UBND TỈNH THỪA THIÊN HUẾ
BAN CHỈ ĐẠO 138 TỈNH

Số: 289/BCĐ

V/v thông báo phương thức, thủ đoạn tội phạm sử dụng công nghệ cao lừa đảo qua mạng

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

Thừa Thiên Huế, ngày 31 tháng 5 năm 2022

Kính gửi:
- Các sở, ban, ngành, cơ quan, đoàn thể thành viên Ban Chỉ đạo 138 tỉnh;
- Ban Chỉ đạo 138 các huyện, thị xã, thành phố Huế.

Thời gian qua, việc ứng dụng công nghệ thông tin, sử dụng các phần mềm chuyên dụng để làm việc, hội họp, học tập, kinh doanh, mua sắm, giao tiếp trực tuyến ở nước ta phát triển mạnh mẽ; nhiều hoạt động, thông tin trao đổi, giao dịch của người dân được thực hiện qua không gian mạng. Lợi dụng tình hình trên, hoạt động sử dụng không gian mạng lừa đảo chiếm đoạt tài sản ngày càng gia tăng với nhiều phương thức thủ đoạn phạm tội mới, hoạt động có tính chất xuyên quốc gia và gây thiệt hại lớn, trong đó nổi lên một số thủ đoạn cụ thể như sau:

1 Xâm nhập, sử dụng bất hợp pháp tài khoản, lập tài khoản giả danh trên mạng xã hội kết bạn, làm quen nhằm lừa đảo chiếm đoạt tài sản.

Các đối tượng tấn công xâm nhập, chiếm quyền điều khiển tài khoản Facebook, Zalo của người thân, bạn bè của người bị hại. Khi chiếm được quyền điều khiển tài khoản Facebook đối tượng giả danh chủ tài khoản, nhắn tin cho bị hại để vay tiền hoặc nhờ chuyển tiền giúp vì lý do vướng mắc chưa thể trực tiếp chuyển khoản được. Ngay sau khi nhận được tiền chuyển từ bị hại, các đối tượng lập tức chuyển tiền sang các ngân hàng khác (tất cả tài khoản trên đều không đứng tên, địa chỉ của đối tượng). Tiếp đó đối tượng thường chuyển tiền vào tài khoản đại lý game cờ bạc, mua thẻ game, thẻ cào viễn thông mang ra các đại lý bán lấy tiền mặt hoặc chuyển vào tài khoản trung gian khác để lấy tiền mặt. Ngoài ra, các đối tượng cũng có thể lập tài khoản Zalo, sử dụng tên, ảnh đại diện và các thông tin giống với tài khoản của người quen của bị hại, sau đó giả danh người quen nhắn tin với bị hại và nhờ chuyển tiền để chiếm đoạt.

2. Kết bạn qua mạng xã hội, xây dựng tình cảm và hứa hẹn gửi quà có giá trị, sau đó yêu cầu chuyển tiền nộp thuế hoặc phí thông quan, nhằm chiếm đoạt tài sản

Đối tượng thông qua mạng xã hội như Zalo, Facebook, Twiter, Instagram… làm quen và kết bạn với các nạn nhân. Sau đó, các đối tượng tự giới thiệu mình là kỹ sư, quân nhân… đang sinh sống tại nước ngoài và tâm sự

tình cảm tạo niềm tin rồi hứa hẹn tặng quà, hứa kết hôn và bảo lãnh đi nước ngoài hoặc ngỏ ý giúp đỡ tạo điều kiện để kinh doanh... Sau khi nạn nhân tin tưởng, đối tượng thông báo sẽ chuyển tiền hoặc đồ vật có giá trị từ nước ngoài về Việt Nam. Kế tiếp, các đối tượng cho người đóng giả làm nhân viên Hải quan, Thuế hoặc Công an... gọi điện thoại thông báo với nạn nhân quà tặng bị tạm giữ khi về đến sân bay, bến cảng do có giá trị lớn nên buộc các nạn nhân phải chuyển tiền để nộp thuế hoặc "hối lộ" cho cán bộ Hải quan, Công an... Sau đó các đối tượng cung cấp số tài khoản cho các nạn nhân yêu cầu chuyển tiền rồi chiếm đoạt tiền của bị hại.

