ỦY BAN NHÂN DÂN HUYỆN BẠCH THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 2761 /UBND-CA V/v tăng cường công tác phòng, chống tội phạm lừa đảo chiếm đoạt tài sản qua mạng internet, mạng viễn thông trên địa bàn huyện.	*Bạch Thông, ngày 21 tháng 12 năm 2021*

Kính gửi:

- Các phòng, ban thuộc UBND huyện;
- UBMTTQ Việt Nam và các Đoàn thể huyện;
- Các cơ quan, đơn vị trên địa bàn huyện;
- Các đơn vị sự nghiệp thuộc huyện;
- UBND các xã, thị trấn.

Trong thời gian vừa qua tình hình tội phạm lừa đảo chiếm đoạt tài sản nhất là lừa đảo chiếm đoạt tài sản qua mạng internet, mạng viễn thông tiếp tục diễn biến ngày càng phức tạp, gây ảnh hưởng xấu tới tình hình an ninh trật tự trên địa bàn. Mặc dù các phương thức, thủ đoạn hoạt động của đối tượng không mới, đã được Cơ quan công an tuyên truyền nhiều trên các phương tiện thông tin đại chúng và trên các trang mạng xã hội. Nhưng thời gian gần đây vẫn còn tình trạng người dân, thậm chí có cả cán bộ, công chức, viên chức bị các đối tượng lừa đảo chiếm đoạt tài sản. Nhằm nâng cao nhận thức và ý thức cảnh giác của nhân dân trước tội phạm lừa đảo chiếm đoạt tài sản trong thời gian tới, UBND huyện Bạch Thông thông báo một số phương thức, thủ đoạn tội phạm lừa đảo chiếm đoạt tài sản như sau:

I. THỦ ĐOẠN

1. Chiếm tài khoản Facebook, Zalo… để lừa đảo chiếm đoạt tài sản

Đối tượng sử dụng mạng internet thực hiện hành vi lừa đảo chiếm đoạt tài sản bằng hình thức chiếm quyền quản trị, sử dụng tài khoản (hack) Facebook của chủ tài khoản, sau đó tìm hiểu nắm lịch sử trò chuyện, giả danh chủ tài khoản nhắn tin tới người thân, quen của họ để trao đổi các nội dung: Hỏi vay tiền hoặc nhờ mua thẻ cào điện thoại, gửi mã thẻ nạp và số seri để bán cho những người chơi game sẽ được hưởng tiền lời; Ngỏ ý nhờ mượn tiền để chuyển khoản đến một tài khoản Ngân hàng nào đó nhằm thanh toán một giao dịch, hoặc nhờ chuyển khoản cho một người khác.

2. Chiếm tài khoản đăng nhập vào dịch vụ ngân hàng trực tuyến

Lợi dụng nạn nhân sử dụng các trang mạng xã hội, mạng internet để mua bán hàng trực tuyến để lừa đảo. Cụ thể: Đối tượng đặt mua hàng trên mạng xã hội (ví dụ: Facebook, Zalo...) mà nạn nhân sử dụng, sau đó nhắn tin đến số điện thoại của nạn nhân thông báo mua hàng và chuyển tiền vào tài khoản ngân hàng kèm theo địa chỉ trang web, yêu cầu nạn nhân truy cập và làm theo hướng dẫn để nhận tiền hàng. Sau khi nạn nhân truy cập vào trang web gửi kèm trong tin nhắn sẽ được hướng dẫn nhập các thông tin gồm: Tài khoản ngân hàng nhận tiền, nhập số

tài khoản, mật khẩu giao dịch online, mã OTP (mã truy cập sử dụng một lần) thì lúc này đối tượng đã có đầy đủ thông tin để truy cập vào tài khoản ngân hàng mà nạn nhân sử dụng qua ứng dụng giao dịch trực tuyến (Smart Banking, Internet Banking, eBanking… tùy tên gọi từng ngân hàng) để chuyển tiền có trong tài khoản của nạn nhân đến tài khoản khác.

