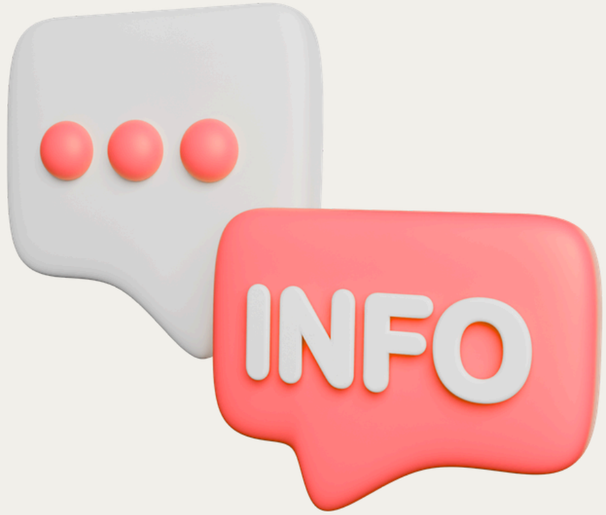
BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG
TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

AGRIBANK

CẨM NANG HƯỚNG DẪN NHẬN BIẾT VÀ CÁCH PHÒNG TRÁNH

21 thủ đoạn lừa đảo của tội phạm công nghệ cao

Giả danh cơ quan chức năng yêu cầu cập nhập thông tin, cài ứng dụng giả mạo



NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người cao tuổi, trẻ nhỏ, người dân ở vùng sâu vùng xa chưa sử dụng nhiều các ứng dụng dịch vụ công.

DẤU HIỆU:

- Đối tượng chủ động liên hệ người dân thông qua thuê bao di động hoặc tài khoản mạng xã hội, xưng danh là cán bộ quản lý hộ tịch, cảnh sát khu vực...;
- Thông báo các chủ trương, chính sách mới, yêu cầu người dân cần cập nhật thông tin. Trong một số trường hợp, đối tượng có thể nói chính xác thông tin cá nhân của người dân để tạo lòng tin;
- Gợi ý về việc làm thủ tục trực tuyến, không cần đi lại;
- Gửi cho người dân đường link hoặc hướng dẫn cài ứng dụng giả mạo chứa mã độc. Các đối tượng hướng dẫn người dân từng bước thực hiện;
- Sau khi chiếm quyền điều khiển thiết bị, các đối tượng tiếp tục yêu cầu người dân làm theo hướng dẫn để gián tiếp cung cấp mã OTP ngân hàng hoặc dữ liệu xác thực sinh trắc học cho chúng.

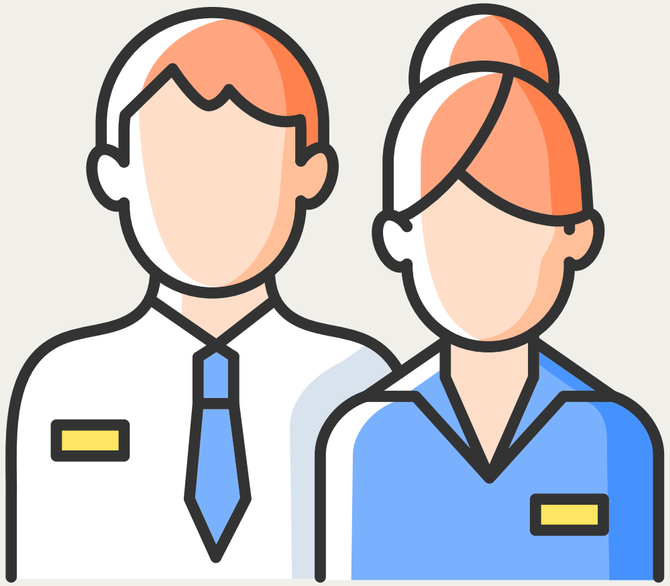
BIỆN PHÁP PHÒNG TRÁNH:

- Cảnh giác khi nhận được các cuộc gọi từ số điện thoại lạ;
- Không cung cấp thông tin cá nhân qua điện thoại, không nhấp vào các ảnh, video, đường dẫn hoặc cài đặt ứng dụng theo sự hướng dẫn của người lạ;
- Tuyệt đối không chia sẻ thông tin, mã OTP ngân hàng cho bất kỳ ai;
- Nếu đã nhấp vào các ảnh, video, đường dẫn hoặc cài đặt ứng dụng hay trong bất kỳ trường hợp nghi vấn bị chiếm quyền điều khiển thiết bị di động, cần thông báo ngay cho Ngân hàng của mình để tạm khóa tài khoản, ngay lập tức tắt nguồn thiết bị di động;
- Trình báo đến cơ quan Công an nơi gần nhất để được hướng dẫn, hỗ trợ.

