



CÔNG AN HUYỆN HÓC MÔN

## THÔNG BÁO

V/v tuyên truyền người dân cảnh giác  
với hành vi ghép mặt, giả giọng để lừa đảo  
(Đính kèm Công văn: /CAHM-PT)

Thời gian qua trên địa bàn cả nước nói chung và Thành phố Hồ Chí Minh nói riêng xuất hiện nhiều vụ lừa đảo qua mạng internet, sử dụng trí tuệ nhân tạo (AI) cắt ghép hình ảnh, video lừa đảo chiếm đoạt tài sản gây hoang mang dư luận, làm ảnh hưởng lớn đến tình hình ANTT, trật tự an toàn xã hội trên địa bàn Thành phố. Trước đây tội phạm mạng chủ yếu liên quan việc giả danh các cơ quan tư pháp như công an, Viện Kiểm soát, toà án... để lừa đảo, chiếm đoạt tài sản. Gần đây, các đối tượng chuyển sang hình thức tìm việc làm online tại nhà, tham gia chứng khoán, mua tiền ảo, nợ tiền điện thoại, con bị tai nạn, chuyển đổi SIM... diễn biến phức tạp, sử dụng những hình ảnh cắt ghép, đưa các quyết định tố tụng của các cơ quan tố tụng lên mạng thực hiện hành vi lừa đảo để các bị hại sợ, tin, buộc phải chuyển tiền.

Loại tội phạm này gây rất nhiều khó khăn trong công tác điều tra, truy vết của lực lượng chức năng vì chúng không chỉ nằm ở trong nước mà chúng nằm ngoài lãnh thổ Việt Nam.

Hiện nay, các đối tượng đã sử dụng công nghệ Deepfake (là công nghệ ứng dụng trí tuệ nhân tạo AI) vào mục đích lừa đảo, chiếm đoạt tài sản.

**Nhận diện công nghệ Deepfake:** Deepfake là cụm từ được kết hợp từ “deep learning” và “fake”, là phương thức sử dụng trí tuệ nhân tạo (AI) để tạo ra các sản phẩm công nghệ giả dưới dạng âm thanh (giọng nói) hình ảnh (khuôn mặt) thậm chí cả tạo ra video để mục đích giả giọng nói, khuôn mặt người quen của bị hại trên mạng xã hội rồi tương tác, khi chiếm được lòng tin, các đối tượng yêu cầu bị hại thực hiện các giao dịch tài chính như: vay tiền, chuyển tiền giúp con đi học,... để lừa đảo, chiếm đoạt tài sản.

### 1. Phương thức, thủ đoạn:

- Các đối tượng tìm kiếm, thu thập thông tin cá nhân, hình ảnh, video có giọng nói được đăng tải công khai trên các nền tảng mạng xã hội... rồi sử dụng công nghệ deepfake để tạo ra giọng nói, khuôn mặt, video rất khó phát hiện thật giả để phục vụ cho mục đích lừa đảo.

- Chúng thường thực hiện cuộc gọi video để giả làm người thân vay tiền, giả làm con, cháu đang du học nước ngoài gọi điện cho người thân nhờ chuyển tiền đóng học phí hoặc giả tạo các tình huống khẩn cấp như người thân bị tai nạn cần tiền gấp để cấp cứu.

- Đặc điểm chung của các cuộc gọi video lừa đảo này thường có âm thanh, hình ảnh không rõ nét, tín hiệu chập chờn giống như trong khu vực sóng di động hoặc wifi yếu để nạn nhân khó phân biệt thật giả, khi người nhận gọi lại kiểm tra

chúng sẽ không nhận cuộc gọi hoặc sử dụng phần mềm cắt ghép hình ảnh, giọng nói để đánh lừa.

