

Số: /STTTT-TTBCXB

Vĩnh Phúc, ngày 14 tháng 7 năm 2023

V/v đẩy mạnh truyền thông về
phương thức, thủ đoạn của tội phạm lừa
đảo, chiếm đoạt tài sản qua mạng Internet

Kính gửi:

- Báo Vĩnh Phúc, Đài Phát thanh và Truyền hình Vĩnh Phúc, Tạp chí Văn nghệ Vĩnh Phúc, Cổng Thông tin - Giao tiếp điện tử Vĩnh Phúc;
- Các cơ quan, đơn vị có Trang thông tin điện tử, bản tin;
- Phòng Văn hóa và Thông tin các huyện, thành phố;
- Trung tâm Văn hóa - Thông tin và Thể thao các huyện, thành phố.

Thực hiện chỉ đạo của UBND tỉnh tại Văn bản số 5373/UBND-VX4 ngày 10/7/2023 về việc giao nhiệm vụ giải quyết ý kiến cử tri và nhân dân 6 tháng đầu năm 2023; để tiếp tục đẩy mạnh công tác truyền thông nâng cao nhận thức pháp luật cho người dân, thường xuyên thông báo về phương thức, thủ đoạn của tội phạm lừa đảo, chiếm đoạt tài sản qua mạng Internet để Nhân dân cảnh giác, chủ động phòng ngừa, tích cực tố giác tội phạm, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị tập trung triển khai mạnh mẽ tuyên truyền một số nội dung trọng tâm sau:

1. Đề nghị các cơ quan báo chí, truyền thông của tỉnh; cơ quan có trang thông tin điện tử

Đề nghị cơ quan, đơn vị dành diện tích đăng tải, thời lượng, tần suất phát sóng phù hợp, tập trung thông tin tuyên truyền:

- Các quy định của pháp luật về phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, nhất là: Luật An ninh mạng, Luật Hình sự,...

- Những phương thức, thủ đoạn, đặc điểm nhận biết và cách phòng tránh đối với loại tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng. Trong đó, tập trung tuyên truyền về: Thủ đoạn gọi điện giả danh cán bộ Nhà nước để lừa đảo chiếm đoạt tài sản; thủ đoạn lợi dụng lòng tham của các cá nhân thông báo trúng thưởng lớn để chiếm đoạt thông tin cá nhân, tài khoản ngân hàng, yêu cầu chuyển tiền; thủ đoạn chiếm quyền sử dụng tài khoản (mạng xã hội Facebook, Zalo...), lập tài khoản mạo danh người khác, tuyên công tác viên làm việc Online, thủ đoạn lợi dụng công nghệ Deepfake làm giả cuộc gọi video,... để thực hiện hành vi lừa đảo chiếm đoạt tài sản.

- Tầm quan trọng của việc bảo vệ các thông tin dữ liệu cá nhân; nâng cao ý thức cảnh giác trong việc cung cấp các thông tin cá nhân cũng như việc xác thực con người trước khi thực hiện việc chuyển tiền bằng hình thức Internet banking; hậu quả, tác hại của việc: bán, cho thuê, cho mượn tài khoản ngân hàng, để các đối tượng xấu sử dụng tài khoản ngân hàng của mình phục vụ việc chuyển, nhận tiền, làm đầu ra cho tài sản chiếm đoạt được.

- Kết quả công tác phòng ngừa, phát hiện, đấu tranh, ngăn chặn của lực lượng chức năng với tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng.

