BỘ CÔNG AN
CÔNG AN TỈNH TRÀ VINH

Số: 80 /TB-CAT-PC02

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

Phòng tham mưu
Công an tỉnh Trà Vinh, Bộ Công an
01-09-2020 16:13:14 +07:00

Trà Vinh, ngày 01 tháng 9 năm 2020

THÔNG BÁO
Phương thức, thủ đoạn hoạt động của đối tượng sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản

Theo đánh giá của Bộ Công an, thời gian qua việc ứng dụng công nghệ thông tin, sử dụng các phần mềm chuyên dụng để làm việc, hội họp, học tập, kinh doanh, mua sắm, giao tiếp,... trực tuyến ở nước ta phát triển mạnh. Đặc biệt, trong bối cảnh dịch bệnh Covid - 19 diễn biến phức tạp, thực hiện chủ trương giãn cách xã hội để phòng, chống dịch của Chính phủ, hầu hết mọi hoạt động sinh hoạt của người dân đều được thực hiện qua không gian mạng. Lợi dụng tình hình trên, hoạt động lừa đảo qua không gian mạng ngày càng gia tăng, nhất là thủ đoạn đối tượng sử dụng mạng viễn thông, mạng xã hội để lừa đảo xảy ra phổ biến tại nhiều tỉnh, thành phố trong cả nước gây thiệt hại hàng trăm tỷ đồng[1], cá biệt có vụ các đối tượng lừa đảo hàng nghìn nạn nhân trên toàn quốc, chiếm đoạt trên 500 tỷ đồng[2], phổ biến nhất là mạo danh các cơ quan thực thi pháp luật như: Công an, Viện Kiểm sát, Tòa án,… gọi điện yêu cầu bị hại cung cấp thông tin hỗ trợ điều tra để đánh cắp thông tin tài khoản và chiếm đoạt tài sản.

Riêng trên địa bàn tỉnh Trà Vinh từ đầu năm 2019 đến nay, đã tiếp nhận tổng số 28 vụ có dấu hiệu của tội phạm sử dụng mạng viễn thông, mạng xã hội lừa đảo chiếm đoạt tài sản, tổng thiệt hại tài sản là 7,35 tỷ đồng, đáng chú ý địa bàn tỉnh đã xảy ra một số vụ lừa đảo trên không gian mạng với thiệt hại hàng tỷ đồng[3]. Qua công tác phòng, chống đối tượng sử dụng công nghệ cao lừa đảo qua mạng trên địa bàn nổi lên một số phương thức, thủ đoạn phổ biến như sau:

- Đối với các vụ lừa đảo qua mạng viễn thông: Đối tượng sử dụng phần mềm máy tính, sử dụng các cuộc gọi qua giao thức kết nối Internet (VoIP) hoặc thiết bị viễn thông khác giả lập số điện thoại cố định hoặc di động có đầu số **+990** (như +**990**692342593), **+84** (như +**84**795877525), **+010** (như +**010**692342593), điện vào

---

[1] Tại An Giang phát hiện 02 vụ với tổng số tiền các đối tượng chiếm đoạt của nạn nhân là gần 5 tỷ đồng; tại Quảng Ngãi phát hiện 03 vụ, với tổng số tiền chiếm đoạt trên 13 tỷ đồng; tại Bình Thuận phát hiện 01 vụ với tổng số tiền chiếm đoạt trên 2 tỷ đồng,...

[2] Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao phối hợp với Công an tỉnh Quảng Nam điều tra, bắt giữ 04 đối tượng người Malaysia, Campuchia và 06 đối tượng người Việt Nam dùng tổng đài giả danh số điện thoại của cơ quan Công an, Viện Kiểm sát đe dọa, lừa lấy thông tin của hơn 100.000 tài khoản ngân hàng, chiếm đoạt 1.690 tài khoản ngân hàng trực tuyến và trên 500 tỷ đồng.

