CÔNG AN HUYỆN THẠCH THÀNH

**CÔNG AN XÃ THÀNH VINH**



**THÔNG BÁO HÌNH THỨC, THỦ ĐOẠN LỪA ĐẢO,**

**CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG**

Thời gian gần đây, tình hình hoạt động của tội phạm lừa đảo chiếm đoạt tài sản thông qua mạng viễn thông, mạng internet, mạng xã hội vẫn diễn biến phức tạp, xảy ra trên toàn quốc với nhiều thủ đoạn mới, tinh vi, gây thiệt hại về tài sản của người dân, đang là vấn đề nhận được nhiều sự quan tâm của toàn xã hội. Các đối tượng lợi dụng bối cảnh bùng nổ công nghệ thông tin, sự mất cảnh giác, sự nhẹ dạ cả tin, tâm lí lo sợ hoặc lòng tham để thực hiện nhiều hành vi lừa đảo nhằm chiếm đoạt tài sản có giá trị cao. Hiện nay, trên không gian mạng đang diễn ra **23 hình thức lừa đảo** với những thủ đoạn như sau:

**1.** **Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo**

Đối tượng giả danh cơ quan công an, viện kiểm sát, tòa án để gọi điện Đe dọa và gây áp lực tâm lý: khống chế, hăm dọa, nói dối về việc có liên quan đến các vụ án đang điều tra, bị phạt nguội giao thông chưa nộp phạt để tạo áp lực và đánh vào lòng sợ hãi của nạn nhân sau đó yêu cầu bạn chuyển tiền vào một tài khoản cụ thể hoặc cung cấp thông tin cá nhân như số thẻ tín dụng, số căn cước công dân, mã số bảo mật và các thông tin nhạy cảm khác nhằm mục đích chiếm đoạt tài sản của bạn, tạo áp lực thời gian, tuyên bố rằng hành động phải được thực hiện ngay lập tức để tránh hậu quả nghiêm trọng. Họ sẽ cố gắng thuyết phục bạn rằng không có thời gian để suy nghĩ hay tham khảo người khác, phải giấu không được cho người thứ ba biết để bảo mật thông tin.

**2.** **Lừa đảo cuộc gọi video Deepfake**: Đối tượng sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo ra những video hoặc hình ảnh giả, tạo ra các đoạn video ngắn giả người thân, bạn bè thực hiện các cuộc gọi ngắn, thường chỉ vài giây sau đó ngắt giữa chừng, bảo là mất sóng, sóng yếu... Yêu cầu chuyển tiền mà tài khoản chuyển tiền không phải của người đang thực hiện cuộc gọi.

**3.** **Lừa đảo tuyển dụng CTV online**: Đối tượng đăng các tin bài tuyển cộng tác viên "việc nhẹ lương cao" - giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn tham gia thực hiện các nhiệm vụ và nạp tiền làm nhiệm vụ để chiếm đoạt tài sản của các nạn nhân.

**4.** **Đánh cắp tài khoản MXH, nhắn tin lừa đảo**

Các đối tượng đánh cắp tài khoản mạng xã hội sau đó nhắn tin mọi người yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu nạp thẻ điện thoại, yêu cầu chuyển tiền hoặc thực hiện hành động khẩn cấp hoặc gửi các đường link lạ.