- Trọng tâm tuyên truyền theo khẩu hiệu “**4 không, 2 phải**”. Gồm:

+ “**4 không**” là: **Không sợ** (không hoảng sợ khi nhận được điện thoại, tin nhắn, các thông tin mà người lạ mặt gửi đến có nội dung xấu liên quan đến cá nhân và người thân); **Không tham** (khi có người lạ gọi điện hoặc gửi tin nhắn thông báo được trúng thưởng hoặc nhận được khoản tiền lớn không rõ nguồn gốc thì không được tin lời các đối tượng); **Không kết bạn với người lạ** (khi có người lạ mặt trên mạng xã hội kết bạn làm quen không rõ là ai, mục đích thì không nên kết bạn, bắt chuyện, nhất là không được cung cấp các thông tin cá nhân để đối tượng có thể lợi dụng); **Không làm** (khi các cá nhân không quen biết yêu cầu cung cấp thông tin cá nhân hoặc yêu cầu chuyển tiền hay làm một số việc thì tuyệt đối không được làm theo).

+ “**2 phải**” là: **Phải thường xuyên cảnh giác** (chủ động bảo mật các thông tin cá nhân, nhất là các thông tin quan trọng như: Thông tin thẻ căn cước công dân; thông tin tài khoản ngân hàng; thông tin tài khoản mạng xã hội...); **Phải tố giác ngay với cơ quan pháp luật khi có nghi ngờ** (khi nhận được các cuộc gọi, tin nhắn hoặc các nội dung nghi ngờ là hoạt động lừa đảo hoặc không có cơ sở khẳng định nội dung thì các cá nhân phải báo ngay cho cơ quan pháp luật để được hướng dẫn xử lý).

- Tiếp tục tuyên truyền, phổ biến về thông tin, các hình thức lừa đảo trên mạng xã hội, mạng viễn thông; từ lừa đảo đánh cắp thông tin cá nhân, lừa đảo tình cảm, lừa đảo đầu tư, giả mạo các trang thương mại điện tử lớn tại Việt Nam và nước ngoài để lừa nạn nhân làm cộng tác viên, ... nhưng mục tiêu cuối cùng của các đối tượng xấu chính là tiền.

- Tham khảo nội dung tuyên truyền về phòng ngừa tội phạm lừa đảo trên mạng xã hội, mạng viễn thông, cụ thể:

+ Tại Phụ lục nội dung tuyên truyền về phòng ngừa tội phạm lừa đảo trên mạng xã hội, mạng viễn thông (gửi kèm theo văn bản này).

+ “**Cẩm nang nhận diện và phòng chống lừa đảo trực tuyến**” do Cục An toàn thông tin - Bộ Thông tin và Truyền thông phát hành có địa chỉ https://khonggianmang.vn/uploads/Cam_nang_nhan_dien_va_phong_tranh_LDTT_7493280830.pdf

2. Đề nghị Phòng Văn hoá và Thông tin, Trung tâm Văn hoá - Thông tin và Thể thao các huyện, thành phố:

- Tham mưu, chỉ đạo và tổ chức triển khai tuyên truyền các nội dung tại mục 1 nêu trên bằng nhiều hình thức khác nhau như: hệ thống đài truyền thanh cơ sở cấp huyện và cấp xã, trang/cổng thông tin điện tử, mạng xã hội: zalo, facebook, fanpage... tới đông đảo tầng lớp Nhân dân.

- Chỉ đạo, thực hiện phát thanh hằng ngày các nội dung tuyên truyền phòng ngừa tội phạm trên mạng xã hội, mạng viễn thông trên hệ thống truyền thanh cấp huyện, đài truyền thanh cấp xã.

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị, quan tâm chỉ đạo, phối hợp thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (B/c);
- Ban Tuyên giáo Tỉnh ủy (B/c);
- Công an tỉnh (P/h);
- GD, các PGD;
- Lưu: VT, TTBCXB.

GIÁM ĐỐC

Đỗ Hữu Vinh

Phụ lục:
**NỘI DUNG TUYÊN TRUYỀN VỀ PHÒNG NGỪA TỘI PHẠM
LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG**

(Kèm theo Văn bản số: /STTTT-TTBCXB
ngày 14/7/2023 của Sở Thông tin và Truyền thông)

**THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO
TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG**

Hiện nay các đối tượng xấu lợi dụng những tiện ích mà công nghệ thông tin mang lại để thực hiện nhiều vụ lừa đảo trên mạng xã hội, mạng viễn thông để chiếm đoạt tài sản có giá trị cao.

