

CHỦ ĐỀ 4:
PHÒNG TRÁNH VÀ XỬ LÝ LỪA ĐẢO QUA MẠNG

Bài 1: Tổng quan về lừa đảo qua mạng



MỤC TIÊU:

- Hiểu lừa đảo qua mạng là gì và thực trạng lừa đảo qua mạng trên thế giới và Việt Nam
- Biết tới các loại lừa đảo qua mạng (phân loại theo dạng tình huống)
- Hiểu và cảnh giác về chiến lược của kẻ lừa đảo qua mạng nhằm tới các đối tượng khác nhau



1. Lừa đảo qua mạng là gì?

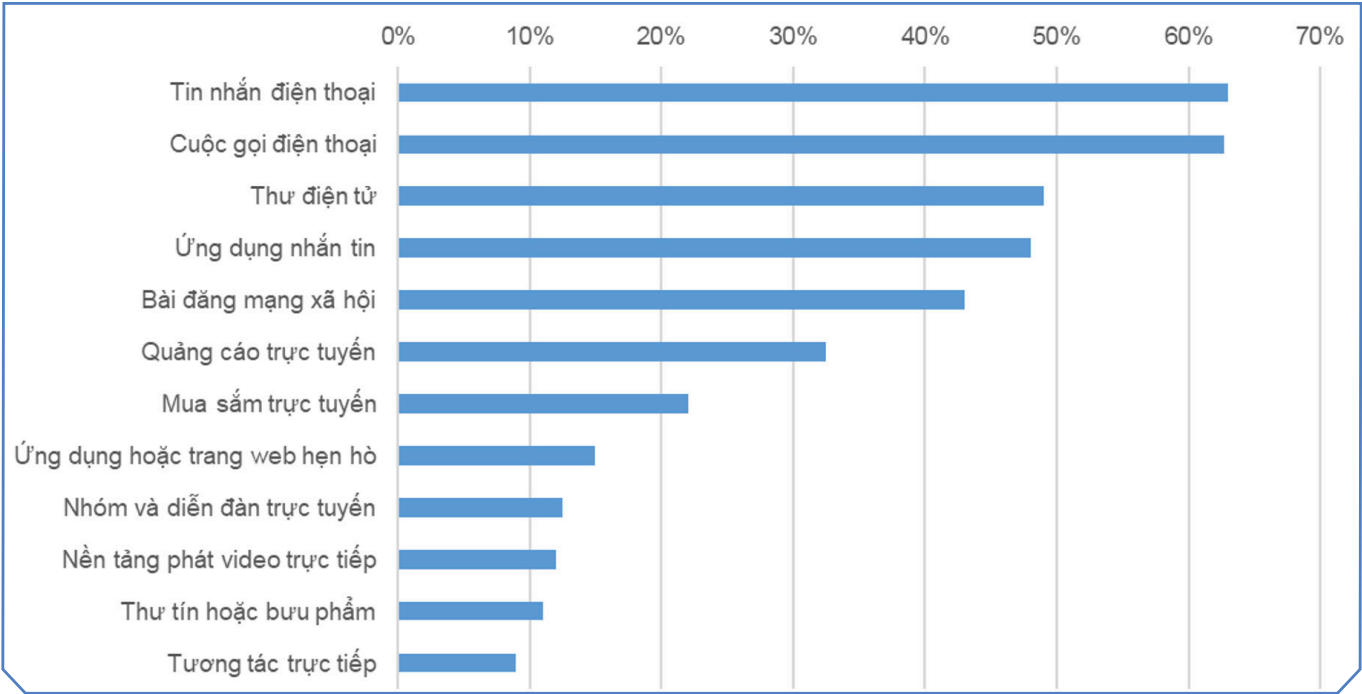


Lừa đảo là hành vi gian lận nhằm đánh cắp các tài sản có giá trị, ví dụ như tiền bạc, thông tin cá nhân, tình cảm...

