UBND TỈNH BẮC KẠN **BAN CHỈ ĐẠO 138**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 3332 /TB-BCĐ	*Bắc Kạn, ngày 17 tháng 9 năm 2021*

THÔNG BÁO
Phương thức, thủ đoạn lừa đảo chiếm đoạt tài sản qua mạng internet, mạng viễn thông

Thời gian qua, các cơ quan chức năng đã tăng cường công tác tuyên truyền, thông báo về tội phạm lừa đảo chiếm đoạt tài sản qua mạng internet, viễn thông đến cán bộ, công chức, viên chức, người lao động và nhân dân biết, phòng ngừa. Tuy nhiên, tình trạng lừa đảo chiếm đoạt tài sản qua mạng internet, mạng viễn thông vẫn diễn ra với các phương thức, thủ đoạn tinh vi, xảo quyệt; đặc biệt chúng lợi dụng sự hoang mang, thiếu hiểu biết trong thời điểm diễn ra dịch bệnh Covid-19 và tâm lý cả tin, hám lợi của nạn nhân để phạm tội. Các vụ lừa đảo qua mạng gây ra thiệt hại lớn về kinh tế của nạn nhân, làm phức tạp thêm tình hình an ninh, trật tự tại địa phương và rất khó khăn trong quá trình điều tra, xử lý của lực lượng chức năng. Để tăng cường công tác tuyên truyền, phòng ngừa tội phạm lừa đảo chiếm đoạt tài sản qua mạng internet, mạng viễn thông, Ban Chỉ đạo 138 tỉnh thông báo một số thủ đoạn của loại tội phạm này như sau:

1. Mạo danh để yêu cầu chuyển tiền

- Thủ đoạn: Giả danh cán bộ các cơ quan chức năng (Công an, Viện kiểm sát, Tòa án, Y tế, Bệnh viện…) gọi điện thoại thông báo đang điều tra các vụ án (thường là án ma túy, rửa tiền) có liên quan đến nạn nhân, hoặc yêu cầu nạn nhân xác nhận thông tin vì có thông tin trùng với nạn nhân có kết quả dương tính với Covid-19, sau đó yêu cầu nạn nhân khai báo thêm các thông tin liên quan, hướng đến việc cung cấp thông tin về tài khoản và tiền gửi trong tài khoản ngân hàng của nạn nhân. Khi biết nạn nhân có tiền gửi tại ngân hàng, đối tượng yêu cầu nạn nhân phải chuyển tiền vào tài khoản của chúng hoặc tự lập một tài khoản mới và chuyển tiền vào đó và cung cấp thông tin, mật khẩu tài khoản đó cho chúng để "cơ quan chức năng" chứng minh đó là nguồn tiền gì? Có phải tiền do phạm tội mà có hay không?...

- Thủ đoạn: Giả danh là kỹ sư, bác sỹ, quân nhân, doanh nhân, phi công, thuyền trưởng… người nước ngoài (bằng cách đưa các hình ảnh giới thiệu là đang sinh sống, kinh doanh tại Anh, Mỹ hoặc đang chiến đấu tại Syria, Ly bia...

trên các mạng xã hội như Facebook, Zalo, Whatsapp, Skype...) để làm quen, kết bạn, hứa kết hôn và bảo lãnh đi nước ngoài, hứa gửi quà tặng có giá trị lớn, trong đó có nhiều ngoại tệ, vàng, trang sức, đồ vật có giá trị lớn. Sau đó các đối tượng giả danh là nhân viên giao nhận hàng, hải quan, thuế vụ, bưu điện... thông báo thùng quà biếu đang bị tạm giữ vì có nhiều ngoại tệ, hàng hóa giá trị lớn và đề nghị nạn nhân phải nộp thuế, lệ phí để nhận hàng.

- **Thủ đoạn:** Giả danh là nhân viên công ty, doanh nghiệp có uy tín trên thị trường gọi điện, nhắn tin thông báo trúng thưởng và yêu cầu nạn nhân chuyển tiền hoặc nạp thẻ điện thoại để làm phí nhận thưởng.

Cách nhận biết, phòng ngừa: Theo quy định của pháp luật, khi làm việc với người dân thì các cơ quan Nhà nước (Công an, Viện kiểm sát, Tòa án, Thuế, Hải quan...), các công ty, doanh nghiệp đều có giấy giới thiệu, giấy mời hoặc trực tiếp gặp mặt để trao đổi công việc và không có quy định gọi điện thoại yêu cầu chuyển tiền. Do đó, tất cả các cuộc điện thoại tự nhận là cơ quan chức năng đang điều tra, giải quyết vụ án, vụ việc; hải quan, thuế thông báo có quà tặng hoặc doanh nghiệp thông báo trúng thưởng... rồi yêu cầu chuyển tiền vào tài khoản đều có nguy cơ là lừa đảo chiếm đoạt tài sản.

