

**ỦY BAN NHÂN DÂN
PHƯỜNG ĐỒ SƠN**

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

Số: /UBND-CA

Đồ Sơn, ngày tháng 8 năm 2026

V/v tuyên truyền, cảnh báo phương thức,
thủ đoạn lừa đảo giả mạo cơ quan nhà
nước hướng dẫn kê khai, nộp thuế đất
nhằm chiếm đoạt tài sản và lừa đảo chiếm
đoạt tài sản trên không gian mạng

Kính gửi:

- Công an phường;
- Các Cơ quan chuyên môn;
- Trung tâm dịch vụ sự nghiệp công.

Thực hiện Công văn số 301/PC02-Đ3A ngày 03/8/2026 của Phòng Cảnh sát hình sự, Công an TP Hải Phòng về tuyên truyền, cảnh báo phương thức, thủ đoạn lừa đảo giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản; Công văn số 300/PC02-Đ3A ngày 03/8/2026; Công văn số 317/PC02-Đ3A ngày 06/8/2026 của Phòng PC02 - Công an TP Hải Phòng về tuyên truyền, cảnh báo phương thức, thủ đoạn lừa đảo chiếm đoạt tài sản trên không gian mạng.

Thời gian gần đây, trên địa bàn cả nước nói chung, địa bàn thành phố Hải Phòng nói riêng tình hình giả mạo cán bộ cơ quan nhà nước và tình hình lừa đảo chiếm đoạt tài sản liên tiếp xảy ra, với nhiều phương thức, thủ đoạn lừa đảo mới và tinh vi, như:

1. Giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản

Tình hình tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng tiếp tục diễn biến phức tạp với nhiều phương thức, thủ đoạn mới, tinh vi, có sự chuẩn bị kỹ lưỡng về kịch bản, tài liệu và công nghệ nhằm tạo lòng tin đối với người dân. Đáng chú ý, các đối tượng lợi dụng việc triển khai các thủ tục hành chính về đất đai, đăng ký biến động đất đai, cấp Giấy chứng nhận quyền sử dụng đất, kê khai hồ sơ địa chính và thực hiện nghĩa vụ tài chính về đất đai để giả mạo cơ quan nhà nước, lừa người dân cài đặt phần mềm độc hại, từ đó chiếm quyền điều khiển điện thoại và chiếm đoạt tiền trong tài khoản ngân hàng; giả mạo thông tin tuyển dụng của các ngân hàng, doanh nghiệp để lừa đảo chiếm đoạt tài sản; giả danh người nước ngoài thực hiện giao dịch chuyển khoản để đổi tiền hoặc mua hàng; giả mạo hoặc chiếm quyền sử dụng tài khoản mạng xã hội của người thân để nhờ chuyển tiền; dụ dỗ đầu tư trên các nền tảng trực tuyến để chiếm đoạt tài sản...

Qua công tác nắm tình hình, lực lượng Công an phát hiện các đối tượng sử dụng mạng xã hội, ứng dụng nhắn tin hoặc gọi điện trực tiếp cho người dân, đồng thời gửi hình ảnh “Giấy mời” giả mạo của cơ quan quản lý nhà nước về đất đai, có đầy đủ quốc hiệu, tiêu ngữ, số văn bản, con dấu, chữ ký và nội dung giống văn bản thật nhằm tạo lòng tin. Theo đó, các đối tượng thông báo người dân thuộc diện phải kê khai, bổ sung hồ sơ đất đai, cập nhật dữ liệu địa chính, cấp mã định

danh gắn với tài sản hoặc thực hiện nghĩa vụ tài chính về đất đai theo chủ trương của cơ quan nhà nước, yêu cầu người dân mang theo điện thoại thông minh và liên hệ trước với “cán bộ hỗ trợ” để được hướng dẫn hoàn thiện hồ sơ điện tử.

Sau khi người dân liên hệ, đối tượng tự xưng là cán bộ Sở Nông nghiệp và Môi trường, Chi nhánh Văn phòng đăng ký đất đai, cơ quan Thuế hoặc cán bộ UBND địa phương, thông báo cần hỗ trợ kê khai trực tuyến, nộp thuế sử dụng đất hoặc xác thực hồ sơ điện tử trước khi đến làm việc.

