

BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 2242 /CAHP-PA05

Hải Phòng, ngày 27 tháng 11 năm 2023

V/v đề nghị tổ chức tuyên truyền phòng
chống lừa đảo trực tuyến qua hệ thống
loa phát thanh tại cơ sở

Kính gửi: Ủy ban nhân dân các quận, huyện thành phố Hải Phòng.

Trong thời gian qua, tình hình tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng tại địa bàn thành phố diễn biến phức tạp và có chiều hướng gia tăng; đối tượng sử dụng các phương thức, thủ đoạn tinh vi, nhiều người dân bị lừa đảo qua mạng với số tiền rất lớn, gây bức xúc trong dư luận, ảnh hưởng tới tình hình an ninh trật tự. Để phòng ngừa, đấu tranh, ngăn chặn hành vi tội phạm này, Công an thành phố Hải Phòng đã phối hợp với các đơn vị, địa phương tăng cường công tác tuyên truyền dưới nhiều hình thức. Tuy nhiên, qua công tác nắm tình hình và trực tiếp tiếp nhận, giải quyết nguồn tin về tội phạm, vẫn còn nhiều người dân chưa được tiếp cận với các nội dung tuyên truyền, bị các đối tượng lừa đảo chiếm đoạt tài sản bằng các thủ đoạn đã được tuyên truyền cảnh báo nhiều lần.

Để tăng cường hiệu quả công tác tuyên truyền, Công an thành phố đề nghị Ủy ban nhân dân các quận, huyện chỉ đạo các phòng, ban chuyên môn và Ủy ban nhân dân các phường, xã, thị trấn tổ chức phát thanh thường xuyên trên hệ thống loa truyền thanh tại cơ sở để tuyên truyền phòng ngừa hoạt động lừa đảo qua mạng.

Công an thành phố gửi kèm nội dung tuyên truyền “**10 phương thức, thủ đoạn hoạt động phổ biến và 10 biện pháp phòng ngừa hoạt động lừa đảo chiếm đoạt tài sản qua mạng**”. File âm thanh để phục vụ sở phát trên hệ thống loa truyền thanh, các đơn vị tải về tại địa chỉ: <https://bit.ly/phongchongluadaoHP>.

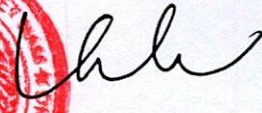
Công an thành phố đề nghị Ủy ban nhân dân các quận, huyện phối hợp thực hiện. Nếu có khó khăn, vướng mắc đề nghị trao đổi trực tiếp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - CATP Hải Phòng (Đồng chí Đại úy Trần Thị Lan Hương; số điện thoại: 0818.212389) để kịp thời phối hợp hiệu quả./. 

Nơi nhận:

- UBND thành phố (để báo cáo);
- Đ/c Giám đốc CATP (để báo cáo);
- Như trên;
- Lưu PA05(Đ3). 

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**




Đại tá Phạm Viêt Dũng



**10 PHƯƠNG THỨC THỦ ĐOẠN HOẠT ĐỘNG PHỔ BIẾN VÀ
10 BIỆN PHÁP PHÒNG NGỪA HOẠT ĐỘNG LỪA ĐẢO
CHIẾM ĐOẠT TÀI SẢN QUA MẠNG**

Hiện nay, tình trạng sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản diễn ra hết sức phức tạp. Các đối tượng phạm tội sử dụng rất nhiều các phương thức, thủ đoạn tinh vi để lừa đảo, gây ra hậu quả nghiêm trọng.

Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an thành phố Hải Phòng thông báo một số phương thức, thủ đoạn phổ biến như sau:

1. Tuyển cộng tác viên Online: Các đối tượng mạo danh nhân viên các sàn thương mại điện tử như: Shopee, Lazada, Tiki, TikTok shop,... tuyển cộng tác viên làm các nhiệm vụ chuyển tiền thanh toán các đơn hàng để tăng tương tác..., hứa hẹn trả lợi nhuận cao. Với một số đơn hàng đầu có giá trị nhỏ, đối tượng chuyển lại tiền gốc và hoa hồng đầy đủ để tạo niềm tin cho người bị hại, sau đó yêu cầu người bị hại thanh toán những đơn hàng có giá trị lớn hơn. Khi người bị hại chuyển tiền, chúng đưa ra các lý do: cộng tác viên thực hiện sai thao tác, chuyển sai số tiền thanh toán, quá thời gian... dẫn đến tài khoản bị khóa và yêu cầu người bị hại chuyển tiền thêm để bảo lãnh, xác minh tài khoản... thì mới cho rút lại tiền gốc và lãi. Chúng tiếp tục nêu ra các lý do khác nhau để giải thích cho việc không rút được tiền; đưa người bị hại vào tình trạng muốn lấy lại tiền nên phải thực hiện theo cho đến khi hết khả năng vay mượn, huy động tiền thì mới biết đã bị mắc lừa.

2. Giả danh cơ quan thực thi pháp luật để lừa đảo chiếm đoạt tài sản: Các đối tượng sử dụng sim không chính chủ, thiết bị chuyển đổi số điện thoại, phần mềm giả mạo các cơ quan chức năng để giả danh là cán bộ Công an, Viện kiểm sát, Tòa án, gọi điện đến người bị hại, thông báo có liên quan đến vụ án hình sự, ma túy, rửa tiền. Giả danh nhân viên viễn thông gọi điện thông báo nợ cước viễn thông, nhân viên điện lực gọi điện thông báo nợ cước. Giả danh Cảnh sát giao thông gọi điện thông báo phạt nguội nhằm gây sức ép, dọa nạt, làm người dân hoang mang, làm giả các lệnh bắt giam, quyết định khởi tố của cơ quan Công an, Viện kiểm sát để đe dọa người bị hại, yêu cầu người bị hại chuyển tiền vào tài khoản do chúng cung cấp để phục vụ công tác điều tra, chứng minh số tiền của người bị hại có liên quan đến tội phạm hay không. Các đối tượng liên tục cho người bị hại nói chuyện với các cán bộ giả danh của các đơn vị khác nhau. Người bị hại nghĩ mình không phạm tội và đồng thời rơi vào tình trạng bị thúc ép, khủng bố tinh thần nên chuyển tiền vào tài khoản do đối tượng cung cấp hoặc tài khoản do mình tạo ra rồi cung cấp mã OTP cho đối tượng, sau đó bị chúng chiếm đoạt tiền đã chuyển.

3. Kêu gọi đầu tư, tài chính, tiền ảo: Đối tượng lập ra các trang web, ứng dụng giao dịch tiền ảo, chứng khoán, ngoại hối... kêu gọi người dân tham gia đầu tư để thu lợi nhuận. Các trang web và ứng dụng này có giao diện hình thức và nội dung rất giống với các trang web chính thống. Các đối tượng còn mời người bị hại tham gia các hội, nhóm trên các nền tảng mạng xã hội như Zalo, Telegram, Viber, Wechat... Chúng dùng nhiều tài khoản khác nhau tham gia nhóm để làm “chim mồi”, khuyến khích người bị hại tham gia. Ban đầu, đối tượng thanh toán khoản tiền từ tiền ảo sang tiền thật rất dễ dàng để người bị hại tin tưởng. Sau đó, các đối tượng sẽ lấy lý do người bị hại thao tác không đúng, hệ thống bị lỗi ... khiến người bị hại không rút được tiền và sẽ bị mất hết số tiền đầu tư.

4. Đánh cắp hoặc tạo tài khoản mạo danh trên mạng xã hội, chủ yếu là Facebook, Zalo sau đó nhắn tin cho bạn bè, người thân để vay mượn tiền và yêu cầu chuyển tiền vào tài khoản ngân hàng cho các đối tượng để chiếm đoạt. Các đối tượng có thể thu thập hình ảnh, thông tin cá nhân của người dùng, lợi dụng công nghệ trí tuệ nhân tạo để làm giả cuộc gọi video, giọng nói của người dùng để phục vụ cho hoạt động lừa đảo.

