



CHỦ ĐỀ 4:

PHÒNG TRÁNH VÀ XỬ LÝ LỪA ĐẢO QUA MẠNG

Bài 3: Các biện pháp phòng tránh và xử lý tình huống lừa đảo qua mạng



MỤC TIÊU:

- Nắm được các biện pháp để phòng tránh các tình huống lừa đảo qua mạng
- Nắm được các cách xử lý khi là nạn nhân của lừa đảo qua mạng



1. Các biện pháp phòng tránh lừa đảo qua mạng

Bạn đã được tìm hiểu về các tình huống lừa đảo qua mạng phổ biến và cách nhận diện chúng để cảnh giác. Tuy nhiên, nhận diện chỉ là một phần của việc tự bảo vệ mình. Để giảm thiểu rủi ro, bạn cần *chủ động áp dụng các biện pháp phòng tránh ngay từ đầu*. Đồng thời, nếu trở thành mục tiêu nhắm tới của những kẻ lừa đảo, việc *xử lý đúng cách* sẽ giúp bạn tránh được nguy cơ trở thành nạn nhân.



Để bảo vệ an toàn cho chính mình và những người xung quanh, bạn có thể tham khảo công thức **3 KHÔNG - 3 KIỂM TRA - 3 CHỦ ĐỘNG** sau đây.

3 KHÔNG



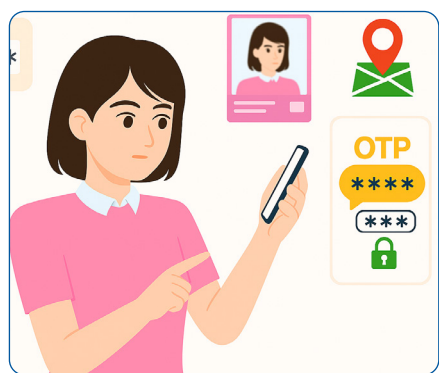
1 - KHÔNG vội vàng bị dẫn dụ, hoảng sợ, hay mềm lòng: Hãy luôn nhớ rằng kẻ lừa đảo thường áp dụng các chiêu trò thao túng tâm lý như đưa ra những khoản lợi trước mắt, xây dựng hình ảnh và hồ sơ hoàn hảo, đặt ra tình

huống khẩn cấp hoặc kể câu chuyện đáng thương. *Giữ bình tĩnh và không để tâm lý bị thao túng* là bước đầu tiên và quan trọng nhất trong mọi tình huống. (Ví dụ, nếu có người gọi điện tự xưng là công an, hãy giữ bình tĩnh, vì cơ quan chức năng thường chỉ làm việc với người dân qua văn bản chính thức hoặc tại trụ sở, không giải quyết qua điện thoại.)



2 - KHÔNG thực hiện các yêu cầu đáng ngờ trước khi xác minh: Mọi yêu cầu như nhấp vào đường dẫn, tải phần mềm, đăng nhập tài khoản, gửi ảnh, gặp mặt, chuyển tiền, thanh toán, đầu tư... đều tiềm ẩn rủi ro. Hãy luôn

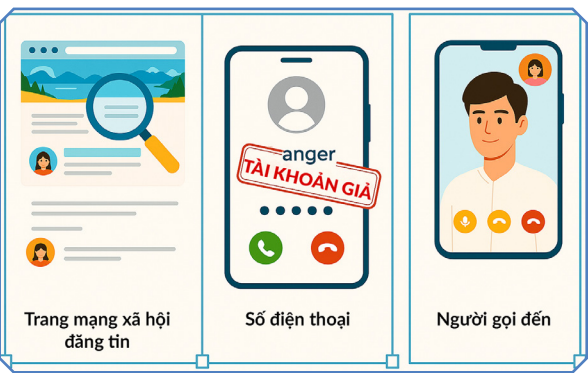
cảnh giác và chỉ thực hiện khi đã xác minh rõ ràng nguồn gốc và tính xác thực của yêu cầu.



