ỦY BAN NHÂN DÂN **HUYỆN BÌNH SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 06 /TB-UBND	*Bình Sơn, ngày 10 tháng 01 năm 2025*

THÔNG BÁO
Phương thức, thủ đoạn hoạt động của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng

Thời gian qua trên địa bàn huyện Bình Sơn nói riêng và tỉnh Quảng Ngãi nói chung liên tục xảy ra nhiều trường hợp bị lừa đảo chiếm đoạt tài sản qua không gian mạng, gây thiệt hại lớn cho nhân dân. Các đối tượng lừa đảo sử dụng các phương thức, thủ đoạn hết sức tinh vi đưa ra các thông tin gian dối nhằm khống chế tâm lý của nạn nhân, hoặc để bị hại tin tưởng, rồi thực hiện hành vi lừa đảo. Để kịp thời phòng ngừa, hạn chế đến mức tối đa không để xảy ra các vụ lừa đảo chiếm đoạt tài sản qua không gian mạng, UBND huyện Bình Sơn thông báo một số phương thức, thủ đoạn lừa đảo trên không gian mạng đang phổ biến trên địa bàn huyện như sau:

1. Một số phương thức, thủ đoạn lừa đảo trên không gian mạng đang phổ biến trên địa bàn huyện

1.1. Thủ đoạn giả danh Công an, Viện kiểm sát, Tòa án

Các đối tượng liên hệ đến tự xưng là cán bộ Công an, Viện kiểm sát, Tòa án,… thông báo bị hại có liên quan đến một tổ chức, đường dây rửa tiền, mua bán người hoặc có vi phạm khi tham gia giao thông đường bộ, gây tai nạn giao thông bỏ chạy,… hiện đang được Cơ quan điều tra khởi tố, bắt tạm giam (đối tượng gửi file hình ảnh Lệnh tạm giam qua điện thoại của bị hại).

Đối tượng yêu cầu truy cập đường link do đối tượng cung cấp hoặc điền thông tin cá nhân vào một website giả mạo hoặc cung cấp mã OTP để chuyển tiền vào tài khoản của chúng với vỏ bọc xác minh, điều tra, xử lý "phạt nguội" ... Và đặc biệt khi gọi lại số điện thoại kia thì đều không liên lạc được.

Phổ biến: Thủ đoạn giả danh lực lượng Công an yêu cầu làm định danh điện tử, làm dịch vụ công, yêu cầu bổ sung, cập nhật giấy tờ tuỳ thân như CCCD, Bảo hiểm, Giấy phép lái xe…

Các đối tượng liên lạc với người bị hại qua mạng xã hội hoặc qua số điện thoại, sau đó tự giới thiệu là Cơ quan Công an yêu cầu người bị hại đăng ký làm định danh mức 2 online, không cần đến trụ sở cơ quan Công an. Các đối tượng yêu cầu bị hại tải app "Congdichvucongquocgia" hoặc chỉa sẻ đường link để đăng nhập. Khi người bị hại tải app hoặc kích vào đường link, các đối tượng sẽ yêu cầu cung cấp các loại giấy tờ cá nhân (CCCD, tài khoản ngân hàng...). Khi bị hại nhập thông tin cá nhân vào, ngay lập tức các đối tượng sẽ chiếm quyền sử dụng điện thoại cá nhân của bị hại và thực hiện thao tác chuyển tiền từ tài khoản của bị hại về tài khoản của đối tượng để chiếm đoạt.

1.2. Thủ đoạn vay tiền online

Đối tượng sử dụng tài khoản mạng xã hội (Zalo, Facebook …) mời chào, quảng cáo vay vốn với nhiều ưu đãi như thủ tục đơn giản, không cần tài sản đảm

bảo, giải ngân trong ngày, hạn mức cho vay lớn, lãi suất thấp, nhanh được giải ngân,…

Sau đó đối tượng yêu cầu cài đặt ứng dụng vay vốn online hoặc gửi đường link vào Website cho vay để làm thủ tục đăng ký vay tiền. Tiếp đó, sau khi nhập các thông tin cá nhân, khách hàng sẽ nhận được thông báo phê duyệt khoản vay. Lúc này bọn chúng sẽ tạo ra một số kịch bản như: Yêu cầu khách hàng chuyển trước một khoản tiền để kích hoạt tài khoản, lệ phí làm hồ sơ vay vốn hoặc bảo hiểm của khoản vay. Thông báo khách hàng nhập sai số tài khoản, cú pháp vay tiền và yêu cầu nộp thêm tiền để "sửa lỗi". Trường hợp khách hàng không đồng ý nộp tiền xử lý khoản vay sẽ bị đe dọa là thủ tục khoản vay đã được duyệt nên dù chưa nhận tiền vẫn bị nhắc nợ trên hệ thống dẫn đến khách hàng lo lắng chuyển tiền để được xử lý.