2. Đánh cắp thông tin tài khoản mạng xã hội hoặc thông tin bảo mật ngân hàng để phục vụ mục đích chiếm đoạt tài sản

- **Thủ đoạn:** Mạo danh là cán bộ ngân hàng yêu cầu nạn nhân cung cấp thông tin tài khoản, thẻ ngân hàng, ví điện tử, mã PIN, OTP để xử lý sự cố liên quan đến các dịch vụ ngân hàng; xác minh nguồn tiền lớn đang chuyển cho nạn nhân…

- **Thủ đoạn:** Mạo danh nhân viên các công ty có uy tín (hoặc người quen) thông báo trúng thưởng (hoặc nhờ gửi nhận tiền) rồi gửi mail/tin nhắn chứa link truy cập vào website giả mạo có thiết kế giống với trang chủ của ngân hàng, yêu cầu nạn nhân nhập thông tin tài khoản, thẻ ngân hàng, ví điện tử, mật khẩu, mã OTP. Sau đó, đối tượng sử dụng các thông tin trên để đăng nhập vào tài khoản của nạn nhân và thực hiện lệnh chuyển tiền, rút tiền khỏi tài khoản.

- **Thủ đoạn:** Đăng tải các đường link có tính chất gây sốc, tò mò, thu hút sự chú ý của người xem (liên kết đến các trang website) có chứa mã độc, khi đến các trang web đó sẽ yêu cầu đăng nhập tài khoản mạng xã hội (Facebook, Zalo…), cung cấp thông tin người dùng, tài khoản ngân hàng, ví điện tử… Qua đó các tin tặc sẽ khai thác thông tin trên, đánh cắp và chiếm quyền sử dụng các

trên để phục vụ mục đích xấu như bán thông tin người dùng, nhắn tin cho bạn bè, người thân vay mượn tiền, nhờ mua thẻ điện thoại…

Cách nhận biết, phòng ngừa: Theo quy định, các ngân hàng không yêu cầu khách hàng cung cấp thông tin tài khoản, thẻ ngân hàng, ví điện tử, mã OTP hoặc bất kỳ thông tin cá nhân của khách hàng qua mail/tin nhắn hay gọi điện thoại; không tò mò nhấn vào các đường link lạ, tuyệt đối không cung cấp các thông tin tài khoản ngân hàng cho bất kỳ cá nhân, tổ chức nào thông qua các cuộc gọi, đường link gửi bằng mail/tin nhắn. Nếu người thân, bạn bè nhắn tin vay mượn tiền qua các mạng xã hội thì gọi điện thoại trực tiếp cho người đó để xác minh thông tin chính xác trước khi chuyển tiền.

3. Huy động vốn với lãi suất cao

Thủ đoạn: Giả là công ty, tập đoàn lớn trên thế giới, quảng cáo đang thực hiện các dự án, lôi kéo nhiều người tham gia đầu tư, huy động vốn với lãi suất cao. Người tham gia phải cài đặt ứng dụng do công ty này tạo ra và chuyển tiền vào tài khoản của công ty để mua một hoặc nhiều gói đầu tư; khi truy cập vào ứng dụng sẽ thấy lợi nhuận tăng dần theo kỳ hạn gửi. Ban đầu, "công ty" có thể quy đổi tài khoản thành tiền để trả cho một số người; tuy nhiên, sau một thời gian huy động được số tiền lớn, các đối tượng tuyên bố phá sản, giải thể và đánh sập ứng dụng chiếm đoạt tiền. Nạn nhân không đòi được quyền lợi vì đây chỉ là các công ty, tập đoàn giả không được công nhận hoạt động tại Việt Nam.

Thực chất của thủ đoạn lừa đảo này là vay tiền của người sau trả cho người trước, lôi kéo được càng nhiều người thì được càng nhiều "hoa hồng"... Do đó, người tham gia trước sẽ trở thành "kẻ môi giới" thực hiện các hành vi "mồi chài", lôi kéo những người thân, quen cùng tham gia.

Cách nhận biết, phòng ngừa: Nâng cao cảnh giác với những thủ đoạn huy động vốn và cho hưởng lãi suất cao; tìm hiểu thật kỹ về thông tin các dự án, các đơn vị, công ty muốn đầu tư và chỉ nên đầu tư vào các công ty đã được cấp phép hoạt động, Khi nghi ngờ một trường hợp nào đó, người dân chỉ cần sử dụng Google để tìm kiếm các thông tin liên quan đến giấy phép kinh doanh tại Việt Nam, nếu không được cấp phép hoạt động thì có nguy cơ cao là lừa đảo.

Đề nghị thủ trưởng các sở, ban, ngành, đoàn thể tỉnh và UBND các huyện, thành phố thông báo, khuyến cáo, tuyên truyền sâu rộng đến cán bộ, công chức, viên chức, người dân và doanh nghiệp cảnh giác trước các thủ đoạn trên. Nếu nghi vấn hoặc phát hiện cá nhân, tổ chức nào có dấu hiệu hoạt động lừa đảo cần

báo ngay cho cơ quan Công an gần nhất hoặc số điện thoại Trực ban Hình sự Công an tỉnh (**069.2549.020**) để được tư vấn, giải quyết theo quy định.

Ban Chỉ đạo 138 tỉnh thông báo đến các đơn vị, địa phương biết, thực hiện./.

Nơi nhận:
Gửi bản điện tử
- TT Tỉnh ủy, HĐND tỉnh | *(báo cáo)*;
- Đ/c Chủ tịch UBND tỉnh |
- Các sở, ban, ngành, đoàn thể tỉnh | *(biết, t/hiện);*
- UBND các huyện, thành phố |
- Công an các đơn vị, địa phương
- Lưu: PV01*(Đ3)*.

KT. TRƯỞNG BAN
PHÓ TRƯỞNG BAN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CÔNG AN TỈNH BẮC KẠN

PHÓ GIÁM ĐỐC CÔNG AN TỈNH
Đại tá Hà Trọng Trung