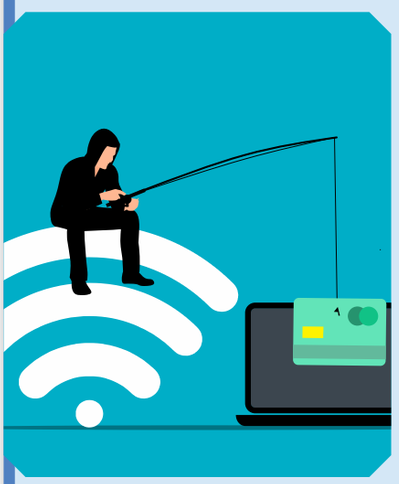
APAC Cybersecurity Fund
The Asia Foundation

VIETNET-ICT

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

Bài 2: Các chiêu trò lừa đảo qua mạng và cách nhận biết

với sự hỗ trợ từ Google.org



MỤC TIÊU:

- Nắm được và cảnh giác với các chiêu trò lừa đảo qua mạng phổ biến.
- Nắm được các dấu hiệu nhận biết các chiêu trò lừa đảo qua mạng.

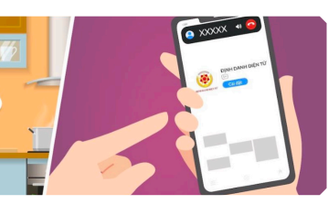
1. Các chiêu trò lừa đảo qua mạng phổ biến tại Việt Nam

Như bạn đã được tìm hiểu ở bài học trước, các hình thức lừa đảo qua mạng ngày càng tinh vi và đa dạng, khiến nhiều người mất cảnh giác và trở thành nạn nhân. Dưới đây là phân tích về *các bước của một số chiêu trò lừa đảo phổ biến* hiện nay, giúp bạn nhận diện và hiểu rõ cách thức hoạt động của kẻ lừa đảo.

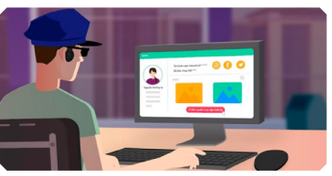
Tình huống 1: Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo (VD: đồng bộ thông tin trên tài khoản định danh VNeID)

Bước 1: Giả danh & liên lạc: Kẻ lừa đảo giả danh công an hoặc cán bộ quản lý gọi điện vận động người dân đồng bộ thông tin trên tài khoản định danh điện tử VNeID.

Bước 2: Thúc giục: Kẻ lừa đảo tiếp tục thúc giục người dân thực hiện gấp, hướng dẫn cách làm trực tuyến để nạn nhân mất cảnh giác.



Bước 3: Dụ cài ứng dụng giả mạo: Kẻ lừa đảo gửi đường dẫn, hướng dẫn tải xuống và cài đặt một ứng dụng giả mạo, có giao diện giống ứng dụng Dịch vụ công quốc gia hoặc VNeID thật.



Bước 4: Chiếm đoạt thông tin: Sau khi nạn nhân cài đặt, ứng dụng giả mạo chiếm quyền truy cập, lấy cắp thông tin ngân hàng, mã OTP.

Bước 5: Chiếm đoạt tài sản: Kẻ lừa đảo sử dụng thông tin đánh cắp để đăng nhập, chuyển tiền nhằm chiếm đoạt tài sản.

Tình huống 2: Lừa đảo qua tin nhắn giả mạo công ty, doanh nghiệp (giả danh ngân hàng hoặc mạng xã hội thông báo tài khoản có vấn đề)

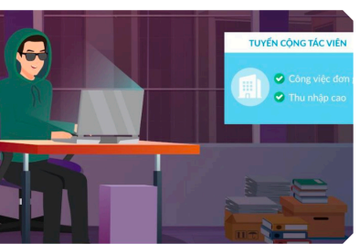
Bước 1: Giả mạo và thông báo vấn đề Kẻ lừa đảo gửi tin nhắn SMS, email hoặc qua mạng xã hội, giả danh ngân hàng hoặc các nền tảng, thông báo tài khoản của nạn nhân có vấn đề, cần xác minh. Tin nhắn kèm một đường dẫn giả mạo có giao diện giống hệt trang web chính thức của ngân hàng hoặc nền tảng mạng xã hội.

