

CÔNG AN TỈNH QUẢNG NGÃI
PHÒNG THAM MƯU

MÔ HÌNH
CẨM NANG ĐIỆN TỬ
VỀ AN NINH, TRẬT TỰ

TẬP 1

PHÒNG CHỐNG LỪA ĐẢO TRỰC TUYẾN

Tháng 7/2025



I. Hướng dẫn tố giác tội phạm qua ứng dụng VNEID

II. Các hình thức lừa đảo phổ biến

- | | |
|---|---------------------------------------|
| 1 | Mạo danh cơ quan pháp luật |
| 2 | Mạo danh nhân viên ngân hàng |
| 3 | Chuyển nhầm tiền vào tài khoản |
| 4 | Lừa đảo cộng tác viên bán hàng online |
| 5 | Nhận quà tặng miễn phí |
| 6 | Bẫy tình |
| 7 | Kêu gọi từ thiện |
| 8 | Khóa thuê bao di động |
| 9 | Các chương trình ngoại khóa hè |





10	DEEPFAKE
11	Quét thẻ QR code nhận tiền
12	Giả danh shipper
13	Đọc sách nhận lương
14	Hỗ trợ xác thực sinh trắc học
15	Các quỹ đầu tư "ảo"

III. Các kỹ năng cơ bản đảm bảo an toàn thông tin cá nhân

1	Hạn chế chia sẻ thông tin cá nhân trên không gian mạng
2	Thiết lập bảo mật hai lớp
3	Chủ động tìm hiểu các mối đe dọa trên không gian mạng



HƯỚNG DẪN TỔ GIÁC TỘI PHẠM QUA ỨNG DỤNG VNEID

CÁC TIỆN ÍCH CỦA APP VNEID

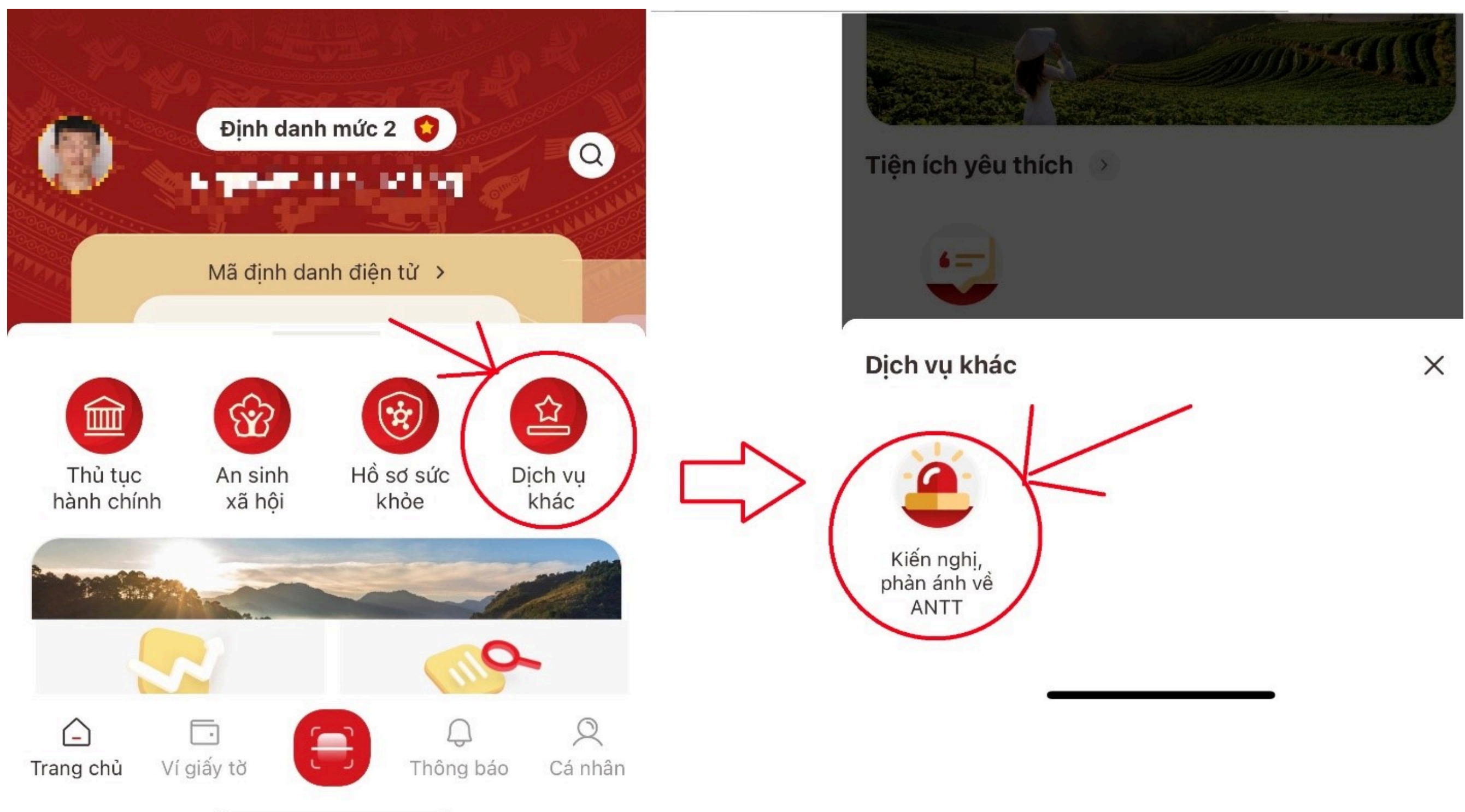


Trước đây, việc tiếp nhận tin báo, kiến nghị phản ánh thông tin liên quan đến an ninh, trật tự và tố giác tội phạm của cơ quan Công an phải thông qua các hình thức trực tiếp với người dân như: Đến trình báo, gọi điện thoại qua đường dây nóng,... Tuy nhiên, hiện nay với sự ra đời của VNeID, chỉ với vài thao tác đơn giản người dân đã có thể tạo hồ sơ kiến nghị, phản ánh ANTT để gửi đến Cơ quan Công an nơi gần nhất.

HƯỚNG DẪN TỔ GIÁC TỘI PHẠM QUA ỨNG DỤNG VNEID

Bước 1: Đăng nhập vào ứng dụng VNEID

Bước 2: Chọn dịch vụ khác, sau đó chọn mục “Kiến nghị, phản ánh ANTT”.



Bước 3: Điền đầy đủ thông tin theo yêu cầu. Người dùng có thể chọn chế độ “Ẩn danh” để bảo mật thông tin. Kiểm tra lại thông tin, sau đó ấn gửi.

Để kiểm tra tình trạng xử lý, người dùng chỉ cần tìm mục “Kiến nghị, phản ánh ANTT”!

MỘT SỐ PHƯƠNG THỨC LỪA ĐẢO PHỔ BIẾN

THỦ ĐOẠN CHUNG

Hầu hết các vụ lừa đảo trên không gian mạng xảy ra đều do sự nhẹ dạ, cả tin của nạn nhân, có thể khái quát thủ đoạn phạm tội như sau:



Mặc dù các đối tượng phạm tội thường xuyên thay đổi các “vỏ bọc” khác nhau, tuy nhiên về cơ bản đều dùng thủ đoạn như đã nêu trên. Vì vậy người dân cần nâng cao cảnh giác, không để trở thành nạn nhân của bọn tội phạm. Sau đây là 15 hình thức lừa đảo phổ biến hiện nay:

1. MẠO DANH CƠ QUAN PHÁP LUẬT

Thủ đoạn: Các đối tượng mạo danh các cơ quan pháp luật (cơ quan Công an, Tòa án, Viện kiểm sát,...) gọi điện cho người dân.