1.3. Thủ đoạn hack facebook hoặc tạo ra tài khoản facebook giống như facebook của người thân, người thân quen để lừa đảo mượn tiền

Đối tượng hack Facebook và chiếm quyền tài khoản chính chủ, đồng thời nhanh chóng tìm kiếm lịch sử tin nhắn của chủ tài khoản để nghiên cứu các mối quan hệ, cách xưng hô, trò chuyện … Hoặc tạo ra tài khoản facebook giống *facebook giống như facebook của người thân, bạn bè để lừa đảo mượn tiền*. Sau đó đối tượng mạo danh chủ tài khoản, dùng lý do có việc gấp, cần tiền ngay, sẽ trả trong thời gian ngắn, để nhắn tin vay, mượn tiền thông qua hình thức chuyển tiền qua tài khoản ngân hàng. Nhiều nạn nhân do thiếu cảnh giác, tưởng đó là người quen nên không kiểm tra mà chuyển tiền ngay vào tài khoản ngân hàng do đối tượng cung cấp. Thậm chí có đối tượng dùng tài khoản có tên tài khoản giống với tên của người thân, bạn bè để yêu cầu bị hại chuyển tiền.

Một số trường hợp các đối tượng sử dụng trí tuệ nhân tạo AI ghép mặt của người thân trong gia đình bị hại để gọi video cho bị hại trong thời gian ngắn tạo lòng tin. Sau đó sẽ lấy lý lo mạng yếu, mắc công việc không nghe gọi điện thoại được để nhắn tin mượn tiền hoặc thúc giục chuyển tiền để xử lý công việc nhằm chiếm đoạt tiền của bị hại.

1.4. Tham gia tổ chức chứng khoán hoặc nhóm trái phiếu điện tử kiếm tiền tại nhà

Thông qua lời quảng cáo của các đối tượng, mạo danh chuyên gia chứng khoán hoặc chuyên gia tư vấn chơi trái phiếu điện tử, hoặc mạo danh và tự nhận là nhân viên của các công ty chứng khoán có tên tuổi như Vndiriect, SSI… Lúc đầu những người bị lừa tham gia click vào đường link tham gia những gói nhỏ lẻ, thì thấy có lãi nên ham và tiếp tục nạp tiền những gói với số tiền lớn dần, tiền lãi ảo trong hệ thống tăng lên nhanh chóng. Nhưng đến khi dừng đầu tư và muốn rút thì các đối tượng sẽ yêu cầu vì số tiền lãi quá cao nên phải đóng phí. Với tâm lý ham số tiền thắng lớn trong chứng khoán hoặc trái phiếu điện tử, mà người bị lừa đã lao vào đóng các khoản phí vô lý và thực tế số tiền ảo kia cũng chẳng có thật.

1.5. Thủ đoạn giả danh cục thuế để thu thuế, yêu cầu cập nhật để khai báo thuế cơ sở, hộ kinh doanh

Các đối tượng liên lạc với bị hại tự giới thiệu là cán bộ của Cục thuế hoặc Chi cục thuế. Các đối tượng đưa thông tin là bị hại đang nợ thuế và yêu cầu phải nộp thuế

cá nhân hoặc thuế doanh nghiệp nếu không sẽ bị phạt hoặc bị xử lý hình sự. Người bị hại tâm lý lo sợ sẽ làm theo yêu cầu các đối tượng và chuyển tiền vào tài khoản ngân hàng do đối tượng cung cấp. Thời gian gần đây, các đối tượng thay đổi phương thức thủ đoạn tinh vi hơn bằng việc yêu cầu người dân bấm vào đường link, tải app *(ứng dụng)* khai báo thuế "Tổng cục Thuế" giả mạo do các đối tượng gửi đến, sau khi cài thì điện thoại bị chiếm quyền điều khiển, tài khoản ngân hàng bị kiểm soát từ xa và bị chiếm đoạt tiền trong tài khoản.

