| | |
|---|---|
| CÔNG AN TỈNH PHÚ YÊN<br>**CÔNG AN THỊ XÃ ĐÔNG HÒA** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 242/CATX-TM<br>V/v tuyên truyền phương thức thủ đoạn của tội phạm sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản | *Đông Hòa, ngày 28 tháng 02 năm 2024* |

Kính gửi:

- Các cơ quan, ban, ngành, đoàn thể thị xã;
- Ủy ban nhân dân các xã, phường.

Thời gian qua, trên địa bàn tỉnh Phú Yên nói chung, thị xã Đông Hòa nói riêng, hoạt động của tội phạm lừa đảo chiếm đoạt tài sản trên mạng viễn thông, mạng internet diễn biến rất phức tạp, với nhiều thủ đoạn mới, tinh vi, gây nhiều thiệt hại cho người dân, bức xúc trong dư luận xã hội. Thủ đoạn phạm tội phổ biến là: Kết bạn làm quen qua mạng xã hội (*facebook, zalo...*), hứa hẹn tình cảm yêu đương, tặng quà rồi lừa đảo; chiếm quyền quản trị (*hack*) hoặc giả lập các tài khoản mạng xã hội của người dân rồi nhắn tin, lừa gạt người thân quen của chủ tài khoản chuyển tiền và chiếm đoạt; tạo lập các website sàn giao dịch tài chính, thương mại điện tử, chứng khoán quốc tế để lôi kéo người dân tham gia đầu tư, sau đó can thiệp vào hệ thống để chiếm đoạt số tiền của người tham gia; đăng thông tin giả mạo về các hoàn cảnh khó khăn để vận động quyên góp rồi chiếm đoạt số tiền huy động được... Theo thống kê, thời gian trước, trong và sau Tết Nguyên Đán Giáp Thìn năm 2024, trên địa bàn thị xã Đông Hòa xảy ra 03 vụ lừa đảo chiếm đoạt tài sản trên không gian mạng, thiệt hại tổng số tiền hơn 500 triệu đồng.

Qua theo dõi, nắm tình hình, có 03 nhóm lừa đảo chính (*giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác*) với 24 hình thức lừa đảo đang diễn ra trên không gian mạng, hướng vào các nhóm đối tượng: Người cao tuổi, trẻ em, sinh viên/thanh niên, công nhân/người lao động, nhân viên văn phòng, gồm:

(*1*) Combo du lịch giá rẻ: Lừa đảo chiếm đoạt tiền bạc, thông tin cá nhân qua các hình thức bẫy mua dịch vụ du lịch trọn gói.

(*2*) Cuộc gọi video deepfake, deepvoice: Các đối tượng sử dụng công nghệ trí tuệ nhân tạo (*AI*) để tạo ra những video hoặc hình ảnh giả, sao chép chân dung nhằm tạo ra các đoạn video giả người thân, bạn bè để thực hiện các cuộc gọi lừa đảo trực tuyến.

(*3*) Giả mạo biên lai chuyển tiền thành công: Các đối tượng lừa nạn nhân mua hàng số lượng lớn trên mạng xã hội; làm giả biên lai chuyển tiền thành công bằng phần mềm.

(*4*) Giả nhân viên y tế báo người thân đang cấp cứu: Gọi điện thoại thông báo người thân đang nằm cấp cứu trong bệnh viện, yêu cầu chuyển tiền mổ gấp.

(*5*) Tuyển người mẫu nhí: Lợi dụng mạng xã hội tiếp cận, dụ dỗ các bậc phụ huynh có con nhỏ đăng ký ứng tuyển người mẫu nhí. Yêu cầu nạn nhân đóng nhiều loại phí hoặc hướng dẫn làm nhiệm vụ qua mạng.

(*6*) Thông báo "*khóa sim*" vì chưa chuẩn hóa thuê bao: Các đối tượng gọi điện thông báo khóa dịch vụ viễn thông. Nạn nhân làm theo hướng dẫn sẽ mất thông tin cá nhân, thông tin tài khoản ngân hàng...

(*7*) Giả danh công ty tài chính: Cung cấp khoản tiền vay với lãi suất thấp, thủ tục đơn giản; yêu cầu nạn nhân đóng phí làm thủ tục rồi chiếm đoạt.

(*8*) Cài ứng dụng, đường dẫn (*link*) quảng cáo cờ bạc, cá độ, tín dụng đen: Các đối tượng gài bẫy quảng cáo, ứng dụng cho vay; nạn nhân sau khi cài đặt ứng dụng và cấp quyền cho ứng dụng truy cập điện thoại sẽ bị kẻ gian chiếm đoạt thông tin cá nhân.

(*9*) Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp: Tạo trang web giả mạo có giao diện giống với trang web của các cơ quan, doanh nghiệp. Người dùng khai báo thông tin trên trang web giả sẽ bị đánh cắp thông tin cá nhân.