Lừa đảo qua mạng là hành vi lừa đảo diễn ra ở bất cứ đâu trên môi trường mạng, bao gồm **mạng viễn thông** (qua cuộc gọi, tin nhắn) hoặc **mạng Internet** (qua mạng xã hội, trang web, thư điện tử, ứng dụng nhắn tin, ứng dụng hẹn hò...).

2. Thực trạng lừa đảo qua mạng trên thế giới và Việt Nam

Theo báo cáo của Liên minh chống lừa đảo toàn cầu (GASA)¹, năm 2024, gần một nửa dân số toàn cầu gặp phải những tình huống lừa đảo ít nhất một lần mỗi tuần. Đa số các tình huống lừa đảo trên thế giới là lừa đảo qua mạng, thông qua hai kênh phổ biến nhất là cuộc gọi và tin nhắn điện thoại (Hình 2.1). Đây cũng được báo cáo là hai kênh lừa đảo phổ biến nhất ở Việt Nam.



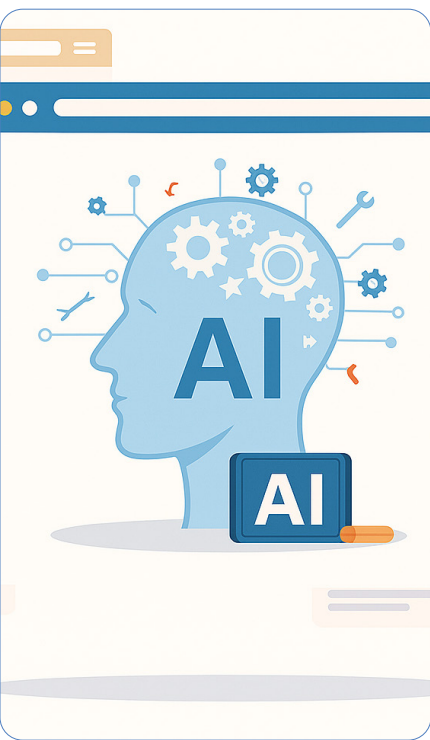
Hình 2.1. Các kênh tiếp cận của kẻ lừa đảo trên toàn cầu (Nguồn: GASA, 2024)

Cũng theo báo cáo của GASA, năm 2024, khoảng 1,03 nghìn tỷ đô la Mỹ đã rơi vào tay những kẻ lừa đảo. Để dễ hình dung, bạn có thể so sánh số tiền này vượt qua tổng tài sản của 5 tỷ phú giàu nhất trên thế giới năm 2024² và lớn hơn cả GDP³ hay giá trị nền kinh tế trong năm của một quốc gia phát triển như Thụy Sĩ.

1 <https://www.gasa.org/research>

2 <https://vcci.com.vn/news/dem-tai-san-top-10-nguoi-giau-nhat-the-gioi-dau-nam-2025>

3 GDP là “Gross Domestic Product”, có nghĩa là tổng sản phẩm quốc nội - là một chỉ tiêu thường được dùng để đo lường tổng giá trị thị trường đối với tất cả các hàng hoá cũng như dịch vụ được sản xuất trong phạm vi lãnh thổ một quốc gia trong một khoảng thời gian nhất định. GDP của Thụy Sĩ năm 2024 đạt khoảng 942 tỷ đô la Mỹ.



Công nghệ mới, đặc biệt là *trí tuệ nhân tạo (AI)*, ngày càng bị lạm dụng trong các vụ lừa đảo trực tuyến. Theo GASA (2024), chỉ 16% người dùng toàn cầu tin rằng họ chưa từng bị AI tấn công, trong khi phần lớn đã tiếp xúc với nội dung giả mạo. Công nghệ deepfake giúp kẻ gian tạo video, giọng nói giả mạo cực kỳ chân thực, khiến lừa đảo tinh vi và nguy hiểm hơn. Đây là lời cảnh báo rằng mỗi người cần nâng cao cảnh giác, trang bị kiến thức và kỹ năng để nhận diện, đối phó với các chiêu trò lừa đảo ngày càng phức tạp.



