ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU TUYÊN TRUYỀN VỀ PHÒNG TRÁNH LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

PHƯƠNG THỨC LỪA ĐẢO

Dẫn dụ người dùng quét mã QR hoặc truy cập website lừa đảo để đánh cắp thông tin cá nhân, từ đó có thể lấy mã OTP, mã xác thực hoặc hack tài khoản mạng xã hội để tiếp tục lừa đảo bạn bè và người thân.

Mời kết nối vào các ứng dụng chat OTT để thao túng tâm lý, thường bắt đầu từ Zalo và dẫn dụ sang các ứng dụng không kiểm soát như Telegram, Viber, WhatsApp, từ đó áp dụng các kịch bản lừa đảo khác nhau.

Lừa nạn nhân cài đặt ứng dụng giả mạo hoặc kích hoạt tệp tin chứa mã độc (đuôi .pdf, .doc, .xlsx, .bat, .zip, .rar, .html, .exe) để chiếm quyền thiết bị, đánh cắp thông tin cá nhân, lấy tiền trong tài khoản, bôi nhọ danh dự hoặc tống tiền.

Tác động tâm lý trực tiếp qua điện thoại để chiếm đoạt tiền, bằng cách yêu cầu chuyển khoản hoặc gửi tiền tại ngân hàng; cũng có thể dẫn dụ nạn nhân nhập cú pháp chuyển sang eSIM để chiếm đoạt số điện thoại của họ.

CÁCH THỨC THỰC HIỆN

Đối tượng lừa đảo thường dẫn dụ nạn nhân bằng những cách sau đây:

Tạo dựng lòng tin: Giả danh tổ chức uy tín như cơ quan nhà nước, ngân hàng, công ty nổi tiếng,... và sử dụng email, tin nhắn hoặc cuộc gọi để tạo lòng tin và yêu cầu thông tin nhạy cảm từ nạn nhân.

Kịch bản lừa đảo: Được biên soạn chi tiết và khéo léo nhằm mục đích dẫn dụ, thao túng tâm lý tạo niềm tin và sự đồng cảm từ nạn nhân; đóng nhiều vai nhân vật khác nhau để tạo ra một câu chuyện hoàn hảo đánh động vào tâm lý của nạn nhân một cách sâu sắc.

Sử dụng biểu mẫu và giao diện giả mạo: Các website lừa đảo thường sao chép giao diện của các website chính thức, sử dụng biểu mẫu đăng nhập hoặc thanh toán giống như thật để đánh lừa người dùng.

Kích thích tâm lý: Đánh vào lòng tham, sự sợ hãi, tính hiếu kỳ, tính tò mò và đặc biệt là tình thương, sự thương hại của con người; thường tạo ra cảm giác khẩn cấp để thúc đẩy nạn nhân hành động ngay lập tức mà không suy nghĩ kỹ lưỡng (ví dụ như thông báo tài khoản sẽ bị khóa nếu không xác nhận thông tin ngay lập tức).

Đưa ra phần thưởng hoặc cơ hội hiếm có: Hứa hẹn giải thưởng lớn, cơ hội đầu tư sinh lời cao hoặc cơ hội việc làm hấp dẫn để thu hút sự chú ý của nạn nhân.

Yêu cầu hành động gấp: Gửi liên kết đến các website giả mạo hoặc mã QR, nơi nạn nhân được yêu cầu nhập thông tin cá nhân hoặc tài khoản; các liên kết này thường được ngụy trang dưới dạng liên kết hợp pháp hoặc phần thưởng.

Làm giả thông báo khẩn cấp: Sử dụng thông báo giả mạo về sự cố bảo mật, viện các lý do nguồn tiền đang bị treo vì phải đóng thuế, cơ quan Công an điều tra, lỗi tài khoản hoặc sự kiện khẩn cấp để yêu cầu nạn nhân cung cấp thông tin ngay lập tức.

