

**BỘ CÔNG AN
CÔNG AN TỈNH BẮC GIANG**

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

Số: 140 /CAT-ANM

V/v đề nghị phối hợp tuyên truyền
phòng, chống tội phạm lừa đảo chiếm
đoạt tài sản trên không gian mạng

Bắc Giang, ngày 30 tháng 5 năm 2022

Kính gửi:

- Ban Tuyên giáo; Ban Dân vận Tỉnh ủy;
- Ủy ban Mặt trận Tổ quốc và các Đoàn thể tỉnh;
- Sở Thông tin và Truyền thông; Sở Giáo dục và Đào tạo;
Sở Văn hóa, Thể thao và Du lịch;
- Ngân hàng Nhà nước Việt Nam chi nhánh tỉnh Bắc Giang;
- Báo Bắc Giang, Đài Phát thanh - Truyền hình Bắc Giang;
- Ủy ban nhân dân các huyện, thành phố.

Ngày 30/3/2022, Công an tỉnh Bắc Giang đã triển khai Kế hoạch số 107/KH-CAT-ANM về việc thực hiện đợt cao điểm tuyên truyền phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng.

Để nâng cao hơn nữa tinh thần cảnh giác, giúp mỗi cán bộ, đảng viên, đoàn viên, công chức, viên chức, người lao động và mọi người dân biết được phương thức, thủ đoạn của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, từ đó chủ động phòng tránh, Công an tỉnh Bắc Giang tiếp tục xây dựng đề cương tài liệu tuyên truyền bao gồm: Bản viết phục vụ việc tuyên truyền bằng hình thức tổ chức các hội nghị, tọa đàm, buổi giao ban, nói chuyện sinh hoạt chuyên đề, sinh hoạt chi bộ và phát trên Đài Truyền thanh và hệ thống loa phát thanh cơ sở; Bản file mềm hình ảnh phục vụ việc tuyên truyền trên các trang mạng xã hội hoặc in pano, áp phích...

(Đề cương tuyên truyền có file mềm kèm theo)

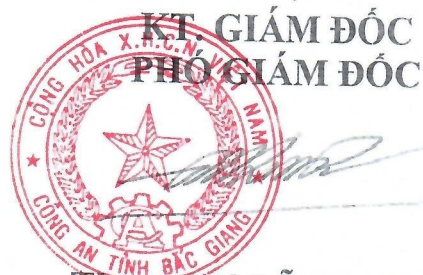
Công an tỉnh Bắc Giang trân trọng đề nghị Ủy ban Mặt trận Tổ quốc tỉnh, các cơ quan, ban, ngành, đoàn thể tỉnh và Ủy ban nhân dân các huyện, thành phố phối hợp tăng cường công tác tuyên truyền phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng trong nội bộ đơn vị, cơ quan, doanh nghiệp và Nhân dân...

Mọi thông tin liên quan đến công tác tuyên truyền cũng như khi phát hiện những vụ việc, đối tượng có dấu hiệu lừa đảo chiếm đoạt tài sản trên không gian mạng đề nghị trao đổi với Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao qua số điện thoại: 0692589936; DD: 0914325080.

Công an tỉnh Bắc Giang trân trọng thông báo./.đkt

Nơi nhận:

- Như trên;
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh; (để b/cáo)
- Đ/c Giám đốc CAT;
- Lưu: VT, ANM (Đ3).



Thượng tá Đỗ Đức Trịnh



ĐỀ CƯƠNG TUYÊN TRUYỀN

(Kèm theo Công văn số 1140 /CV-CAT-ANM ngày 30 tháng 5 năm 2022)

1. Các thủ đoạn giả danh

+ *Giả danh cán bộ Công an, Viện Kiểm sát, Tòa án* gọi điện thông báo người dân có liên quan đến vụ án hoặc xử phạt người 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... Sau đó, người dân lo sợ, chuyển tiền vào tài khoản mà đối tượng yêu cầu thì đối tượng chiếm đoạt.

+ *Giả danh cán bộ Ngân hàng* gọi điện cho bị hại thông báo 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, chiếm đoạt của bị hại.

+ *Giả danh nhân viên nhà mạng* gọi điện thông báo số thuê bao 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 lừa đảo cung cấp, khi người dân đóng tiền vào tài khoản để nhận thưởng thì các đối tượng chặn liên lạc và chiếm đoạt tiền.

+ *Giả danh nhân viên điện lực* gọi điện thông báo nộp tiền điện dưới hình thức chuyển khoản với nội dung: “Bạn đang sử dụng điện cao bất thường, chúng tôi sẽ cắt điện trong thời gian tới, vui lòng bấm số 9 gặp nhân viên tư vấn”. Với các thông báo đó, khách hàng rất dễ bị lừa, chuyển khoản nộp tiền điện và bị đối tượng chiếm đoạt.

2. Thủ đoạn giả mạo tài khoản Zalo, Facebook

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, đối tượng dùng 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.