Với hình thức lừa đảo này thì thường nhóm đối tượng sẽ có các đối tượng người nước ngoài câu kết với đối tượng người Việt Nam để thực hiện hành vi lừa đảo. Đối tượng người Việt Nam sẽ phụ trách việc liên hệ và nhận tiền lừa đảo của nạn nhân.

3. Lừa đảo qua mạng xã hội bằng hình thức gửi tin nhắn trúng thưởng.

Các đối tượng thu thập thông tin số điện thoại hoặc tài khoản mạng xã hội của bị hại sau đó sử dụng số điện thoại sim rác, tài khoản mạng xã hội khác (với tên hấp dẫn như: Tri ân khách hàng, Quà tặng, Chương trình trúng thưởng...hay tên của doanh nghiệp, hoặc của người nổi tiếng). Sau đó, chúng phát tán các tin nhắn trúng thưởng đến các bị hại với nội dung như: Chủ nhân thuê bao/mạng xã hội xxx đã trúng thưởng... để biết chi tiết và làm thủ tục hồ sơ nhận thưởng đề nghị khách hàng truy cập vào đường dẫn giả mạo (các tên miền lừa đảo lấy tên Quà tặng, tri ân, các cơ quan uy tín...) để điền thông tin (Họ tên, ngày tháng năm sinh, địa chỉ, số điện thoại,...). Khi bị hại truy cập và hoàn tất các thủ tục trên website, các đối tượng yêu cầu người dùng nộp lệ phí bằng nhiều hình thức như chuyển khoản, nạp thẻ cào điện thoại nhằm chiếm đoạt tài sản và chiếm quyền điều khiển tài khoản mạng xã hội đó.

4. Thủ đoạn lừa đảo lợi dụng hình thức kinh doanh đa cấp, đầu tư tài chính, đánh bạc qua mạng.

Tình hình kinh doanh trái phép vàng tài khoản, lập sàn giao dịch tiền ảo, tiền kỹ thuật số lôi kéo số lượng lớn người dân tham gia đầu tư trong thời gian vừa qua có diễn biến phức tạp. Chủ sàn trên danh nghĩa là trung gian, môi giới cho các nhà đầu tư kinh doanh vàng tài khoản, tiền kỹ thuật số, tiền ảo nhưng bản chất là các đối tượng lừa đảo. Khi giá tiền ảo, tiền kỹ thuật số, vàng có sự thay đổi, biến động, chủ sàn can thiệp trực tiếp vào các phần mềm giao dịch nhằm mục đích có lợi cho mình nhằm chiếm đoạt tiền của các nhà đầu tư. Với thủ đoạn nêu trên, các đối tượng đã chiếm đoạt hàng trăm tỷ đồng của các nhà đầu tư. Nhiều trường hợp, các chủ sàn sau khi huy động vốn của các nhà đầu tư đã không tiến hành bất kỳ giao dịch đầu tư nào mà thực chất là lấy tiền của nhà

đầu tư sau trả lãi cho nhà đầu tư trước, chúng chiếm đoạt số tiền chênh lệch sau khi trả lãi và đánh sập trang web giao dịch.

Các đối tượng còn lợi dụng hình thức kinh doanh đa cấp, thủ đoạn chính của các đối tượng này là tuyên truyền, tự nhận các Website do chúng xây dựng là các sàn giao dịch thương mại điện tử được Nhà nước cấp phép hoạt động, xây dựng phần mềm với các thuật toán nhằm chia hoa hồng, lôi kéo người tham gia và giới thiệu người khác tham gia để hưởng hoa hồng.

