BỘ CÔNG AN
**CÔNG AN TỈNH BẾN TRE**

Số: 78 /CAT-ANM

V/v cảnh báo thủ đoạn lừa đảo, chiếm đoạt tài sản dịp Tết Nguyên đán Ất Tỵ 2025

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

*Bến Tre, ngày 14 tháng 01 năm 2025*

Kính gửi:
- Các sở, ban, ngành tỉnh;
- Ban Tuyên giáo Tỉnh ủy;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Các tổ chức chính trị - xã hội tỉnh;
- Đài Phát thanh và Truyền hình Bến Tre;
- Báo Đồng Khởi;
- Ủy ban nhân dân các huyện, thành phố.

Hiện nay, các loại tội phạm truyền thống có xu hướng dịch chuyển môi trường hoạt động lên không gian mạng, trở thành một trong những thách thức an ninh phi truyền thống lớn trong giai đoạn hiện nay; trong đó, tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng diễn biến ngày càng phức tạp, gây thiệt hại lớn về kinh tế và bức xúc trong Nhân dân. Mặc dù, thủ đoạn của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng không mới, song cách thức tiếp cận nạn nhân ngày càng tinh vi, chuyên nghiệp, có tổ chức, với số lượng lớn bị hại tại nhiều địa phương trên cả nước. Đặc biệt, dịp Tết Nguyên đán là thời điểm nhu cầu của người dân về mua sắm và giao dịch tiền tệ tăng cao, là điều kiện thuận lợi cho đối tượng lừa đảo chiếm đoạt tài sản trên không gian mạng hoạt động. Do đó, việc nâng cao cảnh giác và phòng ngừa là rất quan trọng.

Để tiếp tục triển khai thực hiện có hiệu quả công tác đấu tranh phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, Công an tỉnh đề nghị các cơ quan, đơn vị, địa phương quan tâm thực hiện một số nội dung sau:

1. Tiếp tục triển khai thực hiện quyết liệt, có hiệu quả Chỉ thị số 21/CT-TTg, ngày 25/10/2020 của Thủ tướng Chính phủ về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản; Kế hoạch số 4120/KH-UBND, ngày 12/8/2020 của Ủy ban nhân dân tỉnh về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản; Công văn số 4509-CV/TU, ngày 19/02/2024 của Tỉnh ủy về việc lãnh đạo, chỉ đạo tăng cường phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng; Công văn số 1474/UBND-NC, ngày 14/3/2024 của Ủy ban nhân dân tỉnh về việc tăng cường phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng.

2. Nâng cao hiệu lực, hiệu quả công tác quản lý Nhà nước trên các lĩnh vực dễ nảy sinh hoặc có sơ hở để tội phạm lợi dụng hoạt động lừa đảo chiếm đoạt tài sản qua mạng; rà soát những khó khăn, bất cập, vướng mắc trong thực hiện chính sách, pháp luật có liên quan để đề xuất sửa đổi, bổ sung, nhằm nâng cao hiệu quả phòng ngừa, ngăn chặn hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng.

3. Đẩy mạnh phong trào toàn dân bảo vệ an ninh Tổ quốc, gắn với xây dựng thế trận An ninh nhân dân trên không gian mạng; phát huy sức mạnh tổng hợp của cả hệ thống chính trị, nhất là vai trò tiên phong, đi đầu của đội ngũ cộng tác viên Ban Chỉ đạo 35, cán bộ, đảng viên, các cơ quan báo, đài,... để tuyên truyền sâu rộng trong xã hội, nâng cao nhận thức, hiểu biết của người dân về phòng ngừa, phát hiện, ngăn chặn cũng như tố giác với cơ quan chức năng khi phát hiện đối tượng, dấu hiệu tội phạm có liên quan.

Công an tỉnh Bến Tre cảnh báo một số phương thức, thủ đoạn của tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng dịp Tết Nguyên đán Ất Tỵ 2025 *(có nội dung tuyên truyền kèm theo)* để phục vụ công tác tuyên truyền. Đề nghị các cơ quan, đơn vị, địa phương quan tâm lãnh đạo, chỉ đạo phối hợp thực hiện có hiệu quả nội dung Công văn này./.