## 2. Nhận diện nguyên nhân:

- Nạn nhân không thường xuyên cập nhật tin tức tuyên truyền của cơ quan chức năng, không nhận diện đúng, đầy đủ phương thức, thủ đoạn của các đối tượng sử dụng công nghệ deepfake để lừa đảo, chiếm đoạt tài sản;

- Người dân có tâm lý chủ quan, không cẩn thận **xác minh qua số điện thoại** của người thân khi nhận được tin nhắn vay tiền, chuyển khoản qua các nền tảng mạng xã hội kể cả khi thấy **số tài khoản nhận chuyển khoản không đúng tên người thân**;

## 3. Đối tượng

- Người già, người lớn tuổi thường có ít kiến thức về công nghệ và khó phân biệt được giữa video thật và video giả;

- Người có ít kiến thức về công nghệ, không cập nhật tin tức về phương thức, thủ đoạn của các loại tội phạm sử dụng mạng xã hội để lừa đảo, không quan tâm đến các vấn đề bảo mật để bị đánh cắp thông tin, dễ bị lừa đảo bởi deepfake;

- Người đang trong tâm trạng tâm lý yếu, đang gặp phải các vấn đề về tâm lý như stress, lo lắng... dễ bị lừa bằng các thông tin giả mạo;

- Người có tài sản lớn, vị trí xã hội cao, người làm kinh doanh, văn hóa... sẽ là đối tượng dễ bị chú ý và có khả năng sập bẫy lừa đảo cao.

## 4. Trước phương thức, thủ đoạn trên, Công an huyện Hóc Môn khuyến cáo:

- Người dân cảnh giác khi nhận bất kỳ tin nhắn, cuộc gọi video với nội dung vay, mượn tiền qua các ứng dụng mạng xã hội như: viber, zalo, facebook, telegram... cần xác minh, kiểm tra lại thông tin bằng cách **gọi lại số điện thoại di động** của người thân (không gọi qua các ứng dụng mạng xã hội) để kiểm tra, đối chiếu thông tin.

- Hạn chế đăng tải các thông tin cá nhân, hình ảnh, video... của bản thân, người nhà tùy tiện lên mạng xã hội để tránh lộ, lọt thông tin cá nhân, người thân để các loại tội phạm lợi dụng thông tin để thực hiện các hành vi lừa đảo.

- Trường hợp nghi vấn đối tượng giả mạo người thân, bạn bè, đồng nghiệp trên mạng xã hội lừa đảo, chiếm đoạt tài sản cần báo ngay cho cơ quan công an xã, thị trấn nơi gần nhất để được hỗ trợ, hướng dẫn xử lý.

TP. Hồ Chí Minh là một thành phố năng động, việc ứng dụng, triển khai công nghệ số, số hóa... để phục vụ người dân ngày càng tốt hơn là nhiệm vụ cũng như thách thức của cả Thành phố nói chung trong công tác bảo vệ dữ liệu cũng như phòng chống tội phạm sử dụng công nghệ để lừa đảo, chiếm đoạt tài sản.

Ngày nay sự bùng nổ của mạng internet, mỗi người dân đều dễ dàng thực hiện các giao dịch tài chính, đầu tư... trên một chiếc điện thoại thông minh, đây cũng là mảnh đất màu mỡ để các loại tội phạm sử dụng công nghệ cho mục đích lừa đảo hướng tới, vì vậy người dân trên địa bàn huyện cần nâng cao cảnh giác, ý thức khi sử dụng mạng xã hội và các dịch vụ trực tuyến khác, tăng cường cập nhật tin tức

tuyên truyền của công an các cấp về công tác phòng, chống tội phạm nhất là tội phạm lợi dụng mạng internet để lừa đảo, chiếm đoạt tài sản để tự bảo vệ mình và người thân trên mạng. Chấp hành nghiêm các quy định của Đảng, Nhà nước trong việc sử dụng mạng internet trong công việc cũng như trong cuộc sống để góp phần xây dựng huyện Hóc Môn ngày càng văn minh, sáng tạo xứng đáng là huyện Hóc Môn của tri thức và sự phát triển./.

## **CÔNG AN HUYỆN HÓC MÔN**