Ngoài ra, thủ đoạn mới hiện nay là các đối tượng xây dựng các sàn Bo (sàn giao dịch quyền chọn nhịn phân), trang web là đại lý game cờ bạc Bacarat. Các hình thức này đều cho phép người chơi lôi kéo người khác tham gia qua các hội nhóm trên mạng xã hội Telegram để được hưởng tiền hoa hồng. Ngoài ra, các đối tượng quản lý website còn bán bảo hiểm tài khoản sau đó chiếm đoạt tiền của người chơi.

5. Lừa đảo, chiếm đoạt tài sản trong mua bán hàng hóa qua mạng Internet.

Các đối tượng thường tạo lòng tin bằng cách thực hiện đúng hợp đồng trong một số giao dịch ban đầu, sau đó đề nghị bị hại chuyển tiền cọc với số lượng lớn trong những lần giao dịch tiếp theo. Các đối tượng nhanh chóng rút hết số tiền cọc đó và không thực hiện giao dịch như trong hợp đồng thỏa thuận. Ngoài ra, đối tượng lợi dụng việc người mua phải trả tiền trước, sau đó các đối tượng không chuyển hàng hoặc giao hàng không phù hợp với nội dung đã thỏa thuận. Đây là những thủ đoạn không mới, tuy nhiên trong thời gian vừa qua, khi dịch bệnh Covid 19 có diễn biến phức tạp, nhu cầu mua bán trực tuyến tăng đột biến khiến các đối tượng lợi dụng các trang mạng xã hội như Facebook, Zalo… đăng tin rao bán các mặt hàng khan hiếm như khẩu trang, nước rửa tay, tinh dầu tràm… nhằm đúng nhu cầu của người tiêu dùng, thực hiện hành vi phạm tội chiếm đoạt tài sản.

6. Thủ đoạn dùng phần mềm gián điệp để chiếm đoạt tài sản

Đối tượng sử dụng phần mềm gửi thư rác (spam) có nội dung khuyến mại, trúng thưởng… gửi đến email của nhiều người. Khi người sử dụng nhận được thông báo chúc mừng đã trúng thưởng một chương trình khuyến mãi chăm sóc khách hàng của một ngân hàng, cùng với nhiều phần tiền thưởng hấp dẫn, kèm theo đó người dùng phải truy cập vào website của đối tượng (với các tên miền gần giống tên miền của ngân hàng) rồi đăng nhập tài khoản ngân hàng của mình và cung cấp mã xác thực OTP (One Time Password) để nhận phần thưởng. Vì chủ quan, người dùng đã làm theo hướng dẫn. Từ đây, đối tượng sẽ chiếm quyền quản trị, kiểm soát mọi hoạt động của người sử dụng máy tính. Loại virus được cài đặt vào máy sẽ tự động theo dõi người dùng, thu thập toàn bộ thao tác trên bàn phím trong đó có hoạt

động giao dịch tài khoản ngân hàng. Đối tượng dùng phương thức này để trộm cắp tài khoản, mật khẩu, mã OTP, sau đó thực hiện hành vi chuyển tiền từ tài khoản của người dùng sang tài khoản khác.

