ngoài, thường tập trung vào các doanh nghiệp vừa và nhỏ tại các địa phương, không có bộ phận quản trị mạng chuyên trách, kiến thức bảo mật chưa cao để lừa đảo. Sau đó thay đổi các thông tin giao dịch chuyển tiền để chiếm đoạt thông qua các hợp đồng kinh tế, các tài khoản nhận tiền do các đối tượng chỉ định thường được mở tại các ngân hàng ngoài lãnh thổ Việt Nam dẫn tới khó khăn trong việc thu hồi tiền và tài sản bị chiếm đoạt.

**6./ Lừa đảo chiếm đoạt tài sản thông qua hoạt động thương mại điện tử.**

Đối tượng sử dụng nhiều thủ đoạn lừa đảo chiếm đoạt tài sản khác nhau như:

+ Ký hợp đồng qua mạng, thực hiện giao dịch đúng hợp đồng trong một số lần đầu để tạo lòng tin, nhưng sau khi đối tác đã chuyển một khoản tiền lớn, chúng nhanh chóng rút tiền để chiếm đoạt và không giao hàng như thoả thuận.

+ Quảng cáo, rao bán hàng hoá… qua các website, diễn đàn, mạng xã hội, email… yêu cầu khách hàng trả tiền trước nhưng không chuyển hàng hoặc chuyển hàng không đúng mẫu mã, số lượng, chủng loại hoặc hàng giả, kém chất lượng….

**7./ Lừa đảo chiếm đoạt tài sản thông qua hình thức phishing lấy cắp thông tin tài khoản InternetBanking, mã OTP của khách hàng và rút tiền.**

- *Dạng gửi thư điện tử:*

Các đối tượng gửi thư điện tử đến các nạn nhân với nội dung: "Yêu cầu xác thực tài khoản ngân hàng, nếu không thực hiện xác thực theo đường link đối tượng cung cấp trong vòng 24h tài khoản ngân hàng sẽ bị tạm khoá".

Nhiều nạn nhân đã tin tưởng vào email dạng này, sau khi truy cập vào đường link sẽ được điều hướng đến một trang website giả mạo có giao diện giống hệt trang chủ của Ngân hàng, đối tượng sẽ yêu cầu nạn nhân nhập thông tin đăng nhập InternetBanking, cung cấp mã xác thực bảo mật OTP, từ thao tác này các đối tượng sẽ có được thông tin truy cập của nạn nhân, sau đó thay đổi phương thức xác thực và truy cập để chiếm đoạt tiền trong tài khoản của nạn nhân.

- *Dạng thông qua hình thức tặng quà, hoặc nhận tiền thưởng, nhận V**oucher** khuyến mại giảm giá sản phẩm để câu dụ khách truy cập vào link:*

Sau khi truy cập vào đường link sẽ được điều hướng đến một trang website yêu cầu nạn nhân nhập thông tin đăng nhập InternetBanking, số điện thoại, cung cấp mã xác thực bảo mật OTP, từ thao tác này các đối tượng sẽ có được thông tin truy cập của nạn nhân, sau đó thay đổi phương thức xác thực và truy cập để chiếm đoạt tiền trong tài khoản của nạn nhân.

**8./ Lừa đảo chiếm đoạt tài sản thông qua dịch vụ OTT (Over the Top)**

Các đối tượng thường lập các website trúng thưởng, gửi tin nhắn qua phần mềm nhắn tin OTT như: Facebook, Zalo, Viber… thông báo cho chủ tài khoản đã trúng thưởng tài sản, hiện vật có giá trị lớn, đề nghị nạp tiền phí để nhận thưởng.

Chúng thường yêu cầu nạn nhân nạp tiền thông qua mua mã thẻ điện thoại, thẻ game hoặc chuyển tiền sang các tài khoản trung gian sau đó chiếm đoạt.