Để thực hiện thủ tục, các đối tượng yêu cầu người dân truy cập đường dẫn do chúng cung cấp hoặc cài đặt một ứng dụng với lý do “hỗ trợ kê khai đất đai”, “phần mềm khai thuế điện tử”, “ứng dụng xác thực hồ sơ”, “phần mềm cập nhật dữ liệu đất đai”... thực chất đây là phần mềm chứa mã độc, khi được cài đặt, đối tượng sẽ chiếm quyền điều khiển điện thoại, đánh cắp thông tin cá nhân, tài khoản ngân hàng, mật khẩu đăng nhập, mã OTP và thực hiện chuyển tiền, chiếm đoạt tài sản của người dân.

2. Giả danh doanh nghiệp logistics, doanh nghiệp vận tải, xuất nhập khẩu, sàn thương mại điện tử hoặc công ty cung ứng dịch vụ để dụ dỗ người dân tham gia thực hiện các “đơn hàng logistics”, “nhiệm vụ trực tuyến”, “ghép đơn”, “đầu tư sinh lời”... nhằm chiếm đoạt tài sản. Nhiều người dân do tin tưởng đã bị các đối tượng chiếm đoạt số tiền rất lớn

Đây là phương thức lừa đảo mới, có nguy cơ tiếp tục phát sinh trên địa bàn nếu người dân không được cảnh báo, tuyên truyền kịp thời. Phương thức, thủ đoạn của các đối tượng như sau: Các đối tượng thường sử dụng tài khoản Zalo, Viber, Telegram, Facebook... chủ động liên hệ với người dân, tự xưng là nhân viên hoặc đối tác của các công ty logistics, vận tải hoặc doanh nghiệp lớn có uy tín.

Để tạo lòng tin, chúng cung cấp hình ảnh căn cước công dân, giấy phép kinh doanh, tài khoản ngân hàng, thậm chí sử dụng tên, logo và website có giao diện giống doanh nghiệp thật.

Sau khi tạo được sự tin tưởng, các đối tượng hướng dẫn người dân truy cập vào website hoặc ứng dụng do chúng tạo ra, yêu cầu đăng ký tài khoản và tham gia thực hiện các “đơn hàng logistics”, “đơn hàng vận chuyển”, “ghép đơn” hoặc “đầu tư nhận hoa hồng”. Ban đầu, người tham gia chỉ phải nạp số tiền nhỏ và được rút tiền thành công để tạo niềm tin rằng hệ thống hoạt động bình thường.

Khi người dân tiếp tục tham gia với số tiền lớn hơn, hệ thống liên tục phát sinh các lý do như ghép đơn giá trị cao, đơn hàng may mắn, nâng cấp tài khoản, phí giải ngân, phí kiểm soát rủi ro, phí xác minh giao dịch, phí tổng kết hoặc yêu cầu nộp thêm tỷ lệ phần trăm trên số tiền muốn rút. Mỗi lần hoàn thành một yêu cầu, các đối tượng lại tiếp tục đưa ra điều kiện mới nhằm buộc nạn nhân chuyển thêm tiền.

Đến khi nạn nhân không còn khả năng chuyển tiền hoặc yêu cầu rút tiền, các đối tượng sẽ khóa tài khoản, cắt liên lạc hoặc đe dọa rằng nếu không tiếp tục nộp tiền thì toàn bộ số tiền đã chuyển sẽ bị tịch thu, sung công quỹ hoặc xử lý theo quy định của pháp luật. Đây đều là những thông tin bịa đặt nhằm gây áp lực tâm lý nạn nhân để tiếp tục chiếm đoạt tài sản.

3. Thủ đoạn giả mạo thông tin tuyển dụng của các Ngân hàng, doanh nghiệp để lừa đảo chiếm đoạt tài sản

Các đối tượng đăng tải thông tin tuyển dụng giả mạo của các ngân hàng, doanh nghiệp lớn trên Facebook, Zalo, Telegram hoặc các hội, nhóm tìm việc. Sau khi người dân nộp hồ sơ, các đối tượng thông báo đã trúng tuyển, mời tham gia phỏng vấn hoặc đào tạo trực tuyến để tạo lòng tin. Tiếp đó, chúng yêu cầu người tham gia chuyển tiền với lý do ký quỹ, xác minh tài khoản, đào tạo, thực hiện nhiệm vụ hoặc đầu tư dự án và hứa hẹn sẽ hoàn trả cả gốc lẫn lợi nhuận. Ban đầu, các đối tượng có thể hoàn trả một khoản tiền nhỏ để tạo niềm tin, sau đó tiếp tục yêu cầu chuyển số tiền lớn hơn với nhiều lý do khác nhau rồi chiếm đoạt toàn bộ số tiền của bị hại.