Sau đó thông báo nạn nhân đang liên quan đến một vụ án, chuyên án của cơ quan Công an hoặc bị kiện vì nợ tiền,... Sử dụng các lời lẽ đe dọa nạn nhân, gây tâm lý hoang mang lo sợ. Tiếp đó các đối tượng liên tục hỏi những câu hỏi liên quan đến thông tin cá nhân của nạn nhân, nhằm đưa nạn nhân vào “ma trận”. Khi sự căng thẳng lên cao, các đối tượng yêu cầu nạn nhân chuyển tiền như một khoản bảo đảm, hoặc phí xử lý vụ án,....

Cách thức xử lý

Khi nhận được điện thoại tự xưng là đại diện cơ quan pháp luật, người dân cần tỉnh táo, không hoang mang lo sợ, không cung cấp thông tin cá nhân, không chuyển bất kỳ khoản phí nào,... thay vào đó đề nghị làm việc trực tiếp tại trụ sở cơ quan. Bởi lẽ, không cơ quan pháp luật nào làm việc thông qua điện thoại.

2. MẠO DANH NHÂN VIÊN NGÂN HÀNG

Thủ đoạn: Các đối tượng tạo các trang web gần giống với trang web của các ngân hàng, hòng đánh vào sự chủ quan của nạn nhân.

GIẢ MẠO NHÂN VIÊN NGÂN HÀNG



Anh đang có món tiền treo trên hệ thống chờ nhận, anh vui lòng cung cấp số CMND và mã OTP để bên em hoàn tất thủ tục chuyển tiền về cho anh

Gửi tin nhắn, sau đó gọi điện cho nạn nhân, giả dạng là nhân viên ngân hàng, thông báo hệ thống bị trục trặc, qua đó yêu cầu nạn nhân đăng nhập lại thông tin trên trang web do chúng tạo ra, từ đó đánh cắp thông tin. Đồng thời, tiếp tục yêu cầu nạn nhân đọc mã OTP (do ngân hàng thật gửi, vì phát sinh giao dịch) để chiếm đoạt tài sản của nạn nhân.

CHÚ Ý

Không cung cấp mã OTP cho bất kỳ ai; chỉ đăng nhập tài khoản ngân hàng tại app chính thống; nếu có vấn đề phát sinh liên hệ làm việc trực tiếp với các ngân hàng

3. CHUYỂN NHĂM TIỀN VÀO TÀI KHOẢN

Thủ đoạn: Các đối tượng cố ý chuyển nhầm tiền vào tài khoản của một người nào đó. Sau khi bên kia nhận được tiền, đối tượng sẽ giả danh là người thu hồi nợ của một công ty tài chính để liên hệ, dọa nạt và yêu cầu họ trả lại số tiền vừa nhận như một khoản vay với số lãi cắt cổ. Một trường hợp khác, đối tượng lừa đảo chuyển tiền cho người bị hại, sau đó liên hệ giới thiệu mình đang sống tại nước ngoài và muốn được nhận lại số tiền mình chuyển nhầm. Để trả lại số tiền, người nhận tiền phải sử dụng dịch vụ chuyển tiền quốc tế qua một đường link. Sau khi điền đầy đủ thông tin tài khoản ngân hàng vào đường link nói trên, toàn bộ số tiền trong tài khoản của bị hại sẽ bị rút sạch.

