

CÔNG AN TỈNH HOÀ BÌNH
CÔNG AN TP HOÀ BÌNH

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

Số: 2040 /TB-CATP-CSHS

TP. Hoà Bình, ngày 05 tháng 6 năm 2023

THÔNG BÁO

Về việc tuyên truyền một số thủ đoạn các đối tượng lợi dụng để thực hiện hành vi lừa đảo chiếm đoạt tài sản qua mạng xã hội, điện thoại di động

TRƯỜNG CB.VHNT TÂY BẮC
Số: 249
ĐẾN Ngày 21/6/2023
Chuyên:

Kính gửi:

- Ủy ban nhân dân các phường, xã;
- Các cơ quan, ban, ngành, đoàn thể trên địa bàn thành phố.

Trong những năm qua, với sự bùng nổ của khoa học công nghệ trong thời đại 4.0, khoa học công nghệ đã mang lại nhiều tiện ích phục vụ cho đời sống hoạt động hàng ngày của con người, hoạt động giao dịch thương mại điện tử, mua sắm đồ đạc phục vụ công việc, nhu cầu sinh hoạt.....đều thông qua các nền tảng ứng dụng mạng xã hội, các gian hàng thương mại điện tử,....Bên cạnh những tiện ích được mang lại đó, cũng kéo theo đó là những bất cập, hệ lụy mà người sử dụng những nền tảng mạng xã hội chưa kiểm chứng lại các thông tin ảnh hưởng trực tiếp đến kinh tế của cá nhân, doanh nghiệp sẽ là cơ hội để các đối tượng xấu lợi dụng để hoạt động phạm tội, đặc biệt là tội phạm sử dụng công nghệ cao để thực hiện hành vi lừa đảo chiếm đoạt tài sản.

Trong thời gian qua, hoạt động của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng hoặc qua điện thoại di động diễn biến rất phức tạp, gia tăng với nhiều phương thức, thủ đoạn mới, tinh vi và ngày càng đa dạng, đối tượng thường lợi dụng lòng tham, niềm tin hoặc sự sợ hãi của bị hại để thực hiện hành vi lừa đảo chiếm đoạt tài sản; gây thiệt hại lớn về tài sản, ảnh hưởng đến đời sống nhân dân.

Để người dân khi sử dụng điện thoại, mạng xã hội không bị mắc bẫy” của các đối tượng lừa đảo. Công an thành phố Hoà Bình kính đề nghị các cơ quan, đơn vị trên địa bàn thành phố cùng Công an các phường, xã tuyên truyền, phát trên sóng truyền thanh của địa phương; Công an các phường, xã phối hợp Đài truyền thanh phường, xã thông báo, phát trên sóng truyền thanh. Công an các phường, xã niêm yết thông báo tại trụ sở UBND phường, trụ sở của đơn vị và các nhà văn hóa khu dân cư, thông báo đến từng khu dân cư và đăng nội dung thông báo lên trang Fanpage Công an phường, xã tổ dân phố một số thủ đoạn các đối tượng lừa đảo thường sử dụng trên mạng xã hội với các nội dung như sau:

Thủ đoạn 1: Giả danh cán bộ Công an, Viện kiểm sát, Tòa án, cán bộ công tác tại các cơ quan nhà nước

Các đối tượng sử dụng phần mềm công nghệ cao 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 thông báo về việc người bị hại đang nợ tiền cước điện thoại, có bưu phẩm gửi các bưu điện

lâu ngày không đến nhận hoặc liên quan đến các vụ án, vụ việc, các đối tượng trong các vụ án... sau đó nổi 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 đang điều tra, nếu không thực hiện đúng theo nội dung chúng đưa ra sẽ bị khởi tố bị can và xử lý theo quy định của pháp luật, làm người bị hại hoang mang, lo sợ để cung cấp thông tin cá nhân và tài khoản ngân hàng của cá nhân. Sau đó đối tượng yêu cầu người bị hại chuyển tiền vào các tài khoản chỉ định, cung cấp mã OTP 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 của bị hại và chuyển tiền đến nhiều tài khoản khác của đối tượng nhằm chiếm đoạt tài sản.

