PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢNTRÊN KHÔNG GIAN MẠNG, MỘT SỐ GIẢI PHÁP PHÒNG VÀ CHỐNG

Nguyễn Đăng Trung
Phòng Tham mưu - Công an thành phố Hải Phòng
Email: trungnd80@gmail.com

Ngày nhận bài: 22/10/2021
Ngày PB đánh giá: 08/11/2021
Ngày duyệt đăng: 12/11/2021

TÓM TẮT: Bài viết làm rõ khái niệm và các đặc điểm của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng; phân tích, nhận diện, tổng hợp các phương thức, thủ đoạn của loại tội phạm này. Trên cơ sở đó đề xuất một số giải pháp đối với các cơ quan chức năng và khuyến cáo đối với người dân để nâng cao hiệu quả phòng ngừa và đấu tranh với loại tội phạm này trong thời gian tới.

Từ khóa: Tội phạm, tội phạm lừa đảo, chiếm đoạt tài sản, không gian mạng, công nghệ cao, an ninh mạng, lừa đảo

METHODS AND TRICKS OF CRIMINAL FRAUD TO APPROPRIATE PROPERTY IN CYBERSPACE SOME SOLUTIONS FOR PREVENTING AND FIGHTING

ABSTRACT: This paper clarifies the concept and features of the criminal fraud to appropriate property in cyberspace; analyzing, identifying and synthesizing methods and tricks of this type of crimes. Those are on the purpose of proposing some solutions for authorities and recommendations for people to enhance the effectiveness of preventing and combating this kind of crime in the coming time.

Keyword: Crime, criminal fraud, appropriare property, cyberspace, high-technology, cyber security, fraud

1. ĐẶT VẤN ĐỀ

Trong điều kiện phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0 hiện nay, không gian mạng trở thành bộ phận cấu thành không thể thiếu và đóng vai trò quan trọng trong xây dựng xã hội thông tin và phát triển kinh tế tri thức. Ở Việt Nam, ứng dụng và phát triển mạnh mẽ công nghệ thông tin trong các lĩnh vực đời sống xã hội, góp phần đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước, phát triển kinh tế, văn hóa, xã hội. Mạng Internet phát triển mạnh mẽ với tốc độ nhanh, chi phối mọi lĩnh vực của đời sống xã hội. Số lượng người dùng Internet ở Việt Nam tính đến năm 2020 là 68,17 triệu người. Số lượng người sử dụng mạng xã hội tăng nhanh, riêng người dùng Facebook tăng gấp 09 lần so với tốc độ tăng dân số, xếp thứ 7 trên thế giới với 58 triệu người dùng. Nhu cầu mua sắm online nhất là từ khi diễn ra dịch bệnh Covid-19 đến nay tăng nhanh. Các ứng dụng thanh toán điện tử được sử dụng ngày càng phổ biến. Riêng trong năm 2020 thương mại điện tử nước ta tăng khoảng 15% đạt quy mô khoảng 13,2 tỷ USD và sẽ tiếp tục tăng trưởng mạnh trong những năm tới. Phần lớn các cơ quan, đơn vị, tổ chức, cá nhân hiện nay sử dụng các ứng dụng mạng trong công

việc, giao dịch, học tập và trao đổi thông tin hàng ngày [1].

Cùng với sự gia tăng của không gian mạng, các loại tội phạm sử dụng công nghệ cao ngày càng phức tạp, nghiêm trọng, gia tăng cả về số vụ và tính chất, mức độ, hậu quả. Trong các loại tội phạm sử dụng công nghệ cao, hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng hiện nay hết sức phổ biến trên nhiều ngành, nhiều lĩnh vực, thủ đoạn hết sức đa dạng, tinh vi, phức tạp và thường xuyên thay đổi, khó nhận diện, phức tạp gây thiệt hại to lớn cho Nhà nước, tổ chức và cá nhân, trở thành vấn đề gây nhức nhối dư luận.