Tại Việt Nam, các vụ việc lừa đảo qua mạng cũng ngày càng gia tăng và diễn biến phức tạp. Chỉ trong vòng một tuần (từ ngày 23 đến 29/12/2024), hệ thống kỹ thuật của Cục An toàn thông tin đã ghi nhận 7.083 phản ánh lừa đảo qua mạng do người dùng Internet Việt Nam gửi về⁴. Đây chỉ là phần nổi của tảng băng chìm, vì theo khảo sát của Hiệp hội An ninh mạng quốc gia năm 2024, chỉ có khoảng gần một nửa những nạn nhân báo cáo khi gặp các vụ việc lừa đảo qua mạng. Cũng theo khảo sát này, cứ 220 người dùng thì có 1 người là nạn nhân của lừa đảo qua mạng. Tổng thiệt hại do lừa đảo qua mạng gây ra trong năm 2024 ước tính lên tới 18.900 tỷ VNĐ⁵.

4 <https://www.vietnamplus.vn/7000-phan-anh-lua-dao-truc-tuyen-37-trang-web-bi-tan-cong-trong-vong-1-tuan-post1005669.vnp>

5 <https://www.nca.org.vn/news/detail/bao-cau-tong-ket-an-ninh-mang-nam-2024-khu-vuc-nguoi-dung-ca-nhan?l=vi>



Từ đầu năm 2025, Việt Nam đã triệt phá nhiều đường dây lừa đảo qua mạng quy mô lớn, gây thiệt hại hàng nghìn tỷ đồng. Ngày 15/1/2025, lực lượng chức năng triệt phá một đường dây xuyên biên giới giả danh cơ quan chức năng, chiếm đoạt gần 1.000 tỷ đồng từ 13.000 nạn nhân⁶. Trước đó, ngày 10/1/2025, công an Đà Nẵng triệt phá một đường dây lừa đảo và rửa tiền quốc tế do người nước ngoài cầm đầu, lừa 1.800 tỷ đồng qua ứng dụng đầu tư giả mạo⁷. Những nỗ lực này thể hiện quyết tâm mạnh mẽ của cơ quan chức năng trong việc đấu tranh với tội phạm mạng. Tuy nhiên, bên cạnh các biện pháp phòng chống từ phía các cơ quan quản lý, *mỗi cá nhân hay doanh nghiệp cũng cần chủ động nâng cao cảnh giác, trang bị kiến thức để nhận diện và ứng phó hiệu quả với các thủ đoạn lừa đảo*, góp phần giảm thiểu thiệt hại và bảo vệ an toàn cho bản thân cũng như cộng đồng.

3. Phân loại lừa đảo qua mạng theo dạng tình huống

Hiện nay, các hình thức và chiêu trò lừa đảo qua mạng ngày càng trở nên đa dạng và tinh vi. Theo một thống kê năm 2023, có tới 24 *tình huống* lừa đảo trên không gian mạng tại Việt Nam nhắm tới các đối tượng khác nhau như người cao tuổi, trẻ em, sinh viên, công nhân, nhân viên văn phòng v.v⁸

6 https://www.vietnamplus.vn/triet-pha-duong-day-lua-dao-xuyen-bien-gioi-gan-1000-ty-dong-post1009286.vnp?utm_source=chatgpt.com

7 https://nhandan.vn/cong-an-da-nang-triet-pha-duong-day-lua-dao-rua-tien-quoc-te-len-den-1800-ty-dong-post857873.html?utm_source=chatgpt.com

8 <https://baochinhphu.vn/nhan-dien-24-hinh-thuc-lua-dao-truc-tuyen-cung-nhieu-hinh-thuc-dan-du-khac-nhau-102230703162727607.htm>