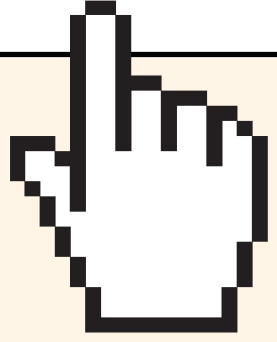
CẢNH BÁO LỪA ĐẢO



3. CHUYỂN NHẢM TIỀN VÀO TÀI KHOẢN



Cách thức xử lý



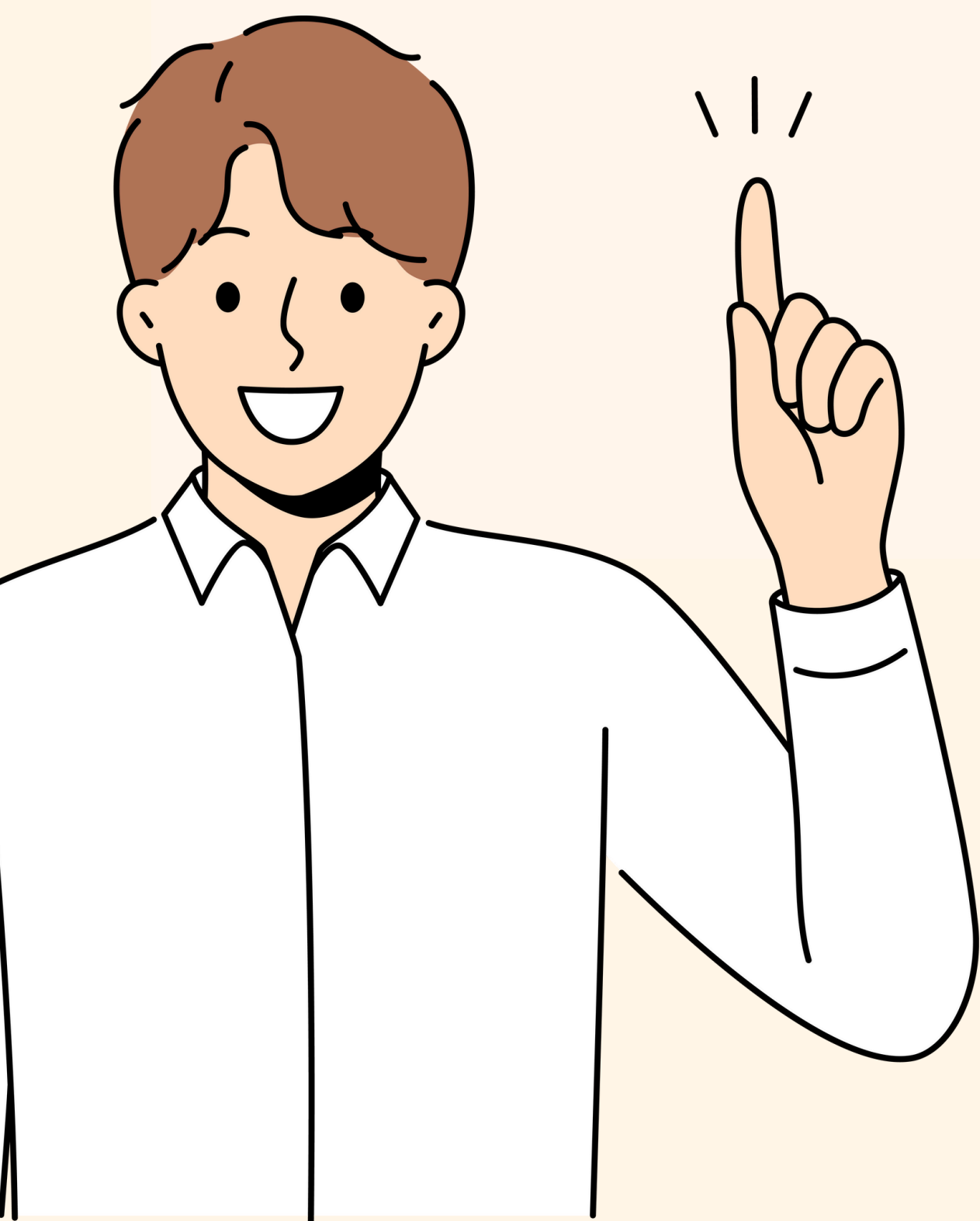
**Phải xử lý
như thế
nào?**

**Không sử dụng số tiền chuyển
nhầm vào mục đích cá nhân**

**Không chuyển trả lại khi chưa xác
định được chủ tài khoản ngân hàng
chuyển tiền đến**

**Tuyệt đối không làm theo
hướng dẫn của các đối tượng**

**Liên hệ ngân hàng hoặc cơ quan
Công an gần nhất để được giải quyết**

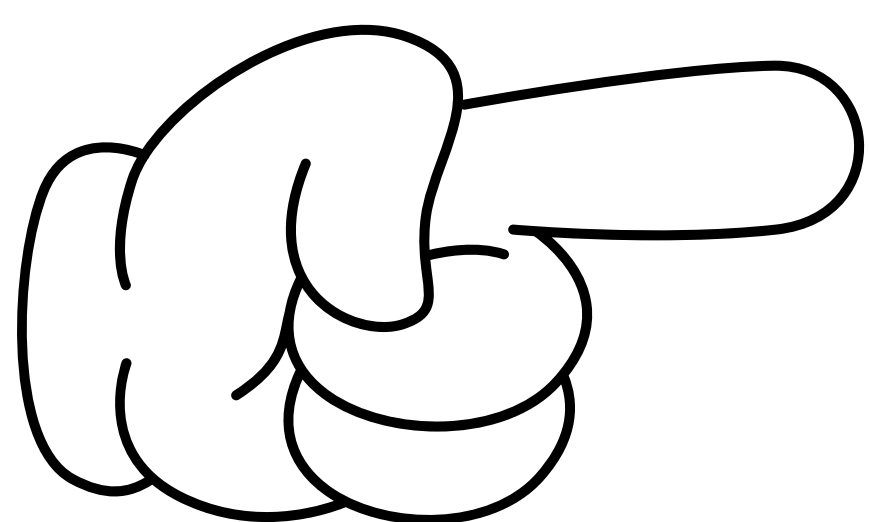


4. LỪA ĐẢO CỘNG TÁC VIÊN BÁN HÀNG ONLINE

Thủ đoạn: Các đối tượng hứa hẹn cho các nạn nhân được hưởng mức hoa hồng cao (chiều trò việc nhẹ, lương cao khi làm cộng tác viên bán hàng online).



Thời gian đầu, với các đơn hàng giá trị nhỏ, nạn nhân sẽ được hưởng hoa hồng đầy đủ. Sau đó, với những đơn hàng có giá trị cao, các đối tượng sẽ chiếm đoạt số tiền các nạn nhân ứng ra để nhận sản phẩm của các đơn hàng. Nhiều người, nhất là những bạn trẻ muốn tìm việc làm thêm hay những phụ nữ đang nuôi con nhỏ, ở nhà rảnh rỗi muốn có thêm thu nhập từ công việc online đã trở thành nạn nhân của các đối tượng lừa đảo kiểu này.



**VIỆC NHẸ MÀ LẠI LƯƠNG CAO
VẬY THÌ CHỈ CÓ LỪA ĐẢO MÀ THÔI
LÀM GIÀU MÀ DỄ THẾ À
THẾ THÌ AI CŨNG ĐẠI GIA CẢ RỒI.**

5. NHẬN QUÀ TẶNG MIỄN PHÍ

Thủ đoạn: Các đối tượng gọi điện giả danh các nhà phân phối, sàn thương mại điện tử nổi tiếng thông báo nạn nhân



nằm trong số các khách hàng may mắn được nhận quà miễn phí. Sau đó chúng yêu cầu nạn nhân kết bạn Zalo với nhân viên tư vấn. Tiếp theo các đối tượng sẽ gửi hàng loạt danh sách quà tặng. Nạn nhân chọn xong sẽ được thêm vào nhóm Telegram, nơi đó đồng bọn của các đối tượng liên tục tương tác khoe rằng đã nhận nhiều món quà lớn. Từ đó đánh vào tâm lý của nạn nhân. Khi gần như đã thao túng được tâm lý nạn nhân các đối tượng bắt đầu yêu cầu chuyển khoản để hoàn thành nhiệm vụ. Và như những thủ đoạn khác khi chiếm đoạt chúng sẽ ngắt liên lạc với nạn nhân.



Nhẹ dạ, cả tin, mong muốn nhận quà miễn phí



Không chuyển tiền ứng trước dù dưới bất kỳ hình thức nào

6. BẦY TÌNH

Thủ đoạn: Riêng với hình thức này được biến tướng dưới nhiều thủ đoạn, cách thức khác nhau, nhưng đều có điểm chung là đánh vào yếu tố tình cảm của nạn nhân:



1. Liên lạc thông qua các app hẹn hò, tạo mối quan hệ tình cảm với nạn nhân; chủ động gửi ảnh nhạy cảm, dùng lời lẽ thân mật dẫn dụ nạn nhân gửi lại hình ảnh nhạy cảm sau đó tổng tiền nạn nhân.
2. Làm quen với nạn nhân tự giới thiệu là người ngoại quốc, sau đó ngỏ ý muốn tặng quà, gửi ngoại tệ về nước. Yêu cầu nạn nhân tự nộp tiền vận chuyển, thuế, phí hải quan khi quà đến cửa khẩu rồi chiếm đoạt.

Đừng để sự hào hoa, hào nhoáng của vẻ bề ngoài đánh lừa. Tìm kiếm tình yêu thật qua thế giới "ảo" không dễ thế đâu bạn ơi!

7. KÊU GỌI TỪ THIỆN



Đây là chiêu trò lừa đảo hết sức tinh vi, các đối tượng đánh vào tâm lý thương người, mong muốn giúp đỡ người khác của mọi người: Chúng ngụy tạo ra những hoàn cảnh khó khăn, bị bệnh hiểm nghèo,... sau đó kêu gọi quyên góp hỗ trợ trên các nền tảng mạng xã hội. Khi tiền từ các nạn nhân đổ về tài khoản chúng nghiêm nhiên chiếm đoạt.



**LÒNG TỐT PHẢI ĐẶT ĐÚNG CHỖ
KHÔNG THÌ SẼ CÒN PHẢI KHỔ DÀI DÀI
KHI MÀ MUỐN GIÚP MỘT AI
KHÔNG TÌM HIỂU KỸ, NHẬN NGAY QUẢ LỪA**

8. KHÓA THUÊ BAO DI ĐỘNG

Thủ đoạn: Các đối tượng lừa đảo tự nhận là nhân viên nhà mạng gọi đến nạn nhân thông báo họ sắp bị khóa thuê bao do thuê bao không chính chủ và yêu cầu thực hiện theo các bước. Nếu không các đối tượng sẽ



đe dọa khóa thuê bao. Sau đó yêu cầu người dùng cung cấp CCCD, mã OTP thông báo về điện thoại, thực hiện theo một số bước từ đó có nguy cơ mất quyền kiểm soát SIM từ đó bị chiếm đoạt tài sản.

