

Số ~~628~~ / CSHS

V/v phòng ngừa hoạt động lừa
đảo chiếm đoạt tài sản thông qua
mạng viễn thông, mạng xã hội,
mạng internet

Đắk Nông, ngày 24 tháng 5 năm 2022

Kính gửi: Sở Giáo dục và Đào tạo tỉnh Đắk Nông

Thời gian vừa qua trên toàn quốc nói chung và địa bàn tỉnh Đắk Nông nói riêng liên tục xuất hiện các vụ lừa đảo chiếm đoạt tài sản trên không gian mạng, nạn nhân thuộc nhiều thành phần, nghề nghiệp khác nhau, trong đó có cả cán bộ, công chức, viên chức, giáo viên... (từ đầu năm 2022 đến nay đã có nhiều trường hợp Giáo viên tại các huyện K'Rông Nô, Đắk Mil, Đắk Song, Đắk G'long, Đắk R'lấp bị lừa đảo chiếm đoạt với số tiền lên đến hàng chục tỷ đồng).

Một số thủ đoạn mà đối tượng lừa đảo sử dụng để chiếm đoạt tài sản thông qua mạng viễn thông, mạng xã hội, mạng internet như:

1. Giả danh các nhà mạng gọi điện thông báo số thuê bao điện thoại của bạn đã trúng thưởng tài sản có giá trị lớn, để nhận được tài sản đó phải mất phí, nếu đồng ý thì mua thẻ cào nạp vào số tài khoản mà các đối tượng cung cấp, khi người dân đóng tiền vào để nhận thưởng thì các đối tượng chặn số liên lạc và chiếm đoạt số tiền đó.

2. Đối tượng giả danh là cán bộ ngân hàng thông báo cho bị hại có người chuyển tiền vào tài khoản nhưng do bị lỗi nên chưa chuyển được hoặc thông báo phần mềm chuyển tiền Internet Banking của khách hàng bị lỗi... nên yêu cầu khách hàng cung cấp mã số thẻ và mã OTP để kiểm tra. Các đối tượng sử dụng thông tin bị hại cung cấp để truy cập vào tài khoản và rút tiền của bị hại.

3. Giả danh cán bộ Công an, Tòa án, Viện Kiểm sát gọi điện thông báo người dân có liên quan đến vụ án hoặc xử phạt nguội vi phạm giao thông, yêu cầu bị hại chuyển tiền vào tài khoản mà các đối tượng lừa đảo đưa ra để phục vụ công tác điều tra, xử lý. Khi người dân lo sợ và chuyển tiền vào các tài khoản mà đối tượng yêu cầu thì các đối tượng chuyển tiếp số tiền đó vào nhiều tài khoản khác và chiếm đoạt.

4. Lợi dụng sự nhẹ dạ và nhu cầu kiếm tiền nhanh của các bị hại, đối tượng giả mạo tuyên công tác viên xử lý đơn hàng cho các sàn thương mại điện tử để thực hiện hành vi chiếm đoạt tài sản. Bằng thủ đoạn lập các trang Facebook giả mạo các

nhân hàng, trang thương mại điện tử như: Tiki.vn, Lazada, TokyoLive, Shopee... và chạy quảng cáo, khi bị hại nhắn tin hỏi cách thức làm cộng tác viên, các đối tượng sẽ gửi thông tin về công ty, nhân viên chăm sóc khách hàng... và yêu cầu gửi thông tin cá nhân, kết bạn Zalo để tư vấn. Ban đầu các đối tượng gửi các đường dẫn các sản phẩm có giá trị nhỏ khoảng vài trăm ngàn đồng để bị hại chọn và xác thực đơn, chụp ảnh đơn hàng gửi cho đối tượng qua Zalo, Facebook, chuyển tiền vào các tài khoản do đối tượng cung cấp và được đối tượng chuyển lại toàn bộ số tiền đã bỏ ra để mua hàng cùng với hoa hồng từ 03 đến 20%. Sau một số lần tạo niềm tin bằng cách trả gốc và hoa hồng như đã cam kết ban đầu, tiếp theo đối tượng viện lý do "bạn đã được công ty nâng hạng" và gửi các đường dẫn sản phẩm trên sàn Lazada, Shopee... có giá trị lớn hơn và tiếp tục yêu cầu bị hại chụp lại hình ảnh sản phẩm đồng thời chuyển tiền. Khi đã nhận được, đối tượng không nhận tiền mà tiếp tục thông báo cho cộng tác viên phải tiếp tục thực hiện nhiệm vụ khác thì mới được chuyển lại tiền và hoa hồng (thực chất là tiếp tục chuyển tiền vào tài khoản đối tượng). Sau đó các đối tượng chiếm đoạt tiền của bị hại.

