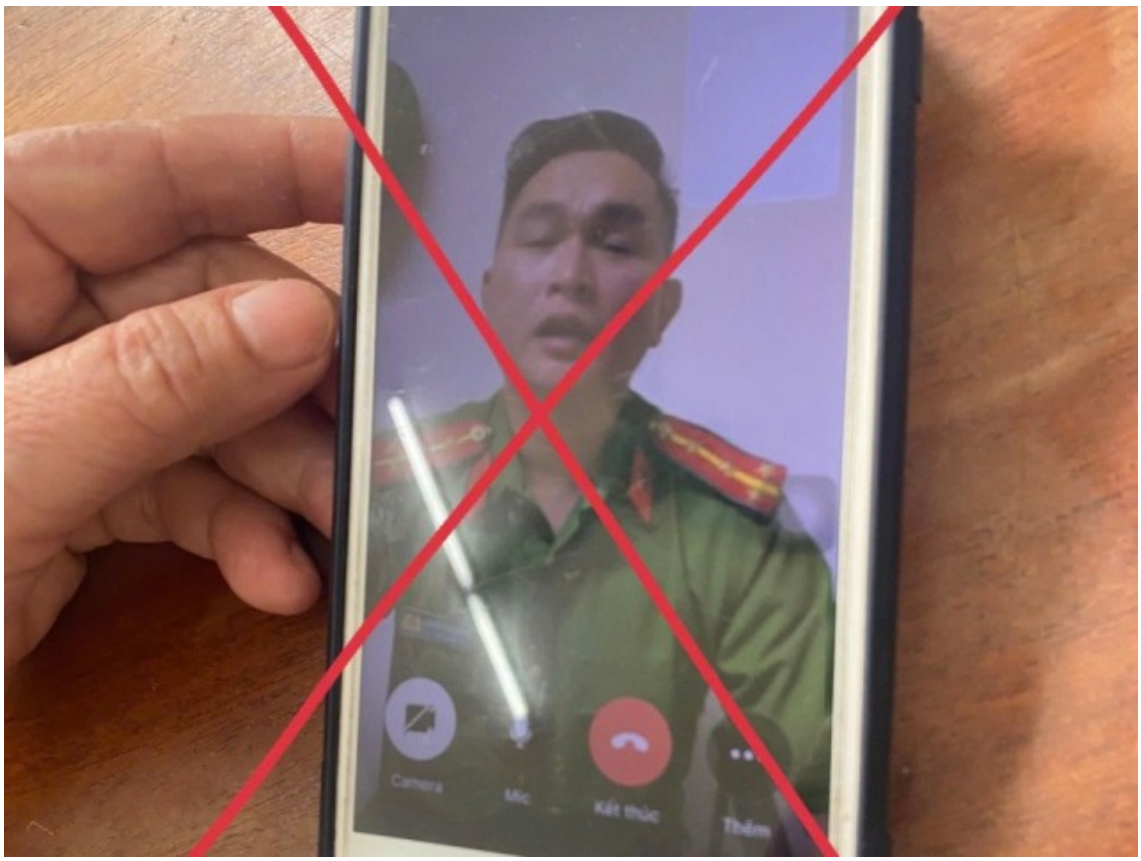
TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cảnh giác với thủ đoạn sử dụng công nghệ Deepfake giả danh Công an lừa đảo

13:32 13/09/2024

Hiện nay, việc các đối tượng giả danh Công an để gọi video Zalo, facetime lừa đảo làm định danh tài khoản ngân hàng của người dân là một hình thức lừa đảo mới. Các đối tượng sử dụng công nghệ deepfake, tạo ra một cán bộ Công an rồi yêu cầu nạn nhân làm theo hướng dẫn. Vì nhẹ dạ cả tin, nhiều người đã sập bẫy...



Các đối tượng sử dụng công nghệ deepfake, tạo ra một cán bộ Công an rồi yêu cầu nạn nhân làm theo hướng dẫn để lừa đảo.

