BỘ CÔNG AN
CÔNG AN TỈNH ĐỒNG THÁP

Số: 44 /CAT - ANM
V/v đề nghị tuyên truyền phương thức, thủ đoạn của tội phạm trên không gian mạng

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Đồng Tháp, ngày 04 tháng 01 năm 2024

Kính gửi:
- Lãnh đạo UBMT Tổ quốc Việt Nam Tỉnh;
- Lãnh đạo các Sở, ngành Tỉnh;
- Lãnh đạo Ngân hàng Nhà nước tỉnh Đồng Tháp;
- Lãnh đạo Ủy ban nhân dân huyện, thành phố.

Thời gian qua, thực hiện chỉ đạo của Ủy ban nhân dân Tỉnh về tăng cường các giải pháp đấu tranh phòng, chống tội phạm sử dụng công nghệ cao trên địa bàn Tỉnh Đồng Tháp, giai đoạn 2022 - 2026 *(Theo Kế hoạch số 50/KH-UBND, ngày 17/02/2022)*, các Sở, Ban, Ngành và Ủy ban nhân dân huyện, thành phố đã tổ chức triển khai, quán triệt thực hiện nghiêm túc, từ đó nâng cao vai trò, trách nhiệm, cũng như hiệu quả công tác phối hợp đấu tranh phòng, chống với loại tội phạm này. Tuy nhiên, tình hình tội phạm sử dụng không gian mạng thực hiện hành vi lừa đảo, chiếm đoạt tài sản có dấu hiệu diễn biến tăng vào dịp cuối năm, với phương thức, thủ đoạn ngày càng tinh vi, xảo quyệt hơn, chúng lợi dụng khoa học công nghệ, nghiên cứu đặc điểm tâm lý, giới tính, độ tuổi, nghề nghiệp của nạn nhân và lợi dụng các sự kiện đang diễn ra để xây dựng kịch bản phù hợp với thực tế hoặc lồng ghép nhiều thủ đoạn trong một kịch bản nên nạn nhân dễ sụp bẫy lừa đảo.

Thời gian tới, nhất là trong các dịp Lễ, Tết Nguyên đán năm 2024, các đối tượng xấu tăng cường các hoạt động lợi dụng không gian mạng để thực hiện các hành vi lừa đảo nhằm chiếm đoạt tài sản của người dân. Để nâng cao hiệu quả công tác đấu tranh phòng, chống tội phạm trên không gian mạng, Công an Tỉnh kính đề nghị các đồng chí tiếp tục chỉ đạo triển khai thực hiện có hiệu quả Công văn số 137/UBND-NCPC, ngày 30/8/2023 của Ủy ban nhân dân Tỉnh về tăng cường các biện pháp phòng ngừa tội phạm sử dụng công nghệ cao để chiếm đoạt tài sản. Đồng thời, quan tâm chỉ đạo tổ chức tuyên truyền, phổ biến sâu rộng đến cán bộ, công chức, viên chức và Nhân dân biết các phương thức, thủ đoạn mà các đối tượng sử dụng để thực hiện hành vi lừa đảo chiếm đoạt tài sản *(Có gửi kèm)*; thường xuyên cập nhật kiến thức về tội phạm mạng qua trang thông tin điện tử của Công an Tỉnh và trang Zalo Official Account, Fanpage Facebook "Phòng An ninh mạng Công an Đồng Tháp" *(Có gửi kèm mã QR)*.

Công an Tỉnh trân trọng cám ơn sự quan tâm, phối hợp của các đồng chí./.

Nơi nhận:
- Như kính gửi;
- Cục A05 - Bộ Công an (để báo cáo);
- Văn phòng UBND Tỉnh (để nắm);
- Các Đ/c Phó Giám đốc (để nắm);
- Phòng TM, Phòng ANM (để nắm, tham mưu);
- Lưu CAT: TM, ANM(LVĐ-21b).

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH ĐỒNG THÁP

Đại tá Nguyễn Văn Hiếu

Công an tỉnh Đồng Tháp
Tài khoản OA

Công an tỉnh Đồng Tháp

Phòng An ninh mạng Công an Đồng Tháp
Tài khoản OA

Phòng An ninh mạng Công an Đồng Tháp
Tài khoản OA

27 THỦ ĐOẠN CỦA TỘI PHẠM TRÊN KHÔNG GIAN MẠNG

(Ban hành kèm theo Công văn số 44 /CAT-ANM, ngày 04 /01/2024)

1. Giả danh cơ quan thực thi pháp luật để lừa đảo: Các đối tượng sử dụng dịch vụ cuộc gọi thoại trên nền Internet (VoIP) gồm các số như: +840..., +882..., +94(10)..., +94(70)... giả danh lực lượng Công an, Viện kiểm sát,... đe dọa bị hại có liên quan đến các đường dây buôn bán ma túy, rửa tiền... đồng thời yêu cầu bị hại phải kê khai và nộp toàn bộ số tiền vào số tài khoản do bọn chúng chỉ định để theo dõi, điều tra làm rõ, sau khi điều tra nếu không có liên quan đến tội phạm sẽ trả lại tiền cho bị hại. Mặc khác bọn chúng gửi hình ảnh lệnh bắt, lệnh phong tỏa tài sản cho bị hại xem qua tài khoản zalo để tạo lòng tin và yêu cầu bị hại không cho người thân biết, sau đó bọn chúng yêu cầu bị hại chuyển tiền vào các tài khoản của bọn chúng cung cấp.

Khuyến cáo:

- Tuyệt đối không chuyển tiền dưới bất cứ hình thức nào khi có người lạ điện thoại vào số điện thoại của mình tự xưng là Công an, Viện kiểm sát, Tòa án (Nếu đã chuyển thì báo ngay ngân hàng phong tỏa ngay số tiền đã chuyển). Vì Công an, Viện kiểm sát, Tòa án không lấy lời khai qua điện thoại và gửi các lệnh bắt qua mạng xã hội.

- Khi thấy những số điện thoại lạ có những đầu số như trên nên ngắt máy ngay, tuyệt đối không làm theo hướng dẫn bọn chúng.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

2. Lừa đảo bằng thủ đoạn "bẫy tình" trên mạng xã hội như: Facebook, Zalo, Twitter,... các đối tượng trong và ngoài nước giả danh quân nhân đang công tác nước ngoài, tìm cách làm quen, "giả vờ" yêu đương để thực hiện hành vi chiếm đoạt tài sản của nhiều phụ nữ bằng cách hứa tặng quà, tiền có giá trị cao như vàng, kim cương, USD... Tuy nhiên, để nhận được tiền, quà tặng đối tượng lừa nạn nhân phải đóng phí dịch vụ, phí hải quan, thuế,... bằng cách chuyển tiền vào tài khoản của bọn chúng.

Khuyến cáo:

- Tuyệt đối không nghe theo lời dụ dỗ của các đối tượng này, bất cứ giá nào cũng không được gửi tiền cho người lạ, khi chưa biết rõ họ là ai.