Bước 2: Chiếm đoạt thông tin: Khi nạn nhân nhấp vào đường dẫn, trang web giả mạo yêu cầu nhập thông tin đăng nhập, số điện thoại, mã OTP hoặc các thông tin cá nhân khác.

Bước 3: Chiếm đoạt tài khoản: Sau khi nhập thông tin, kẻ lừa đảo ngay lập tức chiếm đoạt tài khoản, thay đổi mật khẩu của các tài khoản.

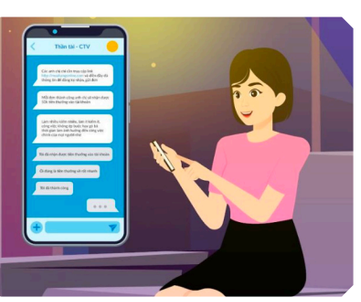
Bước 4: Chiếm đoạt tài sản: Chúng sử dụng tài khoản đã đánh cắp để lừa đảo tiếp bạn bè, người thân (tài khoản mạng xã hội), hoặc rút tiền, thực hiện giao dịch gian lận (tài khoản ngân hàng).

<u>Tình huống 3</u>: Lừa đảo tuyển cộng tác viên trực tuyến (lừa đảo việc làm qua mạng)

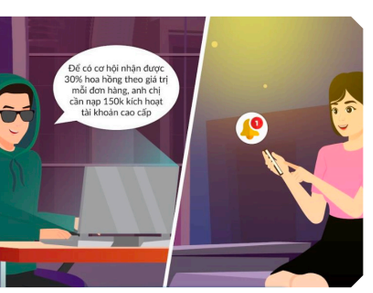


Bước 1: Đưa ra cơ hội hấp dẫn: Kẻ lừa đảo giả danh các công ty gọi điện hoặc đăng bài tuyển cộng tác viên trên mạng xã hội, với cơ hội công việc hấp dẫn, yêu cầu đơn giản.

Bước 2: Mời vào nhóm kín: Nếu đồng ý tham gia, kẻ lừa đảo mời nạn nhân vào các nhóm kín để dễ dàng tương tác và thao túng.

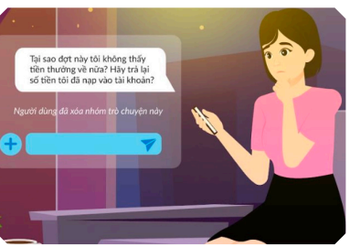


Bước 3: Giao nhiệm vụ nhỏ: Trong nhóm kín, kẻ lừa đảo giao nhiệm vụ nhỏ cho nạn nhân như đặt đơn hàng để nhận hoa hồng (có thể tạo niềm tin bằng cách cho nhiều tài khoản khác xác nhận đã thành công).



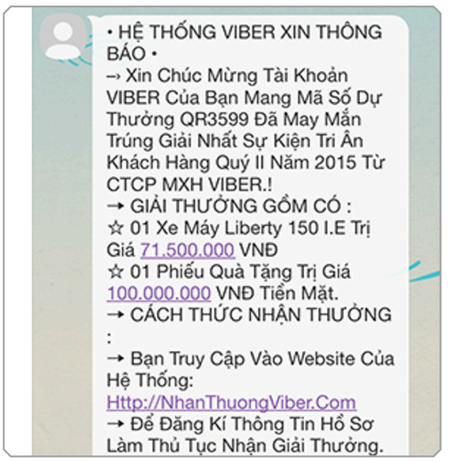
Bước 4: Dụ dỗ tham gia nhiệm vụ lớn: Kẻ lừa đảo dụ nạn nhân tham gia cấp độ cao hơn với phần thưởng lớn hơn, yêu cầu nạp tiền trước.

Bước 5: Từ chối trả tiền: Sau đó, chúng từ chối trả thưởng và viện nhiều lý do khác nhau để ép tiếp tục làm nhiệm vụ, nạp thêm tiền.



Bước 6: Biến mất: Cuối cùng, kẻ xấu khóa tài khoản, chặn liên lạc sau khi lừa được số tiền lớn.