NOTES



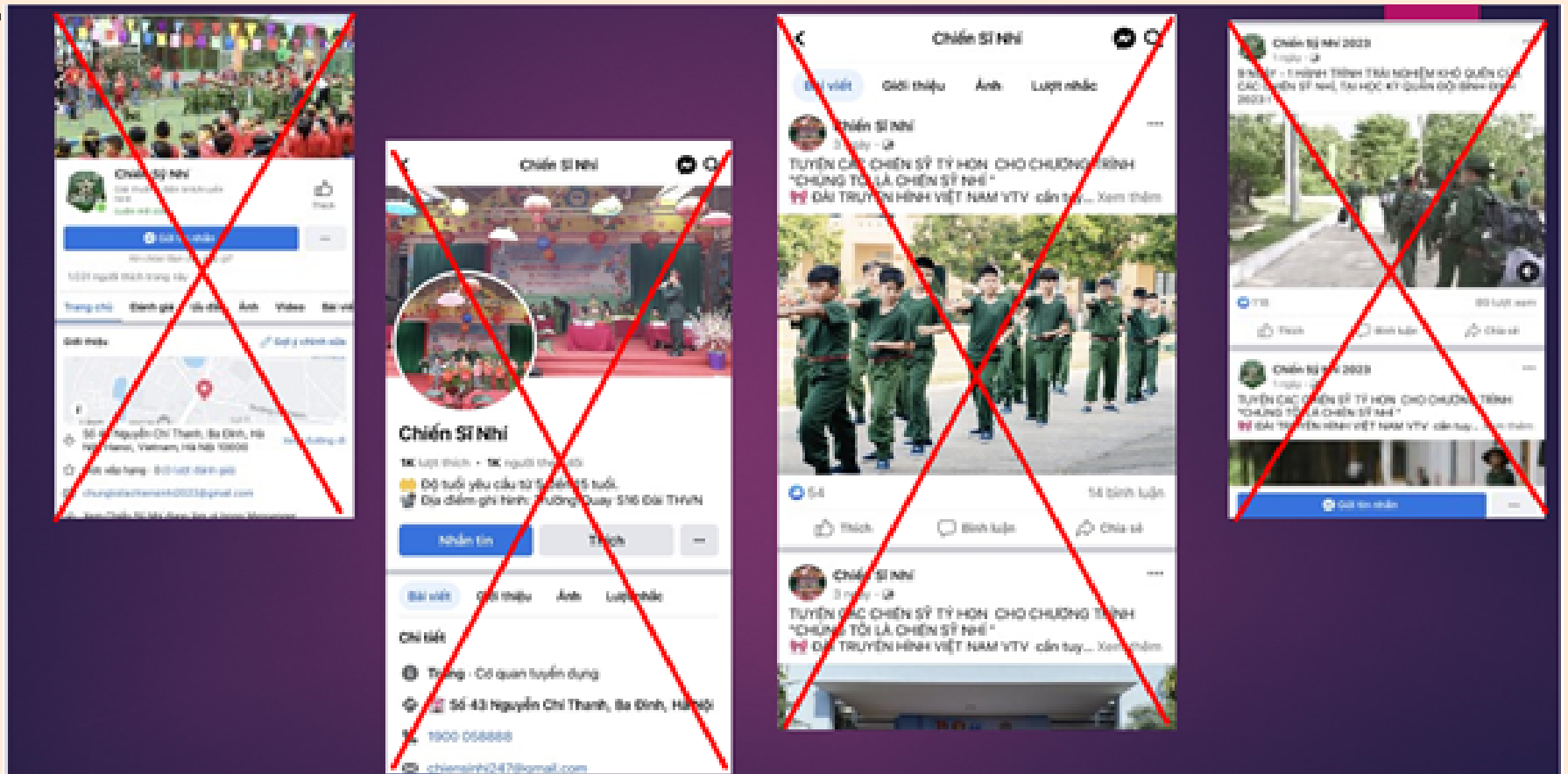
Để kiểm tra thông tin thuê bao soạn tin TTTB gửi 1414.

Mọi hoạt động liên quan đến thuê bao điện thoại nên được giao dịch tại quầy giao dịch.

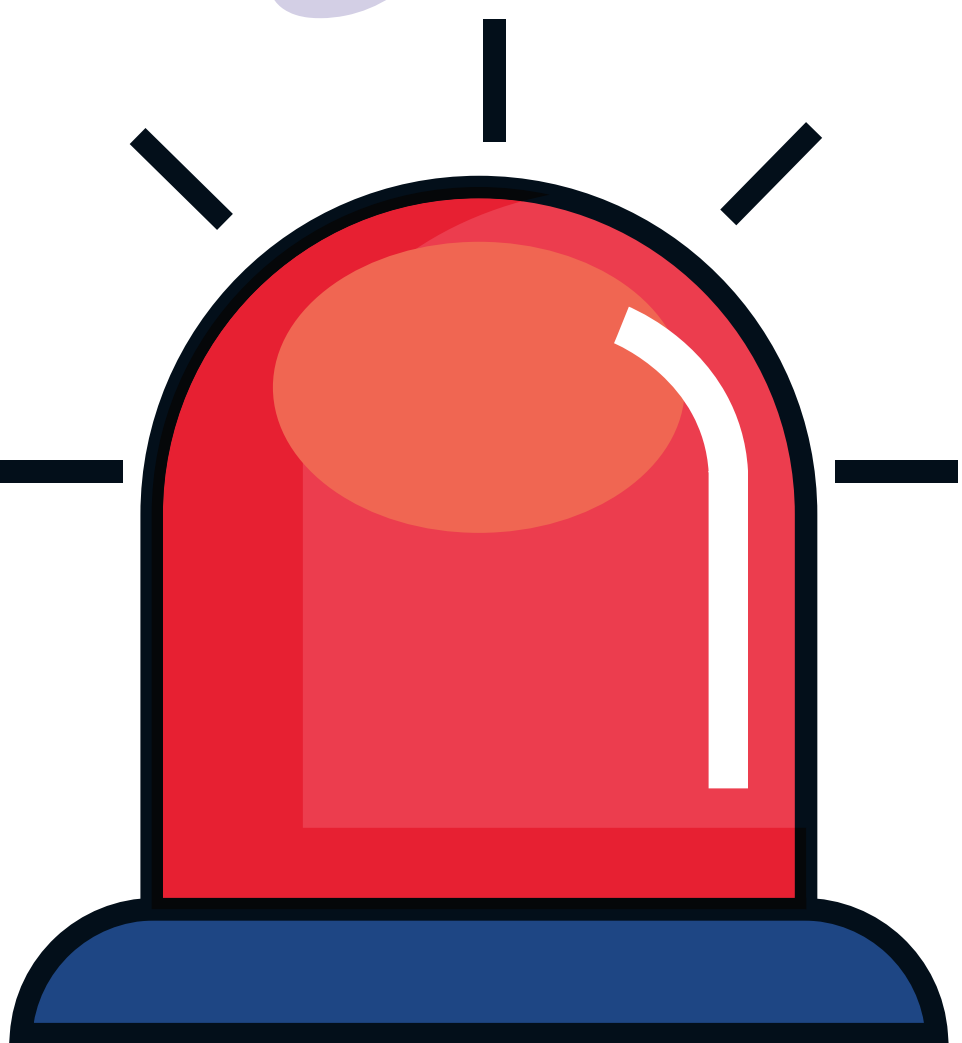
Không bị đe dọa bởi bất cứ lời lẽ nào.

9. CÁC CHƯƠNG TRÌNH NGOẠI KHÓA HÈ

Thủ đoạn: Đây là một dạng biến tướng của hình thức lừa đảo thực hiện nhiệm vụ mua hàng. Điểm mới ở đây là các đối tượng lợi dụng thời gian sắp vào mùa hè, nhu cầu của các phụ huynh học sinh về việc tìm kiếm cho con em các địa điểm, khóa học để tăng kỹ năng mềm trong mùa hè. Vì vậy các đối tượng đã tạo nên các chương trình ngoại khóa ảo, sau đó yêu cầu các nạn nhân thực hiện các nhiệm vụ mua hàng và chiếm đoạt tài sản.