5. Mua hàng trực tuyến với giá rẻ: Các đối tượng đăng tin bán ô tô, xe máy, thiết bị điện tử, đồ tiêu dùng... trên các trang mạng xã hội Facebook, Zalo,... Để mua được hàng, đối tượng yêu cầu phải đặt cọc trước và chuyển tiền vào số tài khoản do chúng chỉ định. Sau khi nhận được tiền đặt cọc, đối tượng không giao hàng, khóa trang mạng và cắt đứt mọi liên lạc với người bị hại.

6. Mạo danh là giáo viên, nhân viên y tế nhà trường hoặc nhân viên y tế bệnh viện liên hệ trực tiếp với phụ huynh học sinh báo tin về việc học sinh bị tai nạn, đang nhập viện cấp cứu, yêu cầu phải nhanh chóng chuyển tiền để đóng viện phí, cấp cứu bệnh nhân, từ đó chiếm đoạt tài sản...

7. Giả yêu đương, gửi nhận quà từ nước ngoài: ... Đối tượng kết bạn qua mạng xã hội Facebook, Zalo, Viber, Telegram.... giới thiệu là người nước ngoài, doanh nhân thành đạt, đang công tác ở nước ngoài làm quen với người bị hại (chủ yếu là phụ nữ), “giả” yêu đương, hứa hẹn tặng quà có giá trị cao. Bố trí các đối tượng khác giả danh nhân viên sân bay, hải quan, bưu điện, thuế... liên lạc với người bị hại để thông báo, yêu cầu phải nộp các loại phí dịch vụ, phí hải quan, thuế, để được nhận quà, tiền, hàng hóa từ nước ngoài gửi về. Đối tượng yêu cầu người bị hại chuyển các khoản phí đó vào số tài khoản ngân hàng do đối tượng cung cấp, sau đó ngắt liên lạc, chiếm đoạt tiền của người bị hại.

8. Vay tiền trực tuyến: ... Đối tượng sử dụng mạng xã hội giả danh nhân viên ngân hàng, công ty tài chính, đăng quảng cáo cho vay tiền với lãi suất thấp, thủ tục nhanh chóng. Sau đó, chúng tạo hình ảnh giả về việc vay tiền rồi yêu cầu người vay nộp trước nhiều khoản tiền như phí mở hồ sơ, phí bảo hiểm, vào số tài khoản chỉ định để được giải ngân. Sau khi chuyển tiền xong, người vay không nhận được tiền giải ngân và không liên lạc được với đối tượng.

9. Cài đặt ứng dụng giả mạo: ... Đối tượng mạo danh là nhân viên cơ quan thuế, gọi điện, nhắn tin cho người bị hại để hướng dẫn cài đặt, sử dụng ứng dụng giả mạo ứng dụng của Tổng cục thuế. Sau khi người bị hại cài đặt ứng dụng này sẽ bị chiếm đoạt các thông tin trong điện thoại; đối tượng xâm nhập vào ứng dụng Internet Banking trên điện thoại và chuyển tiền từ tài khoản ngân hàng, sổ tiết kiệm online của người bị hại đến các tài khoản khác để chiếm đoạt.

10. Thông báo trúng thưởng, quà tặng: Đối tượng sử dụng mạng xã hội hoặc gọi điện thoại, mạo danh các công ty có thương hiệu như Công ty FPT, Siêu thị Điện máy xanh, liên hệ với người bị hại để thông báo các chương trình khuyến mãi hay khách hàng đã trúng thưởng các phần quà có giá trị cao như xe máy SH, điện thoại Iphone, sổ tiết kiệm có giá trị vài trăm triệu đồng... Sau đó, đối tượng yêu cầu bị hại chuyển tiền vào tài khoản do đối tượng chỉ định để làm thủ tục nhận thưởng. Nhưng sau khi nhận được tiền, các đối tượng cắt đứt mọi liên lạc với người bị hại và chiếm đoạt tiền.