4. Thủ đoạn giả danh người nước ngoài thực hiện giao dịch chuyển khoản để đổi tiền hoặc mua hàng

Các đối tượng, chủ yếu là người nước ngoài hoặc giả danh người nước ngoài, đến các cửa hàng tiện lợi, cửa hàng tạp hóa, đại lý đổi tiền hoặc cơ sở kinh doanh để mua hàng hoặc đổi ngoại tệ.

Sau khi thao tác trên điện thoại, đối tượng cho chủ cửa hàng xem hình ảnh hoặc thông báo chuyển khoản thành công đã được chỉnh sửa hoặc làm giả. Tin tưởng giao dịch đã hoàn tất, người bán giao tiền mặt hoặc hàng hóa cho đối tượng. Tuy nhiên, thực tế tài khoản ngân hàng không nhận được tiền và đối tượng nhanh chóng rời khỏi hiện trường để chiếm đoạt tài sản.

5. Thủ đoạn giả mạo hoặc chiếm quyền sử dụng tài khoản mạng xã hội của người thân để nhờ chuyển tiền

Các đối tượng chiếm quyền sử dụng hoặc tạo tài khoản Facebook, Zalo có tên, hình ảnh giống người thân, bạn bè của bị hại, đặc biệt là người đang học tập, lao động ở nước ngoài. Sau đó, chúng nhắn tin thông báo cần chuyển tiền về Việt Nam, nhờ nhận hộ hoặc yêu cầu chuyển tiền để đóng các khoản phí, thuế, lệ phí nhận quà, nhận tiền từ nước ngoài. Do tin tưởng là người thân nhắn tin nên nhiều người đã chuyển tiền vào tài khoản do đối tượng cung cấp và bị chiếm đoạt.

6. Thủ đoạn dụ dỗ đầu tư trên các nền tảng trực tuyến để chiếm đoạt tài sản

Các đối tượng làm quen với người dân qua Facebook, Zalo, WhatsApp, Telegram hoặc các ứng dụng hẹn hò, sau đó giới thiệu cơ hội đầu tư vào chứng khoán quốc tế, tiền điện tử (USDT), ngoại hối (Forex), vàng hoặc các nền tảng đầu tư trực tuyến với cam kết lợi nhuận cao, rủi ro thấp.

Ban đầu, chúng hướng dẫn đầu tư số tiền nhỏ và cho rút cả gốc lẫn lãi để tạo niềm tin. Khi người bị hại đầu tư số tiền lớn, hệ thống vẫn hiển thị lợi nhuận nhưng không cho rút tiền và liên tục yêu cầu nộp thêm các khoản phí như xác minh tài khoản, thuế, phí chống rửa tiền (KYC/AML), phí mở khóa tài khoản, xác minh nguồn tiền hoặc ký quỹ.

Sau khi nạn nhân chuyển tiền, các đối tượng tiếp tục viện nhiều lý do để yêu cầu nộp thêm hoặc cắt liên lạc, chiếm đoạt toàn bộ số tiền đã đầu tư.

Để chủ động phòng ngừa với các loại tội phạm này, Ủy ban nhân dân phường đề nghị các phòng, ban thực hiện tốt một số nội dung sau:

1. Công an phường

- Chủ trì, phối hợp với các đơn vị có liên quan làm tốt công tác tham mưu với Đảng ủy, UBND phường, tiếp tục thực hiện chỉ đạo của Đảng ủy, Giám đốc Công an thành phố, Đảng ủy, UNND phường về phòng ngừa, đấu tranh với các loại tội phạm vi phạm pháp luật.