3 - KHÔNG chia sẻ thông tin cá nhân: Không tiết lộ *căn cước, tài khoản ngân hàng, OTP, mật khẩu, địa chỉ, hình ảnh riêng tư* tùy tiện, đặc biệt là trên mạng xã hội hoặc cho người lạ khi được tiếp cận và yêu cầu. Việc chia

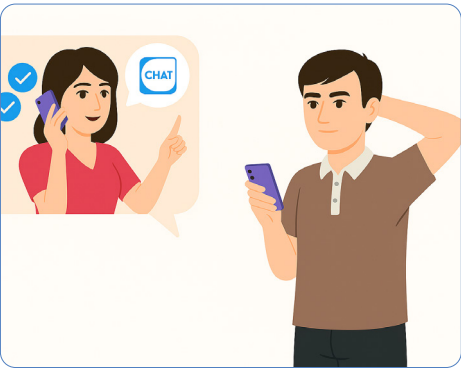
sẻ quá nhiều thông tin khiến kẻ lừa đảo có nhiều dữ liệu để xây dựng kịch bản nhắm tới bạn. Hãy thận trọng khi nói chuyện hoặc kết bạn với người lạ, hoặc nhận được yêu cầu “xác thực tài khoản”, hay cuộc gọi giả danh ngân hàng, cơ quan chức năng.

3 KIỂM TRA



1 - KIỂM TRA nguồn (kênh hoặc người liên hệ): Hãy luôn kiểm tra tính xác thực và độ uy tín của các nguồn thông tin, bao gồm trang mạng xã hội đăng tin, tài khoản liên hệ, số điện thoại, và người gọi đến. Ví dụ, nếu bạn nhận được cuộc gọi

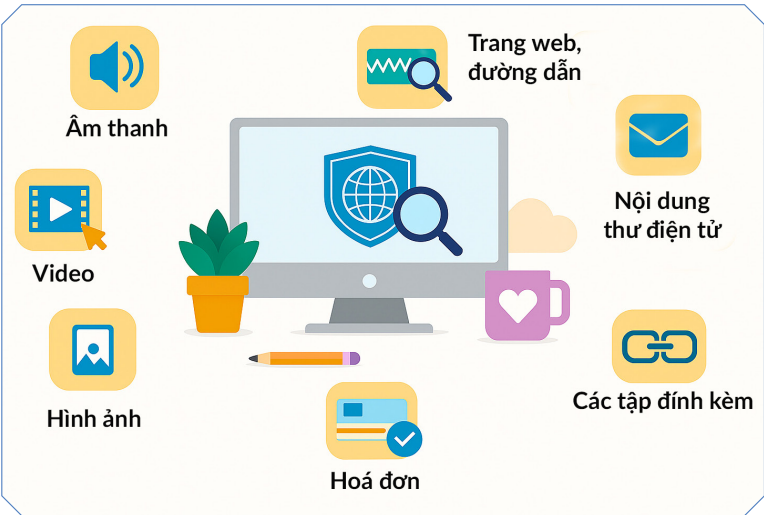
từ ngân hàng, đừng vội làm theo yêu cầu. Hãy kiểm tra xem số điện thoại đó có phải số chính thức của ngân hàng hay không bằng cách tra cứu trên website hoặc gọi tổng đài chính thức.



2 - KIỂM TRA nội dung tình huống: Hãy xác minh lại nội dung tình huống mà bạn gặp phải. Ví dụ, nếu có ai đó hỏi mượn tiền bạn qua mạng xã hội, hãy liên hệ với họ bằng một phương thức khác hoặc gặp mặt để xác minh.

Đừng vội vàng tin vào bất cứ điều gì vì mọi thứ đều có thể chỉ là bịa đặt.

