

LIÊN ĐOÀN LAO ĐỘNG TỈNH TÂY NINH
LIÊN ĐOÀN LAO ĐỘNG
HUYỆN DƯƠNG MINH CHÂU

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

Số: 48/LĐLD

V/v tuyên truyền phòng tránh các phương thức,
thủ đoạn Lừa đảo chiếm đoạt tài sản
trên không gian mạng

Huyện Dương Minh Châu, ngày 12 tháng 5 năm 2022

Kính gửi: - Công đoàn cơ sở trực thuộc LĐLD huyện.

Thực hiện Công văn số 2873/LĐLD, ngày 06/5/2022 của Ban Thường vụ Liên đoàn Lao động tỉnh Tây Ninh về việc tuyên truyền phòng tránh các phương thức, thủ đoạn Lừa đảo chiếm đoạt tài sản trên không gian mạng.

Ban Thường vụ Liên đoàn Lao động huyện đề nghị các công đoàn cơ sở tổ chức triển khai một số nội dung cụ thể sau:

I. Phương thức của các thủ đoạn Lừa đảo chiếm đoạt tài sản

1. *Tuyển cộng tác viên bán hàng online*: người bị hại tìm thấy các quảng cáo trên mạng xã hội (facebook, Zalo) có nội dung về tuyển cộng tác viên (CTV) xử lý đơn hàng trên các trang thương mại điện tử uy tín như Shoppe, Lazada, Tiki... để thưởng hoa hồng từ 10-20% hoặc thu nhập từ 200.000đ-700.000đ/ngày, không cần bằng cấp, kinh nghiệm, làm việc tại nhà, có sử dụng thẻ ATM, điện thoại, laptop... Bị hại nhấn vào đường link tham gia bằng cách để lại số điện thoại. Ngay lập tức, có người liên hệ lại và kết bạn qua zalo để hướng dẫn cách thức thực hiện. Đầu tiên, bị hại sẽ làm nhiệm vụ đặt đơn hàng có giá trị nhỏ bằng cách chuyển tiền mua sản phẩm vào một tài khoản ngân hàng do đối tượng chỉ định và chụp hình chuyển tiền gửi lại cho đối tượng để xác thực, sau khi đối tượng xác nhận bị hại đã chuyển tiền mua đơn hàng thành công sẽ thanh toán lại tiền mua hàng và kèm hoa hồng như đã hứa để tạo lòng tin đánh vào lòng tham vì việc kiếm tiền quá dễ dàng. Sau 1-2 lần làm nhiệm vụ đơn hàng thành công và nhận được tiền hoa hồng, bị hại sẽ được giao nhiều nhiệm vụ mua đơn hàng có giá trị lớn hơn, thực hiện rất nhiều nhiệm vụ để được thanh toán lại số tiền gốc và tiền hoa hồng. Tuy nhiên, khi đã nộp số tiền lớn để đặt mua hàng, thì các đối tượng liên tục đưa ra nhiều lý do khác nhau để yêu cầu bị hại mua thêm hàng. Bị hại vì muốn lấy lại số tiền mua sản phẩm ban đầu nên cứ làm theo và bị chiếm đoạt tiền nhiều lần.

2. *Giả danh công ty bảo hiểm, Công an, Viện kiểm sát... để đe dọa vi phạm pháp luật yêu cầu chuyển tiền*

Lừa đảo theo một kịch bản đã xây dựng với nhiều đối tượng tham gia nhằm đánh lạc hướng bị hại tin tưởng và làm theo mà không kịp suy nghĩ đúng sai. Đầu tiên giả danh công ty bảo hiểm gọi điện thoại báo bị hại đã làm giả hồ sơ bệnh án để