**9./ Lừa đảo thông qua hình thức tư vấn, mua bán thông tin kèo cá độ, dự đoán kết quả lô đề trên mạng Internet.**

- Các đối tượng tự nhận là các "chuyên gia" phân tích kết quả số lô, số đề, kèo các trận thể thao; sử dụng các trang mạng xã hội lập ra dịch vụ soi cầu, lấy số, bạch thủ lô đề rao bán với giá vài triệu đến vài chục triệu đồng.

- Ngoài rao bán số lô đề, các đối tượng còn rao bán các kèo cá độ bóng đá gồm có 3 mức: Mức thứ nhất là chính xác 90%; mức VIP là chính xác 95%; mức siêu VIP chính xác 99,9%.

Nhiều người bị hại đã không ngại chi hàng chục triệu đồng để mua những con số. Đa số các nạn nhân phần vì tâm lý xấu hổ, phần vì biết việc đánh lô đề, cá độ là vi phạm pháp luật nên không trình báo các cơ quan chức năng.

**10./ Lừa đảo thông qua hình thức cho vay tín chấp thủ tục rút gọn (cho vay tiền qua các ứng dụng trên mạng xã hội).**

- Thường là nhóm đối tượng có tổ chức, hoạt động chuyên nghiệp, có kiến thức về lĩnh vực tài chính, công nghệ.

- Các đối tượng thông qua các kênh truyền thông, mạng xã hội để mời chào với các khẩu hiệu như: "Cho vay tiền tín chấp thủ tục rút gọn, giải ngân nhanh, lãi suất ưu đãi…".

- Khi có khách liên hệ vay tiền, đối tượng sẽ phân công đối tượng "Tư vấn viên, hỗ trợ viên" dẫn khách đến các trang website hoặc ứng dụng (app) cho vay của họ có các giao diện, nút chức năng, biểu giá vay và lãi suất… đã được xây dựng công phu, chuyên nghiệp hòng gây dựng niềm tin.

- Sau khi khách nhập các thông tin cá nhân, số điện thoại, số tài khoản ngân hàng và chọn gói vay theo nhu cầu, sẽ buộc khách phải chuyển khoản tiền lệ phí hồ sơ, tiền bảo hiểm khoản vay, tiền chứng minh khả năng chi trả.

- Tiếp đó, sẽ can thiệp vào hệ thống của website hoặc ứng dụng (app) cho vay để tạo ra các thông báo lỗi hệ thống hoặc đổ lỗi cho khách nhập sai thông tin (mặc dù khách điền đúng thông tin vẫn bị sửa thành sai) rồi yêu cầu khách nộp tiền để khắc phục lỗi hoặc để đảm bảo uy tín của khách rằng khách không lừa đảo họ. Các khoản tiền khách nộp để sửa lỗi sẽ được tích luỹ trên hệ thống webiste hoặc ứng dụng (app) cho vay, đối tượng cam kết sẽ hoàn lại toàn bộ số tiền khách đã nộp kèm theo khoản tiền khách cần vay ngay sau khi kết thúc giao dịch; ngược lại, nếu khách không giao dịch tiếp thì sẽ mất toàn bộ số tiền đã nộp trước đó.

- Với tâm lý tiếc tiền khi đã  nộp vào thì nạn nhân sẽ liên tục nộp tiền vào cho đến khi biết mình bị lừa đảo thì mới dừng lại.

Ngoài ra, có thể khẳng định đây là phương thức, thủ đoạn hoạt động mới của loại tội phạm tín dụng đen (cho vay nặng lãi). Khi người dân đăng ký vay tiền dạng này thì ngoài khả năng bị lừa đảo, người dân có thể bị rơi vào một số tình huống sau:

- Các rủi ro không lường trước vì bị lộ thông tin và hình ảnh cá nhân.

- Có thể bị gán vào các khoản vay mà bản thân không hề hay biết do đã cung cấp các loại giấy tờ tuỳ thân, sổ HKTT trước đó cho các đối tượng xấu.

- Trường hợp có thể vay được tiền, nhưng khi chậm thanh toán tiền lãi và gốc sẽ bị các đối tượng bôi nhọ danh dự và đe doạ tinh thần, quấy nhiễu bản thân và những người thân.