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người cao tuổi, người sống một mình, sinh viên, người lao động ngoại tỉnh.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng gọi điện cho người dân tự xưng là nhân viên nhà cung cấp dịch vụ điện, nước, truyền hình, internet...; - Yêu cầu người dân cung cấp thông tin hợp đồng sử dụng dịch vụ; - Thông báo nợ hóa đơn, yêu cầu chuyển khoản gấp để không bị cắt dịch vụ; - Nếu người dân báo đã thanh toán, đối tượng hướng dẫn truy cập đường link hoặc cài ứng dụng giả mạo để quản lý thông tin hợp đồng.	- Kiểm tra trực tiếp với đơn vị cung cấp dịch vụ; - Tuyệt đối không chuyển tiền hoặc cung cấp thông tin cá nhân cho người lạ; - Không cài ứng dụng, nhấn vào link không rõ nguồn gốc theo hướng dẫn; - Báo ngay cho cơ quan chức năng khi phát hiện dấu hiệu lừa đảo.



Giả danh nhân viên công ích thông báo đến hạn đóng tiền điện, nước, truyền hình, internet ...

Giả danh cơ quan chức năng hỗ trợ thu hồi vốn treo hoặc tiền bị lừa đảo trực tuyến

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người đã từng là nạn nhân của lừa đảo trực tuyến.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Các đối tượng lấy danh nghĩa cơ quan Công an, Viện Kiểm sát, Tòa án, Văn phòng luật, luật sư...; - Các đối tượng chủ động liên hệ người dân qua điện thoại hoặc tài khoản mạng xã hội và nói chi tiết về việc người dân đã bị lừa trước đó; - Các đối tượng đăng tải thông tin quảng cáo dịch vụ lấy lại tiền bị lừa, khi người dân liên hệ sẽ yêu cầu trình báo nội dung; - Thông báo với người dân về việc hồ sơ đã được xác lập, xếp số thứ tự lớn, cần mất nhiều thời gian để giải quyết, nếu muốn giải quyết sớm cần chuyển các khoản phí để đẩy nhanh tiến độ, qua đó chiếm đoạt số tiền này; - Một số trường hợp, các đối tượng thông báo việc chuyển tiền bị lỗi, cần nộp các khoản thuế, phí để rút lại số tiền lỗi trước đó.	- Không có bất kỳ cơ quan, tổ chức, cá nhân nào đăng tải thông tin về việc hỗ trợ lấy lại tiền bị lừa đảo trực tuyến. Tất cả các tài khoản mạng xã hội giới thiệu hỗ trợ thu hồi tiền bị lừa qua mạng đều là tài khoản lừa đảo; - Tuyệt đối không làm theo bất kỳ hướng dẫn nào của các đối tượng; - Trình báo đến cơ quan Công an nơi gần nhất để được hỗ trợ, hướng dẫn.

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Phụ huynh, học sinh – sinh viên.

DẤU HIỆU:

- Đối tượng gọi điện, nhắn tin, gửi email giả danh cơ sở giáo dục hoặc tạo lập website, tài khoản mạng xã hội mạo danh cơ sở giáo dục đăng tải thông tin trại hè;
- Thông báo chính sách của Nhà nước về miễn giảm học phí, có thể nhận lại tiền học phí đã nộp trước đó;
- Thông báo đủ điều kiện nhận học bổng, chương trình du học, trại hè...;
- Yêu cầu truy cập đường dẫn chứa mã độc để làm thủ tục nhận lại tiền học phí đã nộp trước đó, dụ dỗ cung cấp thông tin cá nhân, tài khoản ngân hàng, mã OTP ngân hàng để chiếm đoạt tiền;
- Yêu cầu chuyển tiền vào tài khoản ngân hàng giả mạo cơ sở giáo dục để chứng minh tài chính, "đua top sao kê" để xét duyệt đủ điều kiện nhận học bổng, chương trình du học;
- Đề nghị chuyển tiền phí tham dự trại hè, truy cập vào website giả mạo để nạp tiền làm nhiệm vụ, tăng tương tác cho con, thu về lợi nhuận, qua đó chiếm đoạt tài sản.