3. Thủ đoạn lừa đảo thông qua hình thức tuyển cộng tác viên online, tuyển nhân viên làm việc tại nhà

** Trường hợp 1:*

Đối tượng thường đăng các bài tuyển nhân viên, cộng tác viên trên các hội, nhóm Facebook: “tuyển nhân viên xâu vòng tại nhà, không yêu cầu về trình độ, độ tuổi, nguyên liệu có người giao tận nơi... với tiền công hấp dẫn “xâu 1 kg hạt được 350.000 đồng”; hay gia công lì xì, túi đựng hạt giống, làm tranh đá tại

nhà... Để làm những công việc này, người làm phải đặt cọc số tiền là từ vài trăm nghìn đến hàng triệu đồng tiền nguyên liệu. Tuy vậy, khi hoàn thành, bị hại gửi sản phẩm cho bên thuê dịch vụ thì bị trả lời sản phẩm không đạt yêu cầu nên không nhận và chiếm đoạt tiền của bị hại.

** Trường hợp 2:*

Lợi dụng sự nhẹ dạ cả tin và nhu cầu kiếm tiền nhanh của bị hại, các đối tượng giả mạo tuyên cộng 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 nhãn hàng, trang thương mại điện tử như: Tiki.vn, Lazada, Tokyolife, Shopee... và chạy quảng cáo. Khi bị hại nhắn tin hỏi cách thức làm cộng tác viên, các đối tượng sẽ gửi các thông tin về công ty, nhân viên chăm sóc khách hàng... yêu cầu gửi thông tin cá nhân, kết bạn Zalo để tư vấn.

Ban đầu, đối tượng gửi link (đường dẫn) các sản phẩm có giá trị nhỏ khoảng vài trăm nghìn 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 mua hàng cùng với hoa hồng từ 3-20%. Sau một số lần tạo niềm tin bằng cách trả gốc và hoa hồng như cam kết ban đầu, tiếp theo đối tượng viện lý do là “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 chuyển 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. Sau đó các đối tượng chiếm đoạt toàn bộ số tiền của bị hại.

4. Thủ đoạn lừa đảo thông qua các sàn giao dịch trên mạng

Các đối tượng mời chào, lôi kéo bị hại tham gia đầu tư vào các sàn giao dịch tiền ảo do đối tượng thiết lập, cam kết sẽ hưởng lợi nhuận cao khi tham gia hệ thống. Các đối tượng thường quảng bá, đánh bóng tên tuổi bằng cách đăng tin, bài trên mạng xã hội, tổ chức các buổi hội thảo, gặp mặt, tự nhận là chuyên gia đầu tư, người truyền cảm hứng, người dẫn đường... để lừa đảo, kêu gọi đầu tư vào hệ thống do chúng thiết lập. Khi huy động được lượng tiền đủ lớn, các đối tượng sẽ can thiệp vào các giao dịch, điều chỉnh thắng thua hoặc báo lỗi, ngừng hoạt động (sập sàn) để chiếm đoạt tiền của người tham gia.

5. Thủ đoạn cho vay tiền qua ứng dụng (vay tiền online qua app)

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 sẽ gửi các đường link kết nối với CH Play hoặc App Store để các bị hại cài đặt ứng dụng vào điện thoại và làm theo hướng dẫn. Sau đó, khi

bị hại đăng nhập vào ứng dụng vay tiền thì ứng dụng sẽ báo lỗi, các đối tượng yêu cầu bị hại phải chuyển tiền đặt cọc để mở lại tài khoản thì mới giải ngân được, hoặc 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 các đối tượng lừa đảo thông báo nếu không chuyển nữa thì không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền này của bị hại.

6. Một số thủ đoạn lừa đảo khác

+ Đăng các tin, bài bán hàng trên mạng xã hội... Khi bị hại kết nối và đặt cọc hoặc thanh toán số tiền theo thỏa thuận thì các đối tượng chặn liên hệ, đổi số điện thoại... và chiếm đoạt số tiền đã nhận được.

+ Thông báo trúng thưởng tiền, tài sản có giá trị lớn như xe máy, điện thoại, đồng hồ hoặc tiền mặt... Sau đó, đối tượng yêu cầu người bị hại nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng và chiếm đoạt.

+ Gửi tin nhắn SMS giả mạo của Ngân hàng để lừa khách hàng truy cập vào đường link giả, sau đó yêu cầu cung cấp các thông tin bảo mật như tên, mật khẩu đăng nhập, mã OTP, thông tin thẻ... Khi có được các thông tin này, đối tượng sẽ rút tiền trong tài khoản của nạn nhân.

+ Các đối tượng lừa đảo cố ý “*chuyển nhầm*” một khoản tiền đến tài khoản ngân hàng. Tiếp đó, chúng yêu cầu người dùng trả lại số tiền kia như một khoản vay cùng với khoản lãi rất cao. Nếu không trả, các đối tượng sẽ nhắn tin đe dọa, gây phiền hà, ghép hình ảnh bôi nhọ danh dự, nhân phẩm, làm mất uy tín và làm ảnh hưởng đến cuộc sống của bị hại và người thân.

*** Để tránh bị lừa đảo, Công an tỉnh Bắc Giang khuyến cáo:**

1. Không chuyển tiền theo yêu cầu của người lạ hoặc người mới quen biết trên mạng xã hội; Nếu chuyển tiền cho người thân, người quen phải xác thực thông tin qua điện thoại thông thường hoặc gặp mặt trực tiếp;

2. Không bấm vào đường link lạ; không thực hiện theo yêu cầu của các tin nhắn lạ. Không cung cấp mật khẩu và mã xác thực (OTP) cho bất kỳ ai;

3. Báo ngay cho cơ quan Công an nơi gần nhất khi gặp các trường hợp như trên để được hướng dẫn xử lý hoặc số điện thoại: 0692589936; di động: 0914325080.