Ngoài ra, đối tượng cũng sử dụng phương thức, thủ đoạn trên yêu cầu nạn nhân truy cập trang web giả mạo gửi kèm trong tin nhắn hướng dẫn đăng nhập tài khoản, mật khẩu truy cập, Gmail và các thông tin liên quan đến tài khoản mạng xã hội mà nạn nhân sử dụng để mua bán hàng qua mạng thì sẽ bị đối tượng chiếm quyền quản trị, sử dụng tài khoản(hack) sau đó dùng tài khoản này để lừa đảo chiếm đoạt tài sản hoặc yêu cầu nạn nhân trả một số tiền chuộc để sử dụng lại tài khoản.

Các đối tượng cũng giả danh là 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 của bị hại.

3. Làm quen để chiếm đoạt tài sản

Đối tượng gây án là người nước ngoài hoặc giả danh là người nước ngoài sử dụng mạng xã hội Facebook để làm quen với các nạn nhân mà chủ yếu là phụ nữ nhẹ dạ cả tin. Sau một thời gian trò chuyện, tiếp xúc, thậm chí là gọi điện hình ảnh để lấy lòng tin thì đối tượng đề nghị tặng cho nạn nhân những đồ vật có giá trị như tiền, trang sức, điện thoại di động qua chuyển phát nhanh từ nước ngoài về Việt Nam. Sau đó, chúng cấu kết với đối tượng người Việt Nam giả danh nhân viên hải quan, cơ quan thuế, sân bay hoặc công ty chuyển phát nhanh gọi điện cho bị hại thông báo lô hàng chuyển từ nước ngoài về có giá trị lớn và đang bị tạm giữ. Nếu muốn nhận hàng, nạn nhân phải nộp các khoản tiền chuyển phát nhanh, tiền thuế, tiền bảo đảm,... vào các tài khoản do các đối tượng cung cấp.

4. Giả danh công an, cán bộ nhà nước để chiếm đoạt tài sản

Đối tượng gây án giả danh cán bộ Công an, Viện Kiểm sát lừa đảo chiếm đoạt tài sản với thủ đoạn sử dụng giao thức kết nối Internet (VoIP) để giả mạo các đầu số, giống số điện thoại của cơ quan Công an như: +000113, +84000113, +00130000,… gọi đến số máy bàn cố định của bị hại xưng là cán bộ Công an, Viện Kiểm sát đang điều tra vụ án đặc biệt nghiêm trọng, bị hại sử dụng chứng minh nhân dân đăng ký mở tài khoản ngân hàng, tài khoản đó có liên quan đến vụ án mà cơ quan Công an đang điều tra. Để chứng minh bị hại trong sạch, đối tượng yêu cầu bị hại khai báo tài sản với lý do phục vụ cho công tác điều tra, đồng thời yêu cầu bị hại chuyển tiền vào tài khoản ngân hàng do đối tượng lập, khi nào điều tra xác minh nếu không có liên quan đến tội phạm thì trả lại tiền, nếu bị hại không hợp tác sẽ bị bắt để điều tra. Sau khi bị hại chuyển tiền vào tài khoản được chỉ

định, chúng nhanh chóng chuyển tiền qua các tài khoản khác hoặc rút tiền mặt ngay tại các cây ATM hoặc chi nhánh ngân hàng khác.

5. Thông báo trúng thưởng, nhắn tin mời cho vay tiền để chiếm đoạt tài sản

a) Các đối tượng nhắn tin qua Facebook, Zalo, tin nhắn điện thoại thông báo "Bạn đã trúng thưởng chương trình…." Để nhận được tiền thưởng hoặc quà tặng, đối tượng yêu cầu người nhận tiền chuyển khoản vào số tài khoản do đối tượng đưa ra, gồm tiền thuế, tiền chi phí vận chuyển quà tặng, tiền để mua vé máy bay cho những người đến trao thưởng… khi nạn nhân chuyển tiền thì bị các đối tượng chiếm đoạt và không còn liên lạc được.

b) Đối tượng lập tài khoản Facebook, Zalo giả mạo rồi đăng thông tin cho vay ngân hàng với lãi suất ưu đãi, giải ngân nhanh. Khi nạn nhân đồng ý vay tiền, đối tượng yêu cầu họ chuyển trước một số tiền để được giải ngân nhanh hoặc ứng trước cho ngân hàng để ngân hàng giải ngân. Khi nạn nhân chuyển tiền thì các đối tượng chiếm đoạt tiền và không còn liên lạc được.

