PHỤ LỤC 2

Nội dung tuyên truyền các phương thức, thủ đoạn của tội phạm sử dụng công nghệ cao để lừa đảo chiếm đoạt tài sản

(Kèm theo Công văn số 10467/CAHN-PC02 ngày 27/12/2023 của Công an thành phố Hà Nội)

Thủ đoạn thứ 1: Các đối tượng gọi điện cho người dân, tự giới thiệu là cán bộ của các cơ quan nhà nước (cán bộ địa chính, văn phòng đăng ký đất đai, cảnh sát khu vực...) yêu cầu người dân kê khai, bổ sung thông tin CCCD, tài khoản định danh điện tử... hướng dẫn người dân cài đặt các ứng dụng, truy cập website giả mạo (*tải thông qua các đường link do đối tượng gửi, các ứng dụng, website này có chức năng hoặc chứa mã độc có khả năng thu thập thông tin, chiếm quyền sử dụng thiết bị của người dùng*), sau đó chiếm quyền sử dụng thiết bị, tài khoản ngân hàng của người bị hại và chuyển toàn bộ số tiền trong tài khoản đến các tài khoản khác để chiếm đoạt.

Thủ đoạn thứ 2: Các đối tượng đăng bài quảng cáo trên các mạng xã hội (Facebook, Telegram, Tinder…) với nội dung chào mời tham gia các hội, nhóm, câu lạc bộ hẹn hò, quan hệ nam nữ… Sau đó, yêu cầu người bị hại tham gia mua các gói sử dụng dịch vụ, nâng cấp tài khoản, thực hiện nhiệm vụ bình chọn cho gái mại dâm trá hình trên các website do đối tượng tạo lập, có máy chủ đặt tại nước ngoài… để dụ dỗ người bị hại tham gia, sau đó lấy nhiều lý do để yêu cầu người bị hại chuyển tiền thực hiện các nhiệm vụ rồi chiếm đoạt. Ngoài ra, các đối tượng còn dụ dỗ người bị hại trao đổi video, hình ảnh khỏa thân... sau đó sử dụng các hình ảnh này để đe dọa, cưỡng đoạt tài sản của người bị hại.

Thủ đoạn thứ 3: 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.

Ngoài ra, trong thời gian gần đây, nắm bắt được tâm lý người dân hiện nay đã cảnh giác với chiêu trò lừa đảo bằng cách: *gọi điện thoại, tin nhắn cho bạn bè, người thân...nhờ chuyển tiền vay tiền*, các đối tượng đã sử dụng thủ đoạn lừa đảo tinh vi hơn để vay tiền, yêu cầu chuyển tiền thông qua hình thức giả cuộc gọi video. Thủ đoạn của các đối tượng lừa đảo là: *tìm kiếm thu thập thông tin cá nhân, mối quan hệ cá nhân được đăng tải công khai trên các tài khoản mạng xã hội...lấy những hình ảnh, video cũ của người dân. Sau đó, các đối tượng sử dụng công nghệ "Deepfake" (công nghệ ứng dụng trí tuệ nhân tạo) để tạo ra các sản phẩm công nghệ giả dưới dạng âm thanh, hình ảnh, video. Từ đó, các đối tượng, sử dụng các hình ảnh, video giả đó gọi cuộc gọi "video call" để giả làm người thân vay tiền, giả làm con cái đang du học nước ngoài gọi điện cho bố mẹ nhờ chuyển tiền đóng học phí, giả tạo các tình huống khẩn cấp cần phải chuyển tiếp gấp...* Khi thực hiện hành vi lừa đảo, các đối tượng sẽ phát lại

video dưới hình thức mờ ảo, chập chờn như đang ở nơi sóng yếu làm cho người dân tin tưởng là thật và chuyển tiền cho đối tượng chiếm đoạt.