3 - KIỂM TRA các bằng chứng: Hãy kiểm tra kỹ các bằng chứng trong tình huống như các trang web, đường dẫn, nội dung thư điện tử, các tập đính kèm, hóa đơn, hình ảnh, video hoặc âm thanh mà bạn nhận được (theo hướng dẫn ở Bài 2, Chủ đề 4). Hãy nhớ rằng công nghệ ngày nay (như “deepfake”, “deepvoice”) có thể giúp kẻ lừa đảo tạo dựng các bằng chứng chân thực tới mức rất khó nhận diện.



3 CHỦ ĐỘNG



1 - CHỦ ĐỘNG thực hành an toàn số:

Các thực hành về an toàn số mà bạn cần thực hiện như bảo mật các thông tin, đặt mật khẩu mạnh, cài đặt xác thực đa yếu tố, cài đặt quyền riêng tư v.v (Tham khảo Chủ đề 2 và Chủ đề 3)

là những điều cơ bản để giúp bạn bảo vệ toàn diện và giảm thiểu các nguy cơ bị lừa đảo.



2 - CHỦ ĐỘNG cảnh báo với cộng

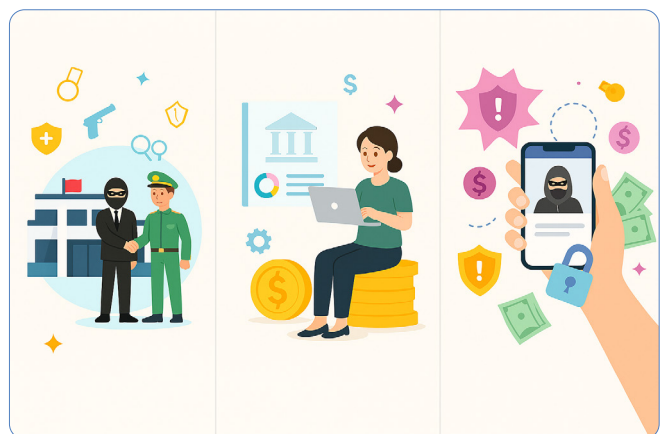
đồng: Chia sẻ và tuyên truyền về phòng tránh lừa đảo không chỉ giúp bảo vệ những người xung quanh mà còn giảm nguy cơ cho chính bạn. Nếu tài khoản của bạn bị chiếm đoạt, hãy

cảnh báo ngay cho người thân, bạn bè để họ không bị lừa bởi kẻ giả mạo.

3 - CHỦ ĐỘNG báo cáo

các tình huống: Khi gặp tình huống lừa đảo, ngay cả khi chưa bị lừa, hãy báo cáo cho ngân hàng, nền tảng mạng xã hội hoặc cơ quan chức năng. Việc này giúp ngăn

chặn kẻ lừa đảo tiếp tục hoạt động, cảnh báo cộng đồng và bảo vệ những người khác khỏi rủi ro tương tự



2. Cách xử lý khi là nạn nhân của lừa đảo qua mạng

BƯỚC 1: CẦN LÀM NGAY

Ngay khi phát hiện bị lừa đảo, bạn hãy thực hiện *càng sớm càng tốt* các việc sau đây:

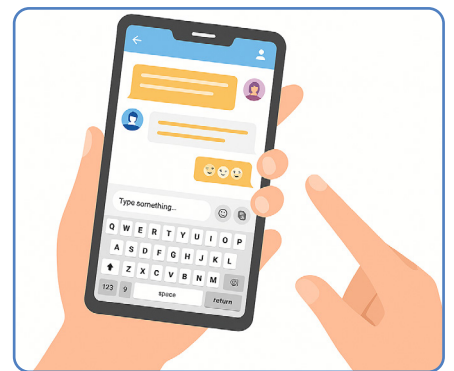
- Dừng mọi giao dịch chuyển tiền
- Liên hệ các đơn vị liên quan như ngân hàng, ví điện tử, đơn vị phát hành thẻ... để yêu cầu hỗ trợ khóa tài khoản và ngừng giao dịch. Dừng ngay các cuộc trò chuyện với kẻ lừa đảo để ngừng bị thao túng
- Rà soát và đổi mật khẩu các tài khoản quan trọng nếu có nguy cơ bị xâm nhập