Tình huống 4: Thông báo "nhận quà trúng thưởng" (giả danh các công ty)



Bước 1: Thông báo trúng thưởng: Giả danh công ty hoặc tổ chức uy tín, gọi điện hoặc nhắn tin qua các nền tảng mạng xã hội, thông báo rằng nạn nhân đã may mắn trúng thưởng.

Bước 2: Gửi đường dẫn xác nhận: Gửi đường dẫn xác nhận và yêu cầu nạn nhân cung cấp thông tin cá nhân để xác nhận danh tính, tạo cảm giác tin tưởng.

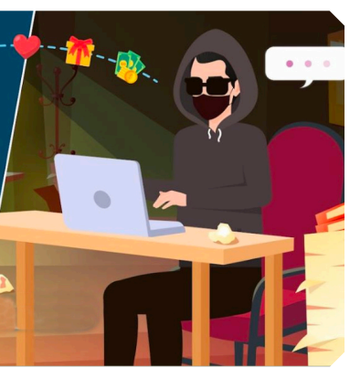
Bước 3: Yêu cầu đóng phí: Một người khác, giả danh nhân viên của công ty, gọi điện xác nhận và yêu cầu nạn nhân đóng một khoản phí vận chuyển hoặc phí xử lý để nhận quà.

Bước 4: Chiếm đoạt tài sản: Tiếp tục viện lý do rằng giao dịch bị lỗi hoặc cần thêm khoản phí xác minh, yêu cầu nạn nhân chuyển tiền thêm nhiều lần.

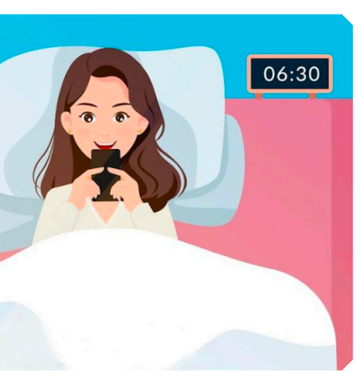
Bước 5: Biến mất: Cuối cùng, kẻ xấu khóa tài khoản, chặn liên lạc sau khi lừa được số tiền lớn.

Tình huống 5: Lừa đảo tình cảm để dẫn dụ đầu tư tài chính, gửi bưu kiện, vay tiền,...

Bước 1: Tiếp cận: Kẻ lừa đảo gửi lời mời kết bạn, mạo danh người nước ngoài giàu có hoặc có hoàn cảnh đáng thương (góa vợ/chồng, tìm bạn cũ...) để tạo sự tin tưởng.

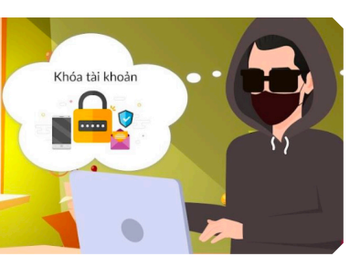


Bước 2: Xây dựng niềm tin: Chúng duy trì trò chuyện hàng ngày, thể hiện sự quan tâm, khen ngợi, hứa hẹn tặng quà, chuyển tiền, gửi các bức ảnh trong cuộc sống hàng ngày để tạo lòng tin với nạn nhân.



Bước 3: Lợi dụng chiếm đoạt tài sản: Sau khi tạo đủ lòng tin, kẻ lừa đảo viện lý do khẩn cấp như gặp tai nạn, bị giữ tiền ở sân bay, cần nạn nhân cho vay gấp hoặc dụ nạn nhân đầu tư với lợi nhuận cao.

Bước 4: Từ chối gặp mặt: Chúng tiếp tục viện đủ lý do từ chối gặp mặt như đang ở nước ngoài, bận công việc, chờ hoàn thành thủ tục... để kéo dài thời gian lừa đảo.



Bước 5: Biến mất: Cuối cùng, kẻ xấu khóa tài khoản, chặn liên lạc sau khi lừa được số tiền lớn.

2. Dấu hiệu chung nhận biết các tình huống lừa đảo qua mạng

Mặc dù các chiêu trò lừa đảo trên thực tế thường rất tinh vi, đa dạng, và không ngừng thay đổi, nhưng chúng thường có một đặc điểm chung. Đó là kẻ lừa đảo sử dụng các chiêu trò **thao túng tâm lý,** khiến nạn nhân mất cảnh giác và dễ rơi vào bẫy. Vậy các chiêu trò này là gì?