Thủ đoạn 2: Giả danh người nước ngoài kết bạn, làm quen trên các trang mạng xã hội như Zalo, Facebook...

Các đối tượng giả danh người nước ngoài sử dụng các trang mạng xã hội như Facebook, Zalo... với các danh nghĩa như quân nhân, doanh nhân để kết bạn rồi làm quen với người bị hại để tạo sự tin tưởng. Sau một thời gian quen biết, đối tượng sẽ chủ động bày tỏ tình cảm với người bị hại, sau đó sẽ gửi quà là tiền mặt hoặc tài sản có giá trị rất lớn qua đường hàng không. Có đối tượng giả danh nhân viên sân bay, hải quan, thuế, yêu cầu người bị hại nộp tiền để nhận được quà. Các đối tượng giả danh tạo ra rất nhiều lý do chưa nhận được quà để người bị hại chuyển tiền làm nhiều lần vào các số tài khoản ngân hàng do đối tượng cung cấp cho người bị hại. Khi người bị hại không còn khả năng tiếp tục chuyển tiền, các đối tượng xóa hoặc chặn ngay tài khoản Facebook, Zalo... và các số điện thoại đã sử dụng để liên lạc. Lúc này, người bị hại không liên lạc được nữa mới phát hiện bản thân bị lừa nhưng đã chuyển tiền hết cho các đối tượng.

Thủ đoạn 3: Giả danh người thân nhờ chuyển tiền rồi chiếm đoạt tài sản

Đối tượng lập tài khoản mạng xã hội (Facebook, Zalo...) hoặc chiếm quyền quản trị tài khoản mạng xã hội (hack) của người khác rồi nhắn tin cho người thân, bạn bè trong danh sách liên lạc của chủ tài khoản để vay, mượn tiền, hoặc nhờ chuyển tiền số lượng lớn vào tài khoản ngân hàng của đối tượng hoặc gửi thông báo lệnh chuyển tiền giả, kèm đường Link trang Web giả mạo ngân hàng, yêu cầu bị hại truy cập, kiểm tra. Kết hợp với mã OTP của ngân hàng lừa lấy được từ bị hại, sau đó kiểm soát tài khoản Internet banking, chiếm đoạt toàn bộ số tiền có trong tài khoản ngân hàng của bị hại.

Thủ đoạn 4: Nhắn tin trúng thưởng

Đối tượng sử dụng Facebook Messenger để thông báo trúng thưởng các tài sản (Xe Honda SH150i, điện thoại, đồng hồ) hoặc tiền mặt (phiếu quà tặng, phiếu đồ xăng...) có giá trị lớn. Sau đó, yêu cầu người bị hại nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Việc chuyển khoản, nạp thẻ phải được thực hiện trong vòng 60 phút đến 90 phút, nếu không sẽ không được nhận và giải thưởng cũng sẽ chuyển cho người khác. Bên cạnh đó, trên trang web để hoàn tất thủ tục hồ sơ nhận thưởng, thông tin về đơn vị tổ chức được dựng lên chi tiết bao gồm cả tên tuổi, địa chỉ những người đã trúng trước đó, CMND của nhân viên hỗ

trợ nhận thưởng khiến người dân mất cảnh giác và chuyển tiền theo yêu cầu của các đối tượng.

Thủ đoạn 5: Chuyển khoản nhằm tiền để lừa đảo, ép vay nặng lãi

Các đối tượng sau khi có được một số thông tin cá nhân của người dùng như tên tuổi, số điện thoại hay thậm chí là địa chỉ, các đối tượng lừa đảo sẽ cố ý “chuyển nhằm” một khoản tiền đến cho người bị hại. Kẻ lừa đảo sẽ giả danh là người thu hồi nợ của một công ty tài chính để liên hệ với bị hại. Lúc này chúng có thể yêu cầu người dùng trả lại số tiền kia như một khoản vay cùng với khoản lãi cắt cổ.