- Cần tỉnh táo với các mối quan hệ trên mạng xã hội, đặc biệt là với người nước ngoài đây là những thủ đoạn của bọn tội phạm dựng lên lợi dụng sự thiếu hiểu biết và đánh vào lòng tham của người dân để lừa đảo.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

3. Lừa đảo bằng thủ đoạn "chuyển tiền làm từ thiện": Các đối tượng giả danh người nước ngoài tìm cách làm quen với bị hại thông qua Facebook, Zalo… và nhờ nhận số tiền lớn để làm từ thiện, nếu nạn nhân đồng ý sẽ được hưởng 30% đến 40% tổng số tiền mà đối tượng gửi về để làm từ thiện. Nhưng để nhận được tiền phải trả các chi phí phát sinh như phí Hải quan, thuế,... bằng cách chuyển tiền vào tài khoản ngân hàng do chúng chỉ định sẵn. Sau khi nhận được số tiền nạn nhân chuyển vào tài khoản, các đối tượng cắt hết liên lạc với nạn nhân.

Khuyến cáo:

- Thận trọng trong việc kết bạn qua mạng internet (Facebook, Zalo…), nhất là đối với những người xưng là người nước ngoài.

- Tuyệt đối không chuyển tiền vào tài khoản của người khác khi chưa biết rõ họ là ai.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

4. Lừa đảo thông qua mua bán hàng trực tuyến: Thông qua việc mua bán hàng trực tuyến trên mạng xã hội Facebook, Zalo các đối tượng lừa đảo đặt mua hàng và gửi đường link giả mạo website thanh toán tiền bằng dịch vụ chuyển tiền trực tuyến (internet banking), yêu cầu bị hại đăng nhập thông tin vào đường link để đánh cắp thông tin thẻ tài khoản ngân hàng rồi chuyển tiền của bị hại qua tài khoản của đối tượng để chiếm đoạt. Hoặc đối tượng rao bán hàng với giá rất rẽ và thỏa thuận bị hại chuyển tiền trước vào tài khoản của đối tượng khi nhận được tiền đối tượng sẽ chuyển hàng sau, thấy giá rẽ nên bị hại mất cảnh giác liền đặt mua hàng và chuyển tiền cho đối tượng. Khi nhận được tiền các đối tượng không giao hàng và cắt hết liên lạc với nạn nhân.

Khuyến cáo:

- Tuyệt đối không cung cấp mã PIN, mật khẩu truy cập, mã OTP, cho người lạ. Đồng thời, không bấm vào các đường link lạ được gửi qua tin nhắn, email, mạng xã hội.

- Hết sức cảnh giác khi mua hàng qua mạng xã hội, cần lựa chọn những cửa hàng uy tín, có địa chỉ rõ ràng, khi mua hàng phải thỏa thuận khi nào nhận hàng thì mới chuyển tiền qua đơn vị giao hàng từ đó hạn chế được rủi do mất tiền.

- Khi phát hiện đối tượng nghi vấn, báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

5. Mạo danh nhân viên Ngân hàng thông báo nâng cấp phần mềm bảo mật cho khách hàng để thực hiện hành vi lừa đảo: Các đối tượng sử dụng các sim rác gọi điện thoại giả danh nhân viên Ngân hàng thông báo đến khách hàng là để nâng cấp phần mềm bảo mật cho khách hàng không để người khác đánh cắp thông tin tài khoản đề nghị khách hàng cung cấp số tài khoản, mật khẩu đăng nhập, mã OTP hoặc gửi đường link cho bị hại yêu cầu đăng nhập làm theo hướng dẫn là điền đầy đủ thông tin số tài khoản, mật khẩu, mã OTP, chứng minh nhân dân… Sau khi đối tượng đã có những thông tin tài khoản thẻ

của bị hại chúng đã chiếm quyền sử dụng rồi chuyển tiền trong tài khoản của bị hại sang các số tài khoản ngân hàng của bọn chúng nhằm chiếm đoạt tài sản.

Khuyến cáo:

- Phải giữ bí mật thông tin bảo mật các dịch vụ ngân hàng, nhất là tuyệt đối không cung cấp số tài khoản, mật khẩu đăng nhập, mã OTP,... cho người lạ, kể cả nhân viên ngân hàng. Tuyệt đối không được bấm vào các đường link lạ được gửi qua tin nhắn, email, mạng xã hội.

- Khi phát hiện các trường hợp nghi vấn cần thực hiện ngay các biện pháp khẩn cấp như yêu cầu ngân hàng phong toả tài khoản và khoá các dịch vụ liên quan. Đồng thời, báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

6. Chiếm quyền sử dụng tài khoản Facebook (hack Facebook) để lừa đảo: Các đối tượng tấn công các tài khoản mạng xã hội Facebook cá nhân của người Việt Nam sinh sống ở nước ngoài, sau đó tìm hiểu mối quan hệ của Facebook vừa chiếm đoạt rồi nhắn tin cho bạn bè, người thân của bị hại để hỏi vay tiền, nhờ thanh toán tiền rồi chiếm đoạt tài sản.

Khuyến cáo:

- Tuyệt đối không nên chuyển tiền ngay cho đối tượng mà phải kiểm tra, xác minh lại tài khoản facebook đó có phải là người thân của mình hay không bằng cách gọi điện thoại trực tiếp để xác minh, nếu đúng thì chuyển tiền, còn không đúng thì tuyệt đối không chuyển tiền.

- Thông tin cho người thân, bạn bè, đồng nghiệp biết là tài khoản facebook của mình đã bị chiếm quyền sử dụng và đang thực hiện hành vi lừa đảo, để người thân, bạn bè, đồng nghiệp biết cảnh giác tránh trường hợp bị lừa.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

7. Lừa đảo qua hình thức trúng thưởng: Đối tượng sử dụng sim rác, sử dụng các trang mạng facebook, zalo, Mesenger... giả mạo các ngân hàng, công ty tài chính thông báo đang có chương trình khuyến mãi, tặng quà tri ân khách hàng và yêu cầu cung cấp các thông tin cá nhân, số tài khoản để tham gia hoặc thông báo bạn đã trúng thưởng một món hàng có giá trị cao như xe máy SH, điện thoại Iphone, sổ tiết kiệm vài trăm triệu đồng Sau đó yêu cầu chuyển tiền vào tài khoản của các đối tượng để làm thủ tục nhận thưởng. Nhận được tiền các đối tượng cắt hết liên lạc với bị hại.

Khuyến cáo:

- Khi nhận được các cuộc gọi thông báo trúng thưởng, người dân cần hỏi rõ họ tên nhân viên, chức danh, đơn vị cung cấp thông tin. Đồng thời, cần phải kiểm tra chương trình khuyến mãi của doanh nghiệp trên website chính thức, liên hệ với đơn vị tổ chức trao thưởng để xác thực thông tin.

