

NỘI DUNG TUYÊN TRUYỀN VỀ PHÒNG NGỪA TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Hiện nay các đối tượng xấu lợi dụng những tiện ích mà công nghệ thông tin mang lại để thực hiện nhiều vụ lừa đảo trên mạng xã hội, mạng viễn thông để chiếm đoạt tài sản có giá trị cao.

Các hình thức lừa đảo trên mạng xã hội, mạng viễn thông liên tục gia tăng không ngừng, từ lừa đảo đánh cắp thông tin cá nhân, lừa đảo tình cảm, lừa đảo đầu tư,... nhưng mục tiêu cuối cùng của các đối tượng xấu chính là tiền.

Tính riêng trong năm 2022, có 3 nhóm lừa đảo chính là giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác, với 16 hình thức lừa đảo thường xuyên diễn ra trên mạng xã hội, mạng viễn thông, cụ thể:

Nhóm 1 - Giả mạo thương hiệu, gồm:

- Giả mạo thương hiệu của các cơ quan, tổ chức, như: Cơ quan nhà nước, ngân hàng, công ty tài chính, công ty chứng khoán... để gửi tin nhắn SMS lừa đảo cho nạn nhân.
- Giả mạo các trang web/blog chính thống để tạo uy tín lừa nạn nhân, thu thập thông tin cá nhân của người dân.

Nhóm 2 - Chiếm đoạt tài khoản, gồm:

- Chiếm quyền sử dụng các tài khoản mạng xã hội, như: Zalo, Facebook, Tiktok... để gửi tin nhắn lừa đảo cho bạn bè, người thân nhằm chiếm quyền tài khoản, lấy cắp thông tin, chiếm đoạt tài sản, bôi nhọ danh dự, tống tiền...
- Sử dụng các ứng dụng, quảng cáo tin dụng đen trên các trang web, gửi qua các thư điện tử rác, tin nhắn SMS, mạng xã hội Facebook, Telegram, Zalo... để dụ dỗ người dùng biến họ thành con nợ trong khi chính nạn nhân cũng không biết.

Nhóm 3 - Các hình thức kết hợp, gồm:

- Sử dụng số điện thoại trong nước, nước ngoài, giả danh cơ quan công an, nhà mạng viễn thông... để gọi điện thoại cho nạn nhân thông báo vi phạm pháp luật và yêu cầu chuyển khoản.
- Sử dụng số điện thoại đầu số lạ gọi điện cho nạn nhân, khi bắt máy nạn nhân sẽ bị trừ tiền trong tài khoản mà không hề biết.
- Giả mạo các trang thương mại điện tử lớn tại Việt Nam và nước ngoài để lừa nạn nhân làm cộng tác viên. Để dẫn dụ nạn nhân, đối tượng chạy quảng cáo lừa đảo trên Facebook hay gửi tin nhắn quảng cáo spam qua SMS.

- Lan truyền tin giả đánh vào tâm lý hiếu kỳ, sự thương người và lòng tin. Để câu views, câu likes và sau đây lừa gạt chiếm đoạt tài sản qua hình thức từ thiện, kêu gọi đóng góp...

- Lừa đảo chiếm đoạt tài sản qua quảng bá bán hàng online trên Facebook (bán hàng giả, chất lượng kém, vé máy bay giả, khuyến mãi giả, hàng ảo hoặc rao bán giả mạo không tồn tại sản phẩm).

- Giả mạo trang cá nhân, tài khoản người dùng trên Facebook, Telegram, Zalo để tạo uy tín và lừa nạn nhân sử dụng dịch vụ hoặc đầu tư.

- Lợi dụng lòng tin và sự thương hại để lừa đảo qua các nền tảng Facebook, Zalo, Tinder, Telegram.

- Lừa đảo cài cắm mã độc thông qua đường dẫn độc hại, phần mềm độc hại. Đối tượng tạo những công cụ, đường dẫn, phần mềm độc hại để chiếm đoạt tài sản, thông tin tài khoản mạng xã hội, ngân hàng.

