UBND HUYỆN CHƯ SÊ
BAN CHỈ ĐẠO PCTP, TNXH VÀ XDPTTDBVANTQ

Số: 536 /CV-BCĐ
V/v phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản sử dụng mạng viễn thông, mạng internet

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập – Tự Do – Hạnh Phúc

Chư Sê, ngày 19 tháng 4 năm 2023

Kính gửi: - Thành viên Ban Chỉ đạo PCTP, TNXH và XDPT toàn dân bảo vệ an ninh Tổ quốc huyện Chư Sê
- Ban Chỉ đạo PCTP, TNXH và XDPT toàn dân bảo vệ an ninh Tổ quốc các xã, thị trấn.

Thời gian gần đây, tình hình tội phạm lừa đảo chiếm đoạt tài sản thông qua mạng viễn thông, mạng internet trên địa bàn huyện Chư Sê nói riêng và tỉnh Gia Lai nói chung diễn biến phức tạp, có chiều hướng gia tăng; hoạt động phạm tội của các đối tượng rất tinh vi, đa dạng về phương thức, gây thiệt hại lớn về tài sản, bức xúc trong dư luận xã hội, ảnh hưởng đến tình hình an ninh, trật tự tại địa phương. Mặc dù các cơ quan chức năng, cơ quan truyền thông thường xuyên thông báo phương thức, thủ đoạn hoạt động của các đối tượng sử dụng công nghệ cao để lừa đảo chiếm đoạt tài sản. Tuy nhiên, vẫn còn nhiều người dân vì thiếu hiểu biết, nhẹ dạ, cả tin, hám lợi, mất cảnh giác...nên để các đối tượng thực hiện hành vi lừa đảo chiếm đoạt tài sản.

Trước diễn biến phức tạp của tội phạm lừa đảo chiếm đoạt tài sản thông qua mạng viễn thông và mạng internet. Ban Chỉ đạo PCTP, TNXH và XDPT toàn dân bảo vệ an ninh Tổ quốc huyện Chư Sê đề nghị Thành viên Ban chỉ đạo huyện và Ban chỉ đạo các xã, thị trấn thông báo triển khai rộng rãi đến từng Thôn, Làng, Tổ dân phố, từng hộ gia đình bằng văn bản, tổng hợp các phương thức thủ đoạn và biện pháp phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng và cách phòng ngừa để nhân dân biết phòng ngừa.

(có phụ lục đính kèm)

Nhận được văn bản này, đề nghị thành viên ban chỉ đạo, các cơ quan đơn vị, UBND các xã, thị trấn triển khai thực hiện./.

Nơi nhận:
- Như kính gửi (để thực hiện);
- CT, các PCT UBND huyện;
- Công an huyện;
- VP HĐND&UBND huyện;
- Lưu: VT, NC, BCĐ (CAH).

TM.BAN CHỈ ĐẠO
TRƯỞNG BAN

CHỦ TỊCH UBND HUYỆN
Rmah H'Bé Nét

PHỤ LỤC

TỔNG HỢP CÁC PHƯƠNG THỨC THỦ ĐOẠN LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG VÀ CÁCH PHÒNG NGỪA

(Kèm theo Công văn số 536 /CV-BCĐ, ngày 13/4/2023 của Ban chỉ đạo PCTP TNXH và XDPT toàn dân bảo vệ ANTQ huyện Chư Sê)

(1) Giả danh cơ quan Công an, Viện kiểm sát, Tòa án gọi điện thoại trực tiếp, gọi video call bằng zalo để hăm dọa bị hại có liên quan đến các vụ án đang điều tra, yêu cầu bị hại chuyển tiền đến các tài khoản do các đối tượng chỉ định hoặc yêu cầu cung cấp mã OTP để xác thực chuyển tiền để kiểm tra, xác minh sau đó chiếm đoạt. Gần đây nhất là thủ đoạn giả danh thầy cô chủ nhiệm gọi điện thông báo con em đang học ở trường bị tai nạn phải cấp cứu tại bệnh viện, yêu cầu phụ huynh học sinh chuyển tiền gấp vào tài khoản do đối tượng cung cấp rồi chiếm đoạt. Hoặc giả danh nhân viên ngân hàng tư vận mở thẻ, hủy thẻ tín dụng... yêu cầu cung cấp thông tin cá nhân, mã xác thực OTP rồi sử dụng các thủ đoạn để chiếm đoạt tài sản.