***Nơi nhận:***
- Như trên;
- Đ/c Giám đốc CAT (để báo cáo);
- Lưu: VT,ANM.TTH.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH BẾN TRE

**Đại tá Võ Công Bình**

**NỘI DUNG**

**Tuyên truyền phương thức, thủ đoạn của tội phạm lừa đảo, chiếm đoạt tài sản dịp Tết Nguyên đán Ất Tỵ 2025**

*(Kèm theo Công văn số 78 /CAT- ANM ngày 14/01/2025 của Công an tỉnh Bến Tre)*

## I. CÁC PHƯƠNG THỨC, THỦ ĐOẠN LỪA ĐẢO QUA MẠNG, CÁCH THỨC NHẬN BIẾT VÀ BIỆN PHÁP PHÒNG TRÁNH

### 1. Sử dụng công nghệ cao, trí tuệ nhân tạo cắt ghép hình ảnh cá nhân để thực hiện các hành vi lừa đảo, đe dọa tống tiền

Các đối tượng sử dụng phần mềm công nghệ cao, trí tuệ nhân tạo cắt ghép khuôn mặt của nạn nhân là lãnh đạo, cán bộ, đảng viên vào các hình ảnh từ các clip trên Internet có nội dung "nhạy cảm" thể hiện việc nạn nhân đang quan hệ tình dục trong nhà nghỉ, khách sạn,… để thực hiện các hành vi lừa đảo, đe dọa tống tiền.

***1.1. Dấu hiệu***

- Các đối tượng tìm kiếm thông tin cá nhân, hình ảnh, số điện thoại của nạn nhân, chủ yếu là nam giới, có điều kiện kinh tế, địa vị xã hội rồi cắt ghép mặt bị hại vào ảnh nhạy cảm trong nhà nghỉ, khách sạn…

- Giả chụp ảnh từ clip quay được tại hiện trường bằng cách dán biểu tượng nút play vào giữa ảnh hoặc dùng điện thoại quay lại ảnh đã cắt ghép.

- Sử dụng "SIM rác", dịch vụ gọi điện thoại qua Internet hoặc thông qua email, tin nhắn SMS, iMessage, Zalo…, thậm chí dịch vụ bưu chính để gọi điện, nhắn tin, gửi thư liên hệ với nội dung tự xưng là "thám tử tư, được người khác ủy thác điều tra, sau một thời gian bí mật theo dõi, phát hiện nạn nhân có những hành vi sa đọa, có mối quan hệ bất chính, ngoài luồng nên đã dùng thiết bị ghi hình bí mật để quay phim, chụp ảnh lại" kèm hình ảnh nhạy cảm đã được cắt ghép, chỉnh sửa cho nạn nhân.

- Yêu cầu nạn nhân chuyển tiền vào tài khoản do đối tượng chỉ định để chuộc lại các clip, hình ảnh này. Nếu nạn nhân không chịu giao số tiền nêu trên, đối tượng sẽ chuyển tất cả các ảnh và clip đã thu thập được lên các trang mạng xã hội, các website lớn; dán hình ảnh xung quanh nơi nạn nhân ở và làm việc; đồng thời, tố cáo tới gia đình, cấp trên và cơ quan liên quan để cho nạn nhân "thân bại danh liệt".

***1.2. Biện pháp phòng tránh***

- Mọi người dân, nhất là cán bộ, đảng viên, công chức, viên chức cần chấp hành nghiêm quy định về công tác bảo vệ bí mật nhà nước, bảo đảm an

toàn thông tin; thường xuyên thay đổi mật khẩu thông tin các tài khoản (mạng xã hội, email,...).

- Tăng cường cảnh giác đối với các tin nhắn, thư được gửi từ người lạ qua Zalo hoặc địa chỉ thư điện tử lạ; tuyệt đối không ấn vào các link, không tải các file, hình ảnh đính kèm do người lạ gửi qua Zalo, thư điện tử hoặc các file nghi ngờ có chứa virus, mã độc, không lưu mật khẩu trên các trình duyệt.

- Đặc biệt, người dân cần bình tĩnh, tỉnh táo, không hoang mang khi nhận được tin nhắn đe dọa như trên. Tuyệt đối không chuyển tiền, không làm theo hướng dẫn của các đối tượng xấu để tránh bị chiếm đoạt tài sản.

