

NHẬN DIỆN PHƯƠNG THỨC, THỦ ĐOẠN HOẠT ĐỘNG CỦA CÁC ĐỐI TƯỢNG GIẢ DANH, MẠO DANH CÁN BỘ QUÂN ĐỘI

I. NHỮNG PHƯƠNG THỨC, THỦ ĐOẠN PHỔ BIẾN

1. Gọi điện xưng là cán bộ, chỉ huy đơn vị trong Quân đội

Các đối tượng tìm cách thu thập thông tin hoạt động quân sự của đơn vị, lãnh đạo, chỉ huy, cán bộ trên Internet, trang mạng xã hội và những người thân quen; tùy thuộc vào số lượng thông tin thu thập được, tiến hành xây dựng kịch bản lừa đảo phù hợp với mục đích của chúng, cụ thể:

- Sử dụng điện thoại hoặc tài khoản mạng xã hội tự giới thiệu là cán bộ Quân đội, đang là chỉ huy, quản lý chiến sĩ, sau đó liên hệ với gia đình của quân nhân cung cấp thông tin không đúng sự thật (chiến sĩ là con, em của gia đình gây thiệt hại tài sản của đơn vị, đang trong quá trình xem xét xử lý kỷ luật; nếu gia đình chuyển tiền vào số tài khoản để đền bù thiệt hại thì đơn vị sẽ bỏ qua lỗi vi phạm, nếu không chuyển tiền sẽ bị khởi tố, xử lý theo pháp luật) tạo tâm lý hoang mang, lo sợ; dẫn dụ gia đình quân nhân chuyển tiền vào số tài khoản để chiếm đoạt.

- Đối tượng sử dụng số điện thoại, tài khoản Zalo (đăng tải hình ảnh quân nhân mặc quân phục để tạo niềm tin), gọi điện đến các nhà hàng, cửa hàng trang thiết bị, dịch vụ nấu ăn, cơ sở mua bán cây giống,... đồng thời gửi địa chỉ chính xác của đơn vị thông qua ứng dụng định vị trên điện thoại. Tiếp đến, các đối tượng đặt mua thêm rượu, sâm quý để làm quà biếu; các loại phân bón, thuốc bảo vệ thực vật mà các mặt hàng này không phổ biến. Khi nhà hàng, cơ sở cây giống không tìm được nguồn hàng theo yêu cầu, đối tượng lừa đảo sẽ hướng dẫn liên hệ với người cung cấp (nơi có nguồn hàng), thực chất đây cũng là đối tượng trong nhóm lừa đảo của chúng. Sau khi chuyển tiền cọc qua số tài khoản thì chúng cắt liên lạc.

2. Tạo các trang nhóm, giả mạo để lừa đảo, trục lợi

Các đối tượng tạo các trang nhóm trên Zalo, Facebook,... thường xuyên sao chép, đăng tải các nội dung liên quan đến Quân đội, hậu phương chiến sĩ giả danh để kêu gọi quyên góp, hỗ trợ, chiêu mộ tuyển sinh, tuyển quân, tuyển dụng hoặc đăng tải các thông tin không chính thống nhằm mục đích xuyên tạc, bôi nhọ hình ảnh.

3. Giả mạo, mạo danh quân nhân, tài liệu, con dấu

Đối tượng đặt mua nhiều quân phục, quân hàm, biển tên, làm giấy tờ giả,... chụp nhiều hình ảnh mang mặc quân phục để tạo niềm tin, tự xưng là cán bộ Quân đội, giới thiệu bản thân là người có mối quan hệ rộng, có khả năng can thiệp, tác động đến nhiều lĩnh vực cũng như chạy chức, chạy quyền, chạy tuyển dụng,... nhằm thực hiện hành vi lừa đảo, trục lợi bất chính, lừa gạt tình cảm hoặc đơn thuần là thể hiện bản thân.

4. Sử dụng Deepfake, chỉnh sửa giọng nói-video-hình ảnh Quân đội

Các đối tượng thu thập thông tin, hình ảnh, giọng nói của quân nhân, thông qua các ứng dụng có chức năng chỉnh sửa giọng nói-video-hình ảnh (như Deepfake) để mạo danh cá nhân, lãnh đạo trong Quân đội gọi điện để ra lệnh, yêu cầu chuyển tiền hoặc thực hiện theo các kịch bản của đối tượng nhằm mục đích lừa đảo, chiếm đoạt tài sản.

II. DẤU HIỆU NHẬN BIẾT

- Đối tượng yêu cầu phải xử lý nhanh, chuyển tiền gấp, cung cấp OTP, mật khẩu, mã xác thực. Kêu gọi ủng hộ nhưng chuyển tiền vào tài khoản cá nhân.
- Địa chỉ liên hệ, số điện thoại không khớp với cá nhân, đơn vị Quân đội. Tác phong, điều lệnh không chuẩn mực; video clip, âm thanh bất thường về ánh sáng, hình ảnh, giọng điệu.
- Văn bản, quyết định sai thể thức, con dấu, sai tên cơ quan, đơn vị; chữ ký mờ, sai định dạng, gửi qua kênh không chính thức.
- Người liên hệ né tránh việc xác minh, không cho gặp trực tiếp, hỏi thúc thực hiện ngay.

III. NHỮNG VIỆC CẦN LÀM NGAY

- Tuyệt đối không cung cấp mật khẩu, mã OTP, thông tin thủ trưởng, cá nhân, đơn vị cho bất kỳ ai.
- Không nhấn vào đường link, file lạ không rõ nguồn gốc.
- Xác minh, đối chiếu ngay qua các kênh thông tin chính thức.
- Lưu chứng cứ, chụp màn hình, ghi lại số điện thoại, email trong trường hợp nghi ngờ mạo danh.
- Báo cáo kịp thời cho cơ quan Bảo vệ an ninh hoặc đơn vị công an, quân sự gần nhất để được hướng dẫn, xác minh, làm rõ thông tin, tránh thiệt hại về tinh thần và tài sản.

IV. BIỆN PHÁP PHÒNG NGỪA

- Không cung cấp thông tin cá nhân: Tuyệt đối không cung cấp, đăng tải hình ảnh, thông tin cá nhân, đồng đội, đơn vị cho bất kỳ ai qua điện thoại, tin nhắn hoặc mạng xã hội nếu không xác thực người nhận là ai.
- Xác minh danh tính: Nếu nhận được cuộc gọi từ người tự xưng là cán bộ quân đội, hãy gọi đến số điện thoại chính thức của cơ quan đó hoặc liên hệ qua các kênh chính thức để xác minh thông tin.
- Không chuyển tiền: Không cung cấp số tài khoản ngân hàng, OTP, mật khẩu cho bất kỳ ai; không chuyển tiền hoặc thực hiện giao dịch tài chính theo yêu cầu của người lạ, kể cả khi bị đe dọa hoặc được hứa hẹn lợi ích.
- Cảnh giác với các đường link và ứng dụng lạ: Không cài đặt ứng dụng, nhấn vào các đường link không rõ nguồn gốc được gửi qua tin nhắn hoặc mạng xã hội.

- Tuyên truyền, phổ biến cho gia đình, địa phương, các trang, nhóm nội bộ về các phương thức, thủ đoạn giả danh, mạo danh quân nhân, đơn vị Quân đội./.