Chính vì vậy, việc nghiên cứu về hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng, đặc biệt là tổng hợp các phương thức, thủ đoạn các đối tượng thường sử dụng để nhận diện các hoạt động này, đồng thời triển khai các biện pháp phòng ngừa, ngăn chặn đấu tranh với loại tội phạm này trong đời sống xã hội là một yêu cầu bức thiết hiện nay.

2. TỔNG QUAN NGHIÊN CỨU

Hiện nay, đã có một số đề tài, công trình nghiên cứu khoa học liên quan đến các vấn đề về an ninh mạng, tội phạm về công nghệ cao. Trên các phương tiện thông tin đại chúng cũng đã có nhiều thông tin về các vụ việc, cảnh báo các phương thức, thủ đoạn về các hoạt động lừa đảo trên không gian mạng trên một số lĩnh vực cụ thể, tuy nhiên, đến nay chưa có công trình nghiên cứu nào chuyên sâu về nội dung này. Để đảm bảo tính mới, lấp khoảng trống trong lĩnh vực nghiên cứu, bài báo sẽ nghiên cứu để làm rõ nội hàm của khái niệm "lừa đảo chiếm đoạt tài sản trên không gian mạng", phân tích những đặc điểm đặc trưng của loại hình tội phạm này; thu thập tài liệu từ tình hình thực tế, phân tích, hệ thống hóa để tổng hợp 06 phương thức, thủ đoạn chủ yếu về các hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng hiện nay; đồng thời, căn cứ trên các chủ trương, chính sách của Đảng, pháp luật của Nhà nước và tình hình thực tiễn để nghiên cứu, đề xuất 08 giải pháp chủ yếu đối với các cấp, các ngành chức năng và người dân nhằm nâng cao hiệu quả công tác phòng ngừa, đấu tranh, ngăn chặn đối với các hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng trong giai đoạn hiện nay và trong thời gian tới.

3. KẾT QUẢ NGHIÊN CỨU

3.1. Khái niệm và đặc điểm của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng

Theo quy định tại Điều 174, Điều 290, khoản 1, Điều 8 Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) và các văn bản hướng dẫn thi hành, tội lừa đảo chiếm đoạt tài sản do người có đủ năng lực trách nhiệm hình sự thực hiện do cố ý, xâm phạm đến khách thể là quyền sở hữu về tài sản của cơ quan, tổ chức, cá nhân mà theo quy định phải bị xử lý hình sự [9].

Điểm đặc trưng của tội lừa đảo chiếm đoạt tài sản là "bằng thủ đoạn gian dối chiếm đoạt tài sản của người khác". Thủ đoạn gian dối của người phạm tội phải có trước hành vi chiếm đoạt và là nguyên nhân trực tiếp khiến người bị hại tin là thật và giao tài sản cho người phạm tội. Đối với hành vi lừa đảo trên không gian mạng, thủ đoạn gian dối ở đây thể hiện bằng việc sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để đưa ra những thông tin sai sự thật nhằm gây lòng tin đối với chủ tài sản, làm chủ tài sản tin tưởng người phạm tội mà trao tài sản cho họ nhằm mục đích chiếm đoạt tài sản.

Căn cứ các quy định của pháp luật và

các khái niệm về mạng máy tính, mạng viễn thông, phương tiện điện tử, không gian mạng, Internet, thiết bị số có thể hiểu: "Tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự do người có năng lực trách nhiệm hình sự thực hiện bằng việc cố ý sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi gian dối nhằm chiếm đoạt tài sản của cơ quan, tổ chức, cá nhân" [8].

Tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng có một số đặc điểm sau:

Tính "ẩn danh" và phương thức hoạt động "phi truyền thống" của tội phạm trên không gian mạng làm cho các đối tượng phạm tội dễ che giấu tung tích đối với người bị hại. Các đối tượng phạm tội có thể ở một địa bàn để thực hiện hành vi lừa đảo ở nhiều địa bàn khác, không có giới hạn về khoảng cách địa lý. Đây là một trong những yếu tố kích thích dẫn đến sự phổ biến của loại tội phạm này trong thời gian qua.