5. Đối tượng sử dụng thông tin cá nhân, hình ảnh của các đồng chí Lãnh đạo các cơ quan, chính quyền, đoàn thể... để thiết lập tài khoản mạng xã hội (Zalo, Facebook...) mạo danh. Sau đó, các đối tượng tạo tài khoản mạo danh để kết bạn, nhắn tin trao đổi vay mượn tiền của bạn bè, người thân, đồng nghiệp, cấp dưới... và chiếm đoạt tiền của các bị hại chuyển đến; hoặc đối tượng lừa đảo sử dụng hack (chiếm đoạt quyền điều khiển) tài khoản mạng xã hội sau đó nhắn tin lừa đảo đến bạn bè của chủ tài khoản mạng xã hội và chiếm đoạt tiền của các bị hại chuyển đến tài khoản ngân hàng do các đối tượng chỉ định.

6. Thủ đoạn cho vay tiền qua app (vay tiền online). Lợi dụng tâm lý vay tiền online thuận lợi, nhanh chóng, không phải ra ngân hàng làm thủ tục, các đối tượng lập ra các trang trên mạng xã hội (Zalo, Facebook) chạy quảng cáo để tiếp cận các bị hại. Sau khi tiếp cận được nạn nhân, các đối tượng gửi đường link kết nối với CH Play để các bị hại cài đặt ứng dụng vào điện thoại và làm theo ứng dụng của app. Sau đó, khi bị hại đăng nhập app để vay tiền thì app sẽ báo lỗi, các đối tượng yêu cầu nạn nhân mua bảo hiểm khoản vay, đóng tiền phí giải ngân... Nhiều bị hại thực hiện chuyển nhiều lần để được vay cho đến khi nghi ngờ bị lừa không chuyển nữa thì không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

Để chủ động phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, Phòng Cảnh sát hình sự Công an tỉnh Đắk Nông đề nghị Sở Giáo dục và Đào tạo tỉnh Đắk Nông chỉ đạo Phòng Giáo dục các huyện, thành phố, Ban Giám hiệu các Trường học trên toàn tỉnh tổ chức phổ biến, quán triệt một số

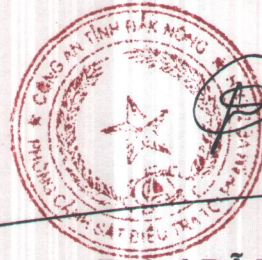
phương thức thủ đoạn của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng nói trên đến toàn thể cán bộ giáo viên, học sinh do mình quản lý, nâng cao tinh thần cảnh giác, phòng ngừa tội phạm, kịp thời cung cấp các thông tin về loại tội phạm này đến Cơ quan Công an gần nhất để xử lý theo quy định của pháp luật.

Trong quá trình thực hiện có gì vướng mắc, các đồng chí trao đổi về phòng Cảnh sát hình sự Công an tỉnh Đắk Nông (Đ/c Hiền, số ĐT: 0978200990) để cùng giải quyết. Rất mong sự quan tâm, phối hợp của quý Cơ quan. *Lưu*

Nơi nhận:

- Như trên (để phối hợp);
- Lưu PC02 (Đ3).

TRƯỞNG PHÒNG



Đ. Trọng Hoãn
Đại tá Đỗ Trọng Hoãn