BIỆN PHÁP PHÒNG TRÁNH:

- Luôn xác minh thông tin tại cơ sở giáo dục chính thống;
- Không truy cập đường dẫn lạ, không cung cấp thông tin và gửi mã OTP ngân hàng cho bất kỳ ai;
- Luôn cảnh giác với những lời mời chào hấp dẫn;
- Trình báo đến cơ quan Công an nơi gần nhất.

Giả danh cơ sở giáo dục thông báo hoàn trả học phí hoặc được nhận học bổng, chương trình du học, tham gia trại hè...

Giả danh cơ sở giáo dục, y tế… thông báo người thân gặp tai nạn

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Phụ huynh học sinh, người có người thân đang đi học/làm xa.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng gọi điện thông báo gấp con/em/bạn bị tai nạn nghiêm trọng, đang được đưa đi cấp cứu tại các cơ sở y tế; - Giọng điệu lo lắng, hối thúc chuyển tiền viện phí ngay để cứu chữa; - Tìm cách không cho liên lạc trực tiếp với người được nhắc đến.	- Giữ bình tĩnh, kiểm tra với nhà trường, cơ sở y tế; - Không chuyển tiền ngay khi chưa xác thực thông tin; - Trình báo cơ quan Công an gần nhất.

Giả danh cơ quan thực thi pháp luật thông báo liên quan đến vụ án nghiêm trọng

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người cao tuổi, học sinh - sinh viên thiếu kiến thức pháp luật, dễ bị dao động tâm lý.

DẤU HIỆU:

- Đối tượng sử dụng thuê bao di động, tài khoản mạng xã hội hoặc gọi điện từ "tổng đài" cho người dân, tự xưng là cán bộ công an, viện kiểm sát, tòa án...;
- Thông báo ông/bà, anh/chị đang liên quan đến vụ án rửa tiền, buôn ma túy..., đưa ra lệnh bắt, quyết định khởi tố... Một số trường hợp, các đối tượng nối máy cho nạn nhân gặp nhiều người với vai trò: kiểm sát viên, luật sư, tòa án, điều tra viên...để tác động vào tâm lý của nạn nhân.
- Yêu cầu nạn nhân chuyển tiền vào tài khoản ngân hàng của chúng để tiến hành xác minh, hoặc yêu cầu mở tài khoản ngân hàng mới, cung cấp thông tin cho chúng, sau đó chuyển hết tiền vào tài khoản mới để "niêm phong", phục vụ công tác điều tra.

BIỆN PHÁP PHÒNG TRÁNH:

- Cơ quan pháp luật không yêu cầu người dân cung cấp thông tin, giải quyết công việc thông qua điện thoại;
- Tuyệt đối không chuyển tiền, không khai báo thông tin cá nhân qua điện thoại;
- Liên hệ cơ quan Công an nơi gần nhất để xác minh thông tin liên quan.

Giả danh cơ sở du lịch, nhà hàng, hộ kinh doanh… rao bán hàng hóa, dịch vụ

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người hay mua hàng online, du lịch, ăn uống, người tiêu dùng phổ thông.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng tạo lập tài khoản mạng xã hội giả mạo, chạy quảng cáo rao bán các loại dịch vụ: combo du lịch, vé máy bay, hàng hóa, thực phẩm… với giá tương đương hoặc thấp hơn sản phẩm thật; - Tài khoản mạng xã hội được đặt tên giống cơ sở thật, đăng tải lại các bài viết từ cơ sở thật, chạy quảng cáo để tăng lượt tương tác. Đáng chú ý, nhiều đối tượng đã thuê, mua hoặc tấn công đánh cắp các tài khoản mạng xã hội được xác thực của nhà cung cấp (có tích xanh) để tăng độ uy tín; - Yêu cầu người dân chuyển khoản đặt cọc hoặc chuyển trước toàn bộ số tiền, sau đó chiếm đoạt và chặn mọi liên lạc.	- Người dân nên lựa chọn mua hàng hóa, dịch vụ từ các cơ sở uy tín, đã từng giao dịch từ trước; - Luôn kiểm tra “Tính minh bạch” của tài khoản mạng xã hội trước khi lựa chọn giao dịch. Các tài khoản giả mạo thường mới được tạo lập hoặc đổi tên trong thời gian gần, vị trí người quản lý có thể ở nước ngoài hoặc ở Việt Nam; - Tìm kiếm thêm thông tin về cơ sở thật từ nhiều nguồn trên mạng internet; - Xác thực kỹ thông tin doanh nghiệp trước khi giao dịch.