Thủ đoạn 6: Giả danh xác minh thông tin tài khoản ngân hàng

Các đối tượng giả mạo cán bộ ngân hàng yêu cầu bị hại cung cấp mật khẩu, mã OTP hoặc thông tin thẻ để xử lý sự cố liên quan đến các giao dịch ngân hàng của người dân để chiếm đoạt tài sản.

Thủ đoạn 7: Giả mạo bán hàng, giả mạo là nhân viên của các trang bán hàng trực tuyến tuyển cộng tác viên bán hàng

Đối tượng lừa đảo mở ra các trang bán hàng Online trên mạng xã hội, yêu cầu khách mua hàng ứng trước một khoản tiền trước khi giao hàng. Những khách hàng nhẹ dạ, cả tin sau khi ứng tiền cho các đối tượng lừa đảo thì sẽ bị chặn tài khoản và không thể nào lấy lại tiền. Một số đối tượng lấy danh nghĩa là nhân viên của các trang bán hàng như Lazada, Shopee... nhắn tin tuyển cộng tác viên, khi người bị hại làm theo yêu cầu của các đối tượng thì thường các đối tượng thường cho số điện thoại không chính chủ để kết bạn và liên lạc qua Zalo yêu cầu bị hại chuyển tiền thực hiện các thao tác trên các trang bán hàng, lần đầu đối tượng sẽ chuyển hoàn lại tiền gốc cùng số % hoa hồng để người bị hại tin tưởng và tiếp tục thực hiện theo yêu cầu, sau đó bị lừa chuyển tiền nhiều lần.

Thủ đoạn 8: Các ứng dụng vay tiền nhanh qua Internet:

Đánh vào tâm lý cần tiền nhanh để giải quyết công việc của bị hại, nhiều đối tượng lập ra các ứng dụng vay tiền nhanh trên mạng xã hội, sau khi bị hại tải các ứng dụng vay tiền về điện thoại hoặc máy tính, chúng yêu cầu bị hại cung cấp các thông tin cá nhân như số chứng minh thư nhân dân, số căn cước công dân, số tài khoản ngân hàng... Sau khi bị hại cung cấp các thông tin, các đối tượng sẽ yêu cầu bị hại chuyển một số tiền nhất định để đảm bảo khoản vay được duyệt và giải ngân. Khi bị hại chuyển số tiền cho các đối tượng, các đối tượng thường sẽ thông báo gửi nhằm số tài khoản hoặc cú pháp gửi không đúng nên yêu cầu gửi lại. Đến khi bị hại không có khả năng chuyển tiền thì các đối tượng sẽ chặn số điện thoại, khóa tài khoản.

Thủ đoạn 9: “giả danh là nhân viên y tế gọi điện thoại cho người bị hại nêu lý do em là con, em, cháu của họ hiện đang nằm cấp cứu trong bệnh viện và yêu cầu chuyển tiền ngay để thực hiện mổ gấp nếu không sẽ ảnh hưởng đến tính mạng, người bị hại do thấy tính khẩn cấp nên đã chuyển tiền ngay theo yêu cầu của chúng, sau đó kiểm tra lại mới biết bị lừa”.