Thủ đoạn thứ 4: Đối tượng đăng tin có nội dung tuyển dụng việc làm online, có thu nhập cao trong các hội, nhóm trên mạng xã hội Facebook, Telegram... hoặc nhắn tin đến máy điện thoại của các bị hại, nếu đồng ý tham gia bị hại sẽ liên lạc với đối tượng với tài khoản Zalo, Telegram... Sau đó, đối tượng giả danh nhân viên các sàn thương mại điện tử Shopee, Lazada, Tiki... để tuyển dụng, giao việc và yêu cầu bị hại ứng tiền chuyển khoản thanh toán các đơn hàng trên các sàn thương mại điện tử trên, sau đó sẽ được thanh toán hoàn trả lại với số tiền lợi nhuận từ 10-15% số tiền thực hiện chuyển khoản. Sau một vài đơn hàng (có giá trị thấp) thành công, các đối tượng yêu cầu bị hại thực hiện thanh toán các đơn hàng có giá trị cao, sau đó lấy nhiều lý do thông báo đơn hành bị lỗi và yêu cầu bị hại thực hiện lại nhiều lần hoặc đổi sang thực hiện đơn hàng có giá trị cao hơn, rồi chiếm đoạt tiền của bị hại đã chuyển và cắt liên lạc với bị hại.

Thủ đoạn thứ 5 : Đối tượng tự lập công ty chứng khoán, website tổ chức kinh doanh sàn ngoại hối (forex), tiền điện tử (altcoin) giả (thực tế không có hoạt động kinh doanh gì). Sau đó, các đối tượng sử dụng mạng xã hội như Zalo, Facebook, Telegram, Tinder... để đăng bài, rồi kết bạn làm quen với người bị hại. Sau một thời gian quen biết, đối tượng giới thiệu, dụ dỗ, lôi kéo bị hại tham gia đầu tư tiền vào các sàn giao dịch điện tử, theo giới thiệu các sàn đều có nguồn gốc từ nước ngoài, liên kết với nền tảng giao dịch điện tử hàng đầu thế giới, cam kết người chơi sẽ được hưởng mức lãi suất cao nhưng lại an toàn có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian, thậm chí người chơi còn được đội ngũ chuyên gia của sàn hướng dẫn đặt lệnh giúp chắc chắn thắng, nhưng bản chất các sàn này đều là phần mềm do đối tượng lập ra. Sau một thời gian, sàn giao dịch thông báo dừng hoạt động để bảo trì, hoặc lỗi không truy cập được, khách hàng không đăng nhập được để rút tiền hoặc bị mất hết tiền kỹ thuật số trong tài khoản, đồng thời các đối tượng cũng khóa các tài khoản Facebook, Zalo, Telegram, Tinder... cắt liên lạc với bị hại.

Ngoài ra, để làm cho người bị hại tin tưởng hơn, các đối tượng thuê người khác đăng ký thành lập các công ty, tạo các website có tên và hình ảnh nhận diện có hình thức gần giống với tên của các Công ty đang hoạt động có uy tín trên thị trường. Sau đó, các đối tượng đến các Ngân hàng mở tài khoản ngân hàng theo tên của Công ty đã mở để sử dụng vào việc nhận tiền của người đầu tư để chiếm đoạt.

Thủ đoạn thứ 6: 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. Để bé được xét tuyển chính thức, các đối tượng sẽ yêu cầu nạn nhân lần lượt hoàn thành các "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 vài nhiệm vụ với sản phẩm phải thanh toán có mệnh giá thấp, bị hại sẽ được hoàn trả tiền gốc và lãi 10%. Đến nhiệm vụ tiếp theo, sản phẩm sẽ có giá hàng triệu đồng. Khi người bị hại chuyển khoản thì sẽ được thông báo sai số lượng, số tiền bị đóng băng và yêu cầu người bị hại phải chuyển lại thì sẽ được hoàn tiền kèm lãi suất. Khi người bị hại muốn rút tiền về tài khoản của minh, các đối tượng đưa ra các lý do như: nộp thuế thu nhập cá nhân, phí rút tiền...để yêu cầu người bị hại phải tiếp tục chuyển tiền cho đối tượng để chiếm đoạt.