Giả danh cơ quan nhà nước, lực lượng vũ trang… đặt mua hàng hóa

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Các cá nhân, tổ chức, hộ kinh doanh… thường xuyên có giao dịch mua bán, đặt hàng online.

DẤU HIỆU:

- Các đối tượng chủ động liên hệ, hỏi mua hàng hóa với số lượng lớn, sau đó tự xưng là cán bộ cơ quan nhà nước, lực lượng vũ trang, lấy nhiều lý do để nhờ đặt gấp một số vật tư, trang thiết bị khác cho đơn vị (giường, tủ,…);
- Hướng dẫn nạn nhân gọi điện đặt vật tư, trang thiết bị khác theo thông tin chúng cung cấp;
- Đưa nhiều số điện thoại (người bán hàng, người giao hàng…) để tạo kịch bản giống như chúng đang giao hàng thật;
- Lấy lý do để yêu cầu người dân chuyển tiền, thanh toán tiền hàng để kịp xuất hàng, liên tục hối thúc người dân thanh toán tiền hàng.

BIỆN PHÁP PHÒNG TRÁNH:

- Chỉ buôn bán mặt hàng do mình cung cấp, không đặt hàng giúp người khác khi không quen biết;
- Không chuyển tiền theo yêu cầu của người lạ;
- Trình báo đến cơ quan Công an nơi gần nhất để được hướng dẫn, hỗ trợ.

Giả danh nhân viên giao hàng thông báo nhận hàng, lừa thanh toán tiền

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người dân hay mua hàng online.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng mạo danh nhân viên giao hàng (Shopee, Lazada, GHTK,...) nhắn tin, gọi điện cho người dân thông báo có đơn hàng, yêu cầu thanh toán tiền phí mua hàng và phí vận chuyển; - Khi người dân chuyển tiền, các đối tượng sẽ lấy lý do là sai cú pháp chuyển tiền nên chưa nhận được tiền, yêu cầu người dân chuyển tiền lại hoặc cung cấp thông cá nhân, truy cập đường dẫn giả mạo. - Một số trường hợp, khi khách hàng không đồng ý nhận hàng, các đối tượng gửi đường dẫn giả mạo xác nhận đơn hàng, yêu cầu cung cấp thông tin hoặc làm theo hướng dẫn để chiếm đoạt tiền trong tài khoản ngân hàng.	- Xác minh đơn hàng thật trước khi thanh toán, không nên tin tưởng vào người giao hàng (kể cả người giao hàng quen); - Không truy cập link xác nhận từ người lạ; - Không chia sẻ thông tin cá nhân, tài khoản ngân hàng với bất kỳ ai.

Giả danh tổ chức, doanh nghiệp thông báo trúng thưởng, nhận quà

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người nhẹ dạ, dễ bị thu hút bởi khuyến mãi.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng mạo danh các Siêu thị, cửa hàng điện máy, doanh nghiệp có uy tín... gọi điện, gửi tin nhắn cho người dân thông báo trúng thưởng nhân sự kiện tri ân khách hàng; - Yêu cầu cung cấp thông tin cá nhân để nhận quà hoặc nộp các loại thuế, phí...; - Dẫn dụ truy cập các đường dẫn có chứa mã độc.	- Liên hệ đến số điện thoại hotline của các cơ sở chính thống để kiểm tra tính xác thực; - Không chuyển tiền trước để "nhận quà"; - Cảnh giác với những thông tin quá tốt, không rõ nguồn.

Giả danh nhân viên tổ chức tín dụng hỗ trợ mở thẻ, nâng hạn mức tín dụng

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Mọi người dân, tập trung chủ yếu vào nhóm người có nhu cầu tài chính, đang dùng thẻ tín dụng.