BƯỚC 2: LƯU GIỮ

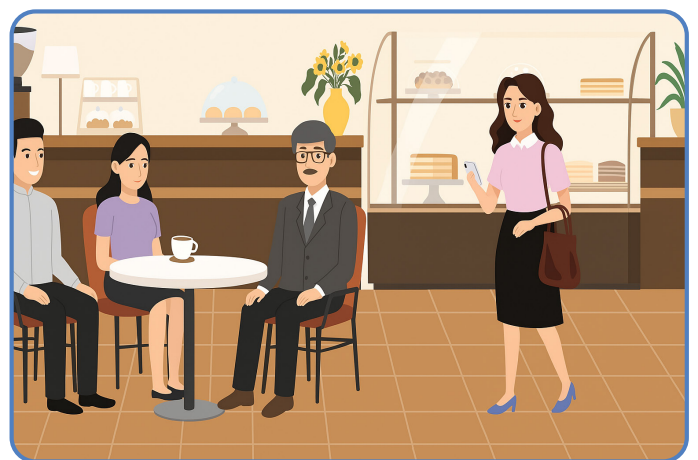
Việc lưu giữ lại *các bằng chứng và thông tin của kẻ lừa đảo* có thể sẽ giúp bạn trong quá trình xử lý vụ việc. Hãy chụp lại và lưu lại các thông tin sau đây:

- Tin nhắn, email, lịch sử giao dịch v.v
- Thông tin của kẻ lừa đảo (trang web, tin nhắn, số điện thoại v.v)



BƯỚC 3: BÁO CÁO

Báo cáo vụ việc kèm theo bằng chứng để ngăn chặn kẻ xấu tiếp tục lừa đảo cũng như được tư vấn hướng khắc phục hậu quả. Bạn có thể:

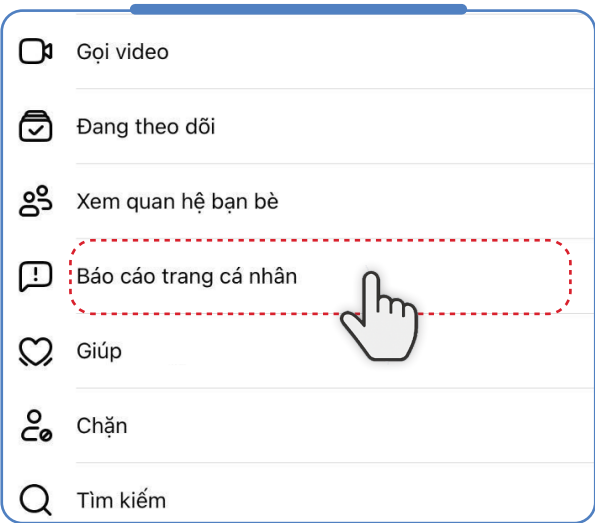


- Báo cáo tài khoản lừa đảo trên các nền tảng mạng xã hội (*tham khảo hướng dẫn bên dưới**).
- Liên hệ cơ quan chức năng như công an khu vực hoặc đường dây nóng Cảnh sát 113 để phản ánh và nhờ hỗ trợ xử lý.
- Cảnh báo cho gia đình và bạn bè để họ có thể đề phòng những trò lừa đảo tương tự có thể xảy ra.