[3] 02 vụ sử dụng mạng viễn thông để lừa đảo xảy ra khoảng tháng 01/2020, tại Khóm 4, Phường 1, TP. Trà Vinh và Khóm 4, thị trấn Trà Cú, huyện Trà Cú, với thủ đoạn giả danh cán bộ tư pháp đang thực thi nhiệm vụ như: Công an, Viện Kiểm sát, Tòa án các đối tượng đe dọa, uy hiếp tinh thần và 2 bị hại đã bị lừa với tổng số tiền trên 1,5 tỷ đồng; vụ sử dụng mạng xã hội lừa đảo tài sản xảy ra tháng 2/2020, chị **V. N. N,** sinh năm 1982, ngụ xã Phong Thạnh, huyện Cầu Kè, từ việc quen biết qua facebook với đối tượng tự xưng là quân nhân Mỹ đang làm việc tại Afghanistan, đang có số tiền lớn khoảng 1.500.000 USD và nhờ chị V. N. **N** cất giữ dùm, do tin lời nên chị V. N. N chuyển tiền đóng các khoản phí vận chuyển cho đối tượng tổng cộng là **10 lần**, với tiền bị lừa đảo **là 1.646.000.000đ** (một tỷ, sáu trăm bốn mươi sáu triệu đồng).

máy bàn, điện thoại di động của bị hại, sau đó các đối tượng tự nhận là nhân viên bưu điện, nhà mạng viễn thông hoặc cán bộ Công an, Viện kiểm sát, Tòa án,... thông báo rằng bị hại hoặc gia đình bị kiện vì nợ cước viễn thông, nợ tiền ngân hàng hoặc có liên quan đến các vụ án, chuyên án lớn (*ma túy, tội phạm rửa tiền, mua bán người xuyên quốc gia,...)* đang được điều tra, giải quyết, do đó cần phải chuyển khoản tiền lớn vào các tài khoản do các đối tượng cung cấp để xác minh, làm rõ. Đối tượng còn uy hiếp bằng cách gửi ảnh dự thảo *"Lệnh bắt tạm giam"* giả có tên của bị hại và đe dọa ***"nếu không chuyển tiền thì sẽ bị bắt tạm giam"*** để bị hại lo sợ mà chuyển tiền cho các đối tượng lừa đảo.

Đối tượng còn yêu cầu bị hại cung cấp thông tin hỗ trợ điều tra bằng cách đăng nhập các đường dẫn như: **http://136.244.70.67/static/104423/protect10.apk; http://78.141.192.168/static/106831/protect10.apk** tải xuống phần mềm có biểu tượng của Bộ Công an *(ứng dụng giả mạo do đối tượng tạo ra và cung cấp)* để bị hại điền vào đó các thông tin gồm: Họ và tên, số điện thoại, chứng minh nhân dân, địa chỉ, số tài khoản ngân hàng, tài khoản và mật khẩu Internet banking và cùng một số thông tin khác. Sau đó, đối tượng lấy thông tin này để đăng nhập vào tài khoản của bị hại, chuyển tiền đến các tài khoản khác của đối tượng và chiếm đoạt tài sản của bị hại. Thủ đoạn này đối tượng chiếm đoạt gần như toàn bộ số tiền có trong tài khoản của bị hại.

- Đối tượng sử dụng tài khoản facebook, zalo,... với *"hồ sơ cá nhân"* thu hút như: Là người nước ngoài (Mỹ, Anh) đang tham chiến ở chiến trường Syria, Afganistan,... để kết bạn với bị hại, nói với bị hại sẽ chuyển quà, tiền về Việt Nam nhờ bị hại nhận và giữ giùm. Để củng cố niềm tin, các đối tượng còn gửi ảnh bưu phẩm và các giấy tờ liên quan đến việc chuyển quà, tiền cho bị hại. Do có lòng tham trước sự hấp dẫn của số tiền lớn, nên nhiều bị hại đã đồng ý nhận và đóng các khoản phí vận chuyển để được số tiền lớn hơn, thông thường các đối tượng trong nhóm lừa đảo sẽ phối hợp theo một kịch bản chuẩn bị trước, liên kết với nhau chặt chẽ, thường là giả danh làm nhân viên Hải quan, Hàng không, Bưu điện,... để gọi điện, yêu cầu bị hại đóng liên tiếp nhiều khoản tiền phí hoặc tiền thuế qua một tài khoản mà chúng cung cấp để làm *"thủ tục"*. Cứ như vậy, cho đến khi bị hại không còn khả năng tài chính để nộp hoặc bị hại nghi ngờ thì nhóm đối tượng lừa đảo cắt liên lạc với bị hại.

- Giả danh nhân viên của các công ty, tạo ra các Website giả và sử dụng mạng xã hội (Facebook, Zalo) nhắn tin trúng thưởng, yêu cầu người dân phải nộp tiền đóng phí nhận quà.