(2) Thông qua hoạt động của các sàn đầu tư chứng khoán quốc tế, giao dịch vàng, ngoại hối, quyền chọn nhị phân (BO), giao dịch tiền ảo, dự án bất động sản... hoặc hoạt động kinh doanh đa cấp trái phép qua mạng để quảng cáo, lôi kéo số lượng lớn người tham gia đầu tư, kinh doanh (với cam kết về các khoản lợi nhuận rất lớn, số tiền đầu tư ít) nhằm mục đích lừa đảo chiếm đoạt số tiền của người tham gia.

(3) Đăng tin tuyển cộng tác viên bán hàng online trên các trang mạng xã hội (zalo, facebook, tiktok...), nhận việc làm tại nhà, không mất thời gian di chuyển, bỏ tiền tạm ứng hoặc thanh toán trước đơn hàng khoảng vài trăm nghìn để đặt hàng, sau đó nhận tiền công kèm theo lãi đơn hàng và tiền thưởng, tuy nhiên sau khi thanh toán đơn hàng và đặt hàng, nạn nhân bị chiếm đoạt số tiền tạm ứng hoặc thanh toán đơn hàng.

(4) Giả mạo các trang thông tin điện tử cơ quan, doanh nghiệp (Bảo hiểm xã hội, Ngân hàng...) đánh cắp, chiếm đoạt thông tin dữ liệu cá nhân của người đăng nhập nhằm lừa đảo chiếm đoạt tài sản hoặc thiết lập các trạm BTS viễn thông giả mạo để phát tán tin nhắn thương hiệu (SMS Brandname) của các ngân hàng để đánh cắp thông tin, tài khoản người dùng sau đó thực hiện hành vi chiếm đoạt tài sản.

(5) Sử dụng nhiều thủ đoạn khác nhau để chiếm đoạt quyền điều khiển tài khoản mạng xã hội (gửi các đường link giả mạo, quảng cáo tuyển dụng, làm việc tại nhà, các trò chơi giải trí trên mạng...), sau đó nhắn tin lừa đảo đến danh sách bạn bè của người bị hại; hoặc chiếm đoạt quyền sử dụng sim điện thoại bằng cách gọi điện tư vấn chuyển đổi hoặc nâng cấp sim điện thoại sang mạng 4G miễn phí, từ đó chiếm đoạt mật khẩu tài khoản ngân hàng, ví điện tử, tài khoản mạng xã hội để thực hiện hành vi chiếm đoạt tài sản...

(6) Lợi dụng sự thiếu hiểu biết của một bộ phận người dân, đối tượng dụ dỗ, lôi kéo mua bán thông tin cá nhân, tài khoản ngân hàng để sử dụng thực hiện các hành vi phạm tội. Hoặc thông qua hoạt động thương mại điện tử để rao bán hàng giả, hàng nhái, rao bán vé máy bay... rồi chiếm đoạt tiền của người tham gia giao dịch.

(7) Đối tượng sử dụng mạng xã hội làm quen, quá trình nói chuyện, khi đã phát sinh tình cảm thì nói mình ở nước ngoài, gợi ý gửi quà tặng và nhờ bị hại nhận, cất giữ khi đối tượng đến Việt Nam. Nếu bị nghi ngờ thì đối tượng gửi cho bị hại tên của đơn vị vận chuyển, đường link và mật khẩu để theo dõi lịch trình di chuyển của lô hàng. Đồng thời giả danh, tự xưng là nhân viên hải quan, gọi điện thoại cho bị hại nói là lô hàng đã đến sân bay nhưng do bên trong có điện thoại, máy tính, nữ trang, tiền... nên phải đóng

phí và yêu cầu bị hại chuyển tiền vào các tài khoản chỉ định để đóng phí, sau đó chiếm đoạt.

(8) Thông qua mạng internet, các đối tượng đã thu nhập hình ảnh, giọng nói của người dùng trên mạng xã hội, sử dụng công nghệ Deepfake tạo ảnh động, video giả mạo người dùng đang nói chuyện trực tuyến với cùng khuôn mặt, âm điệu giọng nói và cách xưng hô. Sau đó đối tượng tạo lập tài khoản giả mạo trên mạng xã hội (facebook, zalo, telegram, intagram…) trùng thông tin và ảnh đại diện của người dùng, kết bạn với nạn nhân trong danh sách bạn bè và nhắn tin vay mượn tiền theo kịch bản sẵn có. Trong một số trường hợp đối tượng chiếm đoạt tài khoản mạng xã hội của người dùng để trực tiếp nhắn tin cho các nạn nhân trong danh sách bạn bè. Để tạo lòng tin với nạn nhân, đối tượng truyền tải Deepfake video có sẵn lên kênh video call, khiến nạn nhân nhận ra hình ảnh, giọng nói của người quen, bạn bè và nhanh chóng chuyển tiền theo yêu cầu của đối tượng.