6. Lừa bán hàng hóa hoặc bán hàng nhận hoa hồng để chiếm đoạt tài sản

Với thủ đoạn này, thường có từ một đến hai đối tượng đến các cửa hàng tạp hóa để chào bán một số mặt hàng nhất định và để lại một số mặt hàng mẫu để trưng bày. Sau đó có đối tượng khác đến đặt mua số lượng lớn những mặt hàng hóa mà các đối tượng ban đầu đã chào bán hàng và đặt cọc số lượng tiền nhất định để làm tin. Lúc này chủ cửa hàng sẽ liên hệ với đối tượng đã chào bán hàng để đặt mua các mặt hàng với số lượng mà đối tượng đặt cọc và trả tiền cho đối tượng bán hàng. Khi nhận được hàng, chủ cửa hàng liên hệ đối tượng đặt cọc đến lấy thì đối tượng lấy lý do chưa đến lấy ngay được, rồi sau đó đối tượng tắt điện thoại, không liên lạc được, không xác định được đối tượng ở đâu. Thực tế đối tượng chào hàng và mua hàng đều cùng một nhóm thực hiện hành vi lừa đảo chiếm đoạt tiền của nạn nhân.

7. Giả danh nhân viên công ty tài chính để gọi điện, nhắn tin đòi nợ

Đây là thủ đoạn mới xuất hiện trong thời gian gần đây: Đối tượng giả danh là nhân viên công ty tài chính nào đó như Công ty tài chính Home credit hoặc các app vay tiền trên điện thoại… gọi điện, nhắn tin đến một số thuê bao nhất định với lý do người này vay tiền của công ty hoặc vay app qua điện thoại đã quá hạn lâu nhưng không trả. Đối tượng yêu cầu người vay phải trả tiền cho chúng dưới hình thức chuyển khoản, nếu chủ thuê bao chưa có tiền trả hoặc chưa trả thì các đối tượng truy cập vào danh bạ, Zalo, Facebook của nạn nhân hoặc sử dụng nhiều số điện thoại nhắn tin, gọi đe đọa yêu cầu trả tiền hoặc gọi điện vào các số trong danh bạ của người này để yêu cầu trả tiền…, thực tế thì chủ thuê và người thân của người này không có ai vay tiền của các đối tượng dưới mọi hình thức.

8. Quảng cáo giới thiệu việc làm tại nhà thông qua mạng xã hội để nhận lợi nhuận cao

Thời gian gần đây xuất hiện tình trạng quảng cáo giới việc làm của trang Công ty "TTC Group" trên mạng xã hội Facebook, người tham gia chơi sẽ được bộ phận chăm sóc khách hàng (CSKH) hướng dẫn đăng ký tài khoản để trở thành

hội viên nhóm. Khi đã thành hội viên nhóm sẽ có một người giới thiệu là lễ tân nhắn tin hướng dẫn từng bước để đăng ký, kích hoạt tài khoản, các bước làm "nhiệm vụ" để được nhận hoa hồng (lợi nhuận suất). Lúc này người tham gia chơi sẽ được bộ phận CSKH hướng dẫn nạp tiền, làm những đơn hàng với mức vốn khoảng từ hơn 100.000đ đến 200.000đ sẽ có lợi nhuận khoảng 70.000đ, mỗi lần nạp sẽ có một số tài khoản ngân hàng khác nhau để người tham gia chơi nạp tiền thông qua App Mobile Bankinh để chuyển và nhận tiền. Sau khi chuyển tiền xong thì bị hại phải chụp lại hóa đơn và báo lại cho bộ phận CSKH để kiểm tra, xác nhận và được hướng dẫn tiếp tục tải App TTC Group và kết bạn với lễ tân để nhận nhiệm vụ đơn sẽ làm, ngoài ra sẽ có thêm người khác đọc lệnh đơn hàng và xác nhận các bước... Nhiệm vụ của người chơi là rà soát đơn hàng được cụ thể hóa bằng các con số do công ty gửi đến và bù các con số vào đơn hàng còn thiếu… Khi bị hại đã hoàn thành 1 đến 2 đơn hàng và nhận được lợi nhận thì các đối tượng yêu cầu bị hại nạp tiền nhiều hơn như từ 1 triệu đồng đến 2 triệu đồng để làm nhiệm vụ sẽ có lợi nhuận cao hơn. Khi bị hại đã chuyển tiền thì các đối tượng đưa ra lý do nhiệm vụ đã hết cần bổ sung thêm tiền để nhận nhiệm vụ mới và sẽ được rút hết tiền gốc, lợi nhuận. Khi bị hại nạp thêm tiền thì đối tượng hẹn bị hại chuyển sang nhóm khác để được nhận nhiệm vụ với gói tiền từ 40 triệu đồng đến 50 triệu đồng và yêu cầu bị hại chuyển tiền tương ứng sẽ nhận được lợi nhuận lên đến 20 triệu đồng, khi bị hại đã chuyển tiền theo yêu cầu thì đối tượng tiếp tục yêu cầu nạp thêm tiền mới nhận được nhiệm vụ và tiền lợi nhuận…Nếu bị hại không nạp tiền theo yêu cầu của đối tượng thì tài khoản bị khóa và mất hết toàn bộ số tiền đã chuyển cho các đối tượng.

