BỘ CÔNG AN
CÔNG AN TỈNH NGHỆ AN

Số 531 /CV-CAT-PA05
V/v cảnh báo một số phương thức, thủ đoạn "Lừa đảo chiếm đoạt tài sản" trên không gian mạng

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

Nghệ An, ngày 15 tháng 3 năm 2022

Kính gửi:
- Các Sở, ban, ngành, đoàn thể cấp tỉnh,
- UBND các huyện, thành phố, thị xã.

Thời gian qua, các cơ quan chức năng đã tăng cường tuyên truyền, thông báo về tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông đến cán bộ, công chức, viên chức, người lao động và nhân dân biết, phòng ngừa. Tuy nhiên, lợi dụng sự hoang mang, thiếu hiểu biết trong thời điểm diễn ra dịch bệnh Covid-19 phức tạp và tâm lý cả tin, hám lợi của nạn nhân nên tội phạm trên diễn ra phức tạp hơn với phương thức, thủ đoạn xảo quyệt, tinh vi hơn. Để làm tốt công tác phòng ngừa tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông, Công an tỉnh thông báo một số thủ đoạn của tội phạm này nổi lên trong thời gian gần đây để các sở, ban, ngành, đoàn thể tỉnh và UBND các huyện, thành phố, thị xã thông báo, khuyến cáo, phổ biến, tuyên truyền sâu rộng đến cán bộ, công chức, viên chức, người lao động và quần chúng nhân dân cảnh giác:

1. Một số phương thức, thủ đoạn nổi lên gần đây của tội phạm "Lừa đảo chiếm đoạt tài sản" trên không gian mạng

1.1. Thủ đoạn giả danh người có chức vụ, quyền hạn để lừa đảo, nhất là giả danh cán bộ công an, viện kiểm sát, tòa án...

Mặc dù đã được các cơ quan chức năng cảnh báo, tuyên truyền rộng rãi nhưng vẫn có nhiều bị hại tin tưởng, chuyển tiền cho các đối tượng lừa đảo. Thủ đoạn hoạt động của loại tội phạm này chủ yếu sử dụng các đầu số điện thoại, không phải là đầu số điện thoại của Việt Nam (+84) gọi điện trực tiếp cho nạn nhân, sau đó, các đối tượng sử dụng nhiều kịch bản khác nhau như: Giả làm nhân viên bưu điện gọi điện thông báo nhận bưu phẩm; nhân viên viễn thông gọi điện thông báo nợ cước; nhân viên điện lực gọi điện thông báo nợ cước, dọa cắt điện; cảnh sát giao thông gọi điện thông báo phạt nguội, gây tai nạn bỏ trốn; vi phạm phòng, chống dịch bệnh Covid-19… Chúng liên hệ với nạn nhân để khai thác thông tin cá nhân, sau đó, sử dụng các thông tin đó làm giả các lệnh bắt, khởi tố của cơ quan công an để đe dọa nạn nhân (thường thông báo nạn nhân liên quan đến các đường dây buôn bán ma túy xuyên quốc gia, rửa tiền), yêu cầu nạn nhân chuyển tiền vào tài khoản do chúng cung cấp để phục vụ công tác điều tra, sau đó chiếm đoạt hoặc yêu cầu nạn nhân tự đăng ký một tài khoản ngân hàng, chuyển tiền vào tài khoản đó, sau đó cung cấp tài khoản, mật khẩu, mã OTP cho các đối tượng, rồi chúng rút tiền trong tài khoản để chiếm đoạt. Quá trình nói chuyện với người dân, các đối tượng thường yêu cầu người dân giữ máy liên tục, tìm nơi riêng tư để nói chuyện và yêu cầu người dân không được tiết lộ thông tin này cho bất kỳ ai.

1.2. Thủ đoạn tuyển "Cộng tác viên online" để lừa đảo chiếm đoạt tài sản

Hình thức lừa đảo bằng việc tuyển "Cộng tác viên bán hàng online" đã xuất hiện từ lâu, tuy nhiên, thời gian gần đây, các đối tượng đã lợi dụng hình thức thuê người đặt hàng ảo để tăng lượng đơn hàng, nhận đánh giá tốt trên các sàn thương mại điện tử như Shopee, Lazada, Tiki, Sendo,…Các đối tượng đã sử dụng "mồi nhử" hấp dẫn như: Mua hàng trực tiếp nhưng không nhận hàng (những kẻ lừa đảo gọi là làm tăng tỷ lệ tương tác mua hàng đối với sản phẩm), việc mua hàng sẽ được thực hiện chuyển khoản qua tài khoản Ngân hàng do đối tượng cung cấp. Mỗi lượt mua hàng thành công sẽ được hưởng hoa hồng từ 10 - 20% số tiền gốc của mỗi đơn hàng, tiền sẽ được chuyển khoản ngược về sau 5 – 10 phút khi đặt hàng thành công (bao gồm cả tiền gốc và hoa hồng). Ban đầu, để tạo lòng tin và kích thích lòng tham của nạn nhân, các đối tượng sẽ cung cấp đường link trên hệ thống Shopee, Lazada, Tiki … của một sản phẩm khoảng một triệu đến hai triệu đồng và tài khoản Ngân hàng cá nhân do đối tượng cung cấp để nạn nhân chuyển khoản với số tiền tương ứng với giá trị trên hệ thống. Ngay sau đó các đối tượng sẽ chuyển khoản ngược lại cho nạn nhân như đã thỏa thuận. Khi nạn nhân đã "cắn câu" chuyển số tiền đến vài chục triệu thì các đối tượng không chuyển khoản ngược lại nữa và đưa ra nhiều lý do khác nhau để nạn nhân tiếp tục "say mồi" như: Nhiệm vụ hoàn thành được 95/100 điểm tín nhiệm, cần tiếp tục chuyển tiền để hoàn thành 100 điểm… và nhiều người tiếp tục chuyển tiền và bị lừa số tiền đến vài trăm triệu đồng.