Thủ đoạn 10: “Hack tài khoản mạng xã hội Facebook, Zalo sau đó nhắn tin cho người bị hại mà trước đó tài khoản mạng xã hội của người bị hại đã kết bạn với những tài khoản đã bị hack nick: Nhắn tin với nội dung, nêu lý do đang cần gấp một số tiền

để chi trả cho việc này, việc kia nhưng hiện tại đang ở xa tài khoản ngân hàng hiện không còn tiền và hẹn đến tối hoặc một lát sau sẽ chuyển tiền lại. Khi người bị hại đồng ý chuyển tiền và yêu cầu cung cấp số tài khoản, các đối tượng sẽ gửi số tài khoản, thông tin tên người thụ hưởng giống với tên người quen của bị hại đã kết bạn, chỉ khác nhau về số tài khoản, điều này làm cho người bị hại tin tưởng đây chính là bạn, người quen của mình nhấn tin và thực hiện giao dịch chuyển tiền qua tài khoản, sau đó mới gọi điện thoại lại để xác nhận thì phát hiện mình đã bị lừa. Sau khi nhận được tiền sẽ cắt liên lạc với người bị hại hoặc chặn tài khoản”.

Để chủ động phòng tránh các hoạt động lừa đảo qua không gian mạng, Công an thành phố Hoà Bình đề nghị cán bộ, nhân dân khi sử dụng các dịch vụ trên không gian mạng phải nâng cao tinh thần cảnh giác, nhất là trong việc cung cấp, trao đổi, chia sẻ thông tin cá nhân trên mạng xã hội. Giữ bí mật thông tin cá nhân, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở, thông tin về tài khoản ngân hàng, tài khoản các dịch vụ trên Internet... cho bất kỳ người lạ nào gọi đến. Không chuyển tiền theo bất cứ yêu cầu nào khi không có căn cứ cụ thể, rõ ràng bằng văn bản của cơ quan có thẩm quyền. Trong mọi trường hợp không cho mượn, thuê các giấy tờ cá nhân như: Căn cước công dân, giấy chứng minh nhân dân, thẻ ngân hàng, không bán, không cho mượn, thuê tài khoản ngân hàng, không nhận chuyển khoản ngân hàng hay nhận tiền chuyển khoản của ngân hàng cho người không quen biết.

*** Lưu ý:**

- Không có nhà mạng nào gọi điện thông báo khoá sim, nợ cước (nếu có tin nhắn từ tổng đài thì ra trung tâm, cửa hàng các nhà mạng đề nghị cung cấp thông tin về việc khoá thuê bao nợ cước).

- Không có việc nhẹ, lương cao, ngồi nhà làm cộng tác viên lương từ 500k/1 ngày (hãy tìm hiểu thật kỹ thông tin về đơn vị đó kéo bị lừa đảo đó)

- Không có kiến thức không tham gia vào đầu tư online.

- Không có người nhà, người yêu, phi công, người nước ngoài... nào mà gửi tiền, gửi quà về và hải quan, sân bay yêu cầu nộp tiền lệ phí.

- Không có việc Bộ Công an, Viện kiểm sát, Toà án nào liên hệ qua điện thoại với công dân (để thông báo lỗi vi phạm, điều tra qua điện thoại)

- Con cháu học ở trường bị tai nạn thì nhà trường sẽ lo trước, không tự ý chuyển khoản, tốt nhất là liên hệ với giáo viên chủ nhiệm.

Công an thành phố Hoà Bình thông báo đến cán bộ và nhân dân được biết để chủ động phòng ngừa, cảnh giác.

Trên đây là nội dung tuyên truyền một số phương thức, thủ đoạn các đối tượng lợi dụng để thực hiện hành vi lừa đảo, chiếm đoạt tài sản qua mạng Internet. Kính đề nghị các cơ quan, đơn vị trên địa bàn thành phố cùng Công an các phường, xã tuyên truyền, phổ biến đến cán bộ, nhân dân trên địa bàn để nâng cao cảnh giác, không bị các đối tượng thực hiện hành vi lừa đảo./.

Nơi nhận:

- Như trên; (để tuyên truyền)
- Công an các phường, xã (để thực hiện)
- Lưu: VT; HS

K.T. TRƯỞNG CÔNG AN THÀNH PHỐ



PHÓ TRƯỞNG CÔNG AN THÀNH PHỐ
THƯỢNG TÁ: Đinh Mai Anh