- Tăng cường công tác tuyên truyền bằng nhiều hình thức phù hợp như tuyên truyền trên các trang thông tin điện tử, Fanpage, Zalo, các nhóm cộng đồng và trong các buổi Hội nghị, hội họp, giao ban, sinh hoạt tổ dân phố để người dân biết, nhận diện và chủ động phòng tránh các thủ đoạn nêu trên. Đồng thời, chủ động nắm tình hình, nhận diện các phương thức, thủ đoạn mới, khi phát hiện các vụ việc có dấu hiệu lừa đảo hoặc người dân đến trình báo, khẩn trương tiếp nhận, hướng dẫn thu thập tài liệu ban đầu và xác minh, báo xử lý cáo Phòng Cảnh sát hình sự, Công an TP Hải Phòng để phối hợp xác minh, xử lý theo quy định.

2. Các Cơ quan chuyên môn

Phối hợp với các đơn vị có liên quan làm tốt công tác tham mưu với UBND phường ban hành các văn bản, kế hoạch chỉ đạo công tác phòng ngừa đối tượng giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản; phòng ngừa lừa đảo chiếm đoạt tài sản trên không gian mạng. Đẩy mạnh công tác tuyên truyền đến gia đình, người thân về các thủ đoạn hoạt động của các loại tội phạm giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản; phòng ngừa lừa đảo chiếm đoạt tài sản trên không gian mạng.

4. Trung tâm dịch vụ sự nghiệp công

Phối hợp với các đơn vị liên quan xây dựng tin bài tuyên truyền sâu rộng trên hệ thống truyền thanh, trong các nhóm Zalo, trên mạng Facebook... đẩy mạnh tuyên truyền chung và tuyên truyền đến từng hộ dân tại các tổ dân phố về phòng ngừa các đối tượng giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản; phòng ngừa lừa đảo chiếm đoạt tài sản trên không gian mạng; giả mạo thông tin tuyển dụng của các ngân hàng, doanh nghiệp để lừa đảo chiếm đoạt tài sản; giả danh người nước ngoài thực hiện giao dịch chuyển khoản để đòi tiền hoặc mua hàng; giả mạo hoặc chiếm quyền sử dụng tài khoản mạng xã hội của người thân để nhờ chuyển tiền; dụ dỗ đầu tư trên các nền tảng trực tuyến để chiếm đoạt tài sản... ***(có nội dung tuyên truyền kèm theo)***.

Yêu cầu Công an phường và các đơn vị liên quan nghiêm túc tổ chức triển khai thực hiện, quá trình thực hiện có khó khăn, vướng mắc báo cáo Chủ tịch UBND phường qua Công an phường để được hướng dẫn, giải quyết./.

Nơi nhận:

- Như kính gửi;
- Lưu: VT, CA.

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

Phạm Hoàng Tuấn

NỘI DUNG TUYÊN TRUYỀN

1. Tuyên truyền, cảnh báo phương thức, thủ đoạn lừa đảo giả mạo cơ quan nhà nước hướng dẫn kê khai, nộp thuế đất nhằm chiếm đoạt tài sản

- Không tin vào các lời mời làm việc trực tuyến, thực hiện đơn hàng logistics, ghép đơn hoặc đầu tư sinh lời với cam kết lợi nhuận cao, rủi ro thấp.
- Không chuyển tiền theo yêu cầu của người quen qua mạng xã hội hoặc những người tự xưng là nhân viên doanh nghiệp khi chưa xác minh chính xác danh tính.
- Không truy cập, đăng ký tài khoản hoặc cung cấp thông tin cá nhân, thông tin ngân hàng trên các website, ứng dụng không rõ nguồn gốc.
- Không tin tưởng tuyệt đối vào hình ảnh căn cước công dân, giấy phép kinh doanh, tài khoản ngân hàng hoặc các giấy tờ do đối tượng gửi qua mạng.
- Tuyệt đối không chuyển thêm tiền với các lý do như mở khóa tài khoản, hoàn thành đơn hàng, nộp phí giải ngân, phí xác minh, phí kiểm soát rủi ro, phí thuế hoặc các khoản phí khác để được rút tiền, vì đây là thủ đoạn phổ biến của các đối tượng lừa đảo.
- Khi phát hiện dấu hiệu nghi vấn hoặc đã bị lừa đảo, cần lưu giữ toàn bộ tin nhắn, số điện thoại, tài khoản ngân hàng, địa chỉ website, hóa đơn chuyển tiền và nhanh chóng trình báo cơ quan Công an nơi gần nhất để được hướng dẫn, xử lý kịp thời.