NOTES



LUÔN LUÔN CẢNH GIÁC, KHÔNG CHUYỂN TIỀN, ỨNG TIỀN KHI CHƯA RÕ ĐỐI PHƯƠNG LÀ AI. KHÔNG THỰC HIỆN BẤT KỲ NHIỆM VỤ NÀO LIÊN QUAN ĐẾN TIỀN.

10. DEEP FAKE



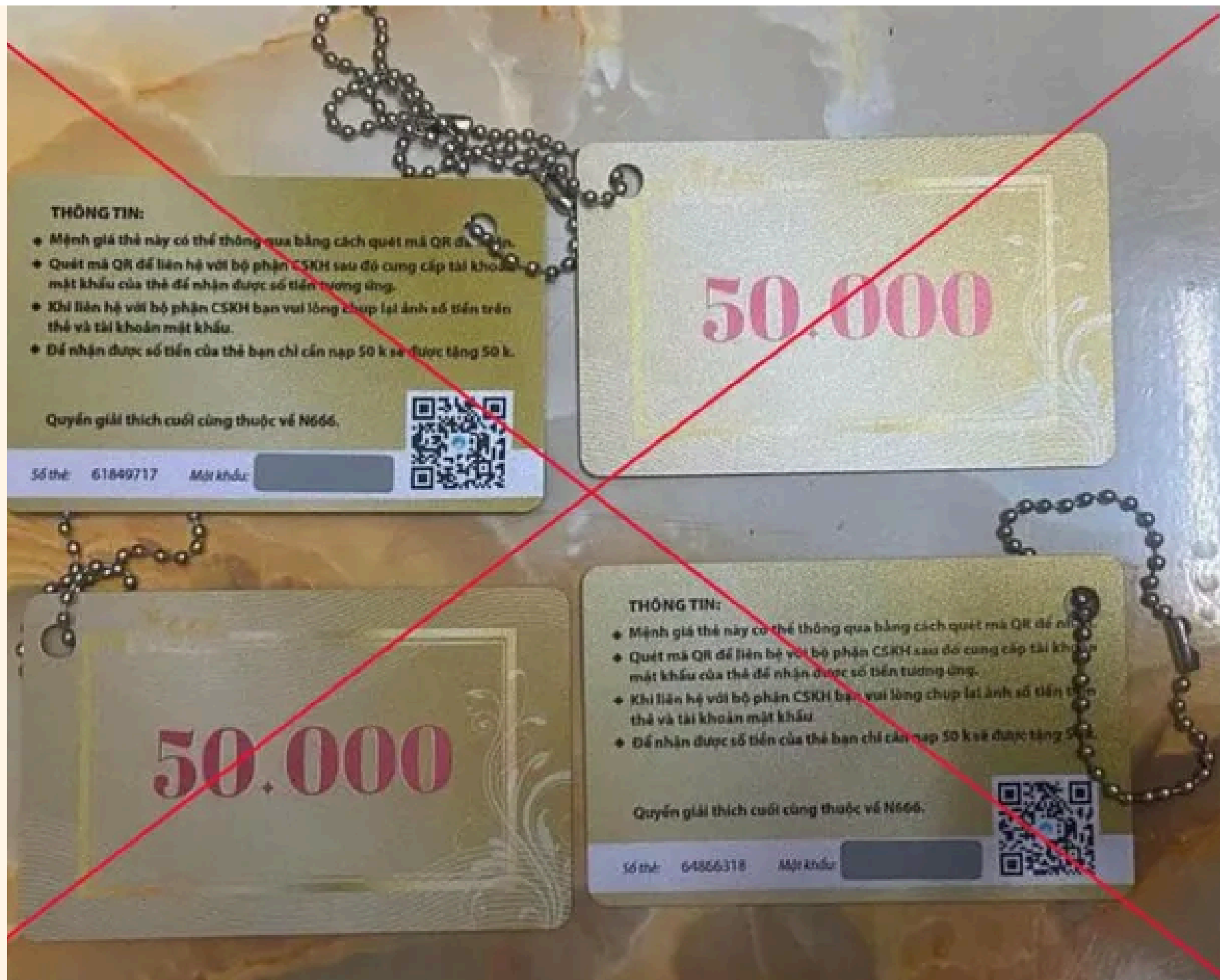
Thủ đoạn: Đây là thủ đoạn hết sức tinh vi của các đối tượng tội phạm, chúng sử dụng công nghệ AI để ghép mặt, giả giọng nói người quen của nạn nhân sau đó gọi điện video hòng tạo niềm tin với nạn nhân, sau đó yêu cầu chuyển tiền, chiếm đoạt tài sản.

Dấu hiệu nhận biết

1. Thời gian gọi rất ngắn, chỉ khoảng vài giây.
2. Khuôn mặt người gọi thiếu cảm xúc, bị “đơ”, các hành động không nhất quán với nhau.
3. Màu da không tương đồng và đồ bóng không đúng.
4. Ngắt giữa chừng, tài khoản chuyển tiền không phải là tài khoản của người gọi.

11. QUÉT THẺ QR CODE NHẬN TIỀN

Thủ đoạn: Các đối tượng lừa đảo treo các thẻ có chứa mã QR lên xe, cửa nhà hoặc khu vực đông dân cư nhằm thu hút sự chú ý của người dân. Các thẻ này có ghi một số mệnh giá



tiền nhất định, muốn nhận số tiền trên người dân phải quét mã QR để liên hệ bộ phận chăm sóc khách hàng. Tuy nhiên, khi quét mã sẽ dẫn đến đường link lạ, nếu tiếp tục thao tác theo sẽ bị chiếm quyền điều khiển điện thoại từ đó chiếm đoạt tài sản trong ngân hàng.

Biện pháp phòng ngừa

1. Không quét mã QR khi chưa xác thực được nội dung.
2. Nếu đã lỡ quét mã QR và nhận thấy các website lạ, nguy cơ giả mạo cao. Lập tức thoát ngay, tuyệt đối không truy cập vào các quảng cáo hiển thị trên website; không cung cấp bất cứ mã OTP nào được gửi đến điện thoại cho website.
3. Tuyên truyền, cảnh báo đến người thân và trình báo cơ quan chức năng gần nhất.

12. GIẢ DANH SHIPPER

Thủ đoạn: Các đối tượng lang thang trên các phiên livestream bán hàng trên mạng xã hội, sau đó các đối tượng tìm kiếm các khách hàng đã đặt hàng qua livestream, qua đó đã thu thập được các thông tin cần thiết của khách hàng như số điện

thoại, loại hàng đã đặt, địa chỉ nhận hàng. Sau đó, đối tượng gọi điện cho các nạn nhân, giả mạo là shipper thông báo đơn hàng đã đến nơi, nêu cụ thể các đặc điểm đơn hàng mà nạn nhân đã đặt; sau đó yêu cầu chuyển khoản trước (khi nạn nhân không có mặt tại nơi giao hàng); chúng thường nêu các lý do như: Cần hoàn thành chỉ tiêu trong ngày,... Khi nạn nhân chuyển tiền, đối tượng thông báo đã gửi nhầm số tài khoản và đó là số tài khoản đăng ký hội viên, nếu không hủy sẽ bị trừ phí hàng tháng; sau đó gửi kèm đường link để nạn nhân đăng nhập và hủy đăng ký hội viên. Nếu nạn nhân truy cập và làm theo sẽ bị chiếm quyền điều khiển tài khoản ngân hàng.