**11./ Lừa đảo thông qua hình thức tuyển dụng lao động.**

- Các đối tượng thông qua các kênh truyền thông, mạng xã hội để mời chào tuyển dụng lao động với các khẩu hiệu như: "Việc làm tại nhà đơn giản, mức lương hấp dẫn, trả lương theo ngày cao".

Khi nạn nhân liên hệ thì sẽ yêu cầu nạn nhận chuyển khoản cọc tiền hàng để gửi hàng về cho làm tại nhà. Tuy nhiên khi nạn nhân chuyển tiền các đối tượng sẽ chiếm đoạt.

Ngoài ra, số đối tượng thực hiện hành vi phạm tội còn gửi các đường link và yêu cầu nạn nhân truy cập, đăng nhập và điền các thông tin theo hướng dẫn của chúng. Sau khi nạn nhân điền, cung cấp đầy đủ các thông tin có liên quan thì số đối tượng phạm tội sẽ chiếm đoạt quyền sử dụng tài khoản ngân hàng, tài khoản mạng xã hội để thực hiện các hành vi chiếm đoạt tài sản.

**12./ Lừa đảo thông qua hình thức đổi tiền.**

Số đối tượng phạm tội thông qua nhiều nguồn tin để khai thác, lấy thông tin về tên, tuổi, số điện thoại của những người đổi tiền uy tín trên địa bàn (chủ yếu là người Trung Quốc) để giả mạo những người này. Sau đó chủ động liên lạc đặt vấn đề đổi tiền với những người có nhu cầu đổi tiền (tiền Trung Quốc sang tiền Việt Nam hoặc ngược lại) trên mạng xã hội với mức phí cao. Sau khi **kết nối**, thống nhất số tiền đổi, số đối tượng phạm tội làm giả tin nhắn báo giao dịch tài khoản ngân hàng (qua hệ thống Internet Banking) và làm giả hoá đơn chuyển tiền qua ngân hàng rồi gửi cho bị hại biết. Khi nhận được tin nhắn thông báo của đối tượng, bị hại không kiểm tra kỹ lại phát sinh giao dịch tiền trong tài khoản cảu mình mà lập tức gửi chuyển tiền cho đối tượng, đối tượng lập tức chiếm đoạt số tiền gửi.

**13./ Lừa đảo thông qua thủ đoạn tạo lập Fanpage kêu gọi từ thiện rồi chiếm đoạt tiền ủng hộ của các nhà hảo tâm.**

Với thủ đoạn các đối tượng sử dụng : Lợi dụng lòng tin của người dân để lừa đảo tiền từ thiện qua mạng xã hội, chúng tạo lập các trang mạng xã hội (chủ yếu trên Facebook), sau đó đăng tải các bài viết, tạo dựng những nội dung không có thật về một số hoàn cảnh đang gặp khó khăn, hoạn nạn cần được giúp đỡ; hoặc giả mạo các trang mạng xã hội chuyên làm từ thiện được nhà nước cho phép, rồi đăng tải các bài viết kêu gọi cộng đồng mạng giúp đỡ. Tinh vi hơn, một số đối tượng

còn sử dụng các bài báo viết về các hoàn cảnh khó khăn đã được đăng tải trên các phương tiện thông tin đại chúng để dẫn nguồn trên Fanpage Facebook, rồi xen cài số tài khoản ngân hàng tiếp nhận từ thiện do các đối tượng tự tạo lập quản lý, để tiếp nhận nguồn tiền ủng hộ.

Các bài viết được các đối tượng đăng tải trên các trang mạng xã hội đã thu hút hàng chục nghìn người quan tâm theo dõi, gửi tiền ủng hộ từ 50.000 đồng đến 5.000.000 đồng. Tuy nhiên, sau khi tiếp nhận số tiền được các nhà hảo tâm chuyển đến, các đối tượng không bàn giao tiền từ thiện cho các gia đình gặp hoàn cảnh khó khăn mà sử dụng hết vào mục đích cá nhân; hoặc chỉ chuyển một phần rất nhỏ để làm hình ảnh nhằm tiếp tục "kêu gọi từ thiện"...

