ỦY BAN NHÂN DÂN **TỈNH THỪA THIÊN HUẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 8987 /UBND-TĐKT	*Thừa Thiên Huế, ngày 25 tháng 8 năm 2023*
V/v tăng cường triển khai các biện pháp phòng, chống tội phạm lừa đảo chiếm đoạt tài sản qua mạng	

Kính gửi:
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- Các cơ quan Trung ương đóng trên địa bàn tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố Huế.

Thời gian gần đây, trên toàn quốc nói chung và trên địa bàn tỉnh Thừa Thiên Huế nói riêng, tình hình tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản trên không gian mạng có chiều hướng gia tăng phức tạp, với nhiều phương thức, thủ đoạn tinh vi, như: (1) Đăng tin giả mạo tuyển cộng tác viên làm việc online; (2) Giả danh cơ quan chức năng; (3) Kêu gọi đầu tư online siêu lợi nhuận; (4) Giả danh người nước ngoài thành đạt; (5) Chiếm quyền điều khiển tài khoản mạng xã hội; (6) Chiếm quyền sử dụng sim số; (7) Giả danh giáo viên chủ nhiệm, nhân viên bảo vệ nhà trường hoặc nhân viên bệnh viện; (8) Lừa đảo đặt tiệc để chiếm đoạt tài sản; (9) Chiếm quyền điều khiển tài khoản ngân hàng; (10) Vay vốn online; (11) Giả danh nhân viên Công ty xổ số cho số đề để đánh lô, đề; (12) Giả danh nhân viên ngân hàng, nhà mạng, nhân viên các sàn thương mại điện tử như Lazada, Shopee, Tiki...

Nhằm chủ động phòng ngừa, đấu tranh, ngăn chặn có hiệu quả đối với tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản trên không gian mạng, Ủy ban nhân dân tỉnh yêu cầu:

1. Các sở, ban, ngành, đoàn thể cấp tỉnh, các tổ chức chính trị - xã hội, cơ quan Trung ương đóng trên địa bàn tỉnh, UBND các huyện, thị xã, thành phố Huế tăng cường công tác tuyên truyền, phổ biến các phương thức, thủ đoạn của tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản đến từng cơ quan, doanh nghiệp, trường học, người dân trên địa bàn, với nhiều hình thức trực quan, dễ tiếp cận như: phát tờ rơi; pa nô, áp phích; tuyên truyền thông qua các buổi họp tổ dân phố, khu dân cư, trên loa phát thanh…; hướng dẫn cán bộ, nhân viên, người dân chủ động xác minh, kiểm tra kỹ 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.

- Đài Phát thanh và Truyền hình tỉnh, các cơ quan thông tấn, báo chí thường xuyên xây dựng tin, bài, phóng sự tuyên truyền, cảnh báo các phương

thức, thủ đoạn của tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản trên không gian mạng; tăng cường thời lượng phát sóng trên các phương tiện thông tin đại chúng.

- Đề nghị Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh và các đoàn thể chính trị - xã hội trên địa bàn tăng cường công tác tuyên truyền phòng, chống tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản trên không gian mạng; thường xuyên thông báo phương thức, thủ đoạn hoạt động của tội phạm thông qua các hội nghị tập huấn, sinh hoạt chuyên đề, các hoạt động an sinh xã hội để cán bộ, công chức, viên chức, đoàn viên, hội viên biết, cảnh giác, chủ động phòng ngừa.

2. Sở Thông tin và Truyền thông tăng cường kiểm tra công tác quản lý sim số của các đơn vị cung cấp dịch vụ viễn thông, không để diễn ra tình trạng mua bán sim "rác"; đề nghị các doanh nghiệp viễn thông, internet, các tổ chức, doanh nghiệp cung cấp dịch vụ trên hạ tầng mạng không cung cấp dịch vụ có nội dung lừa đảo, nghi vấn lừa đảo hoặc có thể bị lợi dụng để lừa đảo; chủ động triển khai các biện pháp cảnh báo, hỗ trợ, bảo vệ người sử dụng; phối hợp gửi tin nhắn cảnh báo các phương thức, thủ đoạn lừa đảo qua mạng đến các thuê bao di động; tạo điều kiện, cung cấp thông tin, dữ liệu, tài liệu phục vụ công tác điều tra, xử lý tội phạm và các hành vi vi phạm pháp luật liên quan đến tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng theo yêu cầu của cơ quan Công an các cấp.