2. Một số cách nhận biết, phòng ngừa

Với thủ đoạn giả danh người có chức vụ, quyền hạn để lừa đảo: Theo quy định của pháp luật, khi làm việc với người dân thì các cơ quan Nhà nước (Công an, Viện kiểm sát, Tòa án, Thuế, Hải quan...), các công ty, doanh nghiệp đều có giấy giới thiệu, giấy mời hoặc trực tiếp gặp mặt để trao đổi công việc và không có quy định gọi điện thoại yêu cầu chuyển tiền. Do đó, tất cả các cuộc điện thoại tự nhận là cơ quan chức năng đang điều tra, giải quyết vụ án, vụ việc; hải quan, thuế thông báo có quà tặng hoặc doanh nghiệp thông báo trúng thưởng... rồi yêu cầu chuyển tiền vào tài khoản đều có nguy cơ là lừa đảo chiếm đoạt tài sản. Bên cạnh đó, theo quy định, các ngân hàng không yêu cầu khách hàng cung cấp thông tin tài khoản, thẻ ngân hàng, ví điện tử, mã OTP hoặc bất kỳ thông tin cá nhân của khách hàng qua mail/tin nhắn hay gọi điện thoại.

Với thủ đoạn tuyển "Cộng tác viên online" để lừa đảo chiếm đoạt tài sản: Các bài tuyển CTV online thường xuyên xuất hiện nhiều trong quảng cáo trên các trang mạng xã hội như Facebook, Zalo,… Các công ty, tổ chức và các sàn thương mại điện tử khi có nhu cầu tuyển dụng việc làm, tuyển cộng tác viên thì sẽ có thông báo rộng rãi trên các phương tiện thông tin đại chúng hoặc qua website của các công ty, tổ chức đó. Do đó, các bài tuyển dụng việc làm nói chung và tuyển cộng tác viên online nói riêng có nguy cơ lừa đảo chiếm đoạt tài sản.

3. Một số khuyến nghị quan trọng

Để chủ động đấu tranh, phòng ngừa loại tội phạm này, Công an tỉnh khuyến nghị một số biện pháp như sau:

- Không nhấn vào các đường link lạ, tuyệt đối không cung cấp các thông tin tài khoản ngân hàng cho bất kỳ cá nhân, tổ chức nào thông qua các cuộc gọi, đường link gửi bằng mail/tin nhắn. Nếu người thân, bạn bè nhắn tin vay mượn tiền qua các mạng xã hội thì gọi điện thoại trực tiếp cho người đó để xác minh thông tin chính xác trước khi chuyển tiền.

- Không cung cấp mã OTP do ngân hàng cung cấp hay thực hiện xóa cài đặt xác thực Smart OTP cho bất kỳ ai;

- 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; không cho mượn, thuê các giấy tờ cá nhân liên quan, không nhận chuyển khoản ngân hàng hoặc nhận tiền chuyển khoản của các ngân hàng cho người không quen biết;

- Khi phát hiện sự việc có dấu hiệu vi phạm pháp luật xảy ra cần thông tin cho cơ quan công an để phục vụ công tác xác minh, điều tra, làm rõ.

Trên đây là một số phương thức, thủ đoạn của tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông, Công an tỉnh thông báo đến các Sở, ban, ngành, đoàn thể cấp tỉnh và UBND các huyện, thành phố, thị xã để chủ động trong công tác phòng ngừa giúp cán bộ, công chức, viên chức, người lao động và quần chúng nhân dân nắm bắt thông tin, góp phần đảm bảo an ninh trật tự trên địa bàn tỉnh./.

Nơi nhận:
- Như trên;
- Các đ/c PGĐ (để p/hợp chỉ đạo);
- Công an các đơn vị, địa phương (để t/hiện);
- Lưu: VTCAT (gốc), PA05(Đ3).

GIÁM ĐỐC

Thiếu tướng Phạm Thế Tùng