MỘT SỐ BIỆN PHÁP PHÒNG NGỪA

1. Tăng cường trau dồi kiến thức về pháp luật, chính sách, thường xuyên theo dõi các thông báo phương thức thủ đoạn phạm tội của cơ quan chức năng trên các phương tiện, thông tin đại chúng. Nghiên cứu, kiểm tra kỹ trước khi thực hiện các giao dịch về tài chính, đề phòng trước những khoản đầu tư mang lại "lợi nhuận cao". Đồng thời tích cực tuyên truyền về thủ đoạn lừa đảo của đối tượng để người thân, bạn bè, nhân dân biết phòng tránh.

2. Đề cao cảnh giác khi nhận các cuộc gọi đến bằng số điện thoại cố định, 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 qua điện thoại, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở... cho bất kỳ đối tượng nào khi chưa biết rõ nhân thân và lai lịch của người đó, đặc biệt không nghe lời của các đối tượng chuyển tiền vào các tài khoản do các đối tượng chỉ định. Lực lượng chức năng, nhất là lực lượng Công an, Viện kiểm sát, Tòa án nếu làm việc với người dân sẽ có giấy mời, giấy triệu tập gửi cho người đó và làm việc trực tiếp tại các trụ sở cơ quan, không làm việc online qua mạng.

3. Điện thoại di động, máy tính cá nhân cần sử dụng chế độ bảo mật nhiều lớp; thường xuyên kiểm tra và cập nhật các tỉnh năng bảo mật, quyền riêng tư trên các tài khoản mạng xã hội, thường xuyên thay đổi để đảm bảo tính an toàn của mật khẩu, không truy cập các đường link lạ, tải và sử dụng các ứng dụng không rõ nguồn gốc. Chuyên viên các công ty tài chính, chứng khoán, phòng giao dịch ngân hàng cần có ý thức bảo mật thông tin trong quá trình thực hiện các giao dịch.

4. Người dân khi mua hàng qua mạng cần sàng lọc, kiểm tra kỹ thông tin quảng cáo, rao bán về hàng hóa, danh tính người bán hàng, lựa chọn địa chỉ uy tín, hình thức thanh toán minh bạch. Không chia sẻ quá nhiều thông tin cá nhân trên mạng xã hội; không cho mượn, cho thuê các giấy tờ cá nhân có liên quan như: Căn cước công dân, giấy chứng minh nhân dân, sổ hộ khẩu, thẻ ngân hàng, không nhận chuyển khoản ngân hàng hoặc nhận tiền chuyển khoản của các ngân hàng cho người không quen biết.

5. Cảnh giác, không tin tưởng vào những chiêu trò nhận thưởng qua mạng mà yêu cầu nạp tiền thẻ điện thoại 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 lớn, những món quà đắt tiền. Đối với các tin nhắn qua mạng xã hội, qua điện thoại người quen, bạn bè nhờ mua thẻ cào điện thoại, nhờ chuyển tiền hộ cần gọi điện trực tiếp để xác nhận thông tin với người nhờ, không nói chuyện qua tin nhắn.

6. Gọi điện bằng số điện thoại để xác nhận là người thân, bạn bè yêu cầu chuyển tiền trước khi chuyển khoản. Chỉ chuyển tiền đến số tài khoản đứng tên của người thân, bạn bè yêu cầu chuyển tiền.

Trường hợp có nghi ngờ về hoạt động lừa đảo chiếm đoạt tài sản, cần giữ tinh thần bình tĩnh, không thực hiện theo yêu cầu chuyển tiền do đối tượng đưa ra. Duy trì liên lạc với đối tượng, lưu giữ các thông tin liên quan như: tin nhắn, hình ảnh, ghi âm đàm thoại, thông tin số điện thoại, tài khoản ngân hàng, tài khoản mạng xã hội, thông tin địa chỉ... của các đối tượng có liên quan. Nhanh chóng đến cơ quan Công an nơi gần nhất trình báo để được tiếp nhận và hướng dẫn giải quyết.