Phối hợp Công an tỉnh, Ngân hàng Nhà nước Việt Nam chi nhánh Thừa Thiên Huế, Sở Công Thương và các cơ quan liên quan tăng cường thanh tra, kiểm tra, xử lý, giám sát các trang thông tin điện tử, tài khoản mạng xã hội của các tổ chức, cá nhân có hành vi huy động vốn, đầu tư trái phép, đòi tiền qua trung gian, quảng cáo mua bán hàng hóa, dịch vụ mua hộ hàng hóa, giới thiệu, quảng cáo đăng tin trên báo chí, trang thông tin điện tử, mạng xã hội, xuất bản phẩm, quảng cáo,… tích hợp trên các sản phẩm dịch vụ bưu chính, viễn thông, công nghệ thông tin, phòng ngừa hoạt động lừa đảo chiếm đoạt tài sản.

3. Ngân hàng Nhà nước Việt Nam chi nhánh Thừa Thiên Huế chỉ đạo các ngân hàng thương mại, tổ chức tín dụng trên địa bàn tỉnh quản lý chặt các hoạt động đăng ký, mở tài khoản, đặc biệt là các tài khoản online; kịp thời phối hợp cung cấp thông tin, phong tỏa tài khoản ngân hàng có dấu hiệu vi phạm khi Cơ quan Công an yêu cầu; đối với các giao dịch nghi ngờ, hướng dẫn khách hàng cụ thể, tránh rút, chuyển tiền cho các đối tượng lừa đảo.

4. Sở Giáo dục và Đào tạo, Đại học Huế, các trường Đại học, Cao đẳng, Trung học dạy nghề trên địa bàn tỉnh thông qua các buổi học ngoại khóa 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.

5. Công an tỉnh chủ trì, tăng cường phối hợp với các cơ quan, đơn vị chức năng triển khai các biện pháp nghiệp vụ, biện pháp kỹ thuật để phòng ngừa, phát hiện, đấu tranh, làm rõ các đối tượng lợi dụng không gian mạng, sử dụng công nghệ cao để lừa đảo chiếm đoạt tài sản; nâng cao hiệu quả công tác tiếp nhận, giải quyết tố giác, tin báo về tội phạm theo Hướng dẫn số 14/HDLN-BCA-VKSNDTC của Bộ Công an, Viện Kiểm sát nhân dân tối cao "về công tác phối hợp tiếp nhận, giải quyết tố giác, tin báo về tội phạm sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản".

Nhận được văn bản này, yêu cầu các sở, ban, ngành, cơ quan, địa phương tổ chức triển khai thực hiện nghiêm túc./.

***Nơi nhận*:**
- Như trên;
- Bộ Công an (để b/c);
- Thường trực Tỉnh uỷ (để b/c);
- CT và các PCT UBND tỉnh;
- VPUB: CVP và các PCVP UBND tỉnh;
- Lưu: VT, TĐKT, VPTT.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thanh Bình

PHỤ LỤC
Một số phương thức, thủ đoạn của tội phạm sử dụng công nghệ cao, lừa đảo chiếm đoạt tài sản trên không gian mạng
(Gửi kèm theo Công văn số 8987/UBND ngày 25/8/2023 của UBND tỉnh)

1. Đăng tin mạo danh tuyển cộng tác viên làm việc online trên các trang mạng xã hội để chiếm đoạt số tiền tạm ứng hoặc thanh toán đơn hàng.

2. Giả danh cơ quan chức năng: Mạo danh Công an, Viện kiểm sát, Tòa án để gọi điện thoại, đọc đúng thông tin cá nhân của nạn nhân (hoặc yêu cầu nạn nhân cung cấp thông tin cá nhân) sau đó thông báo rằng nạn nhân đang bị điều tra liên quan đường dây rửa tiền, mua bán ma túy, tai nạn giao thông … yêu cầu nạn nhân kê khai tài sản, cung cấp thông tin tài khoản ngân hàng hoặc chuyển tiền vào tài khoản theo yêu cầu của các đối tượng để chứng minh trong sạch sau đó chiếm đoạt.

3. Kêu gọi đầu tư online siêu lợi nhuận: Các đối tượng tạo lập các website giả mạo các công ty tài chính, tập đoàn lớn có uy tín (tập đoàn dầu khí, công ty đa quốc gia …), quảng cáo, lôi kéo, kêu gọi số lượng lớn người tham gia đầu tư, cam kết có sự hướng dẫn của các chuyên gia lâu năm và được hưởng siêu lợi nhuận trên các sàn chứng khoán quốc tế, giao dịch vàng, giao dịch tiền điện tử, giao dịch tiền tệ, ngoại hối... Sau một vài lần tạo sự tin tưởng bằng cách thực hiện đúng cam kết với số tiền đầu tư nhỏ, các đối tượng sẽ thực hiện hành vi chiếm đoạt tài sản ở những lượt đầu tư lớn.