**5.** **Lừa đảo tình cảm**

Xây dựng các trang fb với ảnh đại diện đẹp, thu hút sau đó sử dụng các chiêu trò lừa đảo để thu hút sự quan tâm của nạn nhân qua các trang web, áp hẹn hò, diễn đàn kết bạn bốn phương, tìm và tạo một mối quan hệ tình cảm giả với nạn nhân bằng cách sử dụng các chiêu trò như tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa. Dẫn dụ nạn nhân gửi hình ảnh video nhạy cảm (sau đó dùng những hình ảnh này để đe dọa, tống tiền nạn nhân). Một số kẻ lừa đảo tinh vi thì sử dụng nhiều cách khác nhau để thuyết phục nạn nhân tham gia đầu tư vào thị trường tài chính Forex thông qua một sàn giao dịch giả mạo mà kẻ lừa đảo kiểm soát. Khi tham gia đầu tư tài chính Forex, nạn nhân sẽ bị dẫn dụ thắng vài lần tạo niềm tin và lòng tham, sau đó khi thắng số tiền lớn hơn thì nạn nhân sẽ không rút ra được, bắt phải đóng phí giao dịch, đóng thuế hoặc bảo là tài khoản bị sai thông tin, phải đóng tiền để xác minh chứng thực... Cứ thế cho đến khi nạn nhân hết sạch tiền, phá sản.

hoặc gửi hàng bưu kiện có giá trị cao và bắt đóng tiền thuế để nhận.

**6.** **Lừa đảo “chuyển nhầm tiền” vào tài khoản ngân hàng**

Chuyển nhầm tiền vào tài khoản ngân hàng và giả danh người thu hồi nợ để yêu cầu trả lại số tiền là một hình thức lừa đảo nguy hiểm.

* Không chuyển tiền ngay lập tức
* Kiểm tra thông tin chuyển khoản
* Nếu bạn nghi ngờ hoặc trở thành nạn nhân của lừa đảo chuyển nhầm tiền, giả danh thu hồi nợ, hãy ngay lập tức báo cáo sự việc cho cơ quan chức năng, như cảnh sát hoặc ngân hàng, để họ tiến hành điều tra và cung cấp sự hỗ trợ.

**7.** **Lừa đảo cho số đánh lô đề**

Đánh số lô, số đề trên mạng xã hội với các dấu hiệu như phải đóng phí trước, rủi ro mất phí khi không trúng, và phải chia hoa hồng khi trúng là một hình thức lừa đảo nguy hiểm. Các đối tượng tiếp cận người dùng thông qua điện thoại, email, tin nhắn hoặc mạng xã hội, quảng cáo cung cấp số lô, số đề may mắn có khả năng trúng thưởng lớn; sử dụng các câu chuyện thành công, chứng cứ giả và những lời tán tụng để tạo niềm tin và thuyết phục người khác rằng họ có khả năng đưa ra các số lô, số đề chính xác; yêu cầu người khác đóng một khoản phí trước để nhận được các số lô, số đề may mắn. Họ thường đưa ra lý do như phí dịch vụ, phí tiên tri hoặc phí đăng ký.

**8.** **Lừa đảo “combo du lịch giá rẻ”**

Đối tượng đăng các bài viết quảng cáo bán tour du lịch, phòng khách sạn giá rẻ trên mạng xã hội, đề nghị chuyển tiền đặt cọc (từ 30-50% giá trị) để đặt cọc tour du lịch, phòng khách sạn, từ đó chiếm đoạt số tiền đặt cọc.

Đăng bài viết quảng cáo dịch vụ làm visa (thị thực) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa. Sau khi nạn nhân chuyển khoản thanh toán chi phí hoặc một phần chi phí, các đối tượng sẽ để nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ... Sau đó lấy lý do nạn nhân khai thông tin bị thiếu và không trả lại tiền.

Làm giả website/fanpage của công ty du lịch uy tín, làm giả ảnh chụp biên lai, hóa đơn thanh toán và đề nghị nạn nhân chuyển khoản thanh toán chi phí tour du lịch. Sau khi khách hàng chuyển khoản để thanh toán dịch vụ du lịch các đối tượng sẽ chặn liên lạc và xóa mọi dấu vết.

Làm giả/chiếm đoạt tài khoản của người dùng mạng xã hội, liên lạc với người thân trong danh sách bạn bè cho biết đang bị mắc kẹt khi du lịch tại nước ngoài và cần một khoản tiền ngay lập tức.

