BỘ CÔNG AN
CÔNG AN TỈNH TUYÊN QUANG

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

Số: 1998 /CAT-ANMCNC
V/v cảnh báo một số phương thức, thủ đoạn "Lừa đảo chiếm đoạt tài sản" trên không gian mạng

Tuyên Quang, ngày 25 tháng 5 năm 2022

Gửi VP đăng tin trước truyền. Nghiêm

Kính gửi:
- Giám đốc các Sở, ban ngành tỉnh Tuyên Quang;
- Chủ tịch UBND các huyện, thành phố;
- Các tổ chức chính trị xã hội tỉnh Tuyên Quang;
- Đài Phát thanh và Truyền hình tỉnh, Báo Tuyên Quang.

Thời gian qua, các cơ quan chức năng đã tăng cường tuyên truyền, thông báo về tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông đến cán bộ, công chức, viên chức, người lao động và nhân dân biết, phòng ngừa. Tuy nhiên, lợi dụng sự phát triển của công nghệ thông tin, mạng interrnet mà đặc biệt là mạng xã hội; một số bất cập trong quản lý nhà nước liên quan đến lĩnh vực ngân hàng, viễn thông, tài chính; lợi dụng đời sống khó khăn khi dịch covid 19 bùng phát, diễn ra trên diện rộng; tâm lý cả tin, hám lợi của một số người dân nên tội phạm trên diễn ra nhiều hơn, với phương thức, thủ đoạn tinh vi hơn. Từ năm 2019 đến tháng 4/2022, Công an tỉnh Tuyên Quang đã tiếp nhận, xử lý 58 vụ, 72 đối tượng vi phạm pháp luật, gây thiệt hại 10.051.800.000 đồng (Mười tỉ không trăm năm mươi mốt triệu tám trăm nghìn đồng). Để làm tốt công tác phòng ngừa tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông, Công an tỉnh thông báo một số phương thức, thủ đoạn phổ biến để các đơn vị thông báo, phổ biến, tuyên truyền sâu rộng đến cán bộ, công chức, viên chức, người lao động và quần chúng nhân dân cảnh giác, cụ thể:

1. Một số phương thức, thủ đoạn của tội phạm "lừa đảo chiếm đoạt tài sản" trên không gian mạng

- Đầu tư qua các sàn giao dịch tiền ảo, sàn ngoại hối trá hình hoặc đầu tư đào tiền kỹ thuật số theo mô hình kinh doanh "đa cấp"

Loại tội phạm này đã lợi dụng sự thiếu hiểu biết của nhiều người, đánh vào lòng tham và sự cả tin của nhiều cá nhân, biến họ trở thành những nhà đầu tư đa cấp hoặc thành viên của sàn giao dịch tiền ảo mà thực chất là những sòng bạc được điều khiển bởi chính những người sáng lập hệ thống. Các đối tượng lập ra các website đầu tư tài chính, các ứng dụng có giao diện tương tự đầu tư tài chính quốc tế rồi sử dụng nhiều thủ đoạn khác nhau để thu hút, lôi kéo nhiều người tham gia như: Gọi điện thoại tư vấn, gửi tin nhắn, đăng tin quảng bá, mời chào qua các mạng xã hội (Zalo, Facebook...), tổ chức các buổi hội thảo có quy mô lớn, đưa những người tự xưng là chuyên gia về lĩnh vực tài chính đến chia sẻ kinh nghiệm…

Các sàn đều được quảng cáo có nguồn gốc từ nước ngoài, liên kết với nền tảng giao dịch điện tử hàng đầu thế giới, cam kết người chơi sẽ được hưởng mức lãi suất cao, có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian. Để tạo lòng tin, lúc đầu nhà đầu tư rút được lãi nên tin tưởng chuyển tiền tham gia đầu tư lớn hơn, sau đó chúng đánh sập sàn, cắt mọi hình thức liên lạc và chiếm đoạt tài sản.

- Thủ đoạn giả danh người có chức vụ, quyền hạn để lừa đảo, nhất là giả danh cán bộ công an, viện kiểm sát, toà án.....