Hãy cùng tham khảo *hai công thức* sau đây để dễ dàng nhận biết các chiêu trò thao túng tâm lý thường xuất hiện trong một cuộc lừa đảo qua mạng.

- **Công thức 4D: nhận biết một cuộc lừa đảo tài chính và thông tin cá nhân qua mạng**

DOẠ NẠT: Kẻ lừa đảo liên lạc với bạn qua mạng và đưa ra một tình huống khẩn cấp khiến bạn hoảng sợ, lo lắng, hoặc hối thúc cần hành động ngay.

DỰA DẪM: Kẻ lừa đảo liên lạc qua mạng và hỏi sự trợ giúp của bạn như hỏi vay tiền, bình chọn cuộc thi, trợ giúp từ thiện v.v.

DỤ DỖ: Kẻ lừa đảo thông báo rằng bạn được nhận một khoản lợi nhuận bất ngờ, hấp dẫn nào đó quá dễ dàng.

DÀN DỰNG: Kẻ lừa đảo đưa ra các tình huống phức tạp với nhiều chi tiết, có sự tham gia của nhiều người, đồng thời có nhiều bằng chứng tưởng chừng rất thuyết phục.

- **Công thức 4L: nhận biết một cuộc lừa đảo tình cảm qua mạng**

LÔI CUỐN: Kẻ lừa đảo xây dựng một hồ sơ hoàn hảo như có hình ảnh hấp dẫn, công việc lý tưởng, thu nhập cao nhằm thu hút sự chú ý.

LẤY LÒNG: Kẻ lừa đảo nhanh chóng bày tỏ tình cảm, liên tục khen ngợi, thể hiện sự đồng cảm hoặc tặng quà, tiền để chiếm được lòng tin của bạn.

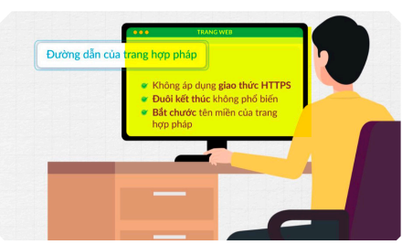
LAY ĐỘNG: Kẻ lừa đảo kể những câu chuyện cảm động, đáng thương để đánh vào lòng trắc ẩn, khiến bạn muốn giúp đỡ.

LỢI DỤNG: Khi đã tạo dựng đủ niềm tin, kẻ lừa đảo bắt đầu yêu cầu chuyển tiền, rủ rê đầu tư, hoặc đòi hỏi những thông tin nhạy cảm như hình ảnh cá nhân.

Ngoài việc nhận diện các chiêu trò thao túng tâm lý, bạn cũng cần xem xét **các bằng chứng và quan sát các yếu tố không đáng tin** tại các *trang web*, *đường dẫn*, *thư điện tử*, *âm*

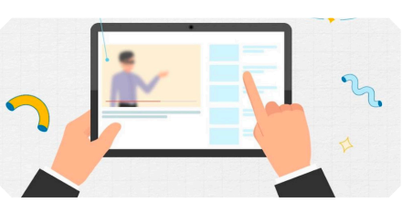
thanh/hình ảnh/video xuất hiện trong các tình huống. Bạn có thể tham khảo bảng liệt kê các yếu tố đáng nghi ngờ sau đây:

TRANG WEB: Tên miền khác biệt so với trang chính thức của các công ty/ tổ chức khi kiểm tra bằng công cụ tìm kiếm (có thể gần giống nhưng không trùng khớp); xuất hiện các cảnh báo, đe dọa, quảng cáo v.v; yêu cầu nhập thông tin cá nhân; chất lượng thiết kế kém; lỗi chính tả, ngữ pháp

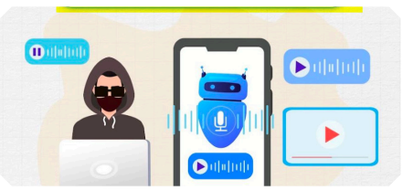


ĐƯỜNG DẪN: Cố bắt chước tên miền của một trang hợp pháp bằng cách chỉ thay đổi một vài ký tự nhỏ; Không bắt đầu với HTTPS://, không có biểu tượng khoá bảo mật ( ); Kết thúc bằng các đuôi không phổ biến như: .info, .asia, .vip, .tk, .xyz...