Mạo danh đại lý bán vé máy bay, tự tạo ra các website, trang mạng xã hội, với địa chỉ đường dẫn, thiết kế tương tự kênh của các hãng hoặc đại lý chính thức, sau đó quảng cáo với các mức giá rất hấp dẫn so với mặt bằng chung để thu hút khách hàng.

Nếu khách hàng liên hệ, các đối tượng sẽ đặt chỗ vé máy bay, gửi mã đặt chỗ để làm tin và yêu cầu khách hàng thanh toán. Sau khi nhận thanh toán, các đối tượng không xuất ra vé máy bay và ngắt liên lạc. Do mã đặt chỗ chưa được xuất ra vé máy bay, nên sẽ tự hủy sau một thời gian và khách hàng chỉ biết được việc này khi đến sân bay.

**9.** **Lừa đảo “khóa SIM” vì chưa chuẩn hóa thuê bao**: mạo danh là nhân viên nhà mạng gọi điện và thông báo số điện thoại của người sử dụng sẽ bị khóa 2 chiều trong 2 tiếng với các lý do như “chưa nộp phạt”, “thuê bao sai thông tin”…yêu cầu cung cấp thông tin, sau đó hướng dẫn người dùng thực hiện các cú pháp sang tên đổi chủ thông tin số điện thoại, cú pháp chuyển hướng cuộc gọi...

**10.** **Giả mạo biên lai chuyển tiền thành công**: các đối tượng lừa đảo là mua hàng số lượng lớn, sau đó vay thêm tiền mặt của nạn nhân rồi chuyển khoản trả, đối tượng đề nghị chuyển khoản theo hình thức Internet Banking cho người bán hàng. Nhưng thực chất là không có việc chuyển tiền thật, mà các đối tượng đã dùng phần mềm tạo bill thanh toán giả rồi đưa cho người bán hàng xem nhằm chứng minh là đã thực hiện việc chuyển khoản.

**11.** **Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu**: đối tượng lừa đảo tự xưng là giáo viên/ nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con em/ người thân họ đang cấp cứu trong tình trạng nguy kịch. Những “thầy cô giáo tự xưng” này thay phiên nhau gọi điện thúc giục cha mẹ chuyển tiền cứu con, nếu không hoặc chậm nộp tiền thì con của họ sẽ nguy hiểm đến tính mạng.

**12.** **Chiêu trò lừa đảo tuyển người mẫu nhí**: thông qua mạng xã hội như Facebook, Zalo, Telegram..., các đối tượng sẽ kết bạn với phụ huynh và mời tham gia ứng tuyển người mẫu nhí cho hãng thời trang. Sau khi nạn nhân “cắn câu”, các đối tượng lừa đảo sẽ đưa vào một group chat để mời tham gia thử thách.

Thử thách cho các phụ huynh khi muốn con mình tham gia vào ứng tuyển “người mẫu nhí” là chuyển khoản để mua sản phẩm hàng hiệu, sau đó cho con em mình làm mẫu chụp ảnh để giới thiệu, quảng bá sản phẩm trên mạng xã hội.

Thông thường ban đầu, chúng trả hoa hồng và tiền làm nhiệm vụ để “kích thích” phụ huynh tham gia. Nhưng khi số tiền chuyển vào tài khoản tăng cao, chúng xóa tung tích nhằm chiếm đoạt số tiền đã chuyển.

**13.** **Giả danh các công ty tài chính, ngân hàng thu thập thông tin**

Các đối tượng lừa đảo tạo lập hàng nghìn tài khoản facebook với các nguồn thông tin giả, tham gia vào các hội nhóm, diễn đàn, đăng bài quảng cáo cho vay tín chấp với lãi suất thấp (chỉ 1%/ tháng), thủ tục vay đơn giản, không cần gặp trực tiếp; nợ xấu vẫn vay được; không thế chấp, không thẩm định, chỉ cần Chứng minh nhân dân hoặc Căn cước công dân và có tài khoản ngân hàng/thẻ ATM là có thể vay được tiền...