- Đối tượng chiếm quyền điều khiển tài khoản mạng xã hội (Facebook) của người dùng (nhất là người đang sinh sống ở nước ngoài), sau đó nhắn tin (qua hệ thống Messenger) cho những người trong danh sách bạn bè của tài khoản đó (hiện sinh sống tại Việt Nam) để nhờ chuyển tiền dùm cho người thân (số tài khoản do đối tượng cung cấp) hoặc nhờ mua dùm một số thẻ cào điện thoại di động rồi nhắn tin mã số thẻ cào cho đối tượng nạp để chiếm đoạt tài sản.

- Giả mạo thư điện tử chỉ đạo, hướng dẫn công tác phòng, chống dịch của lãnh đạo Đảng, Nhà nước, các cơ quan chức năng như: Thủ tướng Chính phủ, Bộ Y tế,... có đính kèm file tài liệu gắn mã độc để lấy cắp thông tin cá nhân. Nội dung thư yêu cầu bị hại tải tệp tin đính kèm hoặc các liên kết trong thư điện tử để xem nội dung chi tiết. Khi bị hại mở

tệp tin, truy cập vào các liên kết hoặc tải ứng dụng theo đường link, virus mã độc sẽ ngay lập tức được tải tự động và cài đặt trên thiết bị cá nhân của bị hại và đánh cắp thông tin để thực hiện các giao dịch chiếm đoạt tài sản sau đó.

- Lừa đảo qua hoạt động trao đổi, mua bán qua mạng: Các đối tượng mở các trang cá nhân bán hàng online để rao bán các mặt hàng thiết yếu, đang khan hiếm như: Khẩu trang y tế, nước rửa tay y tế, đồ bảo hộ,... phục vụ phòng, chống dịch Covid - 19; yêu cầu người mua hàng chuyển tiền vào tài khoản trước để đặt cọc. Sau khi nhận được tiền đặt cọc hay tiền chuyển khoản trước để đặt mua hàng, đối tượng không giao hàng hoặc giao hàng giả, hàng kém chất lượng, sau đó khóa trang mạng của mình, bỏ số điện thoại liên lạc để xóa dấu vết và chiếm đoạt số tiền đã chuyển để mua hàng của bị hại.

- Các đối tượng cài mã độc lên các website quyên góp từ thiện liên quan đến dịch Covid - 19, khi người dân truy cập các website này sẽ bị nhiễm mã độc, bị lấy cắp thông tin cá nhân như số điện thoại, thông tin và mật khẩu các tài khoản thư điện tử, mạng xã hội, thông tin và mật khẩu tài khoản ngân hàng,.... Các đối tượng sẽ sử dụng những thông tin thu được để lừa đảo, chiếm đoạt tài sản của bị hại.

- Các đối tượng mạo danh các cơ quan chức năng phòng, chống dịch điện thoại lấy lý do hướng dẫn nạn nhân các biện pháp phòng, chống dịch bệnh, qua đó lừa nạn nhân cung cấp thông tin dịch vụ ngân hàng điện tử để đánh cắp thông tin và thực hiện giao dịch lấy cắp tiền trên tài khoản.

Thời gian qua, triển khai, thực hiện các biện pháp công tác phòng, chống đối tượng sử dụng công nghệ cao lừa đảo trên không gian mạng, Công an tỉnh đã hỗ trợ, phối hợp với Công an một số tỉnh trong cả nước làm rõ một số vụ án có liên quan đến bị hại trên địa bàn tỉnh[4]. Tuy nhiên, công tác phòng, chống tội phạm lừa đảo trên không gian mạng hiệu quả chưa cao, còn khó khăn, vướng mắc do một số nguyên nhân chủ yếu sau:

- *Về phía bị hại:* Ý thức cảnh giác phòng, chống tội phạm lợi dụng không gian mạng để lừa đảo của một bộ phận người dân trên địa bàn còn hạn chế; khi tiếp nhận các thông tin đe dọa của các đối tượng lừa đảo, bị hại thường có tâm lý hoang mang, lo sợ mất uy tín, danh dự cá nhân và gia đình nên một mình âm thầm giải quyết, làm theo yêu cầu chuyển tiền cho đối tượng; có bị hại đã bị lừa nhưng che giấu không trình báo hoặc trình báo chưa kịp thời, từ đó công tác nắm tình hình, thu thập thông tin, tài liệu đấu tranh với các loại đối tượng này gặp khó khăn.