**2. Giả danh cơ quan công quyền (Công an, Viện kiểm sát, Tòa án, Hải quan...), Văn phòng luật sư, Ngân hàng... gọi điện đe dọa yêu cầu chuyển tiền hoặc hỗ trợ lấy lại tiền đã bị lừa đảo**

Các đối tượng lợi dụng tâm lý hoang mang, lo sợ của người dân khi bị cơ quan chức năng thông báo liên quan đến hành vi vi phạm pháp luật. Chúng sử dụng các ứng dụng gọi điện thoại, giả mạo danh nghĩa cơ quan chức năng, tiến hành theo từng bước: Thu thập thông tin cá nhân; đe dọa liên quan đến hành vi vi phạm pháp luật; yêu cầu chuyển tiền phục vụ công tác điều tra. Ngoài ra, chúng tạo nhiều trang mạng xã hội giả mạo cơ quan công quyền (Công an, Viện kiểm sát, Tòa án, luật sư...) đăng tin quảng cáo hoặc chủ động liên hệ các nạn nhân đã bị lừa đảo chiếm đoạt tài sản bởi các hình thức khác và tuyên bố có thể giúp lấy lại tiền bị lừa, yêu cầu chuyển khoản phí dịch vụ trước nhằm chiếm đoạt tài sản.

***2.1. Dấu hiệu***

- Nhận được cuộc gọi từ số điện thoại lạ hoặc tổng đài ảo (113, BOCONGAN...) thông báo về hành vi vi phạm pháp luật (vi phạm giao thông, liên quan vụ án đang điều tra...). Qua cuộc gọi này, các đối tượng sẽ thu thập thông tin cá nhân của người dân và đe dọa, gây áp lực tâm lý nhằm không cho nạn nhân có cơ hội hỏi ý kiến người thân hoặc cơ quan chức năng. Sau khi thu thập được thông tin, chúng sẽ kết nối người dân đến cuộc gọi khác được giới thiệu là cơ quan kiểm sát, tòa án... để tiếp tục gây áp lực tâm lý, yêu cầu người dân chuyển tiền ngay đến tài khoản của chúng để phục vụ công tác điều tra hoặc xử lý vi phạm giao thông.

- Các đối tượng kết nối với người dân thông qua tài khoản mạng xã hội, tự xưng là cán bộ cơ quan công quyền, thông báo người dân liên quan đến vụ án hình sự đặc biệt nghiêm trọng. Sau khi gây áp lực tâm lý, chúng yêu cầu nạn nhân mở tài khoản ngân hàng mới theo số điện thoại do chúng cung cấp, sau đó chuyển toàn bộ tiền từ tài khoản của nạn nhân (tài khoản liên quan đến vụ án

như đối tượng thông báo) đến tài khoản mới mở để niêm phong, tạm giữ nhằm chiếm đoạt số tiền này.

- Các đối tượng thường gợi ý về việc nếu không thể đến cơ quan chức năng làm việc thì chúng hỗ trợ làm việc thông qua điện thoại. Khi người dân đề nghị gặp mặt, chúng có thể sử dụng công nghệ giả mạo gương mặt (deepfake) với trang phục công an, kiểm sát, tòa án... để gọi điện video với người dân, tìm cách lẫn tránh không gặp mặt trực tiếp.

- Một số nạn nhân sau khi bị lừa đảo bởi các hình thức khác có thể nhận được đề nghị giúp đỡ lấy lại tiền từ các tài khoản mạng xã hội giả mạo cơ quan chức năng (công an, kiểm sát, luật sư...). Các đối tượng thường tạo các trang mạng xã hội đăng nhiều thông tin cảnh báo lừa đảo, thêm người dân vào các nhóm chung với nhiều thành viên đóng vai nạn nhân trong các vụ lừa đảo khác đã lấy được tiền hoặc cũng đang nhờ sự trợ giúp để lấy lại tiền. Khi nạn nhân đồng ý, chúng sẽ yêu cầu chuyển trước khoản phí dịch vụ và chiếm đoạt số tiền này.