Khi có người vay thì yêu cầu người vay cung cấp thông tin cá nhân, như: họ tên, số điện thoại, ảnh chụp CMND/CCCD, ảnh chụp chân dung. phục vụ làm hồ sơ vay, dụ người vay chuyển tiền phục vụ hỗ trợ xác minh, duyệt khoản vay, các đối tượng tiếp tục viện dẫn hàng loạt các lý do khoản vay không được giải ngân xuất phát từ lỗi khai hồ sơ của người vay (như khai sai tên người hưởng thụ, đổi cách viết tên người hưởng thụ từ chữ in thường sang in hoa, không đủ điều kiện vay, thừa hoặc sai một số trên số căn cước công dân.). Từ đó, chúng yêu cầu người vay phải nộp thêm các khoản tiền để bảo đảm khoản vay hoặc khắc phục lỗi hệ thống; hứa hẹn sẽ hoàn trả lại số tiền đã gửi cho khách hàng sau khi khoản vay được giải ngân. Tuy nhiên, khi người vay chuyển tiền vào số tài khoản của các đối tượng cung cấp, các đối tượng sẽ lập tức chiếm đoạt và ngắt liên lạc.

**14.** **Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen...**:Lợi dụng tính năng cho phép đăng thông tin của trang web như đăng hỏi đáp, diễn đàn, tải tập tin, các đối tượng xấu đưa quảng cáo lên. Các ứng dụng vay tiền trực tuyến hay các link quảng cáo cờ bạc, cá độ thường được quảng cáo rộng rãi trên các trang web với những tiêu đề thu hút như *“Không cần thế chấp, lãi suất không đồng”, “Vay siêu tốc, nhận tiền sau 30phút, lãi suất thấp, nhận tiền ngay”...* hoặc nhắn tin qua số điện thoại kèm theo đường link đến ứng dụng. Người có nhu cầu tham gia chỉ cần ấn (click) vào những trang quảng cáo, tải các ứng dụng về máy tính hoặc điện thoại thông minh, nhập các thông tin cá nhân, số tài khoản ngân hàng nhận tiền, ảnh chứng minh nhân dân, ảnh cá nhân và đồng ý cho truy cập vào danh bạ cá nhân.

**15.** **Giả mạo các trang thông tin điện tử cơ quan, doanh nghiệp (BHXH, ngân hàng...)**: Các đối tượng tạo trang web có giao diện gần giống trang web của cơ quan, doanh nghiệp để người dùng nhầm tưởng là trang web của đơn vị cung cấp. Sau đó, các đối tượng sử dụng tin nhắn giả mạo thương hiệu với các nội dung yêu cầu người dùng phải truy cập vào liên kết giả mạo, khai báo thông tin cá nhân, tài khoản ngân hàng và từ đó thực hiện hành vi đánh cắp, chiếm đoạt thông tin để thực hiện hành vi lừa đảo.

**16.** **Phát tán tin nhắn giả mạo thương hiệu (SMS Brandname)**

Các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn lừa đảo tới người dùng với mục đích nhằm chiếm đoạt tài sản.

**17.** **Lừa đảo đầu tư chứng khoán quốc tế, tiền ảo.**

Nhận diện sàn đầu tư chứng khoán quốc tế, giao dịch vàng, ngoại hối, tiền ảo, bất động sản, kinh doanh đa cấp có mục tiêu quảng cáo, lôi kéo số lượng lớn người tham gia đầu tư và có nguy cơ lừa đảo chiếm đoạt tài sản là rất quan trọng để bảo vệ mình và tránh rơi vào các cạm bẫy tài chính.