- *Về phía đối tượng:* Sử dụng phương thức, thủ đoạn rất tinh vi, các đối tượng câu kết thành băng nhóm hoạt động phức tạp, liên tỉnh, thậm chí xuyên quốc gia, phần lớn các đối tượng sử dụng tài khoản giao dịch ngân hàng của người khác hoặc sử dụng giấy chứng minh nhân dân giả để đăng ký thông tin tài khoản ngân hàng nên rất khó xác minh, làm rõ; các nhóm đối tượng lừa đảo có sự chuẩn bị chu đáo, xây dựng

---

[4] Phối hợp Công an tỉnh Quảng Nam điều tra làm rõ 03 vụ đối tượng sử dụng mạng viễn thông giả danh nhân viên bưu điện, cán bộ Công an, Viện Kiểm sát, Tòa án để lừa đảo chiếm đoạt với tổng số tiền hơn 02 tỷ đồng; phối hợp Công an tỉnh Thừa Thiên Huế điều tra làm rõ 01 vụ đối tượng giả danh người nước ngoài, kết bạn qua mạng xã hội rồi lừa đảo chiếm đoạt số tiền hơn 1,6 tỷ đồng.

kịch bản rất chi tiết và luôn chuẩn bị phương án xóa bỏ dữ liệu vi phạm để che dấu hành vi phạm tội, đối phó với lực lượng chức năng.

- *Về phía lực lượng chức năng liên quan:* Công tác phối hợp tuyên truyền phòng, chống tội phạm lừa đảo qua mạng giữa các Sở, ban, ngành, đoàn thể và UBND các cấp còn hạn chế; lãnh đạo một số đơn vị, địa phương ít quan tâm quán triệt, phổ biến nên thời gian qua trên địa bàn vẫn thường xuyên xảy ra các vụ lừa đảo qua mạng, đặc biệt có trường hợp bị hại là lãnh đạo, công chức, viên chức đang công tác trong các cơ quan Đảng, Nhà nước trên địa bàn.

Thời gian tới, Công an tỉnh nhận định các đối tượng lừa đảo trên không gian mạng tiếp tục lợi dụng diễn biến phức tạp trở lại của dịch bệnh Covid - 19 để thực hiện phạm tội và vi phạm pháp luật, nhiều khả năng hoạt động sử dụng mạng xã hội để bán hàng online, việc giao dịch, mua bán các trang thiết bị y tế (khẩu trang, dung dịch sát khuẩn) để phòng, chống dịch bệnh sẽ tiếp tục gia tăng; tình trạng công ty, doanh nghiệp gặp khó khăn trong sản xuất tạm ngưng hoạt động cắt giảm công nhân, người dân không có việc làm, thu nhập không ổn định nên việc kinh doanh, trao đổi mua bán trên không gian mạng kiếm thêm thu nhập sẽ tăng cao, đây là những điều kiện thuận lợi để đối tượng sử dụng mạng xã hội tăng cường hoạt động; thời gian diễn ra Đại hội Đảng bộ lần thứ XI của tỉnh Trà Vinh và Đại hội Đảng bộ toàn quốc lần thứ XIII có nhiều khả năng các đối tượng lừa đảo sẽ tăng cường các hoạt động sử dụng mạng viễn thông để nhắm đến những lãnh đạo đang trong diện quy hoạch, đề cử để gọi điện nhằm thực hiện mục đích lừa đảo như các phương thức, thủ đoạn đã nêu trên.

Thực hiện quy chế, kế hoạch phối hợp với các Sở, ban, ngành, đoàn thể tỉnh trong công tác đảm bảo ANTT trên địa bàn tỉnh, nhất là để phòng, chống hiệu quả đối tượng sử dụng công nghệ cao để lừa đảo qua mạng, Công an tỉnh đề nghị:

(1) Lãnh đạo các Sở, ban, ngành, đoàn thể tỉnh và UBND cấp huyện quan tâm quán triệt, phổ biến các phương thức, thủ đoạn hoạt động nêu trên cho cán bộ, công chức, người lao động nắm, phòng ngừa; theo lĩnh vực, địa bàn phụ trách phối hợp lồng ghép tuyên truyền sâu rộng các thủ đoạn của đối tượng lừa đảo qua mạng cho nhân dân trên địa bàn nắm, cảnh giác đấu tranh, trong đó cần lưu ý tuyên truyền:

- Khi sử dụng internet để tham gia mạng xã hội (facebook, zalo,…) phải thận trọng, tránh để lộ, lọt thông tin cá nhân khi đăng ký, tham gia; khi chia sẻ thông tin, làm quen, kết bạn trên mạng xã hội nên cảnh giác những tài khoản lạ, tài khoản là người nước ngoài, chủ động kết bạn; không cung cấp thông tin cá nhân, chuyển tiền cho người khác khi chưa kiểm tra, xác thực thông tin chính xác của người được nhận, nhất là các trường hợp chuyển tiền, nạp thẻ điện thoại, mua bán hàng online trên mạng.

