TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Công an thành phố Hải Phòng cảnh báo 10 phương thức, thủ đoạn lừa đảo qua mạng

17:48 02/12/2023

Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an thành phố Hải Phòng cảnh báo một số phương thức, thủ đoạn hoạt động phổ biến và 10 biện pháp phòng ngừa hoạt động chiếm đoạt tài sản qua mạng.



Hình ảnh minh họa (Ảnh: internet)

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.

Cụ thể:

1. **Chiêu thức tuyển cộng tác viên online:** Các đối tượng mạo danh nhân viên các sàn thương mại điện tử như: Shoppee, 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.

2. 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.

3. Chúng tiếp tục nêu ra các lý do khác nhau đế giải thích cho việc không rút được tiền; đưa người bị hạivào 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.

4. **Giả danh cơ quan thực thi pháp luật để lừa đảo chiếm đoạt tài sản:** Các đối tượng sử dụng simkhông chính chủ, thiết bị chuyển đổi số điện thoại, phần mềm giả mạo các cơ quan chức năng đểgiả danh là cán bộ Công an, Viện Kiểm sát, Tòa án, gọi điện đến người bị hại, thông báo có liên quan đên 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.

5. 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 chuyến 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.

6. 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.

7. **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.

8. 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.

9. **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 câu chuyển tiền vào tài khoản ngân hàng cho các đối tượng để chiếm đoạt. Các đối tượng có thểthu 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.

10. **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.

11. **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...

12. **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.

13. Bố trí các đổi 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.

14. **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 đểđược giải ngân. Sau khi chuyển tiền xong, người vay không nhận được tiền giải ngân và không liên lạc được với đối tượng.

15. **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 chuyểntiền từ tài khoản ngân hàng, sốtiết kiệm online của người bị hại đến các tài khoản khác đế chiếm đoạt.

16. **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 trinh 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 đểlàm 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 Hải Phòng để nghị mỗi người dân cần nâng cao nhận thức, cảnh giác với các hình thức trên, bảo vệ thông tin cá nhân, thường xuyên kiểm tra và cập nhật các tính năng bảo mật riêng tư; không truy cập đường link trong tin nhắn hay điện thoại; cảnh giác với các website...

Kim Huệ t/h