Để dễ dàng nhận diện và đưa ra các giải pháp phòng tránh phù hợp, chúng ta cần phân loại các hình thức lừa đảo qua mạng, từ đó xây dựng *chiến lược đối phó riêng* cho từng loại. Có rất nhiều cách để phân loại lừa đảo qua mạng. Ở góc độ người dùng, để dễ tiếp cận nhất, bạn có thể *phân loại lừa đảo qua mạng theo các dạng tình huống*, cụ thể như sau:

(1) Lừa đảo tài chính



Lừa đảo qua mạng liên quan trực tiếp tới các **giá trị vật chất**. Hệ lụy của lừa đảo tài chính chủ yếu là mất mát về vật chất. Một số tình huống:

- Lừa đảo tuyển cộng tác viên trực tuyến
- Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu
- Lừa đảo tuyển người mẫu nhí
- Giả mạo biên lai chuyển tiền thành công
- Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp

- Lừa đảo “combo du lịch giá rẻ”
- Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa
- Rao bán hàng giả hàng nhái trên sàn thương mại điện tử
- Lừa đảo cho số đánh đề
- Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng
- Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo
- Lừa đảo qua tin nhắn giả mạo công ty, doanh nghiệp thông báo trúng thưởng
- Lừa đảo “khóa SIM” vì chưa chuẩn hóa thuê bao
- Lừa đảo cuộc gọi video Deepfake, Deepvoice
- Cài cắm ứng dụng, đường dẫn quảng cáo cờ bạc, cá độ, tín dụng đen,...

(2) Lừa đảo thông tin cá nhân



Lừa đảo qua mạng liên quan tới **đánh cắp thông tin cá nhân, thông tin nhạy cảm.**

Hệ lụy của lừa đảo thông tin cá nhân có thể bao gồm chiếm đoạt các tài khoản, mạo danh, bắt nạt, bôi nhọ, tống tiền... dẫn đến các thiệt hại cả về vật chất, tinh thần, và danh tiếng.

Một số tình huống:

- Đánh cắp tài khoản mạng xã hội, nhắn tin lừa đảo
- Đánh cắp thông tin căn cước công dân đi vay nợ tín dụng
- Lừa đảo lấy cắp Telegram OTP
- Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp (bảo hiểm xã hội, ngân hàng...)
- Rải đường dẫn giả mạo lừa đảo thông tin cá nhân, đẩy quảng cáo bẩn trên Facebook

