BỘ CÔNG AN
**CÔNG AN TỈNH LẠNG SƠN**

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

Số: 1846/CAT-PC02

*Lạng Sơn, ngày 15 tháng 4 năm 2020*

V/v tăng cường phòng ngừa, đấu tranh với tội phạm lừa đảo chiếm đoạt tài sản qua mạng viễn thông, Internet



Kính gửi:
- Các sở, ban, ngành, tổ chức đoàn thể tỉnh;
- UBND các huyện, thành phố;
- Các cơ quan báo chí, truyền thông, truyền hình của tỉnh.

Thời gian gần đây, các cấp, ngành trên địa bàn tỉnh đã tập trung chỉ đạo, thực hiện nhiều giải pháp phòng, chống tội phạm lừa đảo chiếm đoạt tài sản nói chung, lừa đảo chiếm đoạt tài sản qua mạng viễn thông, Internet nói riêng, góp phần kiềm chế loại tội phạm này; nhận thức, ý thức tự phòng ngừa, phát hiện, ngăn chặn và tố giác các hành vi lừa đảo của người dân và cơ quan, tổ chức ngày càng được nâng cao. Tuy nhiên, một số người dân mặc dù đã được tuyên truyền, cảnh báo nhưng do nhẹ dạ cả tin, hám lợi vẫn trở thành nạn nhân của các đối tượng lừa đảo qua mạng với số tiền bị chiếm đoạt rất lớn. Theo thống kê từ đầu năm 2020 đến nay, lực lượng Công an đã tiếp nhận 07 vụ công dân trình báo bị các đối tượng thực hiện hành vi lừa đảo qua mạng với số tiền chiếm đoạt gần 900 triệu đồng; thực tế còn nhiều vụ việc nhưng người dân không trình báo cơ quan Công an. Thủ đoạn phổ biến các đối tượng sử dụng là: **(1)** Giả danh, liên kết với đối tượng người nước ngoài làm quen qua mạng xã hội, vờ kết thân, yêu đương, hứa hẹn gửi tiền, quà có giá trị cao, đề nghị đóng các loại thuế, phí để nhận quà; **(2)** Giả danh cán bộ trong các cơ quan thực thi pháp luật (Công an, Viện kiểm sát, Tòa án) đe dọa người bị hại có liên quan đến quá trình điều tra vụ án về ma túy, buôn lậu..., để xác minh làm rõ, đối tượng yêu cầu người bị hại nộp tiền vào các tài khoản định sẵn để kiểm tra sau đó chiếm đoạt; **(3)** Thông báo trúng thưởng, yêu cầu người bị hại chuyển tiền làm chi phí để nhận thưởng; **(4)** Chiếm đoạt quyền kiểm soát các tài khoản mạng xã hội sau đó gửi tin nhắn đến người thân quen trong danh bạ của tài khoản chiếm đoạt để vay, mượn tiền *(có phụ lục chi tiết kèm theo)*. Đặc biệt hiện nay, lợi dụng tình hình dịch bệnh Covid-19 đang diễn biến phức tạp, người dân thực hiện cách ly xã hội, tăng cường sử dụng công nghệ thông tin, không gian mạng để học tập, làm việc, giải trí nên các đối tượng cũng gia tăng hoạt động phạm tội.

Trước tình hình trên, để tăng cường các biện pháp phòng ngừa, đấu tranh với tội phạm lừa đảo chiếm đoạt tài sản qua mạng, Công an tỉnh đề nghị các sở, ban, ngành, tổ chức đoàn thể, cơ quan báo chí, truyền thông, truyền hình của tỉnh và UBND các huyện, thành phố quan tâm, chỉ đạo thực hiện một số nội dung sau:

**1.** Tiếp tục tuyên truyền sâu rộng về tình hình, kết quả công tác đấu tranh với tội phạm lừa đảo chiếm đoạt tài sản trên các phương tiện thông tin đại chúng,

qua tin nhắn điện thoại, mạng xã hội; phương thức, thủ đoạn, hậu quả, tác hại, cách thức phòng ngừa, phát hiện, tố giác các hành vi lừa đảo chiếm đoạt tài sản qua mạng. Quán triệt cán bộ, công nhân viên chức, người lao động nâng cao tinh thần cảnh giác, ý thức bảo vệ tài sản, nghiêm cấm tham gia hoặc tiếp tay cho các đối tượng hoạt động lừa đảo chiếm đoạt tài sản, kiên quyết xử lý nghiêm các trường hợp vi phạm.

