UBND TỈNH LÂM ĐỒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1720 /STTTT - TTr
V/v cảnh báo thủ đoạn cắt ghép hình ảnh cá nhân vào clip "nhạy cảm" để tống tiền

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Lâm Đồng, ngày06 tháng12 năm 2024

HỎA TỐC

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các Ban của Tỉnh ủy;
- UB MTTQ và các tổ chức chính trị - xã hội tỉnh;
- Văn phòng Đoàn đại biểu Quốc hội và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Các huyện ủy, thành ủy;
- Ủy ban nhân dân các huyện, thành phố.

Theo Công an tỉnh Lâm Đồng, hiện nay hoạt động lừa đảo, chiếm đoạt tài sản qua không gian mạng tại địa phương có diễn biến phức tạp với các phương thức thủ đoạn mới rất tinh vi, cụ thể xuất hiện thủ đoạn sử dụng công nghệ cao, trí tuệ nhân tạo để cắt ghép hình ảnh khuôn mặt của lãnh đạo, cán bộ, đảng viên vào các hình ảnh, video, clip có nội dung "nhạy cảm" để thực hiện các hành vi lừa đảo, đe dọa tống tiền. Nhiều trường hợp cán bộ, doanh nhân, người dân trên địa bàn tỉnh đã nhận được các tin nhắn, thư điện tử như trên, có những trường hợp đã chuyển tiền cho đối tượng.

Sở Thông tin và Truyền thông thông báo đến các cơ quan, đơn vị, địa phương biết, đề nghị thông tin đến toàn thể cán bộ, đảng viên, công chức, viên chức, người dân nắm rõ thủ đoạn, hình thức lừa đảo và truyền thông đến người dân để chủ động phòng ngừa, không hoang mang và thực hiện các biện pháp sau:

1. Bảo mật thông tin cá nhân, không chia sẻ thông tin (số điện thoại, nghề nghiệp, địa chỉ nhà ở, nơi làm việc….), hình ảnh cá nhân, hình ảnh người thân trong gia đình, hình ảnh cơ quan nơi làm việc lên các nền tảng mạng xã hội, đặc biệt là những hình ảnh nhạy cảm hoặc có thể bị lợi dụng để cắt ghép. Không chia sẻ thông tin cá nhân cho bất kỳ tổ chức, cá nhân nào khi chưa biết họ là ai và sử dụng vào mục đích gì.

2. Luôn kiểm tra kỹ nguồn gốc thông tin trước khi chia sẻ hoặc tương tác; không truy cập vào các đường dẫn (link) "lạ" (thường được gửi kèm trong tin nhắn hoặc email) và luôn cẩn trọng, cảnh giác, xác minh thông tin ban đầu (số điện thoại, tài khoản mạng xã hội…của đối tượng) khi tiếp nhận các cuộc gọi, tin nhắn từ những nguồn không rõ ràng.

3. Triển khai các biện pháp, giải pháp phòng, chống mã độc (cài đặt phần mềm diệt virus có bản quyền); sử dụng các phần mềm phòng, chống mã độc để

kiểm tra các tệp tin/đường link nhận từ người lạ qua thư điện tử gmail trước khi mở, kích hoạt các tệp tin đính kèm.

4. Thường xuyên theo dõi các thông tin cảnh báo của các cơ quan chức năng về những hiện tượng lừa đảo, về các sự cố an toàn thông tin để kịp thời cảnh giác có giải pháp ứng phó.

5. Đặc biệt, cần bình tĩnh, tỉnh táo, không hoang mang, hoảng sợ khi nhận được tin nhắn, thư điện tử, cuộc gọi đe dọa như trên. Tuyệt đối không chuyển tiền, không làm theo hướng dẫn của các đối tượng xấu để tránh bị chiếm đoạt thông tin, tài sản. Khi xảy ra trường hợp tương tự cần kịp thời phản ánh, báo tin cho cơ quan Công an nơi gần nhất hoặc liên hệ với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh, qua số điện thoại: 0693.449.407 để được hướng dẫn xử lý.