(*10*) Giả mạo SMS brandname, phát tán tin nhắn giả mạo: Các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới người dùng. Nạn nhân làm theo hướng dẫn từ tin nhắn sẽ bị đánh cắp thông tin cá nhân.

(*11*) Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp: Gửi link thanh toán trực tuyến tham gia sàn giao dịch ảo, yêu cầu nạn nhân gửi tiền đặt cọc rồi chiếm đoạt.

(*12*) Lừa đảo tuyển cộng tác viên online: Tuyển cộng tác viên "*việc nhẹ lương cao*" - giả mạo các trang sàn thương mại điện tử (*Tiki, Shopee, Lazada và các thương hiệu lớn*) để chiếm đoạt tài sản của nạn nhân.

(*13*) Đánh cắp tài khoản mạng xã hội, nhắn tin lừa đảo: Chiếm quyền đăng nhập vào tài khoản facebook, zalo nhắn tin cho bạn bè, người thân hỏi vay tiền.

(*14*) Giả danh cơ quan Công an, Kiểm sát, Tòa án: Các đối tượng giả danh cơ quan Công an, Kiểm sát, Tòa án để gọi điện hăm dọa và sử dụng các chiêu trò lừa đảo nhằm chiếm đoạt tài sản của nạn nhân.

(*15*) Rao bán hàng giả, hàng nhái trên sàn thương mại điện tử: Đăng tải quảng cáo mời chào người tiêu dùng mua hàng giả, hàng kém chất lượng không rõ nguồn gốc trên các sàn thương mại điện tử.

(*16*) Đánh cắp thông tin CCCD đi vay nợ tín dụng: Các đối tượng bẫy người dùng internet khai báo thông tin CCCD trên các mẫu khảo sát. Từ đó sử dụng thông tin cá nhân đã đánh cắp để vay nợ tín dụng.

(*17*) Chuyển nhầm tiền vào tài khoản ngân hàng: Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng và giả danh người thu hồi nợ để yêu cầu trả lại số tiền.

(*18*) Dịch vụ lấy lại tiền khi đã bị lừa: Giả danh nhân vật có uy tín, sức ảnh hưởng liên hệ cung cấp dịch vụ lấy lại tiền đã mất cho nạn nhân rồi yêu cầu nạn nhân thanh toán trước hoặc cung cấp thông tin cá nhân.

(*19*) Đánh cắp Telegram OTP: Lập tài khoản telegram giả danh các cơ quan, tổ chức; gửi tin nhắn yêu cầu xác thực tài khoản cho nạn nhân nhằm chiếm đoạt mã OTP để truy cập tài khoản của họ.

(*20*) Tung tin giả về cuộc gọi mất tiền FlashAI: Gọi điện thông bảo tin giả, hướng dẫn phòng tránh cuộc gọi mất tiền FlashAI. Nạn nhân làm theo hướng dẫn sẽ bị chiếm đoạt thông tin cá nhân.

(*21*) Dịch vụ lấy lại tài khoản facebook: Tạo trang web quảng cáo dịch vụ lấy lại tài khoản facebook. Yêu cầu người dùng cung cấp tiền cọc, thông tin cá nhân sau đó chiếm đoạt.

(*22*) Rải link Phishing, Seeding, quảng cáo bẩn trên mạng xã hội: Tạo trang web giả mạo ngân hàng hoặc dịch vụ trực tuyến với mục đích thu thập thông tin cá nhân của các người dùng internet.

(*23*) Dự báo số lô, số đề: Các đối tượng chiêu dụ người dùng chơi đề và yêu cầu nạn nhân chi trả tiền theo tuần, tháng, hoa hồng.

(*24*) Bẫy tình cảm, đầu tư tài chính, gửi bưu kiện, trúng thưởng: Các đối tượng thông qua các trang mạng xã hội và ứng dụng hẹn hò tiếp cận người dùng; lợi dụng tình cảm nạn nhân lừa chuyển tiền, kêu gọi đầu tư tài chính.

Để chủ động phòng ngừa, đấu tranh với tội phạm sử dụng công nghệ cao lừa đảo chiếm đoạt tài sản, Công an thị xã Đông Hòa đề nghị các đồng chí phối hợp tuyên truyền đến toàn thể cán bộ, công nhân viên và quần chúng Nhân dân trong cơ quan, địa bàn biết, nắm vững. Mọi trường hợp phát hiện hành vi vi phạm, kịp thời tố giác đến Công an xã, phường nơi gần nhất hoặc qua Trực ban hình sự Công an thị xã (*điện thoại số: 02573.532.010*) để được hướng dẫn, giải quyết.

Vì xã hội bình yên và hạnh phúc của toàn dân, Công an thị xã Đông Hòa đề nghị các đồng chí quan tâm phối hợp, chỉ đạo thực hiện./.

***Nơi nhận:***
- TT. Thị ủy;
- Chủ tịch UBND thị xã;
- Như kính gửi;
- Lưu TM.

**TRƯỞNG CÔNG AN THỊ XÃ**

**Thượng tá Trần Khắc Quang**