Người dân, đặc biệt là các hộ kinh doanh, buôn bán trên địa bàn huyện khi gặp những ai liên hệ với mình về vấn đề trên, mọi vấn đề liên quan đến thuế không làm theo hướng dẫn của đối tượng đang tự xưng là cán bộ thuế, mà cần trực tiếp liên hệ ngay với Chi Cục Thuế huyện Bình Sơn tại trụ sở hoặc liên hệ đến Đội Thuế các xã, thị trấn để được hướng dẫn.

1.6. Thủ đoạn lừa đảo khi truy cập vào đường link do shipper gửi

Đây là thủ đoạn phổ biến trên địa bàn huyện Bình Sơn thời gian qua. Nếu như trước đây, các đối tượng chỉ lợi dụng những khách hàng mua sắm nhiều, dễ quên đơn hàng để gọi điện yêu cầu chuyển khoản thanh toán thì thời gian gần đây đối tượng lừa đảo đã áp dụng phương thức lừa đảo tinh vi hơn, thông qua việc hướng dẫn người dân cài đặt phần mềm *(app)* giả mạo với "hướng dẫn" để hoàn tiền thanh toán đơn hàng, hoặc huỷ dịch vụ cộng tác làm shipper, bị đe dọa nếu không huỷ thì công ty chuyển phát nhanh sẽ thu phí hàng tháng. Khi cài đặt phần mềm giả mạo, có nguy cơ sẽ bị chiếm quyền điều khiển toàn bộ điện thoại. Các tin nhắn, cuộc gọi đến máy điện thoại của nạn nhân sẽ được ứng dụng kiểm soát, ngầm chuyển về máy chủ do đối tượng quản lý, không hiển thị trên điện thoại của nạn nhân. Nguy hiểm hơn, các đối tượng chiếm quyền điều khiển điện thoại di động từ xa, sau đó truy cập vào tài khoản ngân hàng của bị hại, rồi thực hiện chuyển tiền và chiếm đoạt tiền của bị hại.

1.7. Thủ đoạn lừa đảo xuất khẩu lao động, đưa người ra nước ngoài làm việc

Đánh vào tâm lý người dân muốn làm thủ tục nhanh chóng để xuất cảnh ra nước ngoài lao động, nhóm lừa đảo chủ động tìm kiếm và liên hệ với người có nhu cầu xuất cảnh qua mạng xã hội *(chủ yếu là mạng xã hội Facebook)*, yêu cầu người có nhu cầu xuất cảnh chỉ cần gửi ảnh chân dung và ảnh căn cước công dân để làm thủ tục cấp hộ chiếu phổ thông. Sau một thời gian, các đối tượng gửi ảnh chụp hộ chiếu giả mạo cho người dân, thông báo thủ tục cấp hộ chiếu đã hoàn tất *(hình ảnh hộ chiếu giả mạo đã được đối tượng cắt ghép, chỉnh sửa thông tin để phù hợp với thông tin cá nhân của người dân)*.

Tiếp đó, đối tượng liên lạc với người dân qua điện thoại và tin nhắn trên Facebook, thông báo chi phí để xuất cảnh và yêu cầu người dân nộp trước một khoản tiền vào tài khoản ngân hàng do đối tượng cung cấp để làm visa. Sau khi người dân chuyển tiền, đối tượng xác nhận đã nhận được tiền và hứa hẹn sẽ giúp đỡ để người dân nợ phần còn lại, sẽ trả sau khi ra nước ngoài làm việc. Để tạo niềm tin cho nạn nhân, đối tượng gửi hình ảnh chụp visa giả mạo *(đã cắt ghép và chỉnh sửa)* cho người dân và thông báo rằng họ đã được cấp visa để nhập cảnh; thông báo thời gian xuất cảnh và yêu cầu người dân có mặt tại sân bay để nhận giấy tờ, làm thủ tục xuất cảnh.