12. GIẢ DANH SHIPPER

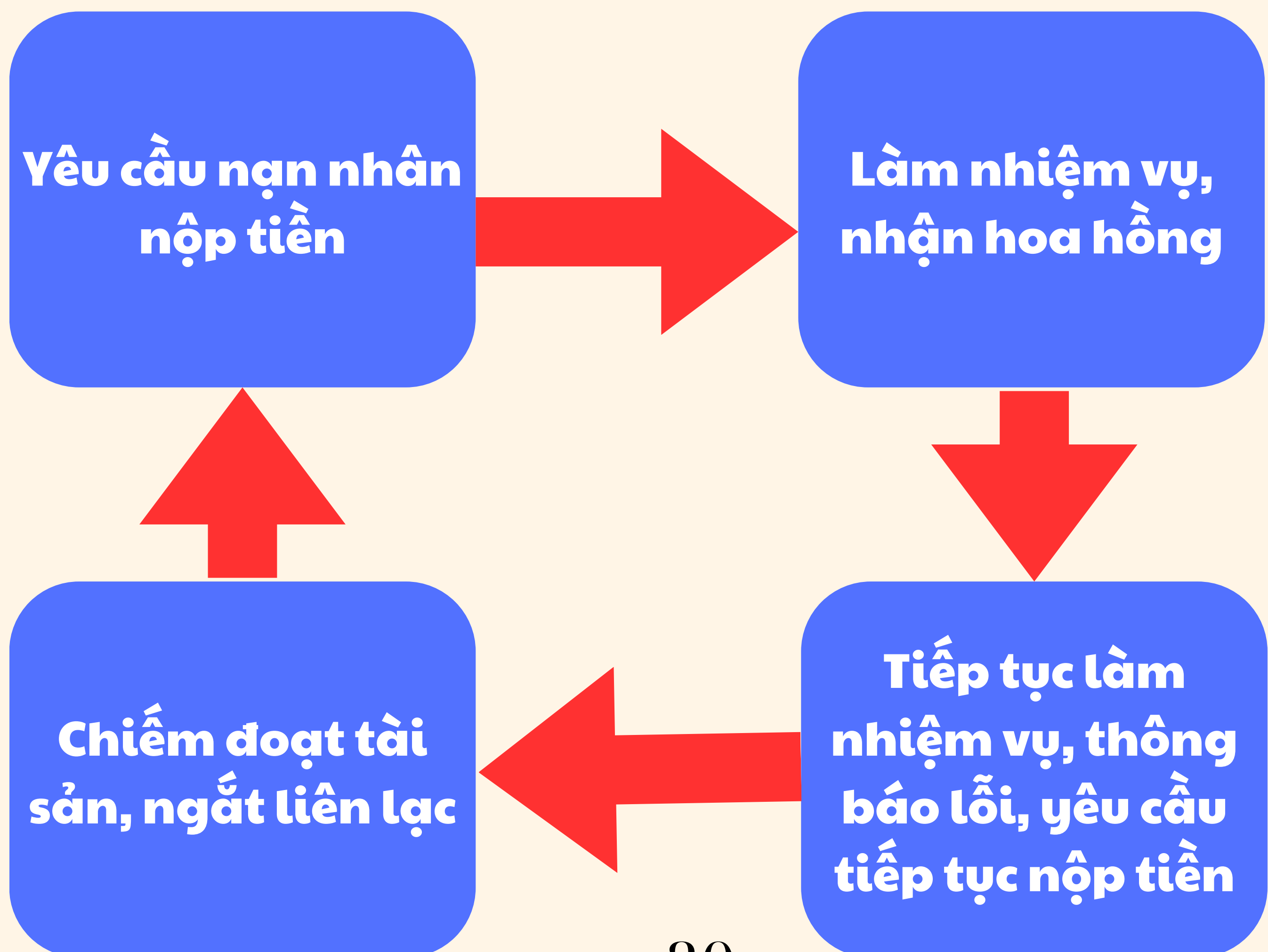
Biện pháp phòng ngừa

1. Không nhận bất cứ đơn hàng nào mình không đặt mua.
2. Không chuyển khoản hoặc thanh toán các đơn hàng không có ảnh chụp rõ mã vận đơn và thông tin người nhận.
3. Không click vào bất kỳ đường link lạ nào do người khác gửi đến.



13. ĐỌC SÁCH NHẬN LƯƠNG

Thủ đoạn: Các đối tượng giả mạo sử dụng hình ảnh, văn bản, công văn của các Công ty sách có thương hiệu và uy tín với bạn đọc điển hình như 1980Books để đăng quảng cáo tuyển dụng qua các nền tảng mạng xã hội hòng tìm kiếm nạn nhân. Khi các nạn nhân liên hệ, các đối tượng sẽ tiếp tục gửi các hợp đồng giả mạo, tinh vi hơn là có cả con dấu và chữ ký giả. Sau đó sẽ thêm nạn nhân vào các nhóm trên Telegram để thực hiện nhiệm vụ “đọc sách mỗi ngày để nhận lương”. Đến đây các đối tượng lại sử dụng phương pháp lừa đảo cũ:



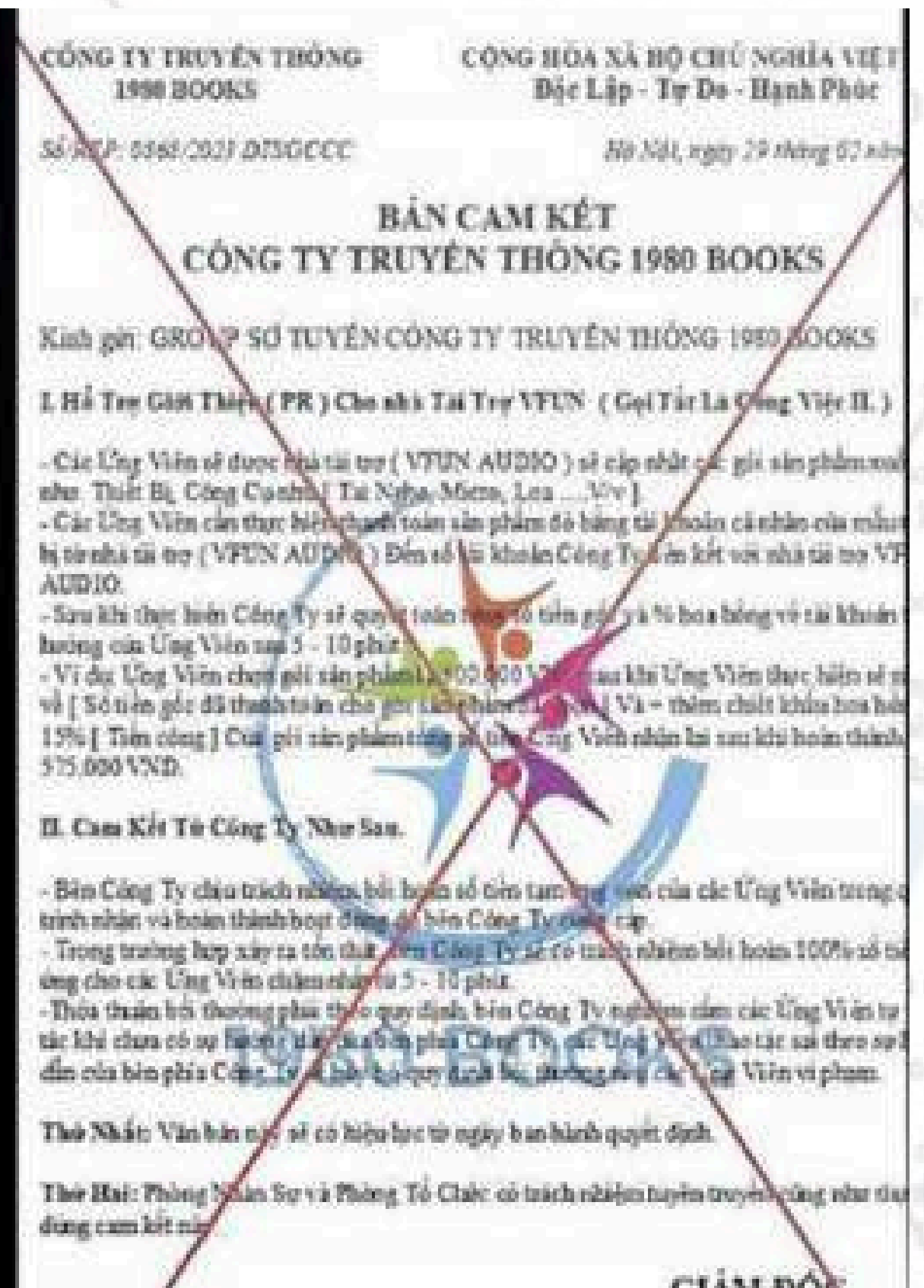
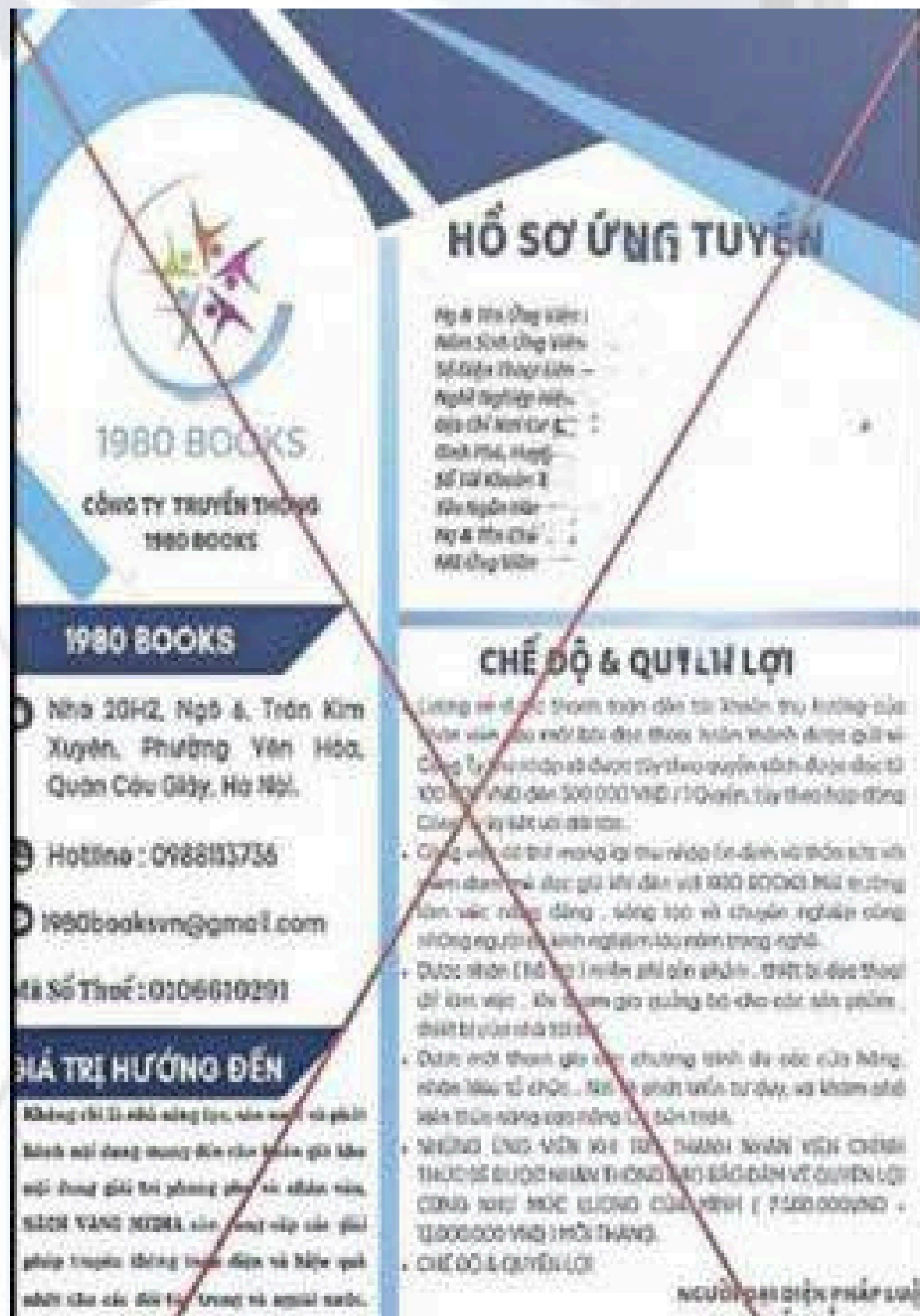
13. ĐỌC SÁCH NHẬN LƯƠNG

Biện pháp phòng ngừa

1. Không chủ động chuyển tiền cho bất cứ “người lạ” nào.

2. Tìm hiểu thật kỹ công việc được mời chào (qua các trang web chính thống).

3. KHÔNG TIN VÀO CÁC LỜI ĐỀ NGHỊ "VIỆC NHẸ LƯƠNG CAO".



14. HỖ TRỢ XÁC THỰC SINH TRẮC HỌC

Thủ đoạn: Các đối tượng lợi dụng quy định về việc phải xác thực sinh trắc học trong giao dịch ngân hàng để lừa đảo chiếm đoạt tài sản, trong thủ đoạn này chúng thường sử dụng 04 hình thức lừa đảo phổ biến gồm:

1. Gọi điện thoại hoặc kết bạn qua Zalo, Facebook

Mạo danh cán bộ ngân hàng, liên hệ với nạn nhân bằng các hình thức như gọi điện, nhắn tin, kết bạn qua các mạng xã hội như Zalo, Facebook... để hướng dẫn, thu thập thông tin sinh trắc học.

2. Lập nick gây nhầm lẫn

Một số đối tượng có thể lập nick gây nhầm lẫn như nhân viên ngân hàng, giả mạo hỗ trợ khách hàng, trà trộn tương tác với những bình luận của khách hàng dưới bài đăng trên mạng xã hội chính thức của ngân hàng để đề nghị khách hàng liên hệ riêng.



14. HỖ TRỢ XÁC THỰC SINH TRẮC HỌC

3. Yêu cầu cung cấp thông tin cá nhân

Yêu cầu khách hàng cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng, hình ảnh căn cước công dân, hình ảnh khuôn mặt, thậm chí cả giọng nói và cử chỉ của khách hàng để được hỗ trợ. Khi có được thông tin và tài khoản của người dùng, đối tượng xấu dễ dàng đăng nhập vào tài khoản và đánh cắp toàn bộ tiền của nạn nhân.

4. Yêu cầu truy cập vào đường link giả mạo

Yêu cầu người dùng truy cập vào đường link giả mạo do chúng tạo ra để tải và cài đặt ứng dụng thu thập sinh trắc học nhưng thực chất là tải về file có chứa mã độc, phần mềm gián điệp nhằm khai thác sâu hơn nữa những thông tin của nạn nhân.