(3) Lừa đảo tình cảm

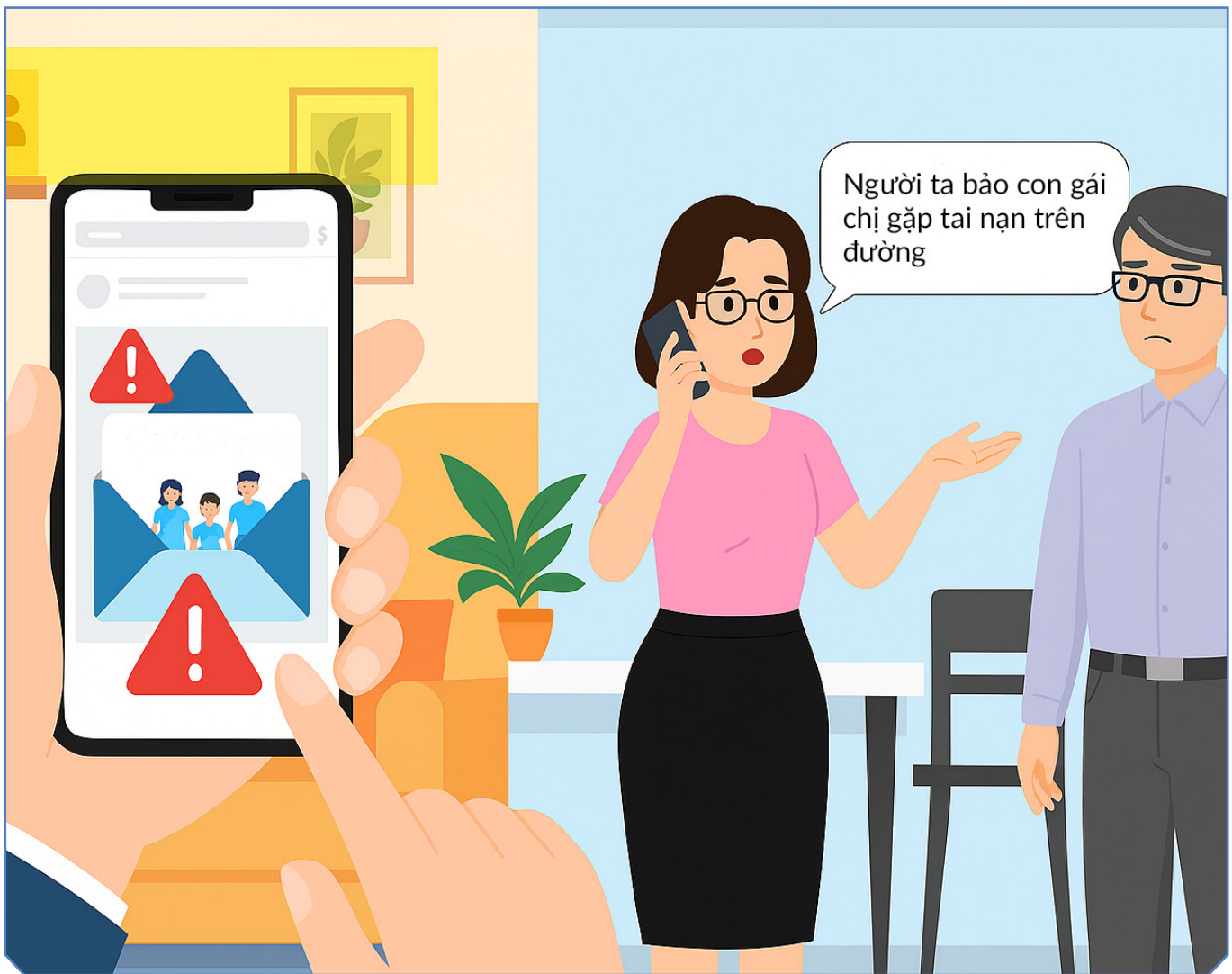


Lừa đảo qua mạng dựa trên cơ sở các mối quan hệ, tình cảm trong hẹn hò hoặc kết bạn qua mạng.

Hệ lụy của lừa đảo tình cảm có thể bao gồm: nạn nhân bị tổn thương cảm xúc, xâm hại, bắt nạt, bôi nhọ. Mất mát tài chính và vật chất cũng là hệ lụy thường thấy của các tình huống lừa đảo tình cảm.

Một số tình huống: Lừa đảo tình cảm để dẫn dụ đầu tư tài chính, gửi bưu kiện, trúng thưởng,...

Trong số ba loại lừa đảo nêu trên, lừa đảo tài chính và lừa đảo thông tin cá nhân có nhiều chiêu trò tương đồng và thường liên quan chặt chẽ, vì vậy có thể kết hợp khi tìm hiểu cách phòng tránh. Theo Hiệp hội An ninh mạng quốc gia, đây cũng là hai loại lừa đảo qua mạng thường gặp nhất tại Việt Nam năm 2024. Cụ thể, các tình huống lừa đảo phổ biến nhất bao gồm: *lừa đảo đầu tư* (Lừa đảo tài chính), *giả danh cơ quan chức năng* (Lừa đảo tài chính hoặc Lừa đảo thông tin cá nhân), và *lừa đảo trúng thưởng/khuyến mãi lớn* (Lừa đảo tài chính).