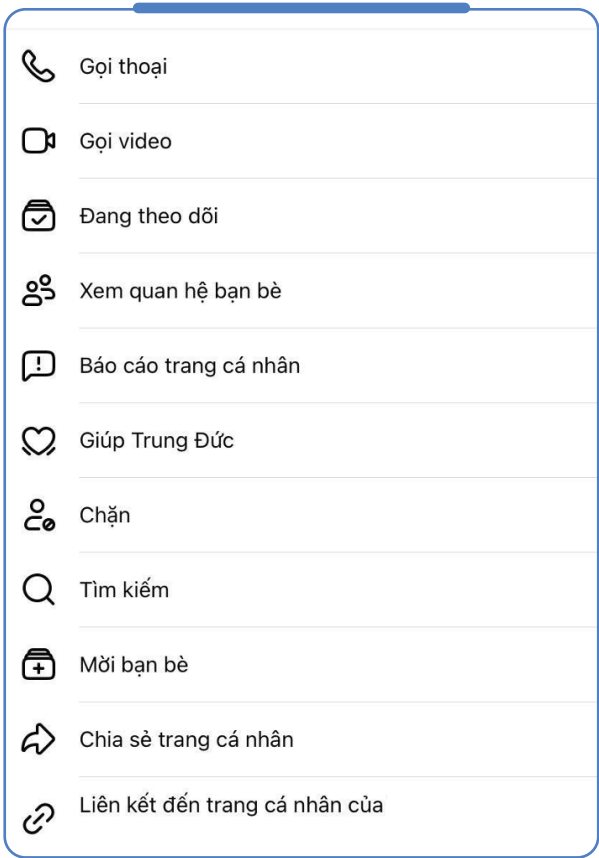
(*) Mỗi nền tảng có cách báo cáo tài khoản khác nhau. Sau đây là hướng dẫn báo cáo tài khoản lừa đảo trên mạng xã hội Facebook:



BƯỚC 1: Vào trang cá nhân của tài khoản đó, bấm vào dấu ba chấm



BƯỚC 2: Chọn **Báo cáo trang cá nhân**



BƯỚC 3: Chọn nội dung báo cáo phù hợp, sau đó xác nhận để hoàn tất.

Như vậy, bạn vừa tìm hiểu các biện pháp phòng tránh và các bước xử lý khi gặp lừa đảo qua mạng. Tuy nhiên, hãy lưu ý rằng các thủ đoạn và kỹ thuật kẻ gian sử dụng sẽ ngày càng tinh vi và phức tạp hơn. Do đó, việc *thường xuyên cập nhật thông tin và cảnh báo từ các kênh truyền thông chính thống và các cơ quan chức năng là vô cùng cần thiết* để giúp bạn bảo vệ an toàn cho bản thân và những người thân xung quanh.

Nội dung chính cần ghi nhớ

1. Công thức 3 KHÔNG - 3 KIỂM TRA - 3 CHỦ ĐỘNG để phòng tránh lừa đảo qua mạng:

- 3 KHÔNG:

- + Không bị dẫn dụ/ hoảng sợ/ mềm lòng
- + Không thực hiện các yêu cầu đáng ngờ trước khi xác minh
- + Không chia sẻ thông tin cá nhân

- 3 KIỂM TRA:

- + Kiểm tra nguồn/ người liên hệ
- + Kiểm tra nội dung tình huống
- + Kiểm tra các bằng chứng

- 3 CHỦ ĐỘNG:

- + Thực hành an toàn số
- + Cảnh báo với cộng đồng
- + Báo cáo tình huống

2. Công thức 3 bước (CẦN LÀM NGAY - LƯU GIỮ - BÁO CÁO) để xử lý khi là nạn nhân của lừa đảo qua mạng

- **CẦN LÀM NGAY:** Khóa tài khoản và dừng mọi giao dịch ngay khi phát hiện dấu hiệu lừa đảo.
- **LƯU GIỮ:** Lưu lại bằng chứng (tin nhắn, email...) và thông tin kẻ lừa đảo.
- **BÁO CÁO:** Liên hệ với ngân hàng, nền tảng và cơ quan chức năng để báo cáo vụ việc.