- Người dân cần bảo mật thông tin cá nhân, không tùy tiện cung cấp số CMND, tài khoản ngân hàng, thẻ tín dụng; thận trọng khi giao dịch điện tử và hạn chế chia sẻ thông tin cá nhân cho người khác.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

8. Quảng cáo tìm người làm việc tại nhà để lừa đảo: Đối tượng sử dụng Facebook đăng quảng cáo tìm người cộng tác bằng hình thức làm việc tại nhà, khi có người liên hệ các đối tượng giới thiệu, tư vấn về các việc làm như: Lắp ráp bút bi, dán tem son, xâu vòng, làm tranh đính đá... Tuy nhiên, muốn nhận sản phẩm về làm khách hàng phải đặt cọc một số tiền nhất định. Đồng thời, hứa hẹn sau khi làm xong sẽ thu lại sản phẩm với mức giá cao gấp 3 đến 5 lần và hoàn trả tiền cọc. Khi khách hàng đồng ý, chúng yêu cầu khách hàng chuyển tiền đặt cọc đơn hàng từ vài trăm ngàn đồng đến vài triệu đồng. Sau khi làm xong sản phẩm nạn nhân liên hệ lại thì không liên lạc được. Số tiền đặt cọc bị các đối tượng chiếm đoạt.

Khuyến cáo:

- Khi tìm việc, người lao động cần đến những trung tâm dịch vụ việc làm của Nhà nước, hoặc các tổ chức chính trị xã hội và của doanh nghiệp có uy tín, có văn phòng, địa chỉ rõ ràng, số điện thoại bàn cố định..., không nên tìm việc làm tại nhà trên mạng xã hội tránh trường hợp "tiền mất tật mang".

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

9. Mạo danh Công ty tài chính lừa cho vay tiền: Đối tượng sử dụng mạng xã hội Facebook giả danh các Công ty tài chính đăng quảng cáo cho vay tiền với lãi xuất thấp, thủ tục nhanh chóng. Khi có người liên hệ để vay tiền các đối tượng tự xưng là nhân viên của công ty tài chính, cam kết cho người vay tiền chỉ cần gửi ảnh sổ hộ khẩu, giấy chứng minh nhân dân và đóng phí hồ sơ từ 500.000 đồng đến vài chục triệu đồng tính theo gói vay là sẽ được giải ngân vay vốn. Để thuyết phục, đối tượng lừa đảo đã chụp ảnh và gửi cho người vay "hợp đồng tín dụng" có đóng dấu đỏ với nội dung đã phê duyệt khoản vay. Tin tưởng, người vay đã đóng phí hồ sơ xong thì không được giải ngân và không liên lạc được với các đối tượng.

Khuyến cáo:

- Khi có nhu cầu vay tiền, người dân cần đến các ngân hàng có địa chỉ rõ ràng trên địa bàn mình sinh sống, tuyệt đối không nghe theo các trang mạng xã hội quảng cáo cho vay tiền với thủ tục đơn giảm, đó là những chiêu trò, thủ đoạn của các đối tượng dựng nên để lừa đảo chiếm đoạt tài sản của người dân.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

10. Mạo danh cơ quan Bảo hiểm xã hội lừa đảo: Đối tượng sử dụng các số điện thoại có đầu số 0555..., 8009.... tự xưng là người của cơ quan bảo hiểm xã hội thông báo cho người dân việc họ đi khám chữa bệnh bằng thẻ bảo hiểm y tế nhưng chưa thanh toán tiền khám chữa bệnh hoặc thông báo người dân đã trục

lợi từ quỹ BHYT,... sau đó yêu cầu người dân cung cấp về nhân thân và nộp một khoản tiền (thông qua tài khoản) để thanh toán chi phí đã khám chữa bệnh hoặc hoàn trả tiền đã trục lợi từ quỹ BHYT, nếu không cơ quan BHXH sẽ báo Công an vào cuộc điều tra, trừ tiền có trong tài khoản ngân hàng của người dân, cắt quyền sử dụng thẻ BHYT của người dân...

Khuyến cáo:

- Người dân cần nâng cao cảnh giác khi nhận được các cuộc điện thoại lạ, tuyệt đối không thực hiện bất cứ yêu cầu nào của các đối tượng, nhất là không chuyển tiền hoặc cung cấp thông tin cá nhân qua điện thoại cho người lạ.

- Cơ quan BHXH không triển khai bất kỳ hình thức điện thoại trực tiếp nào cho người dân thông báo việc họ đã đi khám chữa hệnh bằng thẻ BHYT hoặc nói họ đã trục lợi tiền của quỹ BHYT.

- Trong trường hợp nhận được các cuộc gọi như trên, cần báo ngay cho cơ quan Công an để xử lý hoặc thông báo đến số hotline của BHYT Việt Nam 1900.9068 để được tư vấn, hỗ trợ và giải đáp kịp thời.

11. Giả vờ chuyển tiền nhầm để chiếm đoạt tài sản (Ép vay): Các đối tượng chuyển tiền vào tài khoản của nạn nhân với nội dung cho vay, sau đó có người gọi điện thoại báo rằng mình vừa chuyển nhầm, nhờ nạn nhân trả lại (tài khoản nhận tiền lúc này khác với tài khoản mà đối tượng đã chuyển chuyển tiền cho nạn nhân). Sau một thời gian, người chủ tài khoản chuyển nhầm đòi tiền nạn nhân, chúng đưa ra chứng từ gửi tiền, thông tin chuyển khoản làm bằng chứng, bắt nạn nhân thanh toán tiền lãi vay trong những ngày trước, nếu không trả sẽ bị quấy rối hoặc khởi kiện ra Tòa án.

Khuyến cáo:

Khi tài khoản nhận được tiền chuyển nhầm, người bị chuyển nhầm không nên vội vàng chuyển trả nếu chưa xác định được đó có phải là chủ tài khoản thật sự hay không, nhất là trả lại qua một tài khoản khác, khác với tài khoản chuyển ban đầu. Tốt nhất nên liên hệ với ngân hàng và chuyển trả thông qua ngân hàng, có xác nhận, lưu trữ để tránh những phát sinh không đáng có về sau.

12. Lừa nâng cấp sim 4G để chiếm đoạt tài sản: Lợi dung chính sách hỗ trợ nâng cấp Sim 4G của nhà mạng, các đối tượng lừa đảo đã mạo danh nhân viên nhà mạng gọi điện, nhắn tin hướng dẫn cú pháp để thực hiện nâng cấp sim 3G thành 4G nhằm lừa đảo, chiếm quyền kiểm soát sim điện thoại, sau đó đánh cắp thông tin thẻ tín dụng, lấy mã OTP để thực hiện các giao dịch qua thẻ của người tiêu dùng.

Khuyến cáo:

- Thận trọng trước những cuộc gọi, tin nhắn mời thay sim, nâng cấp sim 4G từ những số điện thoại lạ, bất thường và tuyệt đối không thực hiện các yêu cầu thao tác thay sim qua điện thoại.