Trong các bài học tiếp theo (*Bài 2 - Các chiêu trò lừa đảo qua mạng và cách nhận biết; Bài 3 - Các biện pháp phòng tránh và xử lý tình huống lừa đảo qua mạng*), chúng ta sẽ cùng tìm hiểu chi tiết các chiêu trò lừa đảo, dấu hiệu nhận biết và cách phòng tránh, xử lý chúng.

SUY NGÃM

Hãy cùng xem xét ba ví dụ sau và cho biết nó thuộc loại lừa đảo nào: lừa đảo tài chính, lừa đảo tình cảm, hay lừa đảo thông tin cá nhân?



Trường hợp 1: Một người tự xưng là chuyên gia tài chính, quảng cáo về một cơ hội đầu tư với lợi nhuận “siêu khủng” (lên đến 300% trong 1 tháng). Họ yêu cầu anh T. nạp tiền vào để tham gia đầu tư. Sau khi nhận được tiền, kẻ lừa đảo biến mất, và anh T. mất toàn bộ số tiền đầu tư.



Trường hợp 2: Chị H. làm quen và kết bạn với một người lạ trên mạng. Sau thời gian tìm hiểu, người này yêu cầu chị H. gửi một vài tấm hình nhạy cảm, sau đó người này tiếp tục dùng các bức hình để uy hiếp và ép chị H. thực hiện theo nhiều yêu cầu khác.



Trường hợp 3: Anh M. nhận được một tin nhắn nói rằng bình chọn cho chương trình âm nhạc mà anh yêu thích, anh bấm vào và họ yêu cầu đăng nhập mạng xã hội để bình chọn. Sau khi nhập thông tin, tài khoản của anh bị chiếm quyền sử dụng.

(Gợi ý: Trường hợp 1: Lừa đảo tài chính (tình huống lừa đảo đầu tư); Trường hợp 2: Lừa đảo tình cảm; Trường hợp 3: Lừa đảo thông tin cá nhân)

4. Chiến lược của kẻ lừa đảo qua mạng nhắm tới các nhóm đối tượng khác nhau như thế nào?

Như bạn đã biết, từ đầu năm 2025, nhiều đường dây lừa đảo bị triệt phá tại Việt Nam đều có quy mô lên đến hàng ngàn tỷ đồng - con số tương đương doanh thu của các doanh nghiệp vừa và lớn. Để vận hành ở quy mô này, các nhóm lừa đảo tổ chức theo mô hình bài bản, chia thành nhiều đội nhóm với sự “chuyên nghiệp” không kém gì một công ty thực thụ. Chúng không chỉ xây dựng hệ thống “đào tạo” mà còn lên kịch bản tinh vi để thao túng nạn nhân. Nếu doanh nghiệp phân tích thị trường và khách hàng mục tiêu để tối ưu hoạt động kinh doanh, thì *các nhóm lừa đảo cũng nghiên cứu kỹ “con mồi”* để gia tăng hiệu quả lừa đảo.

Vì vậy, hãy lưu ý rằng **những kịch bản lừa đảo sẽ được điều chỉnh phù hợp với từng nhóm đối tượng khác nhau**. Nếu có ai đó trên mạng đưa ra tình huống liên quan chặt chẽ đến *cuộc sống, nhu cầu hoặc vấn đề cá nhân của bạn*, hãy cảnh giác vì đó có thể là chiêu trò lừa đảo mà chúng nhắm tới bạn. Ví dụ: với người cao tuổi, kẻ lừa đảo có thể nhắm đến các chiêu trò liên quan đến du lịch hoặc thực phẩm chức năng v.v; với phụ huynh, chúng có thể sử dụng kịch bản về tuyển mẫu nhí, con gặp tai nạn v.v; còn với phụ nữ, thanh niên, các hình thức lừa đảo phổ biến có thể xoay quanh tuyển dụng, đầu tư, trúng thưởng hay lừa đảo tình cảm v.v. Ngoài ra, nhìn chung, **đối tượng mục tiêu lý tưởng** mà kẻ lừa đảo thường nhắm tới thường có những đặc điểm sau:

- **Chia sẻ quá nhiều thông tin cá nhân:** Việc thường xuyên công khai địa chỉ nhà, nơi làm việc, số điện thoại, tài khoản ngân hàng, lịch trình hàng ngày...ở trên mạng cũng như ở những nơi khác sẽ vô tình cung cấp dữ liệu quý giá để kẻ xấu tạo kịch bản lừa đảo nhắm vào bạn.