Vừa qua chị P. (SN 1968) trú tại thôn N.H, xã Nhân Trạch, huyện Bố Trạch lên trình báo với Công an xã Nhân Trạch về việc có người lạ xưng là Công an gọi điện cho chị và báo chị có liên quan đến vụ án ma túy, có giao dịch tài khoản liên quan đến vụ án ma túy, sau đó đối tượng hướng dẫn chị đăng ký và sử

dụng Zalo để tiện liên lạc, sau khi đăng ký được tài khoản Zalo thì đối tượng sẽ gọi bằng hình ảnh qua Zalo cho nạn nhân và sử dụng công nghệ Deepfake có hình ảnh của lực lượng Công an rồi thông báo, đe dọa nạn nhân. Thủ đoạn đối tượng là yêu cầu nạn nhân quay phòng ở và chỉ ở một mình trong phòng, nếu thường xuyên có người trong gia đình đi lại thì đối tượng tiếp tục yêu cầu nạn nhân ra khách sạn gần nhất để tiện cho việc liên lạc rồi nhằm mục đích lừa đảo để chuyển tiền cho đối tượng…

Lực lượng Công an khuyến cáo, các nạn nhân bị lừa đảo bằng các hình thức giả danh Facebook, Deepfake… ngày càng có xu hướng gia tăng trên khắp cả nước. Các đối tượng lừa đảo dùng thủ đoạn rất tinh vi, có thể xảy ra với bất cứ ai và bất cứ thời điểm nào. Khi nhận bất kỳ tin nhắn vay mượn tiền thông qua mạng xã hội, người dân cần điện thoại trực tiếp cho người thân để xác minh. Trường hợp nghi vấn đối tượng giả mạo người thân trên mạng xã hội để lừa đảo, chiếm đoạt tài sản, cần báo ngay cho cơ quan công an gần nhất để được hỗ trợ, xử lý kịp thời.

Cơ quan Công an không xử lý các vụ việc bằng hình thức online, tất cả được giải quyết tại trụ sở. Vì vậy, nếu phát hiện ra trường hợp giả danh công an, người dân cần báo ngay cho cơ quan công an để nhanh chóng xác minh, ngăn chặn và xử lý các đối tượng vi phạm theo quy định của pháp luật.

Cách nhận biết và phòng tránh lừa đảo thông qua video Deepfake

Trường hợp lừa đảo và gian lận trực tuyến thông qua việc giả danh công an, ngân hàng, người thân trong gia đình… sử dụng công nghệ Deepfake để chiếm đoạt tài sản đang diễn ra càng nhiều.

Deepfake là một công nghệ trí tuệ nhân tạo cho phép tạo ra những video, hình ảnh và âm thanh giả mạo với độ chân thực khá cao. Vậy nên, bạn cần nắm bắt thông tin để nhận biết video Deepfake để tránh bị lừa đảo và nhận diện thông tin sai lệch.

Kiểm tra chuyển động trên khuôn mặt

Một trong những dấu hiệu dễ nhận biết video giả danh nhất chính chính là chuyển động mắt không tự nhiên và thiếu chớp mắt. Deepfake vẫn đang còn nhiều hạn chế, công nghệ này không thể hoàn toàn mô phỏng được cách chớp mắt tự nhiên của con người hoặc tái tạo chính xác những chuyển động của mắt.

Ngoài ra, bạn còn có thể nhận biết video Deepfake giả mạo thông qua cảm xúc của khuôn mặt không trùng với nội dung, màu da, tóc và răng không giống với thực tế, hoặc xuất hiện những ánh sáng kỳ lạ do việc sử dụng trí tuệ nhân tạo

để tái tạo.

Chất lượng âm thanh

Bạn có thể nhận biết video giả danh được tạo bởi Deepfake thông qua âm thanh, bởi công nghệ này thường tập trung vào tái tạo hình ảnh và video hơn. Cần chú ý đến chuyển động của miệng khi người trong video nói, để kiểm tra xem âm thanh có phù hợp so với hình ảnh hay không.

Theo Ngọc Hoàng/congan.quangbinh.gov.vn