- Khi phát hiện thẻ sim trên máy điện thoại của mình bị vô hiệu hóa, nghi ngờ do bị chiếm quyền kiểm soát sim, người tiêu dùng liên hệ ngay với tổng đài của nhà mạng để yêu cầu khóa sim nhằm ngăn ngừa hoặc giảm thiểu rủi ro kẻ gian sử dụng sim nhận mã OTP nhằm chiếm đoạt tiền của người tiêu dùng thông qua các giao dịch trực tuyến, thanh toán bằng thẻ tín dụng.

13. Lập các sàn giao dịch tiền ảo đa cấp trên mạng để chiếm đoạt tài sản: Các đối tượng lập ra các sàn giao dịch tiền ảo và sử dụng mạng xã hội để đăng quảng cáo với những lời mời gọi hấp dẫn như đầu tư ít sinh lãi cao, ngồi không tiền cũng về, giúp nhau tương tác tiền vào như mưa... Cụ thể: Các sàn giao dịch này cam kết có các chuyên gia hàng đầu hướng dẫn đặt lệnh, người chơi chỉ cần đặt lệnh theo là có lợi nhuận từ 10-15%/ngày (Có sàn quảng cáo mức lợi nhuận cao lên đến 80%/ngày - Sàn Gardenbo). Cách chơi khá đơn giản: người đầu tư mở tài khoản trên Website của các Công ty, sau đó nạp tiền thật vào các tài khoản rồi đổi sang tiền ảo và dùng tiền ảo mua quyền đặt lệnh, trong đó người đầu tư chỉ có hai lựa chọn là dự báo tăng hoặc giảm của các tiền điện tử danh tiếng trên thế giới hoặc là các chỉ số như vàng, đô la, dầu... Sau khi có kết quả, nếu đúng như dự đoán người chơi được 90 đến 95% số tiền đặt lệnh. Còn nếu sai thì khách hàng sẽ mất 100% số tiền.

Khi tham gia, người đầu tư nếu giới thiệu thêm người khác vào hệ thống nhánh dưới của mình, thì được thêm 50% hoa hồng, số tiền hoa hồng tiếp tục tăng lên khi giới thiệu được nhiều người tham gia. Khi một lượng lớn người tham gia hệ thống thì các Công ty này lấy lãi của người sau trả cho người trước.

Ban đầu, để thu hút người tham gia, các Công ty này tạo tính thanh khoản từ tiền ảo sang tiền thật rất dễ dàng để người đầu tư tin tưởng. Đến khi người chơi đầu tư số tiền lớn vào các sàn giao dịch tiền ảo thì bất ngờ sàn bị sập không thể rút tiền về, sàn liên tục báo lỗi không thể truy cập tài khoản, đồng nghĩa với việc người chơi mất sạch tiền đầu tư.

Không khó nhận diện chiêu trò lừa đảo của các Công ty đa cấp bởi có những đặc điểm khá giống nhau như: Các Công ty này có giấy tờ pháp lý không rõ ràng, trụ sở và máy chủ đặt ở nước ngoài. Các nhóm đầu tư thường khoe nhà sang, xe sang, đưa ra những lời lẽ hoa mỹ cam kết mang lại lợi nhuận cao với rủi ro thấp, thậm chí không rủi ro, bao cháy tài khoản... đánh vào lòng tham người đầu tư, làm sao để nộp tiền cho họ nhanh nhất có thể.

Khuyến cáo:

- Không tham gia chơi và làm đại lý trung gian, mua bán "tiền ảo" trong các trò chơi trực tuyến, các sàn giao dịch.

- Tuyệt đối không tham gia và lôi kéo người khác tham gia vào các sàn giao dịch tài chính đa cấp và tiền ảo mà không có sự cho phép của Ngân hàng nhà nước; không đầu tư, góp vốn và kêu gọi góp vốn vào các sàn giao dịch có dấu hiệu vi phạm pháp luật và thiếu căn cứ pháp lý để hoạt động.

- Khi phát hiện thấy hoạt động của các sàn giao dịch có dấu hiệu nghi vấn, hoặc khi bị các đối tượng kêu gọi góp vốn, lôi kéo tham gia vào các sàn giao dịch tài chính đa cấp và tiền ảo hoạt động bất hợp pháp thì báo ngay cho cơ quan chức năng để nhanh chóng tiến hành điều tra xử lý.

14. Lừa đảo với hình thức "cho số đánh đề": Các đối tượng giả mạo nhân viên của các Công ty xổ số kiến thiết lên Facebook, Zalo ảo để quảng cáo, cung cấp số điện thoại hotline để dụ dỗ người chơi. Khi có người liên hệ, các đối tượng sẽ báo giá cho mỗi con số khi mua (mỗi loại số sẽ có mệnh giá khác nhau). Người chơi phải chuyển khoản trước, khoảng 16 giờ chiều hàng ngày

chúng sẽ chuyển số cho người chơi và thúc giục người chơi đánh to, đánh lớn. Để tạo lòng tin cho bị hại, các đối tượng còn đặt làm những con dấu giả của các công ty sổ số, giả mạo chữ ký của lãnh đạo công ty, bảng danh sách lô đề được đóng dấu mật, dấu cam kết từ nhà quay thưởng để gửi cho bị hại, hoặc tung lên mạng xã hội. Khi người mua chuyển khoản xong thì chúng sẽ chặn Facebook, Zalo của họ, còn nếu ngẫu nhiên có người trúng thì chúng sẽ yêu cầu chuyển hoa hồng (10%) giá trị giải thưởng đã trúng cho chúng.

Khuyến cáo:

- Đối với thủ đoạn trên, người dân cần tỉnh táo, cảnh giác, tuyệt đối không hám lợi trước những dụ dỗ của đối tượng tránh trường hợp "tiền mất, tật mang".

- Trong trường hợp đã bị lừa đảo hoặc khi phát hiện đối tượng nghi vấn báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

15. Lừa đảo thông qua thực hiện nhiệm vụ trên các ứng dụng (App) không rõ nguồn gốc: Các đối tượng sử dụng mạng xã hội (Facebook, Zalo) đăng thông tin quảng cáo tìm người làm nhiệm vụ trên các App, với những lời lẻ "có cánh" như: Công việc nhẹ nhàng, dễ thực hiện, không mất nhiều thời gian và đặc biệt là có hoa hồng cao... Để tham gia người chơi phải nạp một khoảng tiền nhất định cho mỗi nhiệm vụ, thông qua tài khoản ngân hàng mà đối tượng cung cấp, sau khi thực hiện nhiệm vụ xong người tham gia sẽ được các đối tượng chuyển lại số tiền gốc và kèm theo tiền hoa hồng. Để tạo lòng tin cho người tham gia, 1, 2 lần đầu các đối tượng chuyển tiền gốc và tiền hoa hồng theo đúng như quảng cáo; đến lần nạp tiền làm nhiệm vụ tiếp theo các đối tượng thông báo đã xảy ra lỗi trong quá trình làm nhiệm vụ và yêu cầu bị hại nếu muốn rút được tiền, phải nạp thêm tiền để làm nhiệm vụ mới thì lúc đó mới rút được tiền, tuy nhiên khi người tham gia nhiều lần nạp thêm tiền theo yêu cầu của đối tượng thì vẫn không nhận lại được tiền đã đầu tư; đến khi người tham gia không còn khả năng nạp tiền nữa thì các đối tượng cắt mọi liên lạc với người tham gia.