Thủ đoạn thứ 7: Đối tượng mạo danh nhân viên nhà mạng gọi điện, nhắn tin cho chủ thuê bao đe dọa khóa sim điện thoại do chủ thuê bao chưa "chuẩn hóa thông tin hoặc 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. Yêu cầu chủ thuê bao phải cung cấp thông tin cá nhân, tài khoản ngân hàng… Nếu không làm theo, SIM của chủ thuê bao sẽ bị khóa. Khi chủ thuê bao không cảnh giác, làm theo yêu cầu của đối tượng thì 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 8: Thông qua mạng xã hội Facebook (tin nhắn Messenger), 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 đối tượng khác giả danh nhân viên sân bay, nhân viên giao hàng… 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 9: 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 10: Đối tượng 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 11: 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 12: 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 13: Đối tượng lập các hộp thư điện tử tương tự gần giống (có thể thêm, bớt một vài chữ, số..) với hộp thư điện tử của các tổ chức, cá nhân kinh doanh, sản xuất có thực hiện các giao dịch bằng thư điện tử, mạo danh đối tác sau đó liên hệ đề nghị các tổ chức, cá nhân chuyển tiền thanh toán hợp đồng vào tài khoản ngân hàng của đối tượng và chiếm đoạt.

Thủ đoạn thứ 14: 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 15: 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 16: Các đối tượng sử dụng phần mềm công nghệ cao (Voice over IP - truyền tải giọng nói qua mạng internet, GoIP - thiết bị chuyển cuộc gọi qua mạng internet thành cuộc gọi GSM thông thường...) có chức năng giả mạo đầu số, giả mạo số điện thoại gọi điện cho bị hại tự xưng là nhân viên Bưu điện, Bưu cục, Trung tâm y tế, Cảnh sát... thông báo về việc người bị hại đang nợ tiền cước điện thoại, có bưu phẩm gửi ở các bưu điện lâu ngày không đến nhận, thiếu nợ tiền ngân hàng do người khác lấy CMND đăng ký mở tài khoản ngân hàng, liên quan đến các vụ án, vụ việc vi phạm luật giao thông đường bộ...; sau đó nối máy cho bị hại nói chuyện với một số đối tượng khác giả danh cán bộ đang công tác tại các Cơ quan Tư pháp (Công an, Viện kiểm sát, Tòa án). Lúc này, các đối tượng thông báo người bị hại liên quan đến vụ án đặc biệt nghiêm trọng đang điều tra nếu không thực hiện đúng theo yêu cầu của chúng đưa ra sẽ bị khởi tố bị can, bắt tạm giam làm người bị hại hoang mang, lo sợ từ đó cung cấp thông tin cá nhân và tài sản cho các đối tượng. Sau đó, đối tượng yêu cầu người bị hại chuyển tiền vào các tài khoản do chúng chỉ định (có thể là tài khoản của bị hai), cung cấp mã OTP... từ đó để chuyển tiền vào tài khoản của chúng hoặc hướng dẫn bị hại tải ứng dụng giả mạo có tên "Bộ Công an" và truy cập để cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng với vỏ bọc xác minh, điều tra. Sau đó, đối tượng chiếm quyền sử dụng tài khoản ngân hàng của bị hại và chuyển tiền đến nhiều tài khoản khác của đối tượng nhằm chiếm đoạt tài sản.

Thủ đoạn thứ 17: Đối tượng lừa mua xe gắn máy, laptop, đồ dùng công nghệ… giá rẻ: 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 người bị hại chuyển thêm tiền để làm thủ tục, giấy tờ, sau khi người bị hại chuyển tiền xong sẽ chiếm đoạt và chặn số liên lạc. Bằng thủ đoạn này, đối tượng có thể lừa bán nhiều loại hàng hoá khác nhau, khi mua khách hàng phải cọc một số tiền nhất định cho các đối tượng chiếm đoạt.