Các hình thức lừa đảo trên mạng xã hội, mạng viễn thông liên tục gia tăng không ngừng, từ lừa đảo đánh cắp thông tin cá nhân, lừa đảo tình cảm, lừa đảo đầu tư,... nhưng mục tiêu cuối cùng của các đối tượng xấu chính là tiền.

Tính riêng trong năm 2022, có 3 nhóm lừa đảo chính là giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác, với 16 hình thức lừa đảo thường xuyên diễn ra trên mạng xã hội, mạng viễn thông, cụ thể:

Nhóm 1 - Giả mạo thương hiệu, gồm:

- Giả mạo thương hiệu của các cơ quan, tổ chức, như: Cơ quan nhà nước, ngân hàng, công ty tài chính, công ty chứng khoán... để gửi tin nhắn SMS lừa đảo cho nạn nhân.

- Giả mạo các trang web/blog chính thống để tạo uy tín lừa nạn nhân, thu thập thông tin cá nhân của người dân.

Nhóm 2 - Chiếm đoạt tài khoản, gồm:

- Chiếm quyền sử dụng các tài khoản mạng xã hội, như: Zalo, Facebook, Tiktok... để gửi tin nhắn lừa đảo cho bạn bè, người thân nhằm chiếm quyền tài khoản, lấy cắp thông tin, chiếm đoạt tài sản, bôi nhọ danh dự, tống tiền...

- Sử dụng các ứng dụng, quảng cáo tin dụng đen trên các trang web, gửi qua các thư điện tử rác, tin nhắn SMS, mạng xã hội Facebook, Telegram, Zalo... để dụ dỗ người dùng biến họ thành con nợ trong khi chính nạn nhân cũng không biết.

Nhóm 3 - Các hình thức kết hợp, gồm:

- Sử dụng số điện thoại trong nước, nước ngoài, giả danh cơ quan công an, nhà mạng viễn thông... để gọi điện thoại cho nạn nhân thông báo vi phạm pháp luật và yêu cầu chuyển khoản.

- Sử dụng số điện thoại đầu số lạ gọi điện cho nạn nhân, khi bắt máy nạn nhân sẽ bị trừ tiền trong tài khoản mà không hề biết.

- Giả mạo các trang thương mại điện tử lớn tại Việt Nam và nước ngoài để lừa nạn nhân làm cộng tác viên. Đề dẫn dụ nạn nhân, đối tượng chạy quảng cáo lừa đảo trên Facebook hay gửi tin nhắn quảng cáo spam qua SMS.

- Lan truyền tin giả đánh vào tâm lý hiếu kỳ, sự thương người và lòng tin. Để câu views, câu likes và sau đây lừa gạt chiếm đoạt tài sản qua hình thức từ thiện, kêu gọi đóng góp...

- Lừa đảo chiếm đoạt tài sản qua quảng bá bán hàng online trên Facebook (bán hàng giả, chất lượng kém, vé máy bay giả, khuyến mãi giả, hàng ảo hoặc rao bán giả mạo không tồn tại sản phẩm).

- Giả mạo trang cá nhân, tài khoản người dùng trên Facebook, Telegram, Zalo để tạo uy tín và lừa nạn nhân sử dụng dịch vụ hoặc đầu tư.

- Lợi dụng lòng tin và sự thương hại để lừa đảo qua các nền tảng Facebook, Zalo, Tinder, Telegram.

- Lừa đảo cài cắm mã độc thông qua đường dẫn độc hại, phần mềm độc hại. Đối tượng tạo những công cụ, đường dẫn, phần mềm độc hại để chiếm đoạt tài sản, thông tin tài khoản mạng xã hội, ngân hàng.

- Thông báo trúng thưởng, quà tặng, khuyến mại để lừa nạn nhân đánh cắp thông tin tài khoản và tài sản thông qua các trang web giả mạo.