DẤU HIỆU:

- Đối tượng mạo danh nhân viên Ngân hàng, doanh nghiệp tài chính gọi điện, nhắn tin cho người dân, giới thiệu nâng hạn mức miễn phí, mở thẻ ưu đãi hoặc chương trình cho vay dễ dàng, mức vay cao;
- Yêu cầu cung cấp thông tin cá nhân;
- Hướng dẫn truy cập đường dẫn hoặc cài ứng dụng có chứa mã độc nhằm đánh cắp thông tin, chiếm quyền điều khiển thiết bị.

BIỆN PHÁP PHÒNG TRÁNH:

- Liên hệ ngân hàng chính thống để xác thực thông tin;
- Không chia sẻ thông tin cá nhân cho người lạ qua mạng;
- Không cài ứng dụng theo hướng dẫn từ người lạ.

Giả danh cơ quan thuế gọi điện yêu cầu hoàn thiện thủ tục

Mọi người dân, tập trung chủ yếu vào nhóm người dân đang kê khai thuế, hộ kinh doanh.

- Xưng là cán bộ thuế thông báo vi phạm, truy thu hoặc thông báo về doanh nghiệp vừa thành lập, cần nộp thuế đăng ký doanh nghiệp;
- Yêu cầu truy cập đường dẫn hoặc cài ứng dụng giả danh phần mềm ngành thuế để kê khai thông tin, từ đó chiếm quyền điều khiển thiết bị, tài khoản ngân hàng.

- Liên hệ với cơ quan thuế chính thống để xác thực thông tin;
- Không làm theo hướng dẫn truy cập đường dẫn hay cài đặt ứng dụng từ người lạ;
- Nếu đã truy cập đường dẫn hoặc cài ứng dụng giả mạo, nhanh chóng liên hệ ngân hàng chủ quản để yêu cầu tạm khóa tài khoản, tắt nguồn thiết bị di động và trình báo đến cơ quan Công an nơi gần nhất để được hướng dẫn.

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người không hạnh phúc trong hôn nhân, người đang tìm kiếm mối quan hệ.

DẤU HIỆU:

- Sử dụng tài khoản mạng xã hội với hình ảnh ưa nhìn, điều kiện khá giả để tiếp cận, làm quen qua mạng xã hội với nhiều lý do như: hỏi về các tấm ảnh, địa điểm, nhắn tin nhầm...;
- Hàng ngày nhắn tin hỏi han, trò chuyện, chia sẻ cuộc sống, thường xuyên quan tâm, thậm chí tặng quà cho nạn nhân để gây dựng tình cảm;
- Sau thời gian tạo lòng tin, đối tượng tiếp tục trò chuyện kèm theo đưa thông tin về công việc hiện tại mang lại lợi nhuận cao cho bản thân;
- Lấy lý do nhờ nạn truy cập vào tài khoản của đối tượng trên trang đầu tư và thực hiện theo các thao tác: nhắn tin cho hệ thống, lấy số tài khoản để nạp tiền, sau khi tiền hiển thị trên tài khoản thì thực hiện lệnh rút tiền. Việc này nhằm mục đích khiến nạn nhân tin rằng chỉ với các thao tác đơn giản đã có thể kiếm được lợi nhuận lớn và dễ dàng rút tiền về, thực chất trang web đầu tư là trang giả mạo, số tiền trên tài khoản cũng do đối tượng tự tạo ra, giả mạo bill chuyển tiền để lừa người dân;
- Dẫn dụ nạn nhân tạo tài khoản, nạp tiền, một vài lần đầu có lợi nhuận, sau đó tiếp tục nạp số tiền lớn rồi chiếm đoạt.

Lừa đảo tình cảm sau đó dẫn dụ đầu tư tài chính, đánh bạc

BIỆN PHÁP PHÒNG TRÁNH:

- Cảnh giác khi có người lạ tiếp cận, tìm cách kết bạn qua mạng, mối quan hệ online phát triển quá nhanh;
- Tuyệt đối không chuyển tiền, đầu tư theo lời dụ dỗ từ người quen qua mạng;
- Tìm hiểu kỹ trước khi tham gia bất kỳ nền tảng tài chính nào;

Lưu ý: Không có công việc nào dễ dàng kiếm tiền mà không mất sức lao động

- Trình báo đến cơ quan Công an nơi gần nhất khi có dấu hiệu là nạn nhân của lừa đảo trực tuyến.