***2.2. Biện pháp phòng tránh***

- Cảnh giác khi nhận được cuộc gọi tự xưng là cán bộ cơ quan công quyền, liên hệ cơ quan chức năng nơi gần nhất hoặc số điện thoại của cơ quan công quyền đăng tải trên các trang chính thống để xác thực thông tin trước khi làm theo yêu cầu của người kết nối. ***Lưu ý: Cơ quan chức năng không làm việc qua điện thoại, chỉ làm việc tại trụ sở cơ quan.***

- Không cung cấp thông tin cá nhân cho bất kỳ ai thông qua điện thoại khi chưa xác thực chính xác danh tính của người liên hệ với mình. Tuyệt đối không chuyển tiền vào các tài khoản ngân hàng do các đối tượng chỉ định để phục vụ công tác điều tra, niêm phong,…

- Không tin vào các lời quảng cáo hỗ trợ lấy lại tiền đã bị lừa đảo. Cơ quan chức năng cần xác minh làm rõ vụ việc, làm việc trực tiếp với nạn nhân, không hỗ trợ lấy lại tiền qua mạng.

- Luôn luôn giữ tâm lý bình tĩnh khi nhận được cuộc gọi thông báo liên quan đến hành vi vi phạm pháp luật hoặc sau khi bị lừa đảo chiếm đoạt tài sản. Trình báo đến cơ quan Công an nơi sinh sống, làm việc để được hướng dẫn cụ thể, không làm theo yêu cầu của các cá nhân, tổ chức khi chưa xác thực danh tính.

**3. Lừa đảo tình cảm sau đó dẫn dụ đầu tư tài chính, làm nhiệm vụ online hoặc gửi tiền, quà có giá trị**

Hình thức lừa đảo tình cảm hiện nay không còn mới, tuy nhiên vẫn có rất nhiều người dân dính bẫy lừa đảo của các đối tượng. Chúng lập ra nhiều tài khoản mạng xã hội ảo, lấy ảnh, thông tin của những người nổi tiếng hoặc có ngoại hình ưa nhìn, vỏ bọc doanh nhân, nhắn tin trò chuyện trong thời gian dài

với nạn nhân (thường là phụ nữ). Trong khi trò chuyện, các đối tượng chia sẻ việc mình kiếm được nhiều tiền thông qua công việc đầu tư, làm nhiệm vụ qua mạng, lôi kéo nạn nhân tham gia cùng nhằm chiếm đoạt tài sản.

Ngoài ra, đối tượng có thể tự xưng mình là người nước ngoài, ngỏ ý muốn gửi quà tặng có giá trị cao cho nạn nhân, sau đó giả danh các cơ quan chức năng (Công an, Thuế, Hải quan, Bưu điện...) đề nghị nạn nhân đóng các khoản phí để nhận được quà.

***3.1. Dấu hiệu***

- Nhận được tin nhắn hỏi thăm từ các tài khoản mạng xã hội (khen hình ảnh đẹp, hỏi thăm khung cảnh, khen ngợi ngoại hình...) với mục đích tiếp cận, làm quen và liên tục hỏi thăm trong một thời gian dài.

- Yêu cầu kết bạn thông qua các tài khoản mạng xã hội, đặc biệt là các ứng dụng hẹn hò, như: Tinder, Bumble, Facebook Dating… Các tài khoản kết bạn thường có vỏ bọc "hào nhoáng", ngoại hình đẹp, cuộc sống giàu có, đi du lịch nhiều nơi...

- Trong thời gian nói chuyện với nạn nhân, các đối tượng thường xuyên chia sẻ về cuộc sống, sinh hoạt... trong đó, lồng ghép nội dung mình đang làm công việc online và kiếm được nhiều tiền từ công việc này. Trong một số trường hợp, các đối tượng nhờ nạn nhân đăng nhập tài khoản của mình trên sàn đầu tư để làm nhiệm vụ giúp vì lý do đang bận việc cá nhân, mục đích tạo niềm tin cho nạn nhân trước khi rủ nạn nhân tham gia chung.

- Khi tham gia đầu tư theo dụ dỗ của đối tượng, nạn nhân có thể nhận được tiền lãi sau một số lần đầu tư ban đầu với số tiền nhỏ. Dần dần hệ thống sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc lấy nhiều lý do để "giam tiền" như: Cơ quan thuế nước ngoài phong tỏa, thao tác sai, lỗi giao dịch... và yêu cầu nạn nhân chuyển thêm tiền để có thể rút toàn bộ về.