Từ đầu năm 2021 đến nay, lực lượng Công an trong cả nước đã liên tiếp phát hiện, xử lý các đối tượng quản trị các trang Fanpage Facebook hoạt động lừa đảo chiếm đoạt tài sản với thủ đoạn tương tự như trên. Điển hình Fanpage "Chia sẻ vì người nghèo", "Hỗ trợ trẻ em", "Quỹ bảo trợ trẻ em", "Phật tại tâm", "Chia sẻ yêu thương", "Kết nối yêu thương", "Quan thế âm bồ tát"...

***Để chủ động phòng ngừa với loại tội phạm sử dụng Công nghệ cao lừa đảo chiếm đoạt tài sản. Công an thành phố Móng Cái khuyến cáo người dân lưu ý một số nội dung sau:***

**1.** Để hạn chế bị lừa đảo trong quá trình mua sắm online, cơ quan Công an khuyến cáo người dân cẩn trọng với những loại hàng hoá, dịch vụ trực tuyến; kiểm tra kỹ hàng hoá, dịch vụ và cơ sở bán hàng trước khi thực hiện giao dịch; khi nhận hàng cũng phải kiểm tra kỹ trước khi thanh toán tiền, tuyệt đối không trả tiền hoặc không biết rõ người bán và uy tín của họ trước khi nhận hàng hoá, xem hàng thực tế trước khi trả tiền hoặc có thể yêu cầu nhận hàng mới trả tiền để tránh rủi ro.

**2**. Đối với thủ đoạn giả danh cơ quan Công an, Viện kiểm sát, Toà án đe doạ người dân có liên quan đến các vụ án (rửa tiền, buôn bán trái phép chất ma tuý…), yêu cầu nạn nhân chuyển tiền vào số tài khoản do chúng yêu cầu để lừa đảo chiếm đoạt tài sản, **Cơ quan Công an khuyến cáo**:

+ Cơ quan Công an, Viện kiểm sát và Toà án không bao giờ trao đổi thông tin vụ án qua điện thoại, khi có yêu cầu làm việc sẽ có giấy mời hoặc giấy triệu tập. Cơ quan Công an, Viện kiểm sát và Toà án cũng không có tài khoản ngân hàng mang tên cá nhân và không yêu cầu đương sự phải chuyển tiền để chứng minh vô tội.

+ Khuyến cáo người dân lưu ý, tất cả số điện thoại giả mạo theo số máy của cơ quan chức năng đều có thêm dấu (+) trước dãy số vì chúng được thực hiện quan mạng Internet (Voip). Nếu chỉ kiểm tra số máy gọi đến qua tổng đài 1080 sẽ không phát hiện được sự giả mạo này.

+ Khi người dân cần tra cứu vi phạm an toàn giao thông các phương tiện của cá nhân thông qua hình ảnh thì tra cứu tại trang web http://www.csgt.vn/ để tránh bị lợi dụng, lừa đảo.

**3.** Đối với các hành vi Lừa đảo chiếm đoạt tài sản thông qua mạng xã hội kết bạn, xây dựng tình cảm và hứa hẹn gửi quà có giá trị. Cơ quan Công an khuyến cáo người dân: Không nên tin tưởng và liên lạc, giao tiếp với các mối làm quen, kết bạn với người nước ngoài hoặc người lạ qua mạng xã hội, qua điện thoại… Không trao đổi hoặc làm theo yêu cầu của các đối tượng giả danh nhân viên giao nhận, hải quan, thuế…; Không cung cấp số điện thoại riêng, số tài khoản, thẻ tín dụng, thông tin cá nhân cho bất kỳ ai. Không đứng tên, chuyển giao tài khoản, nhận tiền giúp bất cứ ai; Tuyệt đối không chuyển tiền dưới bất cứ hình thức nào khi nghi vấn đối tương lừa đảo, chiếm đoạt tài sản (nếu đã chuyển phải báo ngân hàng phong toả ngay số tiền đã chuyển); Nếu gặp trường hợp nghi vấn lừa đảo, người dân cần tìm cách ghi lại thông tin của các đối tượng như số điện thoại, số tài khoản ngân hàng… và thông báo, cung cấp ngày cho cơ quan Công an để điều tra, xử lý và ngăn chặn.