Các dấu vết quan trọng phản ánh về hoạt động phạm tội về mạng máy tính thường tồn tại dưới dạng dữ liệu điện tử, ẩn trong các thiết bị lưu trữ, rất dễ bị xóa bỏ, thay đổi, gây hư hỏng, tiêu hủy, ẩn giấu, mã hóa, làm cho việc phục hồi dữ liệu hết sức khó khăn.

Phạm vi ảnh hưởng rộng, tính chất quốc tế của tội phạm lừa đảo trên không gian mạng nhiều khi cần sự phối hợp của lực lượng chức năng trên nhiều lĩnh vực, địa bàn khác nhau. Sự khác biệt trong hệ thống luật pháp và sự hợp tác quốc tế hạn chế là rào cản làm cho hoạt động đấu tranh phòng, chống tội phạm trên không gian mạng, là điều kiện để loại tội phạm này tiếp tục tồn tại, hoạt động, nhất là đối với đối tượng lừa đảo từ nước ngoài [2].

2. Phương thức, thủ đoạn hoạt động của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng

Tình hình tội phạm lừa đảo, chiếm đoạt tài sản qua mạng diễn ra phức tạp với nhiều phương thức, thủ đoạn khác nhau, gây hậu quả nghiêm trọng, ảnh hưởng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân. Qua tổng hợp các phương thức thủ đoạn chủ yếu bao gồm:

(1) Lừa đảo qua các hình thức giả mạo: Giả mạo là một trong những phương thức, thủ đoạn thông dụng nhất của các đối tượng để thực hiện hành vi lừa đảo, được tiến hành bằng rất nhiều hình thức tinh vi, đa dạng, cụ thể gồm những hình thức chính như sau:

Giả danh các cơ quan, tổ chức thực thi pháp luật: Công an, Viện Kiểm sát, Tòa án... gọi điện thông báo cho người bị hại họ hoặc người thân có liên quan đến các tổ chức tội phạm, đường dây ma túy, mua bán người...; yêu cầu cung cấp thông tin để nhận gửi bưu phẩm hoặc giấy triệu tập, chuyển tiền vào tài khoản chỉ định trước để phục vụ điều tra; đe dọa bắt giữ, xử lý, yêu cầu nạn nhân phải thống kê, khai báo, cung cấp với đối tượng; các thông tin cá nhân, tài khoản ngân hàng nhằm phục vụ điều tra... [3].

Giả mạo website dịch vụ chuyển tiền quốc tế, các ngân hàng thương mại, ví điện tử, nhân viên chăm sóc khách hàng, xử lý sự cố… để lừa người dùng truy cập; giả mạo các doanh nghiệp cung cấp các loại dịch vụ, thông tin hỗ trợ khách hàng, giải đáp thắc mắc về sản phẩm, dịch vụ (như nhân viên các ngành dịch vụ điện, nước, Internet), yêu cầu thực hiện chuyển khoản nộp tiền nếu không sẽ khóa dịch vụ… để tạo sức ép, yêu cầu người bị hại thực hiện theo yêu cầu của đối tượng; giả mạo cán bộ ngân hàng gọi

điện hoặc nhắn tin cho người bị hại thông báo có giao dịch chuyển tiền vào tài khoản nhưng bị treo và yêu cầu cung cấp thông tin đăng nhập, mật khẩu dịch vụ Internet Banking và mã OTP để nhận tiền. Thực hiện rút tiền, chuyển tiền vào tài khoản hoặc thanh toán hóa đơn rồi chiếm đoạt..

Giả mạo các website, cổng thông tin điện tử của cơ quan nhà nước, tổ chức, doanh nghiệp, giả mạo website các chương trình nổi tiếng... để dẫn dụ người dùng truy cập. Khi người dùng điền thông tin đăng nhập thì sẽ bị trộm cắp thông tin cá nhân hoặc cài đặt mã độc vào thiết bị của người dùng, phục vụ cho mục đích chiếm đoạt tài sản.