- Thông báo trúng thưởng, quà tặng, khuyến mại để lừa nạn nhân đánh cắp thông tin tài khoản và tài sản thông qua các trang web giả mạo.

- Thủ đoạn nâng cấp lên sim 4G hay 5G để lừa lấy số điện thoại của nạn nhân nhằm chiếm đoạt thông tin tài khoản và tài sản.

- Giả mạo email của ngân hàng, cơ quan, tổ chức có uy tín để uy hiếp, đe dọa lừa tiền nạn nhân.

- Lập sàn đầu tư tiền ảo crypto, đầu tư đa cấp, đầu tư nhị phân, đầu tư Forex... lừa đảo chiếm đoạt tài sản.

Để bảo vệ người dân trước vấn nạn lừa đảo trên mạng xã hội, mạng viễn thông, các cơ quan chức năng, doanh nghiệp cung cấp dịch vụ, doanh nghiệp an toàn, an ninh mạng đã triển khai nhiều biện pháp kỹ thuật, hoạt động tuyên truyền, nâng cao nhận thức cho khách hàng, người dân.

Đề nghị người dân cần cảnh giác, khi phát hiện các hoạt động nêu trên trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./.

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm lừa đảo đăng tin tuyển cộng tác viên bán hàng online trên các trang mạng xã hội (Zalo, Facebook, Tiktok...), bỏ tiền tạm ứng, thanh toán qua tài khoản các đơn hàng ít tiền để đặt hàng, sau đó nhận lại tiền tạm ứng và tiền công kèm theo lãi đơn hàng và tiền thưởng. Đến các lần tiếp theo, thanh toán đơn hàng với lượng tiền lớn thì bị chiếm đoạt, đồng thời nhận được yêu cầu nộp thêm tiền để hệ thống xử lý lỗi và hoàn trả nhưng không được hoàn trả.

Đề nghị người dân cần cảnh giác, không tham gia hoạt động nêu trên, khi phát hiện trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./.

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm giả danh cơ quan Công an, Viện Kiểm sát, Tòa án... gọi điện thông báo có liên quan đến các vụ án đang điều tra, mua bán ma túy, rửa tiền..., gửi lệnh bắt giữ hay tài liệu liên quan khác qua mạng xã hội để đe dọa, yêu cầu chuyển tiền đến các tài khoản chỉ định hoặc tài khoản mới mở rồi cung cấp thông tin tài khoản để kiểm tra hoặc tải các đường link, phần mềm giả mạo cơ quan, nhằm đánh cắp thông tin tài khoản ngân hàng để chiếm đoạt. Việc các cơ quan chức năng điều tra, xác minh, xử lý tội phạm đều được tiến hành trực tiếp, không thông qua mạng xã hội gửi thông báo, tin nhắn yêu cầu.

Đề nghị người dân cần cảnh giác, không thực hiện theo các yêu cầu của đối tượng và trình báo ngay với cơ quan công an nơi gần nhất để giải quyết./

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm giả mạo là người nước ngoài (sỹ quan, binh lính đang tham gia chiến tranh, làm nhiệm vụ quốc tế tại các khu vực chiến sự... không có người thân) thông qua mạng xã hội làm quen, sau đó lấy lý do gửi quà, đồ vật giá trị, thậm chí là ngoại tệ, vàng có giá trị rất lớn nhờ nhận, quản lý, lưu giữ; sau đó giả danh là nhân viên sân bay, hải quan, thuế... yêu cầu nộp tiền cước vận chuyển, thuế, phí, tiền phạt, chi phí tiêu cực... để chiếm đoạt.

Đề nghị người dân cần cảnh giác, không chuyển tiền vào các tài khoản do đối tượng yêu cầu và trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./

CỤC THÔNG TIN CƠ SỞ