- Hứa hẹn tặng quà có giá trị cao gửi từ nước ngoài về. Đối tượng sau thời gian trò chuyện qua mạng tỏ ý rất yêu mến nạn nhân, muốn tặng cho nạn nhân những món quà có giá trị cao. Tuy nhiên, việc gửi quà về gặp nhiều trục trặc như: Bị cơ quan chức năng tạm giữ do quà giá trị cao, cần các khoản phí để thông quan... Nhiều nạn nhân với tâm lý sẽ nhận được quà giá trị rất lớn nên chấp nhận ứng trước một số tiền để hoàn thiện thủ tục. Thực tế, sau khi nạn nhân chuyển tiền, các đối tượng lại viện ra nhiều lý do để yêu cầu nạn nhân tiếp tục chuyển tiền để nhận được quà.

**5. Lừa đảo chuẩn hóa thông tin cá nhân (thuê bao di động, định danh điện tử VNeID, tài khoản ngân hàng,...), mạo danh "cán bộ" Cơ quan thuế, nhân viên ngành Điện (EVN) để yêu cầu truy cập hoặc cài đặt ứng dụng độc hại**

Đây là hình thức lừa đảo giả danh Cơ quan quản lý nhà nước để yêu cầu người dân truy cập link chứa mã độc hoặc tải về ứng dụng giả mạo chứa mã độc. Sau khi người dân click vào đường dẫn hoặc tải về ứng dụng, cho phép truy cập thiết bị, các đối tượng sẽ thu thập được dữ liệu về thông tin cá nhân, tài khoản ngân hàng... để chiếm đoạt tài khoản ngân hàng, tài sản.

***5.1. Dấu hiệu***

- Cuộc gọi đến từ số điện thoại cá nhân hoặc số điện thoại giả mạo thương hiệu (Brandname) như VNeID, 113, Vinaphone, Viettel,... giả danh cơ quan quản lý nhà nước (cảnh sát khu vực, cán bộ quản lý hộ tịch, nhân viên thuế, nhân viên điện lực, nhà cung cấp dịch vụ viễn thông hoặc nhân viên ngân hàng...), thông báo đề nghị người dân bổ sung hoặc sửa đổi dữ liệu thông tin cá nhân để chuẩn hóa theo quy định hoặc thông báo nạn nhân thiếu nợ tiền điện hoặc chưa thanh toán tiền điện....

- Các đối tượng yêu cầu người dân cung cấp thông tin cá nhân để chuẩn hóa, hoặc truy cập vào các đường dẫn giả mạo, tải ứng dụng chứa mã độc (các ứng dụng giả mạo thời gian gần đây như "ĐỊNH DANH ĐIỆN TỬ", "BỘ TÀI CHÍNH", app giả mạo có giao diện gần giống với trang website chính thức của EVN ...) để chiếm quyền điều khiển thiết bị điện tử hoặc các tài khoản ngân hàng, thuê bao di động... Đối tượng gây áp lực bằng cách đe dọa, nếu không làm theo hướng dẫn thì có thể sẽ bị khóa thuê bao di động, khóa tài khoản ngân hàng hoặc cơ quan Công an sẽ đến nhà làm việc...

- Trong một số trường hợp, các đối tượng sử dụng công nghệ deepface gọi video call cho người dân với trang phục Công an hoặc giả mạo văn phòng làm việc của các cơ quan quản lý nhà nước để tạo lòng tin với nạn nhân.

***5.2. Biện pháp phòng tránh***

- Cảnh giác cao độ khi nhận các cuộc gọi tự xưng là cán bộ cơ quan quản lý nhà nước, nhân viên cơ quan Thuế, ngành Điện, ngân hàng, nhà mạng, ... đề nghị cung cấp thông tin cá nhân.

- Tuyệt đối không cung cấp thông tin, tài khoản cá nhân, tài khoản ngân hàng, mã OTP cho người lạ; không truy cập vào các link, cài đặt ứng dụng không rõ nguồn gốc và thận trọng khi cấp quyền cho các ứng dụng truy cập thiết bị. Nếu lỡ cài đặt và nghi vấn bị chiếm đoạt tài sản, cần liên hệ ngay đến tổng đài hỗ trợ của ngân hàng đang sử dụng để được hướng dẫn khóa khẩn cấp tài

khoản; đồng thời, nhanh chóng sao lưu dữ liệu, gỡ bỏ các ứng dụng nghi ngờ, thay đổi mật khẩu các ứng dụng khác, cài đặt lại thiết bị.