**4.** Đối với các hành vi lừa đảo mà đối tượng yêu cầu cung cấp thông tin có liên quan, đề nghị người dân nâng cao ý thức cảnh giác trong việc:

- Giữ bí mật thông tin bảo mật các dịch vụ ngân hàng (tuyệt đối không tiết lộ mã PIN thẻ, mật khẩu truy cập, mật khẩu giao dịch một lần OTP, mật khẩu truy cập địa chỉ email với người lạ, kể cả nhân viên ngân hàng). Mỗi khi nhận được thông tin cần xác thực người đề nghị thực hiện giao dịch tài chính (Không chuyển tiền cho đối tượng khi chưa xác thực; cảnh giác đối tượng giả mạo quen biết thông qua mạng xã hội, email, điện thoại, thư giấy, tin nhắn (SMS), mạo danh nhân viên ngân hàng, cơ quan nhà nước).

- Mỗi khi thực hiện giao dịch trực tuyến, người dân cần kiểm tra chính xác thông tin của Website và chỉ thực hiện giao dịch tại các Website uy tín, có độ bảo mật cao.

- Khi thực hiện giao dịch tại thẻ ATM, POS, người dùng phải quan sát khe thẻ trên máy ATM, bảo đảm không có thiết bị lạ và che bàn phím khi nhập số PIN.

**5.** Đối với hành vi lừa đảo thông qua hình thức tạo lập Fanpage kêu gọi từ thiện rồi chiếm đoạt tiền ủng hộ của các nhà hảo tâm:

- Cần thận trọng tìm hiểu, kiểm chứng kỹ các thông tin đăng tải kêu gọi ủng hộ từ thiện trên các trang mạng xã hội; yêu cầu công khai, minh bạch thông tin về người cần giúp đỡ hoặc liên hệ với chính quyền địa phương, bệnh viện nơi họ điều trị để kiểm chứng thông tin.

- Để tránh bị kẻ xấu lợi dụng lòng tin để trục lợi, lừa đảo, chiếm đoạt tài sản thông qua việc kêu gọi từ thiện, các nhà hảo tâm nên lựa chọn các quỹ, chương trình từ thiện do Nhà nước, đoàn thể, quỹ xã hội, quỹ từ thiện được cơ quan có thẩm quyền cấp phép đứng ra tổ chức. Trường hợp có nghi ngờ về hoạt động lừa đảo, chiếm đoạt tài sản, cần báo cho cơ quan Công an để kịp thời xử lý.

**6.** Tuyệt đối không giao dịch, vay mượn tiền qua các ứng dụng (app) trên mạng xã hội khi mình không biết rõ địa chỉ, nhân thân cụ thể của người cho vay vì các app cho vay trên mạng xã hội đều là các app có thông tin giả mạo, các app này đều là hoạt động cho vay nặng lãi, và có dấu hiệu lừa đảo chiếm đoạt tài sản.

**7.** Khi phát hiện tài khoản/thẻ phát sinh những giao dịch gian lận hoặc có vướng mắc, người dùng cần liên lạc ngay số đường dây nóng (hotline) ngân hàng có liên quan để được giải đáp. Đăng ký dịch vụ thông báo biến động số dư tài khoản nhằm kịp thời phát hiện và giảm thiểu rủi ro liên quan đến các giao dịch bất thường.

*** Mọi thông tin nghi vấn hoặc phát hiện về lừa đảo thông qua mạng xã hội, mạng internet đề nghị người dân kịp thời thông báo, tố giác, cung cấp thông tin về Công an thành phố Móng Cái qua số điện thoại 02033881210 hoặc 0942812222 để xử lý, giải quyết.**

**Rất mong người dân đọc và chia sẻ, thông báo cho người thân trong gia đình, người dân ở khu phố mình sinh sống biết để phòng tránh những tổn hại về kinh tế mà loại tội phạm này gây ra.**