- **Thiếu kiến thức về an toàn và bảo mật:** Nếu có những thực hành thiếu an toàn như đặt mật khẩu yếu, không bật xác thực hai yếu tố, sử dụng Wi-Fi công cộng mà không cân nhắc các hành động, dễ dàng bấm vào các đường dẫn lạ mà chưa xác minh... sẽ khiến tài khoản và thông tin của bạn dễ bị đánh cắp.
- **Nhẹ dạ cả tin, dễ bị thao túng cảm xúc:** Việc dễ tin vào những lời mời hấp dẫn, câu chuyện cảm động hoặc bị hoang mang trước các cuộc gọi giả danh sẽ dễ khiến bạn rơi vào bẫy lừa đảo.
- **Dễ dàng kết bạn và tin tưởng người lạ:** Chấp nhận kết bạn với tài khoản lạ, chia sẻ thông tin cá nhân quá nhanh với người mới quen trên mạng... có thể dẫn đến nguy cơ bị lợi dụng.
- **Đang gặp nhu cầu cấp bách hoặc tình huống đặc biệt:** Khi cần tìm việc, kiếm tiền nhanh, vay tiền gấp, hoặc đang giải quyết tình huống khẩn cấp, bạn có thể bị mắc bẫy những lời hứa hẹn “giải pháp hoàn hảo” từ kẻ lừa đảo. Những người có thân nhân ở nước ngoài hoặc người Việt Nam sinh sống tại nước ngoài cũng thường trở thành mục tiêu lừa đảo, vì các kịch bản liên quan đến yếu tố nước ngoài khó xác minh hơn.

Nếu bạn nhận thấy mình có những đặc điểm này, hãy suy nghĩ ngay về cách thay đổi và/hoặc cảnh giác để bảo vệ bản thân trước các nguy cơ lừa đảo.



Nội dung chính cần ghi nhớ

1. Lừa đảo là hành vi gian lận nhằm đánh cắp các tài sản có giá trị, bao gồm tiền bạc, thông tin cá nhân, thậm chí cả tình cảm. Lừa đảo qua mạng có thể diễn ra bất cứ đâu trên **mạng viễn thông** (qua cuộc gọi, tin nhắn) hoặc **mạng internet** (qua mạng xã hội, trang web, thư điện tử, ứng dụng nhắn tin, ứng dụng hẹn hò...).
2. Việt Nam nằm trong nhóm các quốc gia bị ảnh hưởng nặng nề bởi lừa đảo trực tuyến. Mỗi người cần **nâng cao cảnh giác** và **trang bị kiến thức, kỹ năng** để giảm thiểu thiệt hại cho bản thân, gia đình và xã hội.
3. Phân loại theo tình huống, lừa đảo qua mạng có thể chia làm ba loại: **Lừa đảo tài chính, lừa đảo thông tin cá nhân, và lừa đảo tình cảm**.
4. Kẻ lừa đảo thường lên kế hoạch dựa trên những thông tin chúng thu thập được từ đối tượng. Hãy cảnh giác và thay đổi nếu bạn có những **đặc điểm dễ trở thành mục tiêu** của kẻ lừa đảo: *chia sẻ quá nhiều thông tin cá nhân, thiếu kiến thức bảo mật, nhẹ dạ dễ bị thao túng, dễ tin tưởng người lạ, hoặc đang có nhu cầu cấp bách*.