Khi người dân đã hoàn toàn tin tưởng, đối tượng gửi "Văn bản xác minh chứng minh nguồn thu nhập và tài chính" giả mạo của Cục Quản lý xuất nhập cảnh và yêu cầu người dân chuyển 50.000.000 đồng vào tài khoản của Cục Quản lý xuất nhập cảnh để chứng minh tài chính *(văn bản này giả mạo, tài khoản chính là tài khoản của đối tượng lập ra để lừa đảo)*. Trên văn bản có ghi rõ mục đích xác minh và cam kết sẽ hoàn trả lại sau khi nộp tiền khoảng 30 - 40 phút. Sau khi thông báo văn bản xác minh chứng minh nguồn thu nhập và tài chính, có đối tượng mạo danh là cán bộ Cục Quản lý xuất nhập cảnh, Bộ Công an liên tục gọi điện thúc giục người dân nộp tiền vào tài khoản của Cục Quản lý xuất nhập cảnh để hoàn thiện hồ sơ.

Với thủ đoạn trên, nhiều người đã sập bẫy "lừa" của đối tượng. Hiện nay, trên mạng xã hội Facebook cũng tràn lan các trang mời gọi người dân đi lao động nước ngoài, trong đó nổi lên là lao động nông nghiệp thời vụ tại Hàn Quốc, với thủ đoạn không cần cọc tiền trước, hoàn thành hồ sơ, có visa mới đóng tiền. Do nhu cầu cần tìm kiếm việc làm nên có rất nhiều người liên hệ với các đối tượng, dẫn đến bị lừa đảo, mất tiền.

Khuyến cáo công dân cần trọng trước các lời mời chào hấp dẫn về việc nhẹ, lương cao, các dịch vụ nhanh, rẻ liên quan đến giấy tờ xuất nhập cảnh, các dịch vụ đi xuất khẩu lao động không rõ nguồn gốc… Liên hệ trực tiếp với Trung tâm Dịch vụ việc làm tỉnh (số 118 Phan Đình Phùng, phường Nguyễn Nghiêm, thành phố Quảng Ngãi) để được tư vấn đi lao động nước ngoài.

Cũng bằng thủ đoạn trên, nhưng nguy hiểm hơn là khi đã có được sự tin tưởng của người bị hại, các đối tượng lừa đảo đưa bị hại xuất cảnh ra nước ngoài bằng cả đường chính ngạch và trái phép… sau đó người lao động bị đưa vào làm việc trong các cơ sở, doanh nghiệp hoặc Casino đánh bạc trực tuyến với tần suất làm việc cao *(15 – 16 giờ/ngày)* với mức lương rẻ mạt, chỉ từ 5 -7 triệu đồng/tháng; ngoài ra bị hại còn bị quản thúc chặt chẽ, không được tự do đi lại, liên hệ với bên ngoài và phải làm việc để trả nhiều loại nợ, phí... Khi không đáp ứng được tần suất làm việc, chỉ tiêu được giao thì bị tra tấn, đánh đập... Qua công tác quản lý, nắm tình hình trên địa bàn huyện Bình Sơn cũng đã phát hiện người dân đã bị đối tượng xấu rủ rê, lôi kéo đưa ra nước ngoài làm việc với những phương thức, thủ đoạn tương tự…

1.8. Thủ đoạn dùng hình ảnh nhạy cảm để tống tiền, cưỡng đoạt tài sản

Các đối tượng là sử dụng tài khoản mạng xã hội (facebook, zalo…) chủ động kết bạn, nhắn tin cho bị hại để dụ dỗ thực hiện cuộc gọi video với các hành động nhạy cảm. Hoặc mạo danh các doanh nghiệp lớn đăng tin tuyển dụng, yêu cầu bị hại phải chứng minh mình không có hình xăm mới được tuyển dụng bằng cách quay video, chụp ảnh khoả thân để gửi cho đối tượng. Quá trình gọi điện, các đối tượng sẽ dụ dỗ bị hại khỏa thân, làm các động tác khiêu gợi, sau đó bí mật quay màn hình toàn bộ cuộc gọi và lưu lại. Thậm chí trong một số trường hợp, các đối tượng thông qua không gian mạng để thu thập hình ảnh, video cá nhân của bị hại và sử dụng công nghệ "deepfake" (kỹ thuật tổng hợp hình ảnh, âm thanh hoặc video để tạo ra những nội dung giả mạo) để ghép, chỉnh sửa thành hình ảnh, video có nội dung nhạy cảm, đồi truy như thật, gây hiểu nhầm cho người xem.