chiếm đoạt tiền bảo hiểm, bị hại phủ nhận. Tiếp theo đối tượng chuyển máy điện thoại cho đối tượng khác giả danh Công an để xác nhận tên của bị hại đã làm giả hồ sơ bảo hiểm và cùng liên quan trong vụ án lớn (buôn bán ma túy, rửa tiền, lừa đảo xuyên quốc gia) do bị hại có tham gia mở tài khoản ngân hàng phục vụ cho việc rửa tiền phạm pháp, bị hại đã có lệnh bắt giam của Viện kiểm sát, Tòa án. Tiếp đó, đối tượng chuyển máy cho đối tượng khác giả danh Viện kiểm sát, Tòa án và yêu cầu bị hại kết bạn Zalo để gửi Lệnh bắt bị can tạm giam có thông tin đúng như bị hại. Nếu bị hại không muốn ra Tòa bị bắt tạm giam thì phải mở một ngân hàng cá nhân và chuyển tất cả tiền có được vào tài khoản này để “nộp Kho bạc Nhà nước”. Nhưng trên thực tế, sau khi bị hại mở tài khoản Ngân hàng đứng tên mình thì bị hại đã cung cấp toàn bộ số tài khoản, mật khẩu Internet Banking, Mã OTP...cho đối tượng đã chiếm quyền điều khiển tài khoản ngân hàng của bị hại và chiếm đoạt toàn bộ số tiền trong tài khoản.

3. Lừa với hình thức tham gia vay tiền qua ứng dụng tên điện thoại

Các đối tượng thường đánh vào tâm lý muốn được vay vốn với số tiền lớn, thủ tục nhanh gọn ở những người đang cần tiền để tiêu dùng. Sau khi tiếp cận được “con mồi”, các đối tượng sử dụng sim, tài khoản thuộc các trang mạng xã hội như Zalo, Messenger để hướng dẫn việc thực hiện các thủ tục vay thông qua các ứng dụng tài chính online như “FC Cerdit”, “CE Credit”, Mirae Asset”...do các đối tượng cung cấp và hướng dẫn bị hại cài đặt trên điện thoại.

Sau khi cài đặt ứng dụng thì điền thông tin cá nhân, các thông tin về gói vay. Đối tượng yêu cầu nộp tiền bảo hiểm khoản vay qua tài khoản ngân hàng do đối tượng hướng dẫn. Sau khi bị hại nộp tiền thì đối tượng chiếm đoạt và thông báo chưa nhận được tiền nhưng đưa ra nhiều lý do như sai tài khoản, sai cú pháp...hoặc thông báo nhận được tiền nhưng đưa ra nhiều lý do khác để yêu cầu nộp thêm tiền như tài khoản yêu cầu vay bị sai hoặc thiếu thông tin, nộp phạt số tiền vay vượt quá định mức vay, trả trước một khoản lãi suất sau khi giải ngân sẽ chuyển đủ tiền cho vay...để chiếm đoạt số tiền lớn, có khi lớn gấp nhiều lần số tiền cần vay.

Hầu hết số tiền thiệt hại qua các thủ đoạn lừa đảo đều chuyển vào tài khoản ngân hàng do đối tượng chỉ định. Số tiền chiếm đoạt được chuyển qua nhiều tài khoản ngân hàng khác nhau và sau cùng là chuyển vào các tài khoản ngân hàng của các đại lý game, sàn giao dịch ảo...để xóa dấu vết, gây khó khăn cho cơ quan Công an trong quá trình điều tra.

4. Biện pháp phòng ngừa, ngăn chặn

- Luôn nâng cao cảnh giác với các thủ đoạn lừa đảo chiếm đoạt tài sản qua mạng.
- Không chuyển tiền vào các tài khoản ngân hàng lạ.
- Cơ quan thực thi pháp luật như Công an, Viện kiểm sát, Tòa án...cuộc gặp gỡ làm việc với người dân thông qua công an cơ sở, không làm việc, gửi lệnh bắt, giam giữ qua điện thoại, mạng xã hội.
- Không vay tiền qua các trang Web, ứng dụng điện thoại không rõ nguồn gốc.

- Cơ quan thực thi pháp luật như Công an, Viện kiểm sát, Tòa án...cuộc gặp gỡ làm việc với người dân thông qua công an cơ sở, không làm việc, gửi lệnh bắt, giam giữ qua điện thoại, mạng xã hội.
- Không vay tiền qua các trang Web, ứng dụng điện thoại không rõ nguồn gốc.

Đề nghị các công đoàn cơ sở quan tâm triển khai nội dung công văn đến cán bộ, công chức, viên chức, người lao động và đoàn viên công đoàn, tuyên truyền rộng rãi cho người thân để nâng cao tinh thần cảnh giác, phòng ngừa tội phạm./.

Nơi nhận

- Như trên;
- Thường trực LĐLĐ tỉnh;;
- Website;
- Lưu: VP.

**TM. BAN THƯỜNG VỤ
PHÓ CHỦ TỊCH**



Thái Thị Bích Thủy