Tuyên truyền, khuyến cáo người dân nâng cao ý thức bảo vệ, bảo mật thông tin cá nhân trên không gian mạng, không tùy tiện cung cấp, khai báo thông tin cá nhân trên các trang mạng, đường link có nội dung không rõ ràng, đặc biệt là thông tin về tài khoản, mật khẩu; không tải, cài đặt, đăng nhập các trang web, đường link, phần mềm lạ vào điện thoại, máy tính; thận trọng khi kết bạn, làm quen với những người nước ngoài, Việt kiều trên mạng xã hội; hỏi ý kiến người khác, kiểm tra kỹ thông tin từ các nguồn chính thống về thông báo trúng thưởng, tặng quà... Khi nhận được lời đề nghị vay mượn, chuyển tiền, mua thẻ nạp từ người thân, bạn bè qua tin nhắn, mạng xã hội cần liên lạc trực tiếp với người đó để xác nhận. Hạn chế sử dụng các điểm truy cập Internet công cộng để đăng nhập, thực hiện giao dịch trên hệ thống ngân hàng điện tử; bật tính năng xác thực 2 yếu tố (2FA) cho các tài khoản cá nhân, đặc biệt là thư điện tử (e-mail), tài khoản mạng xã hội, ngân hàng trực tuyến, tài khoản thanh toán, mua sắm trực tuyến, các dịch vụ lưu trữ đám mây.

**2.** Đề nghị Sở Thông tin và Truyền thông tăng cường quản lý chặt chẽ các thuê bao di động, thuê bao Internet, loại bỏ sim "rác", đảm bảo các thuê bao có đầy đủ thông tin chính chủ; phối hợp với các cơ quan, đơn vị chức năng quản lý chặt chẽ các cuộc gọi từ Internet vào mạng viễn thông theo phương thức VoIP nhằm ngăn chặn các đối tượng giả mạo số điện thoại của cơ quan Nhà nước gọi điện lừa đảo; rà soát các website, tài khoản mạng xã hội của các tổ chức, các nhân có biểu hiện lừa đảo chiếm đoạt tài sản qua mạng Internet và mạng viễn thông để trao đổi với lực lượng Công an có các biện pháp chủ động phòng ngừa, ngăn chặn và xử lý loại tội phạm này. Chỉ đạo các doanh nghiệp cung cấp dịch vụ viễn thông Internet lưu trữ đầy đủ thông tin người dùng, có giải pháp định danh tài khoản, kịp thời phối hợp cung cấp cho các cơ quan chức năng khi có yêu cầu.

**3.** Đề nghị Ngân hàng Nhà nước Việt Nam chi nhánh tỉnh Lạng Sơn chỉ đạo các ngân hàng thương mại quán triệt đến toàn thể cán bộ, nhân viên khi phát hiện các biểu hiện bất thường của khách hàng đến giao dịch như: Người cao tuổi đến rút tiền, gửi số tiền lớn vào các tài khoản ngân hàng ở xa; khách hàng có tâm lý lo lắng, bất ổn, thường xuyên nghe điện thoại, không tắt cuộc gọi trong khi thực hiện giao dịch... thì cần tư vấn, trao đổi và thông báo cho khách hàng về thủ đoạn hoạt động lừa đảo qua mạng để cảnh giác. Dán các thông báo, cảnh báo về thủ đoạn của các đối tượng lừa đảo chiếm đoạt tài sản qua mạng Internet, mạng viễn thông, thiết bị số tại cửa ra vào và quầy giao dịch ở các chi nhánh. Tăng cường giám sát, kiểm tra các máy ATM của ngân hàng để kịp thời phát hiện các thiết bị lạ gắn vào máy; khi phát hiện đối tượng sử dụng thông tin giả, thẻ ATM giả để giao dịch cần nhanh chóng thông báo cho lực lượng Công an nơi gần nhất để phối hợp xử lý. Phối hợp chặt chẽ với các lực lượng chức năng kịp thời phát hiện, ngăn chặn các hành vi lợi dụng hoạt

động thanh toán của ngân hàng để hoạt động phạm tội, cung cấp các thông tin phục vụ công tác điều tra, xác minh trong thời gian sớm nhất khi có yêu cầu.

Công an tỉnh sử dụng số máy trực ban hình sự ***069.2569.159*** của Phòng Cảnh sát hình sự là số điện thoại đường dây nóng tiếp nhận thông tin phản ánh về hoạt động lừa đảo chiếm đoạt tài sản của cơ quan, tổ chức, người dân 24/24h. Thông tin chi tiết, vụ việc cần trao đổi, đề nghị liên hệ Phòng Cảnh sát hình sự - Công an tỉnh, địa chỉ: Số 15, đường Hoàng Văn Thụ - phường Chi Lăng, thành phố Lạng Sơn, SĐT: 069.2569.159 để phối hợp, giải quyết.