- Khi nhận được các cuộc gọi lạ, nhất là các đối tượng xưng nhân viên bưu điện, nhà mạng viễn thông, cán bộ Công an, Viện kiểm sát, Tòa án,... có dấu hiệu nghi vấn, phải bình tĩnh, không làm theo yêu cầu hoặc làm theo dẫn dụ bấm các phím số trên máy điện thoại. Không được cung cấp thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,... trong các trường hợp không quen biết đối tượng, nhất là các đối tượng yêu cầu cung cấp thông tin qua điện thoại; trước những thông tin đe dọa, uy hiếp không nên vội vàng chuyển tiền vào các tài khoản theo yêu cầu của các đối tượng mà trao đổi với người thân, bạn bè hoặc thông báo với lực lượng Công an gần nhất để chủ

động phòng ngừa, đấu tranh; **lưu ý:** Khi các cơ quan tư pháp (*Công an, Viện Kiểm sát, Tòa án*) cần liên hệ người dân làm việc thì phải có giấy mời cụ thể, rõ ràng và nguyên tắc là phải làm việc tại cơ quan, trụ sở của các cơ quan có yêu cầu.

- Trước các tin tức, tiêu đề "hot", "hấp dẫn" có biểu hiện giả mạo, nhiều người xem trên mạng internet và mạng xã hội, không nên truy cập vào xem. Trong trường hợp đã truy cập vào đường link, cần nhanh chóng thay đổi mật khẩu của trang cá nhân để tránh mất tài khoản,…

(2) Đề nghị Sở Thông tin và Truyền thông: Phối hợp với các Công ty Viễn thông trên địa bàn (Vinaphone, Mobifone, Viettel,...) có giải pháp tuyên truyền, phổ biến rộng rãi thủ đoạn của loại tội phạm này đến các thuê bao di động trả trước, trả sau trên địa bàn để biết phòng ngừa, đấu tranh.

(3) Đề nghị Ngân hàng Nhà nước Việt Nam chi nhánh tỉnh Trà Vinh: Đẩy mạnh tuyên truyền đến các nhân viên giao dịch tại các quầy của ngân hàng, tổ chức tín dụng… để nắm các trường hợp rút tiền, chuyển tiền của người dân và tích cực giải thích, thông báo cho người dân biết được thủ đoạn phạm tội của đối tượng sử dụng công nghệ cao, nhất là các hành vi lừa đảo chiếm đoạt tài sản. Đồng thời, cần chú ý giám sát, kiểm tra các tài khoản có các dấu hiệu nghi vấn như: Các tài khoản do người ở khu vực nông thôn, vùng sâu, vùng xa đăng ký mở và mở dịch vụ Internet banking, ngay sau khi mở đã có các khoản tiền lớn (hàng trăm triệu đồng) chuyển đến, các tài khoản này bị rút tiền tại các ATM nước ngoài,... để có biện pháp xử lý và cung cấp cho cơ quan Công an. Ngoài ra, tăng cường kiểm tra, rà soát quy trình, giám sát chặt việc mở tài khoản, phát hành thẻ cho khách hàng để phát hiện, xử lý các trường hợp sử dụng Giấy Chứng minh nhân dân giả, Giấy Chứng minh nhân dân của người khác mở tài khoản,… nhằm kịp thời ngăn chặn thiệt hại về tài sản của những bị hại trong các vụ lừa đảo trên không gian mạng.

Trên đây là một số phương thức, thủ đoạn của đối tượng sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản, Công an tỉnh thông báo đến các Sở, ban, ngành, đoàn thể tỉnh và UBND các huyện, thị xã, thành phố nắm, phối hợp tuyên truyền./.

Nơi nhận:
- Đ/c Giám đốc (để báo cáo);
- Các Sở, ngành, đoàn thể tỉnh (để biết, ph/hợp t. truyền);
- UBND các huyện, thị xã, thành phố (để ph/hợp t. truyền);
- Phòng PA03, PX05 (để biết, tuyên truyền);
- Công an các huyện, thị xã, thành phố (để biết);
- CLB Hưu trí CAT (để biết);
- BLĐ PV01, TTTTCH, TMCS, TMAN (để theo dõi);
- Lưu: VT - PV01, PC02 (Đội 5). 146

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH TRÀ VINH

Đại tá Phan Thanh Quân