Khuyến cáo:

- Tuyệt đối không nghe theo những lời mời, quảng cáo làm nhiệm vụ trên các App không rõ nguồn gốc, với lãi suất cao, đó là chiêu trò, thủ đoạn của các đối tượng dựng lên để lừa đảo chiếm đoạt tài sản của người dân.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

16. Lừa đảo thông qua hình thức tuyển cộng tác viên làm việc tại nhà: Các đối tượng lên mạng xã hội (Facebook, Zalo) đăng thông tin quảng cáo tìm cộng tác viên làm việc tại nhà như giật đơn hàng trên Shopee, Amaron... với lợi nhuận từ 10% trở lên; khi có người liên hệ để nhận làm cộng tác viên các đối tượng hướng dẫn truy cập vào các trang web bán hàng để chọn sản phẩm và đặt đơn hàng, đồng thời chuyển tiền đến số tài khoản mà các đối tượng cho trước. Để tạo lòng tin cho bị hại, 1, 2 lần đầu các đối tượng trả tiền hoa hồng cho cộng tác viên theo đúng như quảng cáo; tuy nhiên đến các lần sau đối tượng diện nhiều lý do như báo lỗi hệ thống, đặt đơn hàng sai,... nên cộng tác viên không

rút được tiền; nếu muốn rút được tiền thì phải đặt thêm đơn hàng khác với số tiền cao hơn, khi cộng tác viên chuyển tiền để đặt đơn hàng mới thì cũng không thể rút được tiền, số tiền đầu tư bị các đối tượng chiếm đoạt.

Khuyến cáo:

- Tuyệt đối không nghe theo những lời mời, quảng cáo tham gia các ứng dụng di động, website "giật" đơn hàng ảo trên mạng, với lãi suất cao, hấp dẫn, đó là chiêu trò, thủ đoạn của các đối tượng dựng lên để lừa đảo chiếm đoạt tài sản của người dân.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

17. Lừa đảo thông qua hình thức giả danh cán bộ viễn thông, cán bộ Cục Văn thư lưu trữ và Công an: Các đối tượng giả danh cán bộ viễn thông, cán bộ của Cục Văn thư lưu trữ... gọi điện thoại cho nạn nhân nói rằng đang nợ cước viễn thông, mở thẻ tín dụng của một ngân hàng nào đó để sử dụng mà không thanh toán... hiện các đơn vị này đã kiện ra Tòa án, Tòa án yêu cầu phải đến ngay để giải quyết, nếu không sẽ chuyển hồ sơ cho Công an tiến hành bắt khẩn cấp phục vụ điều tra và phong tỏa tất cả tài sản. Đối tượng ngõ ý muốn giúp đỡ nạn nhân bằng cách sẽ liên hệ, nối máy với đường dây nóng bên Công an để được giúp đỡ, sau đó có người tự xưng là Công an đang công tác tại Cục Cảnh sát hình sự hoặc cơ quan Cảnh sát điều tra của một địa phương nào đó, như Hà Nội, TP Hồ Chí Minh, Đà Nẵng... đe dọa nạn nhân có liên quan đến các đường dây buôn bán ma túy, rửa tiền... hoặc vụ việc vi phạm pháp luật nào đó và yêu cầu nạn nhân chuyển tiền vào tài khoản của chúng chỉ định để phục vụ công tác điều tra, nếu không sẽ bị bắt ngay và chúng gửi đến nạn nhân các Lệnh bắt, Lệnh phong tỏa tài sản... Do tâm lý sợ hải nên nhiều người đã chuyển tiền cho các đối tượng.

Khuyến cáo:

- Hết sức cảnh giác với số điện thoại lạ, tuyệt đối không làm theo hướng dẫn bọn chúng. Tuyệt đối không cung cấp mã OTP, tên đăng nhập, mật khẩu tài khoản ngân hàng cho bất cứ ai, dưới bất kỳ hình thức nào. Tuyệt đối không chuyển tiền dưới bất cứ hình thức nào khi có người lạ điện thoại vào số điện thoại của mình tự xưng là Công an, Viện kiểm sát, Tòa án (Nếu đã chuyển thì báo ngay ngân hàng phong tỏa ngay số tiền đã chuyển). Vì các cơ quan trên không lấy lời khai qua điện thoại, không điện thoại yêu cầu chuyển tiền phục vụ công tác điều tra và gửi các lệnh bắt qua mạng xã hội.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

18. Lừa đảo thông qua hình thức giả danh cán bộ Cục Quản lý đường bộ và Công an yêu cầu nộp phạt tiền giao thông: Đối tượng giả danh cán bộ Cục quản lý giao thông đường bộ, thông báo đến bị hại có biên lai nộp phạt sắp

hết hạn tại Đà Nẵng và hướng dẫn bị hại liên hệ với Công an Đà Nẵng để giải quyết, sau đó có người gọi điện tự xưng cán bộ Phòng Cảnh sát hình sự Công an Đà Nẵng nói rằng bị hại có liên quan đến đường dây mua bán ma túy xuyên quốc gia, yêu cầu bị hại truy cập vào 01 đường link lạ và cung cấp thông tin cá nhân, tài khoản ngân hàng, rồi chiếm đoạt số tiền của bị hại có trong tài khoản.

Khuyến cáo:

- Hết sức cảnh giác với số điện thoại lạ, tuyệt đối không làm theo hướng dẫn bọn chúng. Tuyệt đối không chuyển tiền dưới bất cứ hình thức nào khi có người lạ điện thoại vào số điện thoại của mình tự xưng là Công an. Vì các cơ quan trên không lấy lời khai, không hướng dẫn cài App hay yêu cầu nạp tiền phạt liên quan đến vi phạm giao thông qua điện thoại và gửi các lệnh bắt qua mạng xã hội.

- Cần trao đổi, tham khảo ý kiến của người thân, bạn bè những thông tin trên để được tư vấn, tránh tình trạng bị lừa đảo.

- Khi phát hiện đối tượng nghi vấn cần báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.