Kích thích sự tò mò: Gửi email hoặc tin nhắn về sự kiện nóng hổi, báo cáo quan trọng hoặc tài liệu hấp dẫn, yêu cầu nạn nhân tải xuống hoặc mở file đính kèm chứa mã độc.

KỸ NĂNG PHÒNG TRÁNH CƠ BẢN

Kiểm tra nguồn gốc thông tin:
Xác định xem thông tin đến từ nguồn đáng tin cậy hay không; kiểm tra tên miền và đường dẫn URL của website; chú ý đến các tên miền khác thường, có lỗi chính tả hoặc không có các chứng chỉ tín nhiệm mạng.

Cẩn thận với các yêu cầu cung cấp thông tin cá nhân, tài chính:
Không chia sẻ thông tin cá nhân hoặc tài chính qua email hoặc tin nhắn cho các đối tượng lạ. Ngoài các đơn vị ngân hàng, các tổ chức hoặc doanh nghiệp uy tín sẽ không yêu cầu cung cấp dữ liệu cá nhân.

Cảnh giác với người lạ kết bạn qua mạng xã hội:
Cảnh giác với người lạ kết bạn qua Zalo, Telegram… Khi có dấu hiệu khả nghi ngay lập tức không kết bạn và không trả lời. Ngoài ra, ẩn đi danh sách bạn bè của mình trên các tài khoản mạng xã hội để tránh bị đối tượng lừa đảo biết đến các mối quan hệ xung quanh của mình.

Cảnh giác với những yêu cầu đặt cọc hoặc chuyển khoản trước:
Tuyệt đối không chuyển tiền cho các đối tượng lạ trong mọi trường hợp. Đối với các giao dịch trực tiếp, người dân được khuyến cáo nên thực hiện trực tiếp hoặc thông qua cá nhân hoặc tổ chức trung gian uy tín.

Cảnh giác với email và tin nhắn lạ:
Các email hoặc tin nhắn lừa đảo thường giả mạo các tổ chức uy tín (cơ quan nhà nước, ngân hàng, công ty công nghệ,…). Kiểm tra kỹ địa chỉ email người gửi, so sánh đối chiếu với địa chỉ email được ghi trên các cổng thông tin điện tử chính thống. Thông thường, các địa chỉ email giả mạo sẽ bao gồm các ký tự thừa, tên miền không chính xác.

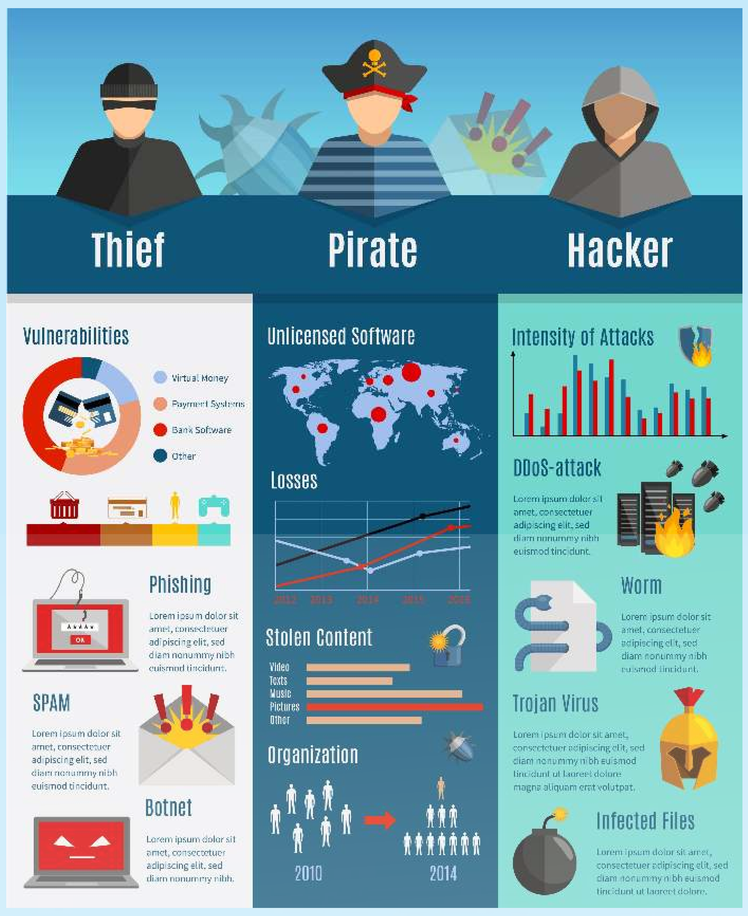
Tìm hiểu thêm về các hình thức lừa đảo phổ biến:
Các loại hình lừa đảo qua mạng như lừa đảo qua email, tin nhắn, mạo danh và lừa đảo chiếm đoạt tài sản đã được phổ biến rất nhiều trên mạng. Việc tìm hiểu và nắm bắt các phương thức này sẽ giúp dễ dàng nhận diện và phòng tránh hậu quả không đáng có. **Theo dõi và cập nhật tại kênh thông tin Cổng không gian mạng quốc gia (Facebook/TikTok) hoặc website Khonggianmang.vn**