Thủ đoạn thứ 18: Đối tượng lập ra các Fanpage trên mạng xã hội Facebook, đăng tải thông tin, hình ảnh về các mặt hàng có nguồn gốc, xuất xứ nước ngoài đang được giảm giá để thu hút khách hàng. Lấy lý do hàng nhập khẩu, phải đặt cọc, không nhận COD (dịch vụ giao hàng thu tiền hộ), đối tượng yêu cầu khách mua hàng phải thanh toán tiền trước hoặc đặt cọc 50% giá trị sản phẩm, chuyển tiền vào các số tài khoản ngân hàng đối tượng cung cấp. Tuy nhiên, sau khi khách hàng chuyển tiền, đối tượng không giao hàng như cam kết, chặn facebook và ngắt liên lạc để chiếm đoạt tiền của khách hàng.

Thủ đoạn thứ 19: Đối tượng sử dụng các thiết bị công nghệ cao, giả lập trạm BTS (trạm thu phát sóng di động) nhắn tin giả mạo thương hiệu của các Ngân hàng uy tín (tin nhắn Brand name - tên hiển thị trên tin nhắn là tên các ngân hàng) với nội dung thông báo thẻ ghi nợ, thẻ tín dụng, tài khoản ngân hàng của người dân tại các ngân hàng này đã bị khóa, đề nghị truy cập theo đường link để xác thực. Đường link các đối tượng cung cấp trong tin nhắn là địa chỉ giả mạo, có cấu trúc, nội dung gần giống địa chỉ website thật của ngân hàng khiến người dân lầm tưởng là website của ngân hàng, sau đó nhập toàn bộ các thông tin tài khoản ngân hàng của bản thân (tên đăng nhập, mật khẩu, mã OTP...) vào website. Qua đó, các đối tượng có được thông tin, chiếm đoạt tài khoản ngân hàng, chuyển tiền trong tài khoản của bị hại đến tài khoản khác để chiếm đoạt.

Thủ đoạn thứ 20: Đối tượng gửi thông báo cho người dân may mắn đã trúng thưởng chương trình quay thưởng của một Công ty, tổ chức nào đó và yêu cầu người dân liên kết thẻ ngân hàng, đăng nhập vào đường link, nhập số tài khoản, mã OTP để nhận tiền; 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 21: Đối tượng tham gia vào các nhóm phụ huynh có con em đang học tại các trường điểm trên địa bàn thành phố. Sau đó, đối tượng sẽ lập các group dạy thêm, học thêm, đăng thông tin của những thầy cô nổi tiếng, có uy tín trong trường; 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 22: Lợi dụng thời gian nghỉ hè, nghỉ lễ của học sinh, các đối tượng đăng các tin trên mạng xã hội quảng cáo giới thiệu tham gia Chương trình trại hè/khóa học ngoại khóa của các cơ quan, tổ chức (VietNamAirline…) cho học sinh tham gia trong kỳ nghỉ hè. Sau đó, đối tượng yêu cầu người bị hại tham gia thực hiện nhiệm vụ chuyển tiền có hưởng lợi nhuận để hoàn thành thử thách đăng ký tham gia chương trình. Lúc này, các đối tượng lấy nhiều ý do yêu cầu người bị hại chuyển tiền rồi chiếm đoạt.

Thủ đoạn thứ 23: Đối tượng giả danh là giáo viên, nhân viên y tế hoặc các cơ quan chức năng khác gọi điện cho phụ huynh học sinh, thông báo con em của họ bị tai nạn, đang đi cấp cứu, yêu cầu phụ huynh phải 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 quan tâm lo lắng cho con em, tội phạm đã yêu cầu phụ huynh phải chuyển tiền, sau đó chiếm đoạt.

Thủ đoạn thứ 24: Đối tượng gọi điện thoại cho phụ huynh học sinh thông báo học sinh đã mua hàng của đối tượng nhưng còn nợ tiền và yêu cầu phụ huynh phải chuyển tiền qua tài khoản ngân hàng để trả tiền cho đối tượng.