Mặc dù đã được cơ các cơ quan chức năng cảnh báo, tuyên truyền rộng rãi nhưng vẫn có nhiều bị hại tin tưởng, chuyển tiền cho các đối tượng lừa đảo. Thủ đoạn hoạt động của tội phạm này chủ yếu sử dụng các đầu số điện thoại, không phải là đầu số điện thoại của Việt Nam (+84) gọi điện trực tiếp cho nạn nhân, sau đó, các đối tượng sử dụng nhiều kịch bản khác nhau: Giả làm nạn nhân bưu điện gọi điện thông báo nhận bưu phẩm; nhân viên viễn thông gọi điện thông báo nợ cước; nhân viên điện lực gọi thông báo nợ cước, doạ cắt điện; cảnh sát giao thông gọi điện thông báo phạt nguội, gây tai nạn bỏ trốn; vi phạm phòng, chống dịch bệnh Covid-19…. Chúng liên hệ với nạn nhân để khai thác thông tin cá nhân, sau đó, sử dụng các thông tin đó làm giả các lệnh bắt, khởi tố của cơ quan Công an để đe doạ nạn nhân (thường thông báo nạn nhân liên quan đến các đường dây buôn bán ma tuý xuyên quốc gia, rửa tiền), yêu cầu nạn nhân chuyển tiền vào tài khoản do chúng cung cấp để phục vụ công tác điều tra, sau đó chiếm đoạt hoặc yêu cầu nạn nhân tự đăng ký một tài khoản ngân hàng, chuyển tiền vào tài khoản đó, sau đó cung cấp tài khoản, mật khẩu, mã OTP cho các đối tượng, rồi chúng rút tiền trong tài khoản để chiếm đoạt. Quá trình nói chuyện với nạn nhân, các đối tượng thường yêu cầu nạn nhân giữ máy liên tục, tìm nơi riêng tư để nói chuyện và yêu cầu nạn nhân dân không được tiết lộ thông tin này cho bất kỳ ai.

- Thủ đoạn tuyển tuyển "Cộng tác viên online" để lừa đảo chiếm đoạt tài sản

Hình thức lừa đảo bằng việc tuyển "Cộng tác viên online" đã xuất hiện từ lâu, tuy nhiên, thời gian gần đây các đối tượng đã lợi dụng hình thức thuê người đặt hàng ảo để tăng lượng đơn hàng, nhận đánh giá tốt trên các sàn thương mại điện tử như Shopee, Lazada, Tiki, Sendo…. Các đối tượng đã sử dụng "mồi nhử" hấp dẫn như: Mua hàng trực tiếp nhưng không nhận hàng (những kẻ lừa đảo gọi là làm tăng tỉ lệ tương tác mua hàng đối với sản phẩm), việc mua hàng sẽ được thực hiện chuyển khoản qua tài khoản ngân hàng do đối tượng cung cấp. Mỗi lượt mua hàng thành công sẽ được hưởng hoa hồng từ 10 – 20% số tiền gốc của mỗi đơn hàng, tiền sẽ chuyển khoảng 5 – 10 phút khi đặt hàng thành công (bao gồm cả tiền gốc và hoa hồng). Ban đầu, để tạo lòng tin và kích thích lòng tham của nạn nhân, các đối tượng sẽ cung cấp đường link trên hệ thống Shopee, Lazada, Tiki…. Của một sản phẩm khoảng một triệu đến hai triệu đồng và tài khoản Ngân hàng cá nhân do đối tượng cung cấp để nạn nhân chuyển khoản với số tiền tương ứng với giá trị trên hệ thống. Ngay sau đó các đối tượng sẽ chuyển khoản ngược lại cho nạn nhân như đã thoả thuận. Khi nạn nhân đã cắn câu

chuyển số tiền đến vài chục triệu thì các đối tượng không chuyển khoản ngược lại nữa và đưa ra nhiều lý do khác nhau để nạn nhân tiếp tục "say mồi" như: Nhiệm vụ hoàn thành được 95/100 điểm tín nhiệm, cần tiếp tục chuyển tiền để hoàn thành 100 điểm,…. khiến nhiều người tin tưởng tiếp tục chuyển tiền và bị lừa số tiền đến vài trăm triệu đồng.