19. Mạo danh Lãnh đạo Tỉnh, Sở, ban, ngành Tỉnh và địa phương để lừa đảo: Đối tượng lấy hình ảnh đại diện từ Zalo, Facebook của các đồng chí lãnh đạo Tỉnh, Lãnh đạo Sở, ban, ngành Tỉnh và địa phương để lập tài khoản Zalo mạo danh, sau đó gửi lời kết bạn rồi nhắn tin mượn tiền hoặc nhờ bạn bè, người thân, đồng nghiệp, cán bộ cấp dưới của người bị mạo danh chuyển tiền cho người thân dùm, nhằm lừa đảo, chiếm đoạt tài sản.

Khuyến cáo:

- Điểm chung của loại tội phạm này là tài khoản giả mạo không để số điện thoại. Do đó, nên cẩn trọng khi đồng ý kết bạn trên Zalo, nhất là những tài khoản có hình ảnh người quen nhưng không hiện số điện thoại. Tuyệt đối không chuyển tiền ngay, dù người yêu cầu chuyển tiền tự xưng là bạn bè, đồng nghiệp, người thân thì cũng phải xác thực lại bằng cách điện thoại hoặc gặp trực tiếp.

- Trong trường hợp phát hiện mình bị mạo danh trên mạng xã hội cần nhanh chóng thông báo rộng rãi để người thân, bạn bè, đồng nghiệp biết, từ đó kịp thời ngăn chặn những hành vi lừa đảo. Đồng thời, thông báo ngay cho cơ quan Công an nơi gần nhất để được hướng dẫn, xử lý.

20. Gọi điện quấy rối, đe dọa, khủng bố đòi nợ: Các đối tượng tự xưng là nhân viên của các công ty tài chính gọi điện, nhắn tin quấy rối, đe dọa theo kiểu khủng bố để gây áp lực, ép buộc người vay phải trả nợ xảy ra phổ biến, đặc biệt các đối tượng gọi điện, nhắn tin cho người thân, bạn bè, đồng nghiệp,... của người vay để tạo áp lực, gây bức xúc trong cơ quan, doanh nghiệp và ảnh hưởng đến tình hình ANTT.

Khuyến cáo:

- Giải thích ngắn gọn về việc không quen hoặc không có trách nhiệm với khoản nợ mà các đối tượng đề cập và hỏi rõ thông tin đơn vị đòi nợ, nhắc nợ để nắm thông tin *(Nên ghi âm cuộc gọi, lưu tin nhắn để làm bằng chứng).*

- Tuyệt đối không cung cấp bất kỳ thông tin gì cho các đối tượng này, không nên đôi co, giải thích hay năn nỉ vì không giải quyết được vấn đề gì cả.

- Sử dụng tính năng có sẵn trên điện thoại để chặn các cuộc gọi, tin nhắn làm phiền để giảm phiền hà. Đối với các trang Facebook cá nhân có thể khóa các bình luận của người lạ.

- Trong trường hợp bị đối tượng sử dụng một số thuê bao gọi điện quá 5 lần/1 ngày để quấy rối thì có thể liên hệ nhà mạng của thuê bao trên để phản ánh, kiến nghị nhà mạng chặn cuộc gọi không mong muốn *(cuộc gọi rác)* hoặc truy cập vào hệ thống tiếp nhận tin nhắn rác, thư điện tử rác, cuộc gọi rác của Cục An toàn Thông tin thuộc Bộ Thông tin và Truyền thông qua đường link: https://thongbaorac.ais.gov.vn.

- Có yêu cầu bằng văn bản gửi tới công ty tài chính đã quấy rối, gọi điện giục nợ để khiếu nại về biện pháp đôn đốc, thu hồi nợ về đòi tiền cá nhân, tổ chức không có nghĩa vụ trả nợ.

- Gửi đơn tố cáo tới cơ quan Thanh tra, giám sát ngân hàng hoặc các chi nhánh Ngân hàng Nhà nước trên địa bàn Tỉnh để kiến nghị giải quyết hành vi vi phạm pháp luật của công ty tài chính hoặc gửi đơn tố cáo lên cơ quan Công an, nếu công ty tài chính tiếp có hành vi sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để quấy rối, đe dọa tinh thần,...

21. Giả danh nhân viên y tế thông báo người thân đang cấp cứu: Các đối tượng lừa đảo tự xưng là giáo viên, nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con em, người thân họ đang cấp cứu trong tình trạng nguy kịch. Những "thầy cô giáo tự xưng" này thay phiên nhau gọi điện thúc giục cha mẹ chuyển tiền cứu con, nếu không hoặc chậm nộp tiền thì con của họ sẽ nguy hiểm đến tính mạng.

Trong trường hợp này, các đối tượng sử dụng chiêu thức đánh vào tâm lý, tình cảm của nạn nhân, hình thành trạng thái bất an, lo sợ và hoảng loạn khi phụ huynh phải nghe tin người thân mình đang cấp cứu. Để hoàn toàn thao túng tâm lý nạn nhân trong thời gian ngắn, các đối tượng thường trình bày không rõ ràng, sử dụng những ngôn từ tiêu cực nhằm kích động cảm xúc như nguy kịch, bị thương nặng, có thể không qua khỏi. Đáng nói, một số đối tượng còn thuộc lòng thông tin về trường, lớp học của con, tên giáo viên chủ nhiệm, thầy cô, hiệu trưởng khiến phụ huynh nhất thời tin tưởng.

Khuyến cáo:

- Hạn chế chia sẻ thông tin, hình ảnh cá nhân, con cái, danh tính của mình lên mạng xã hội.

- Hủy bỏ các dịch vụ không còn nhu cầu để hạn chế bớt việc các đơn vị giữ thông tin cá nhân.

- Khi nhận các cuộc điện thoại, tin nhắn có dấu hiệu bất thường, người dân cần bình tĩnh xác minh thông tin, xem xét một cách tỉnh táo, cẩn thận, không vội vã trả lời hay thực hiện theo nội dung mà đối tượng đưa ra.

- Trong trường hợp nghi vấn đối tượng giả mạo để lừa đảo, chiếm đoạt tài sản, cần báo ngay cho cơ quan công an gần nhất để được hỗ trợ, xử lý kịp thời.

22. Thông báo khóa SIM chưa chuẩn hóa thông tin thuê bao: Thông thường các đối tượng thực hiện các bước lừa đảo như sau:

- Các đối tượng mạo danh là cán bộ, nhân viên của cơ quan quản lý Nhà nước hoặc nhà mạng gọi điện và thông báo số điện thoại của người sử dụng sẽ bị khóa 2 chiều trong 2 tiếng với các lý do như "chưa nộp phạt", "thuê bao sai thông tin".

- Sau khi yêu cầu cung cấp thông tin, chúng sẽ tiếp tục hướng dẫn người dùng thực hiện một số bước tiếp theo như: thực hiện các cú pháp sang tên đổi chủ thông tin số điện thoại, cú pháp chuyển hướng cuộc gọi...

- Khi đã chiếm được quyền nhận cuộc gọi, các đối tượng sẽ đăng nhập ứng dụng, tài khoản mạng xã hội... của nạn nhân và khai báo quên mật khẩu đăng nhập, chọn tính năng nhận cuộc gọi thông báo mã OTP.