- Thủ đoạn nâng cấp lên sim 4G hay 5G để lừa lấy số điện thoại của nạn nhân nhằm chiếm đoạt thông tin tài khoản và tài sản.

- Giả mạo email của ngân hàng, cơ quan, tổ chức có uy tín để uy hiếp, đe dọa lừa tiền nạn nhân.

- Lập sàn đầu tư tiền ảo crypto, đầu tư đa cấp, đầu tư nhị phân, đầu tư Forex... lừa đảo chiếm đoạt tài sản.

Đề bảo vệ người dân trước vấn nạn lừa đảo trên mạng xã hội, mạng viễn thông, các cơ quan chức năng, doanh nghiệp cung cấp dịch vụ, doanh nghiệp an toàn, an ninh mạng đã triển khai nhiều biện pháp kỹ thuật, hoạt động tuyên truyền, nâng cao nhận thức cho khách hàng, người dân.

Đề nghị người dân cần cảnh giác, khi phát hiện các hoạt động nêu trên trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./.

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm lừa đảo đăng tin tuyển cộng tác viên bán hàng online trên các trang mạng xã hội (Zalo, Facebook, Tiktok...), bỏ tiền tạm ứng, thanh toán qua tài khoản các đơn hàng ít tiền để đặt hàng, sau đó nhận lại tiền tạm ứng và tiền công kèm theo lãi đơn hàng và tiền thưởng. Đến các lần tiếp theo, thanh toán đơn hàng với lượng tiền lớn thì bị chiếm đoạt, đồng thời nhận được yêu cầu nộp thêm tiền để hệ thống xử lý lỗi và hoàn trả nhưng không được hoàn trả.

Đề nghị người dân cần cảnh giác, không tham gia hoạt động nêu trên, khi phát hiện trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./.

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm giả danh cơ quan Công an, Viện Kiểm sát, Tòa án... gọi điện thông báo có liên quan đến các vụ án đang điều tra, mua bán ma túy, rửa tiền..., gửi lệnh bắt giữ hay tài liệu liên quan khác qua mạng xã hội để đe dọa, yêu cầu chuyển tiền đến các tài khoản chỉ định hoặc tài khoản mới

mở rồi cung cấp thông tin tài khoản để kiểm tra hoặc tải các đường link, phần mềm giả mạo cơ quan, nhằm đánh cắp thông tin tài khoản ngân hàng để chiếm đoạt. Việc các cơ quan chức năng điều tra, xác minh, xử lý tội phạm đều được tiến hành trực tiếp, không thông qua mạng xã hội gửi thông báo, tin nhắn yêu cầu.

Đề nghị người dân cần cảnh giác, không thực hiện theo các yêu cầu của đối tượng và trình báo ngay với cơ quan công an nơi gần nhất để giải quyết./.

THÔNG TIN VỀ TỘI PHẠM LỪA ĐẢO TRÊN MẠNG XÃ HỘI, MẠNG VIỄN THÔNG

Theo thông báo của Bộ Công an, hiện nay, tội phạm giả mạo là người nước ngoài (sĩ quan, binh lính đang tham gia chiến tranh, làm nhiệm vụ quốc tế tại các khu vực chiến sự... không có người thân) thông qua mạng xã hội làm quen, sau đó lấy lý do gửi quà, đồ vật giá trị, thậm chí là ngoại tệ, vàng có giá trị rất lớn nhờ nhận, quản lý, lưu giữ; sau đó giả danh là nhân viên sân bay, hải quan, thuế... yêu cầu nộp tiền cước vận chuyển, thuế, phí, tiền phạt, chi phí tiêu cực... để chiếm đoạt.

Đề nghị người dân cần cảnh giác, không chuyển tiền vào các tài khoản do đối tượng yêu cầu và trình báo ngay với cơ quan công an nơi gần nhất để được giải quyết./.