- Thủ đoạn lừa đảo cho vay nhanh với lãi suất thấp qua Zalo, điện thoại, app

+ Lừa đảo vay tiền qua Zalo

Zalo là một mạng xã hội được rất nhiều người dùng tin tưởng sử dụng. Lợi dụng điểm này những đối tượng lừa đảo sẽ mạo danh thành các công ty tài chính có uy tín để lừa gạt khách hàng và chiếm đoạt tài sản.

Những đối tượng này sẽ mạo danh là những công ty TNHH dịch vụ vay tiền hoặc công ty thương mại Việt Nam,… sau đó sẽ gửi các tin nhắn tới từng tài khoản của khách hàng qua Zalo để mời mọc vay vốn với lãi suất thấp. Sẽ không yêu cầu giấy tờ tùy thân nhưng vẫn vay được 10 đến 70 triệu mà lãi suất chỉ 0,5%/tháng. Khách hàng chỉ cần gửi giấy tờ tùy thân sau đó đóng phí bảo hiểm hoặc phí hồ sơ là sẽ vay được. Nhưng thực chất, khách hàng sẽ không nhận được bất cứ khoản tiền vay nào cả mà vẫn bị mất tiền phí đóng cho những đối tượng này. Hoặc khách hàng có thể nhận được tiền từ những đối tượng này, tuy nhiên số tiền nhận được sẽ thấp hơn nhiều so với số tiền đã đăng ký vay. Nhưng lãi suất vẫn bị tính trên số tiền đã đăng ký vay và với lãi suất cao hơn gấp nhiều lần so với ban đầu. Nếu như khách hàng có ý định không trả tiền lãi các đối tượng sẽ dùng thủ đoạn xã hội đen để dọa, đòi nợ một cách trắng trợn.

+ Lừa đảo vay tiền qua điện thoại

Lừa đảo cho vay tiền qua điện thoại cũng là một thủ đoạn phổ biến mà những kẻ mạo danh vẫn thường làm hiện nay. Chúng sẽ chạy quảng cáo trên Google, Faebook,… với nội dung cho vay tiền mà không cần thế chấp hoặc chứng minh thu nhập. Có thể nhận được tiền ngay trong ngày sau khi đăng ký.

Nếu như có ai đó sập bẫy thì chắc chắn sẽ nhận được yêu cầu đóng tiền bảo hiểm hoặc tiền cọc cho khoản vay. Thậm chí có những kẻ còn yêu cầu đóng tiền lãi trước khi vay vốn. Những kẻ này sẽ tạo ra những quy trình vay vốn như thật để cho khách hàng tin tưởng chúng. Sau khi đã nhận được tiền của người vay, thì chúng sẽ chặn hết mọi phương thức liên lạc.

+ Lừa đảo vay tiền online qua app

Vay tiền online qua app hiện nay nổi lên như một hình thức cho vay tiền mới. Khách hàng chỉ cần cài đặt ứng dụng trên điện thoại, sau đó đăng ký các khoản vay theo mong muốn của bản thân mà không phải làm thủ tục hoặc sử dụng bất kỳ loại giấy tờ nào. Nhưng bên cạnh những app vay tiền uy tín thì những app cho vay tiền tín dụng đen núp bóng app vay tiền nhanh cũng có rất nhiều. Họ sẽ cho vay tiền với các điều kiện đơn giản, nhưng sau đó sẽ thu lãi

suất với lãi suất cao hơn gấp nhiều lần với quy định của ngân hàng nhà nước. Thậm chí có những app thu lãi suất lên tới 1000%.

- Gửi link bình chọn, chiếm đoạt tài sản Facebook, nhắn tin vay tiền trong danh sách bạn bè

Các đối tượng thường sử dụng 02 phương thức để hack tài khoản Facebook của người dùng là hack Facebook bằng cách dò mật khẩu hoặc lập một trang web giả mạo, có giao diện giống hệt website chính thức của Facebook, rồi dẫn dụ người dùng đăng nhập tài khoản bằng website giả mạo này để đánh cắp thông tin mật khẩu...