- Từ đó, chúng dễ dàng kiểm soát, chiếm đoạt tiền trong ví, tài khoản ngân hàng liên kết với ví điện tử.

Khuyến cáo:

- Chủ động kiểm tra thông tin chuẩn hóa: Chủ động kiểm tra thông tin đã chuẩn hóa hay chưa thông qua các công cụ, hướng dẫn từ nhà mạng.

- Không thực hiện theo yêu cầu từ số lạ: Chỉ thực hiện theo các thông báo cập nhật, chuẩn hóa thông tin từ các kênh chính thức của các doanh nghiệp viễn thông di động sử dụng cho mục đích nhắn tin, gọi điện thông báo đề nghị chuẩn hóa thông tin thuê bao.

- Tham khảo nguồn tin chính thống: Người dân cần biết thêm thông tin chi tiết có thể truy cập vào các trang web hoặc gọi điện đến tổng đài chăm sóc khách hàng của doanh nghiệp di động để được hỗ trợ, hướng dẫn.

- Đến trực tiếp các điểm giao dịch: Đối với các thuê bao đã bị khóa hai chiều, người dân phải đến trực tiếp các điểm giao dịch của các nhà mạng để thực hiện chuẩn hóa và mở khóa liên lạc lại.

23. Cuộc gọi Deepfake: Deepfake đang là một mối đe dọa đối với sự trung thực và tin cậy của video và hình ảnh. Các đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video hoặc hình ảnh giả, sao chép chân dung để tạo ra các đoạn video giả người thân, bạn bè để thực hiện các cuộc gọi lừa đảo trực tuyến. Phần lớn hình thức lừa đảo trực tuyến này nhắm tới việc lừa đảo tài chính. Nên khi người dân nhận được các cuộc gọi liên quan đến các nội dung về tài chính thì nên tỉnh táo xác nhận thêm.

Dấu hiệu nhận diện cuộc gọi Deepfake:

- Thời gian gọi thường rất ngắn, chỉ vài giây.

- Khuôn mặt thiếu tính cảm xúc và khá "trơ" khi nói, hoặc tư thế trông lúng túng, không tự nhiên, hoặc là hướng đầu và cơ thể trong video không nhất quán với nhau.

- Màu da của nhân vật trong video bất thường, ánh sáng kỳ lạ, bóng đổ không đúng vị trí, trông rất giả tạo, không tự nhiên.

- Âm thanh cũng là một vấn đề có thể xảy ra trong video. Âm thanh sẽ không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.

- Ngắt giữa chừng, bảo là mất sóng, sóng yếu...

- Yêu cầu chuyển tiền mà tài khoản chuyển tiền không phải của người đang thực hiện cuộc gọi.

Khuyến cáo:

Nếu nhận được một cuộc gọi yêu cầu chuyển tiền gấp, trước tiên hãy bình tĩnh và xác minh thông tin:

- Liên lạc trực tiếp với người thân, bạn bè thông qua một kênh khác xem có đúng là họ cần tiền không.

- Kiểm tra kỹ số tài khoản được yêu cầu chuyển tiền. Nếu là tài khoản lạ, tốt nhất là không nên tiến hành giao dịch.

- Nếu cuộc gọi từ người tự xưng là đại diện cho ngân hàng, hãy gác máy và gọi trực tiếp cho ngân hàng để xác nhận cuộc gọi vừa rồi có đúng là ngân hàng thực hiện hay không.

- Các cuộc gọi thoại hay video có chất lượng kém, chập chờn là một yếu tố để bạn nghi ngờ người gọi cũng như tính xác thực của cuộc gọi.

24. Lừa đảo thông qua dịch vụ lấy lại tiền đã bị lừa: Đánh vào tâm lý hoang mang của những người vừa bị lừa đảo qua mạng, kẻ xấu lại cung cấp dịch vụ lấy lại tiền bị lừa để tiếp tục chiếm đoạt tài sản nạn nhân.

Gần đây không chỉ nở rộ các hình thức lừa đảo qua mạng xã hội, mà còn có hình thức "thừa nước đục thả câu", đánh vào tâm lý hoang mang của những người vừa bị mất tiền. Các đối tượng xấu đã đóng vai luật sư, nhân viên ngân hàng, kỹ sư công nghệ thông tin...cung cấp "dịch vụ hỗ trợ lấy lại tiền bị lừa" nhưng thực chất là để đưa nạn nhân "vào tròng" thêm một lần nữa.

Dấu hiệu nhận biết:

- Nghiên cứu danh tính để giả mạo: Các đối tượng lừa đảo sẽ tìm kiếm những cá nhân, tổ chức có danh tiếng thật và đáng tin cậy để thu thập thông tin.

- Tạo một nhân vật giả trên danh tính thu thập: Trên nền những thông tin thu thập, các đối tượng lừa đảo xây dựng một nhân vật tin tưởng và đáng tin cậy thông qua việc tạo các hồ sơ giả, trang web giả hoặc tài liệu giả.

- Thiết lập liên lạc: Các đối tượng lừa đảo tiếp cận nạn nhân hoặc những người liên quan dưới danh tính giả đã được xây dựng. Sau đó các đối tượng lừa đảo sử dụng các kỹ thuật thao túng tâm lý để thuyết phục và xây dựng lòng tin của nạn nhân.

- Trình bày cơ hội: Các đối tượng lừa đảo thuyết phục nạn nhân rằng họ có khả năng khôi phục lại số tiền đã mất thông qua việc đề cao khả năng chuyên môn, mối quan hệ hoặc phương pháp độc quyền mà nạn nhân là ứng cử viên lý tưởng cho nhiệm vụ này.

- Yêu cầu thanh toán: Sau khi nạn nhân tin tưởng vào khả năng, các đối tượng lừa đảo sẽ yêu cầu thanh toán dưới dạng phí xử lý, phí pháp lý, hoặc bất kỳ lý do hợp lý nào khác.

- Tạo tình huống xử lý giả để giục nạn nhân thanh toán: Nếu nạn nhân vẫn chưa chuyển tiền, các đối tượng lừa đảo tiếp tục giả mạo, cung cấp thông tin đang cập nhật, xử lý tình huống cho nạn nhân qua đó thúc giục nạn nhận chuyển tiền để chiếm đoạt tài sản.

Khuyến cáo:

- Hãy luôn kiểm tra và xác nhận rõ ràng nguồn gốc và mục đích của giao dịch chuyển tiền trước khi thực hiện. Không chuyển tiền dựa trên các yêu cầu đột xuất, không xác định hoặc không rõ ràng.

- Kiểm tra kỹ các thông tin liên quan đến người nhận và số tài khoản trước khi thực hiện giao dịch chuyển tiền. So sánh thông tin với nguồn tin chính thức hoặc thông qua ngân hàng chủ quản để đảm bảo tính xác thực.