- Liên hệ trực tiếp đến Công an phường/xã nơi cư trú khi nhận được yêu cầu chỉnh sửa, bổ sung thông tin cá nhân; liên hệ đến số hotline của nhà mạng, ngân hàng khi nhận được yêu cầu chuẩn hóa thông tin thuê bao hoặc tài khoản ngân hàng.

**6. Giả danh nhân viên giao hàng (shipper) thuộc các công ty vận chuyển để lừa đảo, chiếm đoạt tài sản**

Với sự phát triển mạnh mẽ của thương mại điện tử, dịch vụ giao, nhận hàng tại nhà cũng phát triển mạnh, tuy nhiên, đây cũng là môi trường, điều kiện thuận lợi để các đối tượng đánh vào tâm lý người mua do chủ quan hoặc không có điều kiện nhận sản phẩm trực tiếp để giả mạo là nhân viên giao hàng (shipper) nhằm lừa đảo chiếm đoạt tài sản.

***6.1. Dấu hiệu***

- Đối tượng lừa đảo tổ chức thu thập thông tin khách hàng đặt mua sản phẩm từ các bình luận công khai tại các buổi bán hàng trực tuyến (Livestreams) trên các nền tảng mạng xã hội hoặc mua thông tin khách hàng qua các kênh thông tin khác.

- Giả danh là shipper thuộc các công ty vận chuyển để gọi tới khách hàng vào giờ hành chính hoặc khi khách hàng không có nhà. Do không thuận tiện để nhận hàng và số tiền thanh toán không lớn nên khách hàng dễ dàng đồng ý với đề nghị để hàng vào trong sân nhà hoặc vị trí khác theo thỏa thuận và chuyển khoản thanh toán đến số tài khoản do đối tượng cung cấp.

- Khi người dân chuyển khoản thành công, đối tượng tiếp tục thông báo có sự nhầm lẫn, số tài khoản vừa nhận tiền chỉ là số tài khoản đăng ký làm hội viên shipper hoặc tài khoản của công ty giao hàng.

- Đối tượng gửi đường dẫn liên kết đến trang web và số điện thoại giả mạo của đơn vị giao hàng, hướng dẫn nạn nhân thực hiện việc lấy lại tiền và đăng ký hủy thành viên shipper để chiếm đoạt quyền sử dụng điện thoại, thông tin cá nhân, chiếm đoạt quyền kiểm soát tài khoản ngân hàng, tài khoản ví điện tử… rồi chiếm đoạt tài sản.

***6.2. Biện pháp phòng tránh***

- Nâng cao tinh thần cảnh giác khi nhận số điện thoại lạ, không chuyển khoản khi chưa thấy sản phẩm đã đặt; không nên chuyển tiền cho người lạ và cần xác minh thật kỹ các thông tin trước khi chuyển khoản.

- Tuyệt đối không ấn vào bất cứ link nào do người lạ gửi tới để tránh "mắc bẫy" lừa đảo.

- Khi phát hiện có những dấu hiệu bất thường, phải dừng giao dịch ngay và trình báo vụ việc đến cơ quan Công an nơi gần nhất để kịp thời xử lý.

## II. THỰC HIỆN "4 KHÔNG, 2 PHẢI" ĐỂ TRÁNH BỊ LỪA ĐẢO TRÊN MẠNG

### 1. "4 KHÔNG"

***- Không sợ:*** Không hoảng sợ khi nhận được điện thoại, tin nhắn, các thông tin mà người lạ gửi đến có nội dung xấu liên quan đến cá nhân và người thân thông báo có liên quan vụ án, vụ việc.

***- Không tham:*** Không tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một các dễ dàng, những lợi nhuận phi thực tế, không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ, lương cao".

***- Không kết bạn với người lạ:*** Khi có người lạ mặt trên mạng xã hội muốn kết bạn làm quen với bạn, mời tham gia các hội, nhóm không rõ mục đích thì không nên kết bạn, bắt chuyện, tham gia, 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.

### 2. "2 PHẢI"

***- 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 CC/CCCD, 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 pháp luật để được hướng dẫn xử lý./.