Sau khi có được những hình ảnh, video này, các đối tượng gửi lại cho bị hại và yêu cầu chuyển tiền cho chúng. Nếu không chúng sẽ gửi những nội dung này cho

bạn bè, người thân, đồng nghiệp của bị hại hoặc công khai lên không gian mạng. Không dừng lại ở đó, nếu bị hại chuyển tiền theo yêu cầu, các đối tượng sẽ liên tục đề nghị bị hại chuyển tiền nhiều lần với số tiền ngày càng tăng cho đến khi bị hại không còn khả năng tài chính… Hoạt động lừa đảo này rất chuyên nghiệp, có tổ chức và có kịch bản rõ ràng. Các đối tượng thường nhắm vào tâm lý lo sợ bị hạ uy tín, nhân phẩm, danh dự, ảnh hưởng đến công việc, hạnh phúc gia đình của bị hại.

2. Để phòng ngừa, ngăn chặn không để tội phạm lừa đảo qua không gian mạng tiếp tục xảy ra, UBND huyện Bình Sơn đề nghị các cơ quan, đơn vị tuyên truyền nội dung sau:

2.1. Lực lượng vũ trang và các cơ quan nhà nước tuyệt đối không làm việc với người dân qua không gian mạng, không yêu cầu người dân cung cấp thông tin tài khoản ngân hàng, mã OTP, không yêu cầu người dân thực hiện việc chuyển tiền, giao dịch vào tài khoản cá nhân.

2.2. Cơ quan pháp luật không thực hiện việc bắt, xử lý đối với bất kỳ cá nhân nào khi chưa tiếp nhận nguồn tin tội phạm, chưa làm việc trực tiếp với cá nhân liên quan, chưa có sự kiểm sát, phê chuẩn của Viện kiểm sát nhân dân cùng cấp, trừ trường hợp bắt quả tang, bắt người có quyết định truy nã.

2.3. Đề nghị người sử dụng điện thoại hạn chế chia sẻ thông tin cá nhân khi truy cập Internet và tham gia mạng xã hội, xác minh thông tin cụ thể trước khi thực hiện các giao dịch qua Internet, mạng xã hội và trước khi thực hiện việc chuyển tiền cho người khác. Không chuyển khoản ngân hàng giao dịch với bất kỳ cá nhân, tổ chức nào khi chưa tự mình kiểm tra cá nhân đang yêu cầu chuyển khoản đó có đúng là nhân sự đang công tác, làm việc cho cá nhân, tổ chức đó hay không; hoặc chưa kiểm tra công ty, doanh nghiệp có đang triển khai chương trình đó hay không.

2.4. Không cài bất kì app *(ứng dụng)* nào khi làm việc online qua số điện thoại và mạng xã hội zalo, facebook. Để phòng tránh lừa đảo, mọi dịch vụ *(bao gồm dịch vụ công)* và các công tác khác đang được lực lượng chức năng, doanh nghiệp triển khai, hướng dẫn trực tiếp tại trụ sở làm việc.

2.5. Đề nghị khi gặp phải trường hợp có phương thức, thủ đoạn như trên thì báo ngay cho Công an xã, thị trấn nơi gần nhất hoặc báo cho trực ban Công an huyện Bình Sơn để được hướng dẫn (SĐT: 0255.3851285).

Đề nghị Thủ trưởng các cơ quan, đơn vị và Chủ tịch UBND các xã, thị trấn khẩn trương triển khai thực hiện./.

Nơi nhận:
- Như trên;
- TT Huyện ủy, HĐND huyện;
- CT, các PCT UBND huyện;
- UBMTTQVN và các tổ chức CT-XH huyện;
- Các Cơ quan chuyên trách TMGV Huyện uỷ;
- Công an huyện;
- Các phòng, ban thuộc UBND huyện;
- Viện KSND huyện; Tòa án nhân dân huyện;
- Các cơ quan, đơn vị đóng trên địa bàn huyện;
- UBND các xã, thị trấn.
- VP HĐND&UBND: C, PCVP, CVNC;
- Lưu VT.

CHỦ TỊCH

ỦY BAN NHÂN DÂN HUYỆN BÌNH SƠN T. QUẢNG NGÃI

Nguyễn Ngọc Trân