- Khi bạn nhận được cuộc gọi, tin nhắn hoặc yêu cầu thông tin cá nhân qua điện thoại, hãy xác minh danh tính của người gọi bằng cách yêu cầu thông tin địa chỉ, số điện thoại liên hệ hoặc liên lạc lại qua một kênh tin cậy khác.

- Nếu nghi ngờ hoặc trở thành nạn nhân của lừa đảo chuyển nhầm tiền, giả danh thu hồi nợ, hãy ngay lập tức báo cáo sự việc cho cơ quan chức năng, như cảnh sát hoặc ngân hàng, để họ tiến hành điều tra và cung cấp sự hỗ trợ.

- Luôn luôn giữ cảnh giác và không đồng ý thực hiện bất kỳ giao dịch tài chính nào mà không có đầy đủ thông tin và xác minh. Bảo vệ thông tin tài chính cá nhân của bạn và tìm hiểu thêm về các hình thức lừa đảo phổ biến để tránh trở thành nạn nhân.

25. Giả mạo cơ quan Công an hướng dẫn người dân đăng ký tài khoản định danh điện tử để chiếm đoạt tài sản: Các đối tượng là sử dụng số điện thoại gọi cho nạn nhân, giới thiệu là Công an địa phương nơi thường trú của nạn nhân để hướng dẫn cài đặt, kích hoạt tài khoản định danh điện tử mức độ 2, yêu cầu nạn nhân truy cập vào đường link: *https://d.anmgov.one* để tải ứng dụng *(có chứa mã độc)* tên AN NINH MẠNG có logo của Cục An toàn thông tin - Bộ Thông tin và Truyền thông. Khi nạn nhân tải ứng dụng về, đối tượng sẽ hướng dẫn cách cài đặt ứng dụng để thu thập thông tin cá nhân, thông tin tài khoản ngân hàng, yêu cầu nạn nhân cấp quyền truy cập. Sau khi cấp quyền, đối tượng lừa đảo có thể kiểm soát, theo dõi, điều khiển điện thoại nạn nhân từ xa. Mục tiêu chính của đối tượng là nhắm đến thông tin đăng nhập tài khoản ngân hàng và tin nhắn mã OTP để thực hiện lệnh chuyển tiền từ tài khoản của nạn nhân đến tài khoản của đối tượng để chiếm đoạt.

Khuyến cáo:

- Nêu cao tinh thần cảnh giác, tuyệt đối không tải ứng dụng lạ, không rõ nguồn gốc hoặc làm theo hướng dẫn của các đối tượng, không cung cấp tài khoản ngân hàng, mã OTP cho bất kỳ ai và thận trọng, xem xét kỹ khi cấp quyền truy cập cho các ứng dụng không rõ nguồn gốc.

- Trường hợp cài đặt, kích hoạt tài khoản định danh điện tử mức 2, người dân liên hệ trực tiếp cơ quan Công an gần nhất để được hướng dẫn.

- Nếu phát hiện vụ việc có dấu hiệu như trên, báo ngay cho cơ quan Công an gần nhất để được hướng dẫn, xử lý.

26. Mạo danh cán bộ Tổng cục Thuế cài ứng dụng giả mạo: Các đối tượng là sử dụng số điện thoại, mạng xã hội Zalo, Facebook để liên lạc với nạn nhân mời lên cơ quan Thuế để định danh điện tử. Sau đó, thuyết phục nạn nhân tải ứng dụng giả mạo rồi hướng dẫn cài đặt và chấp nhận cho phép truy cập toàn bộ quyền trên điện thoại để hoạt động, bao gồm cả quyền truy cập dữ liệu cá nhân và đọc tin nhắn. Nếu nạn nhân đồng ý, đối tượng có thể kiểm soát, theo dõi điện thoại từ xa và mục tiêu chính của chúng nhắm đến là thông tin đăng nhập tài khoản ngân hàng.

Khuyến cáo:

- Thận trọng, hết sức cảnh giác, tuyệt đối không tải ứng dụng "lạ", luôn kiểm chứng thông tin qua các kênh chính thống bằng cách gọi điện trwucj tiếp đến các Cơ quan Thuế.

- Khi có nhu cầu sử dụng các ứng dụng, người dân chỉ nên tải ứng dụng trên các kho ứng dụng uy tín *(CH Play, App Store)*; đồng thời, tuyệt đối không cấp cho ứng dụng toàn quyền điều khiển thiết bị.

- Khi phát hiện thiết bị nghi vấn bị chiếm quyền điều khiển, người dân cần tỉnh táo, nhanh chóng rút sim, cài đặt chế độ máy bay và nhanh chóng đến cửa hàng điện thoại nhờ chuyên gia tư vấn. Sau đó, cần liên hệ các ngân hàng có liên quan để kiểm tra tài khoản và bảo mật lại tài khoản để đảm bảo an toàn.

- Nếu phát hiện vụ việc như trên, báo ngay cho cơ quan Công an gần nhất để được hướng dẫn, xử lý.

27. Mạo danh Công ty điện lực: Đối tượng là sử dụng các số điện thoại giả danh nhân viên của "Tổng công ty Điện lực" yêu cầu khách hàng cung cấp thông tin cá nhân, yêu cầu nộp tiền điện hoặc các khoảng phí liên quan dịch vụ điện và thực hiện hành vi lừa đảo với các lý do như: Khách hàng sẽ bị cắt điện hoặc cắt hợp đồng trong vòng 02 giờ kể từ thời điểm nhận cuộc gọi hoặc khách hàng đang vi phạm ở một hợp đồng khác mà khách hàng không trực tiếp thực hiện. Khi nạn nhân yêu cầu gặp Công an thì chúng sử dụng số điện thoại khác thông báo có liên quan đường dây rửa tiền, yêu cầu gửi toàn bộ tài khoản ngân hàng để tiến hành kiểm kê. Do lo sợ nên nạn nhân làm theo yêu cầu của nhóm đối tượng và bị lừa đảo chiếm đoạt tài sản.

Khuyến cáo:

- Hết sức cảnh giác với số điện thoại lạ, tuyệt đối không làm theo hướng dẫn bọn chúng.

- Tuyệt đối không cung cấp mã OTP, tên đăng nhập, mật khẩu tài khoản ngân hàng cho bất cứ ai, dưới bất kỳ hình thức nào.

- Tuyệt đối không chuyển tiền dưới bất cứ hình thức nào khi có người lạ điện thoại vào số điện thoại của mình tự xưng là nhân viên Công ty điện lực *(Nếu đã chuyển thì báo ngay ngân hàng phong tỏa ngay số tiền đã chuyển).*

- Cần trao đổi, liên hệ với số điện thoại chăm sóc khách hàng của Công ty điện lực để kiểm chứng thông tin.

- Khi phát hiện đối tượng nghi vấn, báo ngay cho cơ quan Công an nơi gần nhất để hỗ trợ điều tra, phát hiện, xử lý.