**18.** **Rao bán hàng giả hàng nhái qua sàn thương mại điện tử**

Rao bán hàng giả và hàng nhái trên mạng xã hội và các sàn thương mại điện tử với giá cực kỳ hấp dẫn, thường rẻ hơn rất nhiều so với giá thị trường, không cung cấp đủ thông tin chi tiết về sản phẩm, như thông số kỹ thuật, nguồn gốc, chất lượng, thông tin về nhà cung cấp và bảo hành, áp đặt áp lực mua hàng nhanh chóng bằng cách khuyến khích mua hàng ngay lập tức với lý do rằng hàng chỉ có số lượng giới hạn hoặc đang có nguy cơ hết hàng, sản phẩm nhận được đánh giá và nhận xét tích cực một cách quá mức, không tự nhiên hoặc không có đáng tin cậy (tạo lòng tin, yêu cầu chuyển khoản trực tiếp qua ngân hàng, thanh toán bằng ví điện tử không rõ nguồn gốc, hoặc yêu cầu cung cấp thông tin thẻ tín dụng một cách đáng ngờ.Người bán không cung cấp thông tin liên hệ rõ ràng, như địa chỉ, số điện thoại hoặc email hoặc có lịch sử phản hồi tiêu cực, có nhiều khiếu nại từ người mua trước đó hoặc không có đủ đánh giá và phản hồi từ khách hàng.

**19.** **Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa**

* Đối tượng xây dựng các tài khoản, trang web giả hoặc tài liệu có thể tin tưởng và đáng tin cậy. Tiếp cận nạn nhân, Sử dụng ngôn ngữ thuyết phục và các chiến thuật để xây dựng lòng tin của họ.Thuyết phục nạn nhân rằng họ có khả năng khôi phục lại số tiền đã mất. Sau khi nạn nhân tin tưởng vào khả năng của kẻ lừa đảo, đối tượng sẽ yêu cầu thanh toán phí xử lý, yêu cầu pháp lý hoặc bất kỳ lý do hợp lý nào khác.

**20.** **Lừa đảo lấy cắp Telegram OTP**

Tạo một profile giả mạo, đánh cắp hình ảnh của 1 người uy tín có liên quan đến nạn nhân để tạo sự tin cậy: thường dùng sự kiện đáng tin cậy và hấp dẫn để đảm bảo người khác tin tưởng và tham gia vào quá trình.

Gửi thông báo giả từ tài khoản Telegram được giả danh như một cơ quan chính phủ, tổ chức tài chính, hoặc một người có uy tín cao. Bảo rằng đang nghi ngờ có 2 tài khoản giả mạo nạn nhân, nên cần nạn nhân chụp hình screenshot để xác minh coi có đúng không, nhưng trong lúc này kẻ lừa đảo đã dùng số điện thoại của nạn nhân và chọn chức năng quên mật khẩu của Telegram, lúc này khi chụp hình screenshot thì vô tình để nạn nhân thấy luôn mã OTP từ Telegram mới gửi về.

Nhận thông tin OTP: Khi người khác chụp màn hình và cung cấp cho kẻ lừa đảo, lúc đó có thể nhận được mã OTP thông qua hình ảnh đó. Sử dụng mã OTP để truy cập vào tài khoản Telegram của họ.

**21.** **Lừa đảo tung tin giả về cuộc gọi mất tiền như FlashAI**

Thông tin rằng chỉ bằng việc nhận cuộc gọi voicecall bạn có thể bị mất tiền là KHÔNG chính xác.

Không có cách nào để người dùng bị trừ tiền chỉ bằng việc nhận cuộc gọi voicecall thông thường trên điện thoại di động. Việc các đối tượng làm vậy nhằm mục đích câu views, likes và gây hoang mang dư luận xã hội.

Mục đích là lừa đảo người dùng bằng cách thuyết phục họ THAO TÁC theo hướng dẫn để tiết lộ thông tin cá nhân.