Để phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an thành phố đề nghị mỗi người dân:

1. Đề cao cảnh giác khi nhận các cuộc gọi từ người gọi tự xưng là cán bộ các cơ quan Nhà nước, đặc biệt là lực lượng Công an để thông báo, yêu cầu điều tra vụ án không liên quan đến mình. Không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở, mã OTP, số tài khoản ngân hàng. Không nên nghe và làm theo những lời hướng dẫn, giới thiệu, dụ dỗ làm theo các cách thức làm việc nhẹ nhàng, kiếm tiền dễ dàng... đặc biệt không nghe lời của các đối tượng chuyển tiền vào các tài khoản được chỉ định. Khi nhận được các cuộc gọi có nội dung như trên, cần liên lạc ngay với các đồng chí cảnh sát khu vực, công an xã, phường, thị trấn nơi mình cư trú.

2. Bảo vệ thông tin cá nhân, không công khai các thông tin như: ngày tháng năm sinh, số chứng minh nhân dân, căn cước công dân, số điện thoại, số tài khoản ngân hàng ... lên mạng xã hội để tránh bị các đối tượng lợi dụng khai thác, sử dụng vào mục đích lừa đảo; cần chọn lọc thông tin trước khi chia sẻ công khai lên mạng xã hội.

3- Thường xuyên kiểm tra và cập nhật các tính năng bảo mật, quyền riêng tư trên các tài khoản ngân hàng, tài khoản mạng xã hội và cần bảo mật tuyệt đối thông tin của các tài khoản trên, bao gồm: tên đăng nhập, mật khẩu, mã xác thực (OTP) hoặc số thẻ tín dụng,... không cung cấp cho bất kỳ cá nhân, tổ chức nào khi chưa xác định được danh tính.

4- Không truy cập các đường link trong tin nhắn hay email lạ không rõ nguồn gốc; không thực hiện giao dịch theo yêu cầu của các đối tượng lạ khi nhận được điện thoại, tin nhắn có nội dung liên quan đến giao dịch ngân hàng.

5- Cảnh giác khi tiếp cận các website, ứng dụng trong các tin nhắn nhận được, bao gồm các tin nhắn thương hiệu, tin nhắn từ các đầu số ngắn; tuyệt đối không truy cập vào các website, ứng dụng có nguồn gốc, nội dung không rõ ràng.

6- Cảnh giác, không tin vào những thông báo nhận thưởng qua mạng mà yêu cầu cung cấp thông tin hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Tìm hiểu kỹ thông tin khi kết bạn với những người lạ trên mạng xã hội, đặc biệt là những người hứa hẹn cho, tặng số tiền, tài sản lớn, không rõ lý do.

7- Cảnh giác với những trang web giả mạo dịch vụ chuyển tiền quốc tế, trang web ngân hàng... lưu ý chỉ nên nhập thông tin tài khoản ngân hàng trên trang web, ứng dụng chính thức của ngân hàng có uy tín.

8- Đối với các tin nhắn qua mạng xã hội hay qua điện thoại của người quen, bạn bè nhờ mua thẻ điện thoại, nhờ chuyển tiền hộ, cần trực tiếp gọi điện thoại để xác nhận kỹ thông tin trước khi chuyển tiền theo yêu cầu của người đó.

9- Không cài đặt lên điện thoại, máy tính các ứng dụng chưa được xác thực trên kho ứng dụng trước yêu cầu của đối tượng lạ. Khi phát hiện sim điện thoại bị vô hiệu hóa, cần gọi ngay cho bộ phận chăm sóc khách hàng của nhà mạng để yêu cầu hỗ trợ, xác minh. Nếu bị mất điện thoại, cần khẩn trương báo cho nhà mạng để khóa sim kịp thời.

10- Không mở hộ, cho thuê, bán tài khoản ngân hàng cho người khác, đặc biệt là những đối tượng không quen biết. Khi phát hiện đối tượng có hành vi mua hoặc thuê người khác mở tài khoản ngân hàng, cần báo ngay cho cơ quan Công an để có biện pháp xử lý theo quy định của pháp luật./.