II. CÁCH PHÒNG TRÁNH

- Nâng cao khả năng bảo mật của các tài khoản cá nhân Google, Facebook, Zalo… bằng cách thêm số điện thoại để bật xác thực 2 bước, để dễ dàng khôi phục lại tài khoản khi bị mất mật khẩu. Cảnh báo được khi bị đối tượng chiếm quyền truy cập, sử dụng tài khoản mạng xã hội.

- Tăng cường bảo mật, bảo vệ thông tin cá nhân, chống bị đánh cắp thông tin tài khoản bằng cách cài các phần mềm diệt virut cho máy tính, điện thoại. Thường xuyên cập nhật phiên bản mới nhất của hệ điều hành máy tính, điện thoại để tăng cường bảo mật.

- Nâng cao ý thức cảnh giác trước các thủ đoạn của bọn tội phạm, chú ý phân biệt các trang web giả mạo, lấy địa chỉ gần giống trang web uy tín để người dùng nhập tài khoản vào và đánh cắp, ví dụ các trang có dạng: faceboook.com (giả mạo trang facebook.com), googlle.com (giả mạo google.com)… đọc kỹ địa chỉ trang web khi trang web yêu cầu nhập thông tin tài khoản để đảm bảo thông tin không bị đánh cắp.

- Liên lạc với người nhận tiền bằng điện thoại để xác minh trước khi thực hiện yêu cầu chuyển tiền, chuyển thẻ điện thoại của người khác.

- Cảnh giác trước các tin nhắn trúng thưởng, nhận quà tặng mà phải nộp trước thuế, phí; các giao dịch mua bán trên mạng chỉ nên thực hiện giao dịch với

các địa chỉ bán hàng uy tín. Cảnh giác với các thủ đoạn quảng cáo làm việc online trên các trang mạng xã hội để nhận tiền hoa hồng.

- Cảnh giác trước các cuộc gọi, tin nhắn mà đối tượng yêu cầu bạn giữ bí mật, không cho người thân biết khi nhận giải thưởng, thực hiện chuyển tiền… và các thủ đoạn, hành vi chào bán hàng của đối tượng.

- Các cuộc gọi tự nhận là cán bộ Công an, Viện kiểm sát, Tòa án… có thông tin liên quan pháp luật yêu cầu chuyển tiền cần xác nhận với cơ quan Công an địa phương nơi gần nhất để xác thực. Không thực hiện các yêu cầu qua điện thoại.

Đề nghị các Phòng, ban, ngành, đoàn thể và UBND các xã, thị trấn 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 huyện Bạch Thông (02093.850.585) để được tư vấn, giải quyết.

UBND huyện thông báo đến các đơn vị, địa phương biết, thực hiện./.

Nơi nhận:
- Như trên (th/hiện);
-CT, PCT UBND huyên;
- TTVHTT truyền thông huyện;
- Lưu VT, THNC.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Đinh Quang Hưng