Sở Thông tin và Truyền thông đề nghị các đơn vị quan tâm thực hiện./.

(Gửi kèm theo các thủ đoạn cắt ghép hình ảnh cá nhân vào clip "nhạy cảm" để tống tiền)

Nơi nhận:
- Như trên;
- Đ/c Phạm S - Phó CT UBND tỉnh (báo cáo);
- GĐ Sở (báo cáo);
- Trang TTĐT Sở;
- Lưu: VT, TTr.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LÂM ĐỒNG

Vương Tôn Kiên

THỦ ĐOẠN CẮT GHÉP HÌNH ẢNH CÁ NHÂN VÀO CLIP "NHẠY CẢM" ĐỂ TỐNG TIỀN

Bước 1: Các đối tượng tìm kiếm thông tin, số điện thoại, hình ảnh, các mối quan hệ của nạn nhân (thường là nam giới, có điều kiện kinh tế, địa vị xã hội, trong đó có một số lãnh đạo cơ quan, đơn vị, doanh nghiệp) từ nhiều nguồn khác nhau, chủ yếu là thông tin, hình ảnh được đăng tải trên các trang mạng xã hội, địa chỉ trang web, trang thông tin điện tử, nơi công tác, làm việc của lãnh đạo, cán bộ, doanh nhân…

Bước 2: Các đối tượng sử dụng phần mềm công nghệ cao, trí tuệ nhân tạo cắt ghép khuôn mặt của nạn nhân vào các hình ảnh từ các clip trên Internet có nội dung "nhạy cảm" thể hiện việc nạn nhân đang quan hệ tình dục trong nhà nghỉ, khách sạn. Đối tượng còn giả chụp ảnh từ clip quay được tại hiện trường bằng cách dán biểu tượng nút play vào giữa ảnh hoặc dùng điện thoại quay lại ảnh đã cắt ghép.

Bước 3: Đối tượng sử dụng "SIM rác", dịch vụ gọi điện thoại qua Internet hoặc thông qua email, tin nhắn SMS, iMessage, Zalo…, thậm chí dịch vụ bưu chính để gọi điện, nhắn tin, gửi thư liên hệ với nội dung tự xưng là "thám tử tư, được người khác ủy thác điều tra, sau một thời gian bí mật theo dõi, phát hiện nạn nhân có những hành vi sa đọa, có mối quan hệ bất chính, ngoài luồng nên đã dùng thiết bị ghi hình bí mật để quay phim, chụp ảnh lại" kèm hình ảnh nhạy cảm đã được cắt ghép, chỉnh sửa cho nạn nhân. Đối tượng yêu cầu chuyển vài trăm triệu đồng đến hàng tỷ đồng vào tài khoản ngân hàng hoặc ví tiền ảo (USDT) do chúng chỉ định để chuộc lại các clip, hình ảnh này. Đối tượng còn cam đoan, sau khi nhận được tiền sẽ đưa hết toàn bộ chứng cứ, hình ảnh cho nạn nhân và tuyệt đối giữ bí mật. Nếu nạn nhân không chịu giao số tiền nêu trên, đối tượng sẽ chuyển tất cả các ảnh và clip đã thu thập được lên các trang mạng xã hội, các website lớn; dán hình ảnh xung quanh nơi nạn nhân ở và làm việc, đồng thời tố cáo tới gia đình, cấp trên và cơ quan liên quan để cho nạn nhân "thân bại danh liệt".

Bước 4: Trường hợp nạn nhân do lo sợ, nhắn tin, liên lạc với đối tượng, các đối tượng sẽ hướng dẫn mua tiền điện tử và chuyển đến các tài khoản ví điện tử theo chỉ định, sau đó sẽ chiếm đoạt toàn bộ số tiền./.