"NGUYÊN TẮC VÀNG" BẢO VỆ BẢN THÂN KHỎI LỪA ĐẢO TRỰC TUYẾN

1 **Nguyên tắc 1:** Hãy chậm lại
Đối tượng lừa đảo thường tạo ra cảm giác cấp bách nhằm vượt qua khả năng nhận định của bạn; những cuộc gọi, tin nhắn,... thúc giục phải hành động nhanh như: Thời gian khuyến mãi đã hết, nếu không chuyển tiền bây giờ bạn và người thân phải thực hiện các thủ tục tố tụng,... Trong tình huống này, bạn hãy dành thời gian suy nghĩ kỹ và đặt câu hỏi tìm hiểu kỹ nội dung, thông tin để tránh bị thao túng tâm lý, dồn vào tình huống xấu.

2 **Nguyên tắc 2**: Kiểm tra tại chỗ
Bạn hãy tìm hiểu thêm để xác thực thông tin nhận được, nếu nhận được một cuộc gọi không mong muốn, bạn hãy tra cứu số ngân hàng, cơ quan hoặc tổ chức đang gọi đến và liên hệ lại trực tiếp.

3 **Nguyên tắc 3**: Dừng lại! Không gửi
Không một cá nhân hoặc cơ quan nào yêu cầu thanh toán ngay tại chỗ; vì vậy, nếu bạn cảm thấy giao dịch không đáng tin, hãy dừng lại vì có thể đây là dấu hiệu lừa đảo.



QUY TẮC "6 KHÔNG"

KHÔNG cung cấp thông tin cá nhân, địa chỉ, số điện thoại, số tài khoản ngân hàng cho đối tượng không quen biết; thận trọng rà soát và kiểm tra kỹ thông tin trước khi thực hiện các giao dịch chuyển tiền.

KHÔNG kết bạn và nói chuyện với người lạ, đặc biệt là những tài khoản có hình ảnh ngoại hình đẹp và bắt mắt; tuyệt đối không nhận lời mời tham gia các hội nhóm mà không rõ mục đích đối tượng.

KHÔNG truy cập, đăng nhập vào các đường dẫn, liên kết, website, ứng dụng hoặc mở tệp đính kèm đến từ người gửi không xác định, không rõ nguồn gốc.

KHÔNG có cán bộ cơ quan nhà nước, Bộ Công an, Viện Kiểm sát, Tòa án hay đơn vị tài chính,… gọi điện để điều tra qua điện thoại, yêu cầu phải cung cấp thông tin cá nhân hay đóng tiền.

KHÔNG thực hiện chuyển khoản trước, tuyệt đối không đặt cọc, chuyển khoản tiền cho các đối tượng lạ trong bất cứ trường hợp nào.

KHÔNG nhận những tài sản, món quà không rõ nguồn gốc, những lợi nhuận "phi thực tế" không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ lương cao",...