Thiết lập các trạm BTS giả mạo các doanh nghiệp viễn thông để chặn, chuyển hướng các thuê bao di động của người dùng nhằm thu thập thông tin, dữ liệu để chiếm đoạt tài sản (Bộ Công an đã phát hiện xử lý vụ việc các đối tượng thiết lập trạm BTS giả mạo của MobiFone để chuyển hướng các cuộc gọi của khách hàng, đánh cắp thông tin thực hiện hành vi lừa đảo chiếm đoạt tài sản).

(2) Lừa đảo qua các hình thức kinh doanh, giao dịch, thương mại điện tử trên không gian mạng

Giao dịch thương mại điện tử: Các đối tượng mở các trang bán hàng online, sau đó quảng cáo, rao bán các mặt hàng, quảng cáo mời làm nhà phân phối mặt hàng của công ty, yêu cầu người tiêu dùng chuyển khoản hay đặt cọc để đặt mua, sau đó không giao hàng hoặc giao hàng giả, hàng kém chất lượng, hàng cũ hỏng, hàng không rõ nguồn gốc, xuất xứ, không đúng bản chất sản phẩm rao bán, giao không đủ số lượng đặt mua, sau đó cắt liên lạc, xóa dấu vết. Xâm nhập bất hợp pháp vào các website bán hàng, thanh toán trực tuyến trộm cắp thông tin thẻ tín dụng của người nước ngoài, sau đó đặt mua hàng hóa trực tuyến có giá trị cao chuyển về Việt Nam tiêu thụ.

Tạo lập các sàn giao dịch, website, ứng dụng kiếm tiền, sử dụng "mồi nhử" là các khoản lợi nhuận cao để kêu gọi, lôi kéo đầu tư, kinh doanh tiền ảo, ngoại hối... theo mô hình đa cấp. Sau đó, can thiệp vào hệ thống kỹ thuật làm nhà đầu tư thua lỗ hoặc đánh sập để chiếm đoạt tài sản (Điển hình như ứng dụng CoolCat kêu gọi người chơi tham gia dự đoán tỷ giá vàng, ngoại tệ, tiền ảo... website "webshopping.cc" và "shop555.cc" lôi kéo người dân tham gia đầu tư dưới hình thức tranh đơn hàng ảo...) [4].

Sử dụng phương thức kinh doanh đa cấp: Các đối tượng lừa đảo sử dụng các khoản lợi nhuận lớn để hấp dẫn, lôi kéo số lượng lớn người dân đầu tư vào các dự án ảo, sau đó đánh sập hệ thống để chiếm đoạt tài sản. Hoạt động của các sàn giao dịch quyền chọn nhị phân (BO) gia tăng, quảng cáo rộng rãi trên các mạng xã hội như là "sản phẩm" công nghệ tài chính, ứng dụng "blockchain" trong cuộc cách mạng 4.0, khiến "nhà đầu tư" lầm tưởng các sàn này được cấp phép hoạt động tại Việt Nam như: Wefinex, Raidenbo, Rosichi, The Legend... Các sàn giao dịch BO này thực chất do các đối tượng trong nước thiết lập, điều hành; thông qua đối tượng môi giới để quảng cáo, lôi kéo người chơi tham gia.

(3) Lừa đảo thông qua thư điện tử, mạng xã hội và các diễn đàn trên không gian mạng

Chiếm quyền điều khiển tài khoản các hộp thư điện tử của các doanh nghiệp, cá nhân, sau đó giả danh gửi thư điện tử cho đối tác, thay đổi các nội dung của hợp đồng xuất nhập khẩu, thay đổi tài khoản thanh toán bằng tài khoản của đối tượng lập

lên để khách hàng chuyển tiền vào. (Lực lượng chức năng đã phát hiện các băng nhóm hacker là người nước ngoài, chủ yếu là người Nigeria, sử dụng thủ đoạn trên; nhiều doanh nghiệp, cá nhân Việt Nam có hợp đồng kinh tế với nước ngoài bị lừa đảo chiếm đoạt số lượng tiền rất lớn, từ 2 - 3 nghìn USD, đến hàng trăm nghìn USD…)