THƯ ĐIỆN TỬ: Địa chỉ thư điện tử có đuôi không phải tên miền chính thức của một đơn vị uy tín; Đính kèm các tập tin khi cài đặt sẽ thực hiện các tác vụ trên thiết bị (có đuôi như *.exe*, *.scr*, *.bat*, *.cmd*, *.vbs*, *.js*, *.zip*, *.rar*, *.iso* hoặc *.pdf*, *.exe*); Lỗi chính tả, ngữ pháp



ÂM THANH/HÌNH ẢNH/VIDEO có thể bị mờ, kém sắc nét và thiếu độ mượt mà; cử động khuôn mặt không tự nhiên, có độ trễ hoặc không khớp hoàn toàn với lời nói; các chi tiết nhỏ có thể bị nhòe, méo hoặc hiển thị không chính xác.



(Lưu ý: Với sự phát triển của trí tuệ nhân tạo, các video và giọng nói giả mạo **sử dụng công nghệ như "deepfake[1]", "deepvoice[2]"** ngày càng chân thực, khiến những dấu hiệu này có thể sẽ càng *khó nhận biết hơn*.)

SUY NGẪM

Trong số các tên miền trang web sau đây, tên miền nào là tên miền chính thức của Ngân hàng Chính sách xã hội?

- http://vbsp.xyz
- https://vbsp.org.vn/
- http://vbsp.tk
- https://vb-sp.info
- http://vb-sp.nganhang.vip

(Gợi ý: Bạn có thể lên công cụ tìm kiếm và gõ "Trang web Ngân hàng Chính sách xã hội", sau đó bạn có thể tìm thấy trang web chính thức của Ngân hàng Chính sách xã hội là https://vbsp.org.vn/.)

1 **Deepfake** là một công nghệ tạo hoặc chỉnh sửa hình ảnh, video để giả mạo khuôn mặt và giọng nói. Nó có thể bắt chước khuôn mặt, cử động, lời nói của một người rất tinh vi, khiến họ trông như đang làm điều họ chưa từng làm.

2 **Deepvoice** là công nghệ tạo giọng nói nhân tạo giống con người. Nó giúp máy tính học và mô phỏng giọng nói, thậm chí bắt chước giọng một người chỉ với vài phút dữ liệu giọng nói mẫu.

Nội dung chính cần ghi nhớ

1. Các tình huống lừa đảo qua mạng rất đa dạng, tinh vi và phức tạp. Chúng thường có điểm chung là kẻ lừa đảo thường áp dụng các chiêu trò **thao túng tâm lý** nạn nhân.
    - **Công thức 4D** để nhận biết một cuộc lừa đảo tài chính và thông tin cá nhân qua mạng điển hình: *Dọa nạt - Dựa dẫm - Dụ dỗ - Dàn dựng*
    - **Công thức 4L** để nhận biết một cuộc lừa đảo tình cảm qua mạng điển hình: *Lôi cuốn - Lấy lòng - Lay động - Lợi dụng*
2. Ngoài các chiêu trò thao túng tâm lý, người dùng cần chú ý các **dấu hiệu bất thường** của các trang web, đường dẫn, hoặc thư điện tử xuất hiện trong các tình huống.
    - **Trang web:** tên miền khác so với trang chính thức của các công ty/ tổ chức, xuất hiện các hộp thông báo bất ngờ, yêu cầu nhập thông tin cá nhân, chất lượng thiết kế kém hay có các lỗi chính tả.
    - **Đường dẫn:** không áp dụng giao thức HTTPS, kết thúc bằng các đuôi không phổ biến, bắt chước tên miền của các trang hợp pháp.
    - **Thư điện tử:** địa chỉ thư có đuôi không phải tên miền chính thức, đính kèm các tập tin thực thi, và có các lỗi chính tả.
    - **Âm thanh/ Hình ảnh/ Video:** chất lượng kém, thiếu rõ nét, không mượt mà và các chi tiết nhỏ có thể thiếu chính xác.