Lừa đảo tình cảm, thu thập hình ảnh nhạy cảm để tống tiền

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người sử dụng mạng xã hội tìm kiếm các mối quan hệ online, người thiếu thốn tình cảm.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng có thể thông qua các ứng dụng trò chuyện, kết bạn trên mạng để tiếp cận yêu đương, thân mật, gạ gẫm gọi video nhạy cảm; - Quá trình trò chuyện video, đối tượng thường gợi ý để nạn nhân quay rõ nét chân dung, khuôn mặt, khung cảnh xung quanh để ghi lại hình ảnh; - Sau khi đã có hình ảnh nhạy cảm, đối tượng sử dụng tài khoản mạng xã hội hoặc thuê bao di động nhắn tin, gọi điện với người dân và yêu cầu chuyển tiền, nếu không sẽ gửi các hình ảnh, video đó cho bạn bè, người thân, nơi làm việc và công khai lên mạng; - Khi nạn nhân chuyển tiền, chúng sẽ dựa vào lý do đó để tiếp tục đòi tiền thêm nhiều lần nữa, đến khi nạn nhân không đủ khả năng chuyển thêm.	- Không trò chuyện video với người lạ trên mạng xã hội; - Cẩn trọng khi kết bạn, kết nối ghép đôi trên mạng xã hội; - Tuyệt đối không chuyển tiền và làm theo yêu cầu của các đối tượng, khóa tài khoản mạng xã hội của bản thân và người quen nhằm hạn chế sức lan tỏa của hình ảnh, video; - Lưu lại tất cả bằng chứng và trình báo cơ quan Công an nơi gần nhất.

Lừa đảo tình cảm, hứa hẹn tặng quà giá trị cao

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người độc thân hoặc không hạnh phúc trong hôn nhân.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Đối tượng xây dựng tài khoản mạng xã hội ảo với hình thức hào nhoáng, bóng bẩy, chủ động kết bạn hoặc tìm cách làm quen qua mạng, giới thiệu đang sống, công tác ở nước ngoài; - Sau khi trò chuyện một thời gian, đối tượng hứa hẹn gửi quà đắt tiền về Việt Nam cho nạn nhân; - Đối tượng giả danh nhân viên hải quan hoặc đơn vị giao hàng yêu cầu đóng các loại phí như: thuế, tiền vận chuyển, kiểm tra hàng... hoặc nộp tiền bảo đảm vì hàng giá trị cao.	- Cẩn trọng khi kết bạn qua mạng, không đặt niềm tin vào các mối quan hệ chưa gặp mặt trực tiếp hoặc chưa nắm rõ thông tin cá nhân của đối phương; - Tuyệt đối không chuyển bất kỳ loại thuế, phí nào để nhận quà.

Lừa đảo tham gia đầu tư sàn chứng khoán, tiền ảo, đa cấp… sau đó khóa, "đánh cháy" tài khoản hoặc đánh sập sàn

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người muốn làm giàu nhanh, ít hiểu biết về tài chính.

DẤU HIỆU:

- Đối tượng gọi điện hoặc nhắn tin qua mạng xã hội cho người dân, mời tham gia sàn đầu tư online, nếu đồng ý tham gia thì người dân sẽ được cho tham gia vào nhóm chuyên gia chia sẻ các lệnh "VIP", cam kết lãi suất cao;
- Ban đầu cho thắng và rút thử số tiền nhỏ để tạo lòng tin, dần dần dụ dỗ đầu tư số tiền lớn;
- Khi nạn nhân nạp nhiều tiền thì dùng nhiều lý do khóa tài khoản, không rút được tiền, yêu cầu chuyển thêm tiền để nộp thuế, chứng minh tài chính hoặc thậm chí cho "sập" sàn.

BIỆN PHÁP PHÒNG TRÁNH:

- Không đầu tư vào nền tảng không có pháp lý rõ ràng;
- Không tin vào lời mời đầu tư "lợi nhuận cao, rủi ro thấp" từ các cá nhân, tổ chức qua mạng.

Lừa đảo qua hình thức tuyển cộng tác viên cho các sàn thương mại điện tử, làm nhiệm vụ hưởng lương cao

Sinh viên, người thất nghiệp, người có nhu cầu làm việc tại nhà để kiếm thêm thu nhập.

- Đối tượng đăng thông tin hoặc gửi tin nhắn tuyển dụng trên các ứng dụng mạng xã hội: việc nhẹ, lương cao, làm việc online với lời mời chào hấp dẫn, dễ dàng kiếm thêm thu nhập;
- Giao nhiệm vụ "tăng tương tác", "đặt đơn ảo",... và yêu cầu nộp tiền để hoàn thành nhiệm vụ;
- Sau khi nạp nhiều tiền thì không thể rút tiền hoặc bị chặn liên hệ.