Sau khi hack được một tài khoản Facebook, các đối tượng lừa đảo nghiên cứu kỹ thông tin cá nhân, sở thích, lịch sử trò chuyện với bạn bè của chủ Facebook bị hack và dựa trên các thông tin đó sẽ giả là chủ của tài khoản Facebook bị hack gửi tin nhắn trò chuyện với những người có quan hệ gia đình, làm ăn thân thiết với chủ Facebook, để thực hiện các hành vi lừa đảo phổ biến như vay tiền, nhờ mua đồ, mua thẻ điện thoại; nói mình mới mua nhà, bất động sản, xe hơi ở nước ngoài nên thiếu tiền và cần vay tiền gấp để đặt cọc...

Các tài khoản Facebook mà các đối tượng lựa chọn để hack thường là tài khoản của những người lớn tuổi, vì những người này thường đặt mật khẩu tài khoản một cách dễ nhớ, giản đơn. Hoặc các chủ tài khoản Facebook đang sinh sống tại nước ngoài, để khi bị lừa đảo vay tiền, nhờ mua đồ, mua thẻ điện thoại... các bị hại sẽ khó liên hệ ngay được với chủ Facebook để kiểm chứng thông tin.

2. Một số cách nhận biết, phòng ngừa

- Với thủ đoạn đầu tư qua các sàn giao dịch tiền ảo, sàn ngoại hối trá hình hoặc đầu tư đào tiền kỹ thuật số theo mô hình kinh doanh "đa cấp"

Các đối tượng gọi điện thoại tư vấn, gửi tin nhắn, đăng tin quảng bá, mời chào qua các mạng xã hội (Zalo, Facebook...), tổ chức các buổi hội thảo có quy mô lớn tại các địa điểm sang trọng, đưa những người tự xưng là chuyên gia về lĩnh vực tài chính đến chia sẻ kinh nghiệm, thổi phồng giá trị, cam kết lợi nhuận siêu khủng, đánh luôn thắng, không có rủi ro hoặc rủi ro thấp,... khiến nhiều người dân lầm tưởng là hoạt động hợp pháp và đồng ý chuyển tiền kinh doanh. Do vậy, người dân, nhà đầu tư trước khi bỏ vốn vào những lĩnh vực này nên tham khảo, tư vấn thêm từ cơ quan chức năng, các tổ chức tín dụng.

- Với thủ đoạn giả danh người có chức vụ, quyền hạn để lừa đảo

Theo quy định của pháp luật, khi làm việc với người dân thì các cơ quan Nhà nước (Công an, Viện kiểm sát, Toà án, Thuế, Hải quan...), các tổ chức, cá nhân đều có giấy mời, giấy giới thiệu hoặc trực tiếp gặp mặt để trao đổi công việc và không có quy định gọi điện yêu cầu chuyển tiền. Do đó, tất cả các cuộc gọi 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 cao là lừa đảo

chiếm đoạt tài sản. Bên cạnh đó, 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.

- Với thủ đoạn tuyển "Cộng tác viên online" để lừa đảo chiếm đoạt tài sản

Các bài tuyển cộng tác viên online thường xuyên xuất hiện nhiều trong quảng cáo trên các trang mạng xã hội như Facebook, Zalo… Các công ty, tổ chức và các sàn thương mại điện tử khi có nhu cầu tuyển dụng việc làm, tuyển cộng tác viên thì sẽ có thông báo rộng rãi trên các phương tiện thông tin đại chúng hoặc qua website của công ty, tổ chức đó. Do đó, các bài tuyển dụng việc làm nói chung và tuyển cộng tác viên online nói riêng có nguy cơ lừa đảo chiếm đoạt tài sản.

- Với thủ đoạn lừa đảo cho vay nhanh với lãi suất thấp

Các đối tượng nhắn tin, gọi điện mời chào cho vay tiền với lãi suất thấp và không cần điều kiện, thủ tục hoặc gặp mặt. Tất cả đều là những chiêu trò lừa đảo, khi thấy các lời chào này bạn hãy chặn ngay lập tức để không bị làm phiền nữa. Tuyệt đối không được tin tưởng những lời mời chào vay vốn từ những người lạ không rõ nguồn gốc. Không tham gia vào các hội nhóm vay tiền trên mạng để tránh bị dụ dỗ vay tiền. Đối với những khoản vay tại công ty tài chính hay ngân hàng uy tín họ sẽ không yêu cầu đóng phí hồ sơ. Nếu có nhu cầu vay tiền thì hãy đến công ty tài chính hay ngân hàng uy tín.