Biện pháp phòng ngừa

1. Cảnh giác trước các cuộc gọi tự xưng là cán bộ nhân viên ngân hàng. Tuyệt đối không chia sẻ, cung cấp thông tin cá nhân cho người khác qua điện thoại, mạng xã hội.
2. Liên hệ trực tiếp đến số hotline của ngân hàng bạn đang sử dụng để được hỗ trợ giải quyết

15. CÁC QUỸ ĐẦU TƯ “ẢO”

Thủ đoạn: Các đối tượng tạo ra các sản phẩm giao dịch có tên gần giống với các sản phẩm đầu tư có danh tiếng. Sau khi dẫn dụ được các khách hàng đầu tư, trong một vài phiên giao dịch đầu, bằng thủ đoạn tạo các giao dịch ảo trên website và ứng dụng do các đối tượng cung cấp, tài khoản liên tục có lợi nhuận, thậm chí gấp nhiều lần số tiền đã nạp vào tài khoản, tuy nhiên khi muốn rút tiền thì ứng dụng báo lỗi hoặc báo chưa đủ hạn mức đối ứng. Các đối tượng tiếp tục dụ dỗ, lôi kéo, ép buộc nạn nhân chuyển thêm tiền vào tài khoản của chúng với nhiều lý do khác nhau. Khi thấy các nạn nhân không còn khả năng chuyển tiền, các đối tượng vô hiệu hóa tài khoản của nạn nhân hoặc khiến cho các tài khoản của nạn nhân không đăng nhập được nhằm chiếm đoạt số tiền mà nạn nhân đã nạp.



15. CÁC QUỸ ĐẦU TƯ “ẢO”

Biện pháp phòng ngừa

1. Người dân cần phải tìm hiểu kỹ càng thông tin trước khi tham gia đầu tư tài chính trên không gian mạng; chỉ nên tham gia đầu tư những sản giao dịch uy tín.
2. Thường xuyên tìm hiểu thông tin liên quan đến lĩnh vực đầu tư, luôn đối chiếu, so sánh thông tin, tìm hiểu thông tin từ nhiều nguồn khác nhau trước khi tham gia đầu tư.
3. Tuyệt đối không nên nghe và làm theo lời dụ dỗ về việc đầu tư tài chính trên không gian mạng từ những đối tượng không quen biết.



CÁC KỸ NĂNG CƠ BẢN ĐẢM BẢO AN TOÀN THÔNG TIN CÁ NHÂN

1

Hạn chế chia sẻ thông tin cá nhân trên không gian mạng

2

Thiết lập bảo mật hai lớp

3

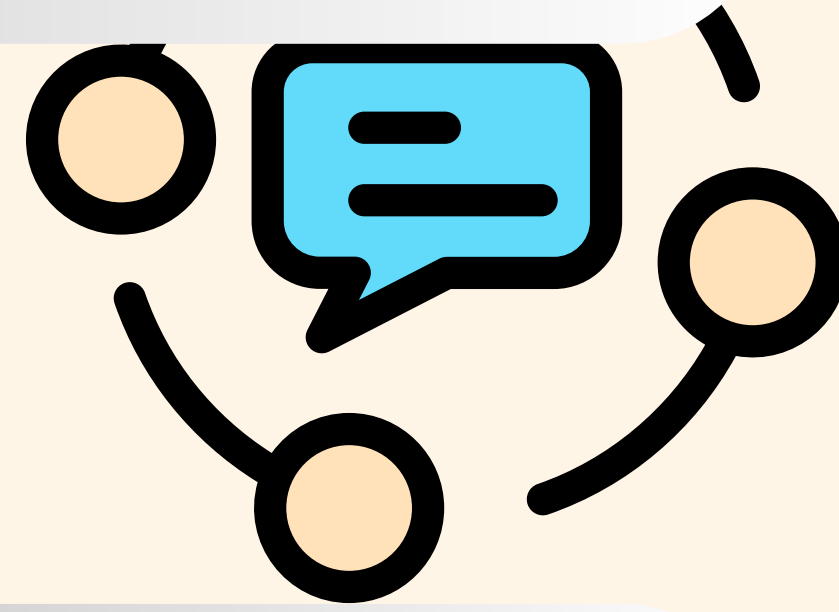
Chủ động tìm hiểu các mối đe dọa trên không gian mạng



1. HẠN CHẾ CHIA SẺ THÔNG TIN CÁ NHÂN

1

Không nên gửi thông tin cá nhân như căn cước công dân, hộ chiếu, bằng lái xe... qua mạng



Cảnh
báo

2

Chỉ cung cấp cho cá nhân, tổ chức thực sự tin tưởng



3

Không đăng tải hình ảnh và các thông tin cá nhân lên các trang mạng xã hội như: facebook, zalo, instagram,...

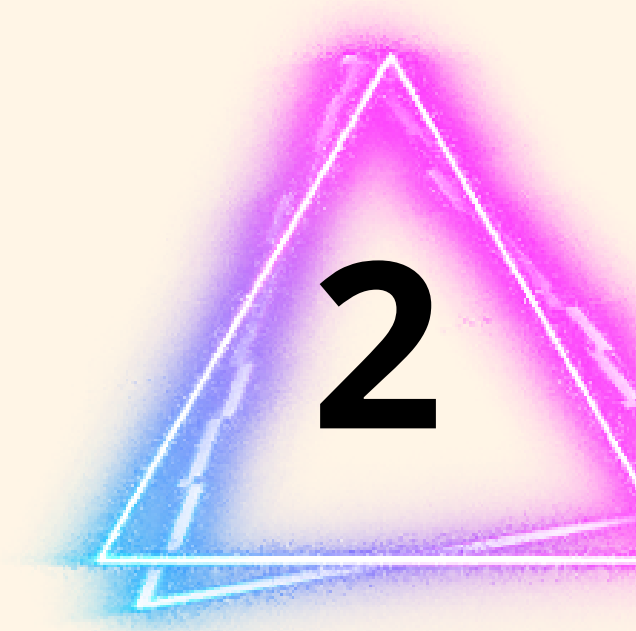


2. THIẾT LẬP BẢO MẬT HAI LỚP



1

Thiết lập mật khẩu bảo vệ các tài khoản mạng xã hội của bản thân. Chỉ đăng nhập trên các thiết bị và trang web “tin cậy”



2

Mật khẩu nên dài hơn 8 ký tự và bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt; nên đổi mật khẩu thường xuyên và không nên sử dụng mật khẩu giống nhau cho nhiều tài khoản khác nhau



3

Người dân cần lập mật khẩu 2 lớp để khi có kẻ xấu truy cập vào tài khoản của mình sẽ được cảnh báo đến điện thoại đã đăng ký với nhà cung cấp dịch vụ

3. CHỦ ĐỘNG TÌM HIỂU

- Luôn luôn chủ động tìm hiểu về các phương thức bảo mật thông tin, cập nhật những tin tức mới nhất về các mối đe dọa bảo mật và học cách phòng ngừa chúng.
- Cần sử dụng các công cụ bảo mật như phần mềm chống virus và phần mềm chống đánh cắp thông tin để bảo vệ tài khoản của mình trên các nền tảng mạng xã hội.

HÃY CHIA SẺ CẨM NANG NÀY ĐẾN NGƯỜI THÂN, BẠN BÈ ĐỂ CÙNG CHUNG TAY PHÒNG NGỪA LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG VÀ HÃY CÙNG NHAU ĐÓN CHỜ CÁC TẬP TIẾP THEO CÁC BẠN NHÉ!

Mọi thông tin, thắc mắc liên quan đến cẩm nang, vui lòng liên hệ đến Phòng Tham mưu, Công an tỉnh Quảng Ngãi, địa chỉ 174 Hùng Vương, phường Trần Phú, thành phố Quảng Ngãi./.