- Không đóng tiền hay đặt cọc cho bất kỳ việc làm nào chưa rõ thông tin;
- Cảnh giác với lời mời làm việc quá dễ dàng;
- Không tham gia làm việc khi chưa kiểm chứng kỹ thông tin của người cung cấp việc làm qua mạng.

Phát tán mã độc xâm nhập hệ thống của tổ chức, doanh nghiệp, thay đổi email, tài khoản nhận tiền

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Doanh nghiệp, tổ chức thường xuyên có hoạt động giao dịch thanh toán với đối tác nước ngoài.

DẤU HIỆU:

- Các đối tượng đã tìm cách gửi email kèm mã độc từ trước nhằm xâm nhập hệ thống của cơ quan, tổ chức, doanh nghiệp;
- Tạo email giả, thay đổi thông tin tài khoản ngân hàng nhận tiền và gửi cho đối tác nước ngoài.

BIỆN PHÁP PHÒNG TRÁNH:

- Xác minh cẩn thận email, hóa đơn thanh toán qua nhiều nguồn;
- Không nhấp vào các đường dẫn lạ từ người lạ hoặc kiểm tra lại tính chính xác của đường dẫn từ người gửi trước khi mở;
- Sử dụng và thường xuyên cập nhật hệ thống bảo mật cho doanh nghiệp.

Đưa thông tin sai sự thật, dẫn dụ truy cập đường dẫn chứa mã độc

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người tò mò, thiếu niềm tin, thường xuyên sử dụng mạng xã hội.

DẤU HIỆU:

- Gửi tin nhắn với nội dung "sốc", "nóng", "bí mật", "bóc phốt"... có nội dung giật gân như: vợ/chồng ngoại tình, xem hình ảnh hoặc click vào đường dẫn để xem chi tiết...;
- Chèn đường dẫn đến trang chứa mã độc để đánh cắp thông tin, chiếm quyền điều khiển thiết bị;
- Hướng dẫn nạn nhân làm theo các thao tác để xem nội dung, thực chất tìm cách thu thập thông tin tài khoản, mã OTP ngân hàng, dữ liệu sinh trắc học nhằm chiếm đoạt tiền trong tài khoản ngân hàng.

BIỆN PHÁP PHÒNG TRÁNH:

- Cẩn trọng trước những thông tin đến từ người lạ, không ấn vào ảnh, video hoặc truy cập các đường dẫn không rõ nguồn gốc;
- Không chia sẻ tin tức chưa kiểm chứng;
- Nếu đã truy cập đường dẫn giả mạo, nhanh chóng liên hệ ngân hàng chủ quản để yêu cầu tạm khóa tài khoản, tắt nguồn thiết bị di động và trình báo đến cơ quan Công an nơi gần nhất để được hướng dẫn.

Một số hình thức lừa đảo khác (cho số lô đề, đổ thạch, xổ số nước ngoài, cắt ghép hình ảnh tống tiền…)

NHÓM NGƯỜI BỊ TỘI PHẠM NHẮM ĐẾN:

Người thích cờ bạc, mê tín dị đoan, thiếu hiểu biết về công nghệ, người có uy tín, địa vị trong xã hội.

DẤU HIỆU	BIỆN PHÁP PHÒNG TRÁNH
- Sử dụng tài khoản mạng xã hội quảng cáo dịch vụ “cho số”, “bùa tài lộc”, “xổ số trúng lớn”, “cắt đá tìm ngọc”, “xổ số nước ngoài”…; - Chủ động nhắn tin cho nạn nhân để gửi video/ảnh ghép giả mạo để đe dọa tống tiền.	- Không tham gia các hội nhóm mê tín, đánh bạc online hoặc các hình thức kiếm tiền dễ dàng trên không gian mạng; - Không chia sẻ hình ảnh riêng tư lên mạng xã hội; - Lưu lại các tài liệu, bằng chứng và trình báo cơ quan Công an nơi gần nhất.

BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG
TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

AGRIBANK

Bảo vệ bản thân, bảo vệ gia đình khỏi tội phạm công nghệ cao

Chung tay xây dựng một không gian mạng an toàn!