- Với thủ đoạn gửi link bình chọn, chiếm đoạt tài sản Facebook, nhắn tin vay tiền trong danh sách bạn bè

Để dẫn dụ người dùng Facebook thiếu cảnh giác đăng nhập vào các đường link giả mạo, các đối tượng thường dùng 3 thủ đoạn lừa đảo sau: (1) Gửi tin nhắn thông báo chủ các tài khoản Facebook bị báo chí xuyên tạc với nhiều nội dung khác nhau và yêu cầu kích vào đường link, đăng nhập tài khoản Facebook của mình để tiếp tục xem nội dung mà báo chí viết. (2) Gửi tin nhắn thông báo các chủ tài khoản đã có gia đình là có vợ, chồng đi ngoại tình và bị các đối tượng chụp ảnh, ghi hình lại; chủ tài khoản Facebook muốn lấy hình ảnh và biết cụ thể thì đăng nhập vào tài khoản Facebook để xem hình ảnh, video được tải lên Internet. (3) Gửi tin nhắn thông báo các chủ tài khoản là con, bạn bè thân thiết... đang tham dự một cuộc thi, hiện đã lọt Top 10 nên cần lượt chia sẻ để tăng like, lượt xem, bình chọn nên nhờ chủ tài khoản đăng nhập Facebook và làm theo hướng dẫn của website...Thực chất, các đường link này đều là đường link giả mạo được các đối tượng thiết kế tương tự website chính thức của Facebook để đánh cắp mật khẩu và tài khoản người dùng.

Mọi người dùng Facebook cần nâng cao cảnh giác trước thủ đoạn nhắn tin vay tiền, nhờ mua đồ, mua thẻ điện thoại trên Facebook... cần gọi điện thoại trực tiếp cho chủ tài khoản Facebook để xác minh thông tin và nội dung trao đổi. Chỉ đăng nhập tài khoản trên website chính thức của Facebook; tuyệt đối không đăng nhập vào các trang web nghi vấn hoặc yêu cầu đăng nhập tài khoản một

cách bất thường. Người dùng cần cài đặt mật khẩu Facebook có yếu tố bảo mật cao; hạn chế sử dụng các thông tin như họ tên, biệt danh, ngày tháng năm sinh để cài đặt mật khẩu; luôn cài đặt mã xác thực 2 yếu tố qua điện thoại hoặc hòm thư điện tử tin cậy; luôn cài đặt cảnh báo đăng nhập, để kịp thời phát hiện các đăng nhập từ thiết bị bất thường... Từ đó, không để các đối tượng lợi dụng lừa đảo chiếm đoạt tài sản của người dùng Facebook trong thời gian tới.

3. Để chủ động đấu tranh, phòng ngừa loại tội phạm này, Công an tỉnh khuyến nghị một số biện pháp như sau:

- Không 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;

- Không cung cấp mã OTP do ngân hàng cung cấp hay thực hiện xoá cài đặt xác thực Smart OTP cho bất kỳ ai;

- Thường xuyên kiểm tra và cập nhật các tính năng bảo mật, quyền riêng tư trên các tài khoản ngân hàng, tài khoản mạng xã hội; không cho mượn thuê các giấy tờ cá nhân liên quan, không nhận chuyển khoản ngân hàng hoặc nhận tiền chuyển khoản của các ngân hàng cho người không quen biết;

- Khi phát hiện sự việc có dấu hiệu vi phạm pháp luật xảy ra cần thông tin cho cơ quan Công an để phục vụ công tác xác minh, điều tra, làm rõ.

Trên đây là một số phương thức, thủ đoạn tội phạm "Lừa đảo chiếm đoạt tài sản" qua mạng Internet, mạng viễn thông, Công an tỉnh trân trọng thông báo để các đơn vị chủ động trong công tác phòng ngừa giúp cán bộ, công chức, viên chức, người lao động và quần chúng nhân dân nắm bắt thông tin, góp phần đảm bảo ANTT trên địa bàn tỉnh./.

Nơi nhận:
- Đ/c Giám đốc CAT (để báo cáo);
- Như trên (để phối hợp thực hiện);
- Lưu: VT, ANMCNC(Đ2).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Hà Phúc Thịnh