

Số: /BQL-VP
V/v cảnh báo hình thức lừa đảo sử dụng
công nghệ trí tuệ nhân tạo

Hải Phòng, ngày tháng năm 2024

Kính gửi:

- Các phòng chuyên môn;
- Trung tâm Dịch vụ việc làm - Đào tạo - Xúc tiến đầu tư;
- Các doanh nghiệp trong các Khu công nghiệp, Khu kinh tế.

Ngày 09/12/2024, Sở Thông tin và Truyền thông có Công văn số 2813/STTTT-TTS về việc cảnh báo hình thức lừa đảo sử dụng công nghệ trí tuệ nhân tạo.

Thời gian gần đây, Sở Thông tin và Truyền thông đã ghi nhận phản ánh của một số cá nhân trên địa bàn thành phố về việc bị các đối tượng sử dụng công nghệ Deepfake để thực hiện hành vi cắt ghép, phát tán các hình ảnh nhạy cảm trên mạng xã hội nhằm đe dọa bôi nhọ danh dự, nhân phẩm và uy tín cá nhân, lừa đảo, chiếm đoạt tài sản. Đây là một hình thức lừa đảo sử dụng công nghệ Deepfake - công nghệ trí tuệ nhân tạo (AI) có khả năng tạo ra những video hoặc hình ảnh giả mạo như thật để thực hiện hành vi phạm tội.

Thủ đoạn của các nhóm lừa đảo này là sử dụng hình ảnh, thông tin cá nhân của nạn nhân (chủ yếu là nam giới có địa vị xã hội) được kẻ gian thu thập từ nhiều nguồn khác nhau: mạng xã hội, địa chỉ trang web, trang thông tin điện tử, nơi công tác, làm việc... Các đối tượng sử dụng phần mềm công nghệ cao, trí tuệ nhân tạo, cắt ghép khuôn mặt của nạn nhân vào các video clip, hình ảnh nhạy cảm lưu truyền trên không gian mạng và tự xưng là “thám tử tư” nhắn tin, gọi điện đe dọa với mục đích tống tiền. Khi nạn nhân lo sợ, hợp tác, các đối tượng sẽ hướng dẫn mua tiền điện tử, chuyển đến các tài khoản ví điện tử theo chỉ định để chiếm đoạt.

Để phòng tránh lừa đảo, Ban Quản lý Khu kinh tế Hải Phòng (Ban Quản lý) thông báo và đề nghị các phòng chuyên môn, đơn vị sự nghiệp của Ban Quản lý và các doanh nghiệp trong các Khu công nghiệp, Khu kinh tế thực hiện tuyên truyền, cảnh báo, khuyến cáo rộng rãi:

1. Các cá nhân cần kiểm tra và điều chỉnh cài đặt quyền riêng tư tài khoản trên không gian mạng để hạn chế ai có thể xem và truy cập ảnh cá nhân. Hạn chế việc chia sẻ ảnh công khai với người lạ; Không nên chia sẻ thông tin cá nhân trên mạng, bao gồm ảnh, địa chỉ, số điện thoại, hoặc các thông tin nhạy cảm khác; Cần trọng khi kết bạn và chia sẻ thông tin với người lạ.

2. Các cá nhân khi nhận được tin nhắn, cuộc gọi có nội dung đe dọa tổng tiền cần bình tĩnh, không hoảng sợ, cần thông tin ngay cho người trong gia đình, bạn bè; Không hoang mang, sợ hãi, không thực hiện yêu cầu của các đối tượng, ví dụ như: yêu cầu tiền chuộc; yêu cầu chuyển tiền để điều tra, chứng minh vô tội; yêu cầu truy cập vào đường link web; yêu cầu cài ứng dụng (app) để xác minh 2 thông tin, bảo mật; trình báo ngay với lực lượng công an, chính quyền địa phương hoặc Sở Thông tin và Truyền thông qua đường dây nóng 0899252555 để được hướng dẫn giải quyết.

Ban Quản lý cử đồng chí **Nguyễn Thành Đạt** (*Chuyên viên Văn phòng đại diện Ban Quản lý tại các khu công nghiệp, khu kinh tế, SĐT 0868426463*) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:

- Như trên;
- Sở TT&TT;
- Lãnh đạo Ban (để b/c);
- Công thông tin điện tử Heza;
- Lưu: VP/BQL.

**KT. TRƯỞNG BAN
PHÓ TRƯỞNG BAN**

Bùi Ngọc Hải