Rất mong sự quan tâm, phối hợp của các cơ quan, đơn vị./.

***Nơi nhận:***
- Như trên;
- Đ/c Hồ Tiến Thiệu - PCT UBND tỉnh (Báo cáo);
- Đ/c Giám đốc CAT (Báo cáo);
- Lưu CAT (PC02,PV01).

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

**Đại tá Vũ Hồng Quang**

# PHỤ LỤC CHI TIẾT

**Về thủ đoạn hoạt động phổ biến của tội phạm lừa đảo qua mạng**

*(Kèm theo Công văn số 1846/CAT-PC02, ngày 15/4/2020 của Công an tỉnh)*

Từ ngày 01/01/2020 đến 09/4/2020, trên địa bàn tỉnh xảy ra 07 vụ lừa đảo chiếm đoạt tài sản bằng các hình thức như: Kết bạn qua mạng xã hội Zalo, Facebook lừa gửi quà từ nước ngoài về (02 vụ); Chiếm đoạt tài khoản mạng xã hội sau đó giả danh chủ tài khoản gửi tin nhắn vay, mượn tiền (02 vụ); Gọi điện thoại giả danh Công an, Viện kiểm sát, Tòa án đe dọa nạn nhân có liên quan đến các đường dây tội phạm để tống tiền nạn nhân (02) vụ; Thông báo trúng thưởng giá trị lớn sau đó yêu cầu nộp tiền để nhận quà (01 vụ) với tổng số tiền chiếm đoạt của các bị hại trên 881.000.000đ. Thủ đoạn của các đối tượng:

**Thủ đoạn thứ nhất**: Thông qua mạng xã hội như Zalo, Facebook... các đối tượng làm quen và kết bạn với các nạn nhân, đặc biệt là phụ nữ. Các đối tượng đưa ra những thông tin giả giới thiệu về điều kiện, hoàn cảnh của bản thân như là quân nhân, kỹ sư, bác sỹ... hiện đang chiến đấu, làm việc ở chiến trường, đã ly hôn và sống độc thân, hiện có nguồn tài sản lớn, gửi các hình ảnh về giấy căn cước, hộ chiếu và nơi làm việc cho nạn nhân để tạo lòng tin. Sau đó đối tượng ngỏ ý gửi tặng quà có giá trị lớn như: Tiền mặt, vàng, kim cương, đồ điện tử đắt tiền... cho nạn nhân hoặc đề nghị nạn nhân nhận giúp nguồn tiền chuyển từ nước ngoài về để sau này sang Việt Nam đầu tư kinh doanh, mua bất động sản. Khi nạn nhân đồng ý, các đối tượng đề nghị nạn nhân cung cấp địa chỉ, số điện thoại, số chứng minh để gửi đến đồng thời gửi cho nạn nhân hình ảnh gói quà bên trong có nhiều ngoại tệ, trang sức, vật dụng đắt tiền. Sau một khoảng thời gian, các đối tượng người Việt Nam liên lạc, tự xưng là nhân viên an ninh sân bay, hải quan, nhân viên giao hàng, cán bộ thuế...đưa ra các thông tin giả cản trở việc nhận gói quà (như hàng bị tạm giữ tại sân bay vì trong đó có nhiều ngoại tệ, hàng hóa có giá trị phải nộp lệ phí, bảo hiểm, thuế thu nhập cá nhân, phí chuyển đổi ngoại tệ...) và yêu cầu nạn nhân chuyển tiền vào các tài khoản các đối tượng cung cấp để giải quyết vấn đề, sau khi nhận được tiền, các đối tượng nhanh chóng sử dụng hình thức chuyển tiền qua hệ thống Internet banking để chuyển lòng vòng đến nhiều tài khoản khác nhau để chiếm đoạt. Sau mỗi lần nạn nhân chuyển tiền, các đối tượng lại đưa ra các lý do mới cho đến khi nạn nhân không còn khả năng chuyển tiền cho các đối tượng.