7. Hình thức lừa đảo giả danh người khác gọi điện thoại nhằm lừa đảo chiếm đoạt tài sản.

Đối tượng sử dụng phần mềm VoIP (Sử dụng ứng dụng truyền tải giọng nói qua mạng máy tính, giả số điện thoại hiển thị trên màn hình...). Để thực hiện hành vi lừa đảo, các đối tượng thường tiếp cận nạn nhân bằng công nghệ VoIP (cuộc gọi đến có số điện thoại hiển thị trên màn hình điện thoại người nhận là các số giống với số trực ban cơ quan công an...) để thông báo chủ thuê bao đang nợ tiền cước, đang bị nhà mạng khởi kiện... Sau đó chúng nối máy với đối tượng khác tự xưng là cán bộ Công an, Viện kiểm sát, Tòa án để giải quyết. Các đối tượng này thông báo bị hại đang liên quan đến vụ án nghiêm trọng mà cơ quan công an đang điều tra (ma túy, rửa tiền...), yêu cầu cung cấp thông tin cá nhân, tài khoản ngân hàng và chuyển tiền vào tài khoản do chúng chỉ định để phục vụ điều tra. Khi bị hại chuyển tiền xong, chúng sẽ nhanh chóng rút tiền hoặc chuyển tiền sang tài khoản khác và chiếm đoạt. Hoặc giả mạo là cán bộ ngân hàng, điện lực gọi điện hoặc nhắn tin cho bị hại yêu cầu cung cấp thông tin tài khoản đăng nhập, mật khẩu và mã số OTP để nhận tiền chuyển khoản. Sau đó các đối tượng rút tiền, chuyển tiền sang tài khoản khác hoặc thanh toán các hóa đơn nhằm chiếm đoạt tài sản.

Để kịp thời phòng ngừa, ngăn chặn và đấu tranh xử lý với các đối tượng lừa đảo qua mạng, Công an tỉnh - Cơ quan Thường trực Ban Chỉ đạo 138 tỉnh trân trọng đề nghị các sở, ban, ngành, cơ quan, đoàn thể, địa phương quan tâm phối hợp:

1. Các sở, ban, ngành, cơ quan, đoàn thể cấp tỉnh, các tổ chức chính trị - xã hội, cơ quan Trung ương đóng trên địa bàn tỉnh, Ban Chỉ đạo 138 các huyện, thị xã, thành phố Huế tăng cường hơn nữa công tác tuyên truyền, phổ biến các phương thức, thủ đoạn trên đến cán bộ thuộc cơ quan mình quản lý và người dân trên địa bàn biết để nâng cao cảnh giác, chủ động xác minh thông tin trước khi giao dịch, chuyển tiền; không cung cấp thông tin cá nhân cho người lạ dưới bất cứ hình thức nào, tránh sập bẫy các đối tượng.

2. Sở Thông tin và Truyền thông, Ngân hàng Nhà nước chi nhánh Thừa thiên Huế tăng cường công tác quản lý, xử lý nghiêm đối với các tổ chức, cá nhân phát hành, mua bán sim rác, tài khoản ngân hàng rác;

Chỉ đạo Trung tâm Giám sát, điều hành đô thị thông minh tỉnh Thừa Thiên Huế (HueIOC) phối hợp các đơn vị nghiệp vụ của Công an tỉnh thường

xuyên tuyên truyền, phổ biến, cảnh báo các phương thức, thủ đoạn lừa đảo qua mạng qua ứng dụng Hue-S và các kênh thông tin, mạng xã hội.

3. Sở Giáo dục và Đào tạo, Đại học Huế, các trường Đại học, Cao đẳng, Trung học dạy nghề trên địa bàn thông qua các buổi học ngoại khóa cần phổ biến, quán triệt cho các em học sinh, sinh viên nắm các phương thức, thủ đoạn của tội phạm lừa đảo qua mạng; yêu cầu các em không cung cấp, đăng ký thuê bao di động, mở tài khoản ngân hàng để bán, cho, tặng người khác sử dụng, tránh bị các đối tượng lợi dụng, lừa đảo.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để báo cáo);
- Trưởng Ban Chỉ đạo 138 tỉnh (để báo cáo);
- Đ/c Giám đốc Công an tỉnh (để báo cáo);
- Lưu: VT, VPTT.

KT. TRƯỞNG BAN
PHÓ TRƯỞNG BAN

CÔNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH THỪA THIÊN HUẾ

PHÓ GIÁM ĐỐC CÔNG AN TỈNH
Đại tá Đặng Ngọc Sơn