2. Tuyên truyền phòng ngừa lừa đảo chiếm đoạt tài sản trên không gian mạng

- Tuyệt đối không tin vào các cuộc gọi, tin nhắn hoặc hình ảnh giấy mời được gửi qua Zalo, Facebook, Messenger, SMS... nếu chưa được kiểm chứng.
- Không cài đặt bất kỳ ứng dụng nào theo hướng dẫn của người lạ hoặc từ các đường dẫn không phải kho ứng dụng chính thức (App Store, CH Play).
- Không cấp quyền điều khiển điện thoại hoặc các quyền truy cập đặc biệt cho các ứng dụng không rõ nguồn gốc.
- Không cung cấp số tài khoản ngân hàng, tên đăng nhập, mật khẩu Internet Banking, mã OTP hoặc thông tin cá nhân cho bất kỳ người nào qua điện thoại hoặc mạng xã hội.
- Việc kê khai đất đai, thực hiện nghĩa vụ tài chính về đất đai, nộp thuế và các thủ tục hành chính chỉ thực hiện thông qua các cổng thông tin điện tử chính thức của cơ quan nhà nước hoặc trực tiếp tại cơ quan có thẩm quyền, không làm theo hướng dẫn của các cuộc gọi, tin nhắn từ người lạ.

3. Giả mạo tuyển dụng; giả danh người nước ngoài; giả mạo hoặc chiếm quyền sử dụng tài khoản mạng xã hội của người thân để nhờ chuyển tiền; dụ dỗ đầu tư

- Khi nhận được giấy mời hoặc thông báo có dấu hiệu nghi vấn, người dân cần chủ động liên hệ trực tiếp UBND cấp xã, Chi nhánh Văn phòng đăng ký đất

đại, cơ quan Thuế hoặc cơ quan Công an nơi gần nhất để kiểm tra, xác minh trước khi thực hiện.

giả mạo thông tin tuyển dụng của các ngân hàng, doanh nghiệp để lừa đảo chiếm đoạt tài sản; giả danh người nước ngoài thực hiện giao dịch chuyển khoản để đòi tiền hoặc mua hàng; giả mạo hoặc chiếm quyền sử dụng tài khoản mạng xã hội của người thân để nhờ chuyển tiền; dụ dỗ đầu tư trên các nền tảng trực tuyến để chiếm đoạt tài sản...

- Cảnh giác với các thông tin tuyển dụng, lời mời đầu tư hoặc các giao dịch tài chính được quảng cáo trên mạng xã hội.

- Tuyệt đối không chuyển tiền để ký quỹ, xác minh tài khoản, thực hiện nhiệm vụ, đầu tư hoặc nộp các khoản phí theo yêu cầu của người lạ trên mạng.

- Khi nhận được tín nhắn vay tiền, nhờ chuyển tiền hoặc nhận tiền từ nước ngoài qua tài khoản Facebook, Zalo, Messenger..., cần liên hệ trực tiếp với người thân bằng điện thoại hoặc gặp trực tiếp để xác minh trước khi chuyển tiền.

- Đối với các trường hợp mua bán, đòi tiền hoặc giao dịch với người lạ, đặc biệt là người nước ngoài, chỉ giao tiền hoặc hàng hóa sau khi kiểm tra và xác nhận tiền đã thực sự được ghi có vào tài khoản ngân hàng, không tin vào hình ảnh chụp màn hình hoặc thông báo chuyển khoản trên điện thoại của đối tượng.

- Chỉ đầu tư thông qua các tổ chức, doanh nghiệp, công ty chứng khoán, sàn giao dịch được cơ quan có thẩm quyền cấp phép, không tham gia các nền tảng đầu tư không rõ nguồn gốc hoặc được giới thiệu qua mạng xã hội.

- Không cung cấp thông tin cá nhân, số tài khoản ngân hàng, mật khẩu, mã OTP hoặc các thông tin bảo mật khác cho bất kỳ cá nhân nào.

- Khi phát hiện dấu hiệu nghi vấn hoặc đã trở thành nạn nhân của các vụ lừa đảo, cần nhanh chóng liên hệ ngân hàng để đề nghị hỗ trợ phong tỏa giao dịch (nếu còn kịp thời), đồng thời trình báo ngay cơ quan Công an nơi gần nhất để được hướng dẫn, xử lý.