

Số: 633 /CAT-PA05

Hòa Bình, ngày 27 tháng 3 năm 2023

V/v một số thủ đoạn lừa đảo chiếm đoạt tài sản trên không gian mạng

Kính gửi: Các sở, ban, ngành, đoàn thể trong tỉnh.

Thời gian qua, tình hình tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng diễn biến phức tạp, gây bức xúc trong dư luận xã hội, ảnh hưởng đến an ninh, trật tự và hoạt động, đời sống của người dân, gần đây tại nhiều địa phương xuất hiện một số thủ đoạn lừa đảo chiếm đoạt tài sản trên không gian mạng mới, tinh vi hơn, nổi lên là:

**(1) Sử dụng công nghệ Deepfake<sup>1</sup> làm giả cuộc gọi video nhằm chiếm đoạt tài sản:**

+ *Phương thức, thủ đoạn:* Thông qua mạng Internet, các đối tượng thu thập hình ảnh, giọng nói của người dùng trên mạng xã hội, sử dụng công nghệ Deepfake<sup>2</sup> tạo ảnh động, video giả mạo người dùng đang nói chuyện trực tuyến với người cùng khuôn mặt, âm điệu giọng nói và cách xưng hô.

Đối tượng tạo lập tài khoản giả mạo trên mạng xã hội trùng thông tin và ảnh đại diện với người dùng, kết bạn với nạn nhân trong danh sách bạn bè và nhắn tin vay mượn tiền theo kịch bản sẵn có. Trong một số trường hợp, đối tượng chiếm đoạt tài khoản mạng xã hội của người dùng để trực tiếp nhắn tin cho các nạn nhân trong danh sách bạn bè. Để tạo lòng tin với nạn nhân, đối tượng truyền tải Deepfake video có sẵn lên kênh video call (*Facebook, Zalo, Telegram...*) khiến nạn nhân nhận ra hình ảnh và giọng nói của người quen và nhanh chóng chuyển tiền theo yêu cầu của đối tượng.

Với công nghệ Deepfake, video giả mạo có độ chính xác cao, rất khó phân biệt thật giả. Tuy nhiên, video do đối tượng tạo sẵn thường có nội dung chung chung, không phù hợp hoàn toàn với ngữ cảnh thực tế giao tiếp với nạn nhân, có thể khiến nạn nhân nghi ngờ, phát hiện. Để che lấp khuyết điểm trên, các đối tượng tạo ra video với âm thanh khó nghe, hình ảnh không rõ nét giống cuộc gọi video có tín hiệu chập chờn được thực hiện trong khu vực phủ sóng di động/wifi yếu.

<sup>1</sup> Deepfake là công nghệ ứng dụng trí tuệ nhân tạo AI tạo ra các sản phẩm công nghệ âm thanh, hình ảnh và video làm giả đối tượng ngoài đời thực với độ chính xác rất cao. Dựa trên tệp tin, hình ảnh khuôn mặt, giọng nói của một người ngoài đời thực, Deepfake sẽ sử dụng thuật toán để tái tạo lại khuôn mặt và giọng nói phù hợp với nét mặt, biểu cảm của một người, sau đó tạo ra video giả mạo đối tượng ngoài đời thực.

<sup>2</sup> Các phần mềm Avatarity, My Heritage, Morphin, DeepFaceLab, Faceswap... được chia sẻ trên Internet.



+ *Biện pháp phòng ngừa*: Tuyên truyền đến cán bộ, nhân viên nắm được thủ đoạn của tội phạm, khi nhận bất kỳ tin nhắn vay mượn tiền thông qua mạng xã hội cần gọi điện trực tiếp qua số điện thoại người nhận 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.

**(2) Mạo danh giáo viên, nhân viên bệnh viện lừa đảo phụ huynh bằng thủ đoạn thông báo con cấp cứu, chuyển tiền viện phí gấp:**

+ *Phương thức, thủ đoạn*: Các đối tượng mạo danh giáo viên, nhân viên y tế nơi học sinh đang học gọi điện thoại thông báo cho phụ huynh về việc con bị chấn thương khi hoạt động thể dục hoặc bị tai nạn đang nhập viện nên cần tiền để mổ gấp.

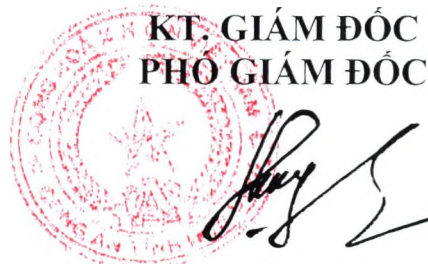
Đối tượng tạo sự tin tưởng bằng cách thông tin chính xác về tên, tuổi của học sinh, phụ huynh sau đó chuyển điện thoại đến người tự xưng là bác sĩ khoa cấp cứu bệnh viện để trao đổi, thông tin về tình trạng bệnh kèm yêu cầu chuyển tiền để mổ cấp cứu gấp. Do tâm lý lo lắng, nhiều phụ huynh học sinh không nghi ngờ và đã chuyển tiền qua số tài khoản ngân hàng do đối tượng cung cấp.

+ *Biện pháp phòng ngừa*: Khi nhận được các cuộc gọi có nội dung như trên, có thể thực hiện một số biện pháp sau: Gọi điện cho giáo viên chủ nhiệm của con để xác nhận; gọi điện đến số điện thoại đường dây nóng của các bệnh viện (*có trên Trang thông tin điện tử của các bệnh viện*) để xác nhận. **Lưu ý**: Việc đóng viện phí trước rồi mới được cấp cứu là không có căn cứ; các bệnh viện chỉ thu tiền lệ phí khám, chữa bệnh bằng tiền mặt hoặc qua số tài khoản ngân hàng của bệnh viện (*không thu qua tài khoản của các cá nhân*).

Công an tỉnh đề nghị thủ trưởng các sở, ban, ngành, đoàn thể trong tỉnh có biện pháp tuyên truyền phù hợp, kịp thời để cán bộ, nhân viên nắm được các thủ đoạn nói trên và phòng ngừa, không để bị tội phạm sử dụng không gian mạng lừa đảo chiếm đoạt tài sản. /.

**Nơi nhận:**

- Như trên;
- Lưu: VT, PA05 (Đ2).



**Trung tá Bùi Việt Hùng**