**22.** **Lừa đảo dịch vụ lấy lại Facebook**

Tạo ra một trang web giả mạo hoặc gửi email giả mạo cho người dùng Facebook, hoặc chủ động nhắn tin cho người dùng Facebook, tuyên bố rằng họ là dịch vụ lấy lại tài khoản và có thể giúp nạn nhân khôi phục tài khoản bị mất. Yêu cầu thông tin cá nhân nhạy cảm như tên đăng nhập, mật khẩu, số điện thoại, địa chỉ email, mã OTP, hoặc thông tin thẻ tín dụng để xác minh danh tính và thực hiện việc lấy lại tài khoản. Hoặc bắt nạn nhân phải đóng một khoản tiền cọc trước và khi đã đạt được mục đích, kẻ lừa đảo khóa chặn cuộc trò chuyện với nạn nhân hoặc xóa luôn tất cả các dấu vết.

**23.** **Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook**

* Kẻ lừa đảo tạo một trang web giả mạo có giao diện tương tự như một trang web đáng tin cậy như ngân hàng hoặc dịch vụ trực tuyến. Trang web này được thiết kế để thu thập thông tin cá nhân và đăng nhập của người dùng khi họ nhập vào.
* Tạo một đường link hấp dẫn: Tạo một đường link hấp dẫn sử dụng một tiêu đề hoặc mô tả mà người dùng có thể quan tâm, chẳng hạn như "Nhận ngay ưu đãi đặc biệt" hoặc "Kiểm tra tài khoản của bạn" hoặc "Bạn bị bóc phốt" hoặc các sự kiện đang hot trending xu hướng trên mạng xã hội. Đảm bảo đường link này giống như một đường link đáng tin cậy để gây thiện cảm và khó phát hiện.
* Rải link và seeding quảng cáo bẩn trên Facebook: Kẻ lừa đảo sử dụng các tài khoản giả mạo hoặc các tài khoản đã bị xâm nhập để rải link và seeding quảng cáo bẩn trên Facebook. Đăng bài viết, nhận xét, bình luận hoặc quảng cáo với đường link đã được tạo, hấp dẫn người dùng để nhấn vào.
* Lừa đảo và đánh cắp thông tin, tài sản: Khi người dùng nhấn vào đường link lừa đảo, họ sẽ được chuyển hướng đến trang web phishing mà kẻ lừa đảo đã tạo. Từ đó, kẻ lừa đảo có thể thu thập thông tin cá nhân, tài khoản hoặc đăng nhập của họ và sử dụng để lừa đảo hoặc đánh cắp tài sản.

**BIỆN PHÁP PHÒNG TRÁNH**

Giữ bí mật thông tin bảo mật các dịch vụ ngân hàng (tuyệt đối không tiết lộ mã PIN thẻ, mật khẩu truy cập, mật khẩu giao dịch một lần OTP, mật khẩu truy cập địa chỉ email với người lạ, kể cả nhân viên ngân hàng, Công an qua điện thoại).

Không đăng tải, chia sẻ hình ảnh CCCD trên mạng xã hội. Không cung cấp thông tin CCCD cho những dịch vụ không thiết yếu, các dịch vụ không có cam kết bảo đảm an toàn thông tin cá nhân. Không cho người khác mượn CCCD nếu không có mục đích chính đáng.

xác thực người đề nghị thực hiện giao dịch tài chính (không chuyển tiền cho đối tượng khi chưa xác thực; cảnh giác đối tượng giả mạo quen biết thông qua mạng xã hội, email, điện thoại, thư giấy, SMS, mạo danh nhân viên ngân hàng, cơ quan Nhà nước); kiểm tra thông tin của trang website khi thực hiện giao dịch trực tuyến (chỉ nên thực hiện giao dịch tại các website uy tín, có độ bảo mật cao…); hạn chế sử dụng mạng wifi công cộng, tại quán cafe để đăng nhập, thực hiện giao dịch trên hệ thống ngân hàng điện tử...