4. Giả danh người nước ngoài thành đạt: Mạo danh là Quân nhân, Bác sỹ, Doanh nhân thành đạt người nước ngoài kết bạn làm quen qua mạng xã hội (facebook, messenger, whatsapp…) và hứa hẹn sẽ gửi quà hoặc tiền có giá trị lớn. Sau đó, các đối tượng đồng bọn tự xưng là hải quan, cán bộ thuế, nhân viên sân bay, nhân viên vận chuyển hàng… gọi điện yêu cầu nộp các khoản phí để nhận quà và chiếm đoạt.

5. Chiếm quyền điều khiển tài khoản mạng xã hội: Tạo đường dẫn (link) giả mạo có giao diện giống với các chương trình đã phát trên truyền hình như Biệt tài tí hon, Bình chọn ảnh đẹp… Sau khi nạn nhân kích vào đường dẫn, cung cấp các thông tin bảo mật về tài khoản mạng xã hội (tên tài khoản, mật khẩu…) để đăng nhập và tham gia bình chọn thì tài khoản của nạn nhân sẽ bị đối tượng chiếm quyền điều khiển, mạo danh nạn nhân nhắn tin đề nghị người thân, bạn bè (có trong danh sách bạn bè) cho mượn tiền hoặc nhờ chuyển tiền để chiếm đoạt.

6. Chiếm quyền sử dụng sim số: Giả danh nhân viên chăm sóc khách hàng của các nhà mạng gọi điện để hỗ trợ giải quyết sự cố hoặc nâng cấp miễn

phí dịch vụ sim từ 3G lên 4G, hướng dẫn nạn nhân soạn tin nhắn theo cú pháp, từ đó sim điện thoại của nạn nhân sẽ bị khóa và chuyển quyền sử dụng sang sim (sim trắng) của đối tượng. Đối tượng sử dụng sim chiếm đoạt được để khôi phục thông tin bảo mật liên quan các tài khoản ngân hàng của nạn nhân và chiếm đoạt toàn bộ số tiền có trong tài khoản hoặc tiến hành đăng ký các khoản vay trên mạng internet của các công ty tài chính để chiếm đoạt.

7. Giả danh giáo viên chủ nhiệm, nhân viên bảo vệ nhà trường hoặc nhân viên bệnh viện: Giả danh giáo viên chủ nhiệm, nhân viên bảo vệ nhà trường hoặc nhân viên bệnh viện gọi điện cho phụ huynh báo tin về việc người thân của họ bị tai nạn, đang được nhập viện cấp cứu, yêu cầu phải chuyển tiền nhanh để đóng viện phí, sau đó chiếm đoạt.

8. Lừa đảo đặt tiệc để chiếm đoạt tài sản: Sử dụng mạng viễn thông, mạng xã hội gọi điện đặt tiệc tại các nhà hàng kèm theo các yêu cầu đặc biệt như chuẩn bị một số món ăn, đồ uống, quà tặng hiếm có trên thị trường. Sau đó giới thiệu "Đại lý" để nhà hàng liên hệ đặt mua và chiếm đoạt tiền đặt cọc từ nhà hàng.

9. Chiếm quyền điều khiển tài khoản ngân hàng: Sử dụng dịch vụ "SMS Brandname" mạo danh các ngân hàng gửi tin nhắn thông báo với các nội dung như *tài khoản được kích hoạt trên thiết bị lạ, tài khoản được thanh toán ở nước ngoài, xác thực tài khoản, hủy dịch vụ…,* đề nghị kích vào các đường dẫn (link) cho trước để thay đổi thông tin; hoặc yêu cầu đăng nhập tài khoản ngân hàng vào đường dẫn (link) do đối tượng cung cấp để thanh toán online nhằm mục đích chiếm quyền điều khiển tài khoản ngân hàng và chiếm đoạt tài sản.

10. Vay vốn online: Quảng cáo các khoản vay với lãi suất thấp, yêu cầu nộp các khoản phí, cọc đảm bảo để hoàn tất thủ tục vay và chiếm đoạt. Hoặc, cho vay với lãi suất "cắt cổ" và bị đe dọa, khủng bố tinh thần nếu không trả đúng hạn.

11. Giả danh nhân viên Công ty xổ số cho số đề để đánh lô, đề: Giả danh nhân viên Công ty xổ số, thể hiện bản thân biết trước kết quả xổ số, đề nghị nộp tiền mua số để đánh lô, đề và chiếm đoạt.

12. Giả danh nhân viên ngân hàng, nhà mạng; nhân viên các sàn thương mại điện tử như Lazada, Shopee, Tiki… thông báo nạn nhân là người may mắn trúng thưởng, đề nghị đóng một số khoản phí để hoàn tất thủ tục nhận thưởng và chiếm đoạt.