**Thủ đoạn thứ hai**: Các đối tượng sử dụng công nghệ VoIP (Voice over Internet Protocol), các ứng dụng tạo số điện thoại ảo, thiết lập các tổng đài tự động gọi đến số điện thoại của nạn nhân tự xưng là Cơ quan Công an, Viện kiểm sát, Tòa án nhân dân, đưa ra các thông tin giả để cho nạn nhân tin là họ có liên quan đến các vụ án như: Các thông tin cá nhân của nạn nhân hiện đang được sử dụng để mở tài khoản ngân hàng, trong tài khoản có lượng tiền lớn liên quan đến đường dây tội phạm ma túy; nợ tiền cước viễn thông; nợ ngân hàng...) và đe dọa sẽ bắt, tạm giam nạn nhân nếu không hợp tác, một số trường hợp các đối tượng sử các phần mềm để chỉnh sửa, cắt ghép ảnh đưa các thông tin của nạn nhân vào các Lệnh/Quyết định giả của Cơ quan điều tra, Viện kiểm sát, Tòa án rồi gửi cho nạn nhân. Khi nạn nhân lo sợ, các đối tượng nói sẽ giúp điều tra, xác minh làm rõ, sau

đó yêu cầu nạn nhân cung cấp các thông tin cá nhân, thông tin về các tài khoản ngân hàng, tài khoản tiết kiệm và yêu cầu nạn nhân chuyển tiền vào tài khoản của cơ quan điều tra để kiểm tra, nếu xác minh không liên quan thì sẽ được trả lại đầy đủ. Do lo sợ nên một số nạn nhân đã chuyển toàn bộ số tiền trong tài khoản ngân hàng, tài khoản tiết kiệm cho các đối tượng. Ngay sau khi nhận được tiền của nạn nhân, các đối tượng lập tức chuyển tiếp đến nhiều tài khoản thuộc các hệ thống ngân hàng khác sau đó chiếm đoạt.

**Thủ đoạn thứ ba**: Các đối tượng mạo danh là cán bộ ngân hàng, nhà mạng di động, nhân viên các công ty sản xuất, mua bán xe máy, ô tô gọi điện, nhắn tin cho nạn nhân thông báo trúng giải thưởng giá trị như sổ tiết kiệm, tiền mặt, xe máy, ô tô... Sau đó đối tượng yêu cầu nạn nhân nộp các khoản phí như tiền thuế, lệ phí đăng ký xe máy, ô tô, lệ phí quay phim, chụp ảnh...để nhận thưởng, khi nạn nhân đồng ý chuyển tiền các đối tượng cung cấp thông tin tài khoản ngân hàng để nạn nhân chuyển tiền vào và chiếm đoạt

**Thủ đoạn thứ tư**: Các đối tượng sử dụng các thủ đoạn (như sử dụng phần mềm gián điệp, dụ dỗ nạn nhân truy cập vào các trang web có mã độc, các trang web giả mạo cổng thông tin điện tử của cơ quan tổ chức, trang bình chọn các cuộc thi trên truyền hình sau đó yêu cầu nhập thông tin hoặc gọi điện giả danh nhân viên kỹ thuật các công ty yêu cầu nạn nhân cung cấp thông tin) để chiếm đoạt quyền sử dụng tài khoản mạng xã hội Zalo, Facebook, tài khoản icloud, tài khoản email của người nạn nhân *(ví dụ: Đối tượng gửi đường link, địa chỉ web nhờ bình chọn cho con, cháu tham gia cuộc thi "Giọng hát Việt nhí" và hướng dẫn truy cập vào các trang web giả mạo như: https://binhchonchocacbenhinam2019.weebly.com; https://amnhactuyenchon2020.weebly.com để bình chọn; Giả mạo nhân viên kỹ thuật của Zalo, Facebook, nhân viên ngân hàng gọi điện yêu cầu cung cấp mã số OTP...).*

Sau khi chiếm đoạt được tài khoản các đối tượng nghiên cứu tin nhắn của nạn nhân với người khác để tìm hiểu các mối quan hệ thân thiết, cách nói chuyện với bạn bè để mạo danh chủ tài khoản nhắn tin hỏi vay tiền, những người đồng ý cho vay sẽ được các đối tượng hướng dẫn chuyển tiền vào các tài khoản ngân hàng đã chuẩn bị để chiếm đoạt.

Một số trường hợp các đối tượng giả danh người ở nước ngoài mua hàng hóa sau đó gửi email, tin nhắn giả thông báo của ngân hàng về việc tài khoản đã nhận được tiền, kèm theo liên kết đến các trang web giả mạo dịch vụ chuyển tiền quốc tế, yêu cầu nạn nhân nhập thông tin tài khoản ngân hàng để nhận tiền (ví dụ: *https://dichvuwesternunionquocte24hss.weebly.com*). Thực chất đây là các trang web giả mạo để đánh cắp thông tin tài khoản./.