Khi thực hiện giao dịch thẻ tại ATM, POS phải quan sát khe thẻ trên máy ATM, bảo đảm không có thiết bị lạ và che bàn phím khi nhập số PIN. Khi phát hiện tài khoản/thẻ phát sinh những giao dịch gian lận hoặc có vướng mắc, phải gọi liên lạc ngay số hotline ngân hàng liên quan. Đăng ký dịch vụ thông báo biến động số dư tài khoản nhằm kịp thời phát hiện và giảm thiểu rủi ro liên quan đến các giao dịch bất thường.

Cảnh giác với các cuộc gọi tự xưng Công an, viện kiểm sát, nhân viên ngân hàng… thông báo giám định, trúng thưởng, nhận quà, xác minh và đe dọa, yêu cầu chuyển tiền vào tài khoản chỉ định. Tuyệt đối không chuyển tiền, nộp tiền vào tài khoản người khác khi không xác định được cụ thể họ là ai, sử dụng tiền vào mục đích gì, không có giấy tờ từ cơ quan chức năng chứng minh mục đích, nội dung làm việc cụ thể.

Công an xã Thành Vinh khuyến cáo trên đây là thủ đoạn lừa đảo công nghệ cao phổ biến nhất hiện nay, người dân cần nêu cao cảnh giác, chia sẻ rộng rãi, tuyên truyền đến người thân, bạn bè các thủ đoạn trên, tránh "mắc bẫy các đối tượng xấu". Để làm việc với người dân, cơ quan Công an sẽ trực tiếp gửi “ **giấy mời, giấy triệu tập**” hoặc gửi qua Công an địa phương và “**TUYỆT ĐỐI**” không yêu cầu công dân chuyển tiền vào tài khoản ngân hàng. Cơ quan Công an “**KHÔNG**” có tài khoản ngân hàng đứng tên riêng của bất kì cá nhân, tổ chức nào. Đặc biệt:

+ Không sợ: Không hoảng sợ khi nhận được điện thoại, tin nhắn, các thông tin mà người lạ mặt gửi đến có nội dung xấu liên quan đến cá nhân và người thân.

+ Không tham: Khi có người lạ gọi điện hoặc gửi tin nhắn thông báo được trúng thưởng hoặc nhận được quà, khoản tiền lớn không rõ nguồn gốc thì không được tin lời các đối tượng.

+ Không kết bạn với người lạ: Khi có người lạ mặt trên mạng xã hội kết bạn làm quen không rõ là ai, mục đích thì không nên kết bạn, bắt chuyện, nhất là không được cung cấp các thông tin cá nhân để đối tượng có thể lợi dụng.

+ Không làm: Khi các cá nhân không quen biết yêu cầu cung cấp thông tin cá nhân hoặc yêu cầu chuyển tiền hay làm một số việc thì tuyệt đối không được làm theo.

+ Phải thường xuyên cảnh giác: Chủ động bảo mật các thông tin cá nhân, nhất là các thông tin quan trọng như: Thông tin thẻ căn cước công dân; thông tin tài khoản ngân hàng; thông tin tài khoản mạng xã hội...

+ Phải tố giác ngay với cơ quan pháp luật khi có nghi ngờ: Khi nhận được các cuộc gọi, tin nhắn hoặc các nội dung nghi ngờ là hoạt động lừa đảo hoặc không có cơ sở khẳng định nội dung thì các cá nhân phải báo ngay cho cơ quan Công an để được hướng dẫn xử lý.

Mọi người dân khi phát hiện có các dấu hiệu của tội phạm “Lừa đảo chiếm đoạt tài sản trên không gian mạng” với các thủ đoạn hoạt động như trên cung cấp thông tin, tố giác tội phạm đến Công an huyện Thạch Thành, đường dây nóng **02373.877.003** hoặc liên hệ Công an xã Vinh số điện thoại Trực ban **02373883113**; Đ/c Hắc Văn Năm – Trưởng Công an xã: **0915570696; 0961562366**: để được hỗ trợ và góp phần vào công tác phòng ngừa, đấu tranh, ngăn chặn. xử lý tội phạm./.

**CÔNG AN XÃ THÀNH VINH**