Chiếm quyền điều khiển các tài khoản mạng xã hội (Facebook, Zalo, Twitter, Viber....) của người dùng, sau đó mạo danh người dùng để lừa đảo bạn bè, người thân (như nhờ hỗ trợ tài chính, vay tiền, nhờ mua thẻ điện thoại, yêu cầu người thân, bạn bè của người tiêu dùng thực hiện các giao dịch…), đối tác nhằm chiếm đoạt tài sản. Để chiếm đoạt quyền quản trị các tài khoản mạng xã hội, các đối tượng thường sử dụng các thủ đoạn dẫn dụ người dùng mạng xã hội truy cập vào các liên kết do các đối tượng lập nên với các nội dung hấp dẫn người dùng như trò chơi, bói toán, khảo sát tâm lý, khuyến mại, mua hàng giảm giá,... qua đó sử dụng mã độc để trộm cắp thông tin trong thiết bị người dùng.

Lừa đảo qua làm quen, kết bạn trên mạng: Với sự thông dụng của các diễn đàn, phần mềm, các mạng xã hội, các ứng dụng trò chuyện, làm quen, kết bạn, các đối tượng sử dụng các thông tin ảo, ảnh giả, video giả, tạo dựng nhiều kịch bản tinh vi để tạo lòng tin cho người bị hại. Một số đối tượng sử dụng tiếng Anh giả danh làm người nước ngoài, tìm và kết bạn với những người có nhu cầu kết hôn với người ngoại quốc, sau đó sử dụng các lý do để người bị hại chuyển tiền phục vụ cho các mục đích trá hình (như nộp phí để nhận quà, để hối lộ, thực hiện thủ tục Hải quan...).

(4) Lừa đảo qua các dịch vụ viễn thông: Các đối tượng lừa đảo sử dụng các dịch vụ viễn thông đặc biệt là tin nhắn lợi dụng sự mất cảnh giác của người dùng để chiếm đoạt tiền cước viễn thông. Cụ thể như:

Sử dụng các loại tin nhắn rác, tin nhắn gài bẫy, gọi điện thoại đến đầu số giá trị gia tăng, mời người dùng sử dụng hoặc xem các thông tin như thời tiết, giá vàng, thông tin thời sự….để lừa đảo người dùng nhắn tin, gọi điện đến đầu số giá trị gia tăng, thực hiện các dịch vụ mà người dùng không sử dụng đến (tin nhắn cho các đầu số này thường có cước phí cao từ 3.000 - 15.000 đồng/tin).

Sử dụng phần mềm gián điệp cài trên điện thoại thông minh tự động gửi tin nhắn đến đầu số giá trị gia tăng (wap charging) một cách tự động và do đó cước phí viễn thông của người dùng bị trừ tiền mà người dùng không hay biết.

Sử dụng kỹ thuật để chiếm đoạt quyền sử dụng thẻ SIM người dùng (“hack” SIM) là hình thức đặc biệt nguy hiểm do đối tượng có thể trộm cắp không chỉ tiền trong tài khoản mà còn có thể bán lại tài khoản cho người khác hoặc chiếm đoạt tiền trong ngân hàng khi SIM đó được liên kết với tài khoản ngân hàng của người bị hại [5] .

(5) Cài mã độc, phần mềm gián điệp, vào thiết bị của người dùng, thu thập thông tin để phục vụ hoạt động lừa đảo: Thông qua việc dẫn dụ người dùng truy cập vào các liên kết bất hợp pháp. Các tập tin chứa mã độc có thể được tải, cài đặt và mở tự động trên thiết bị cá nhân của bị hại; cài đặt các phần mềm gián điệp (spyware) vào máy tính, điện thoại của người dùng. Các phần mềm gián điệp có chức năng thu thập dữ liệu, thông tin, tài liệu, hình ảnh... trong các thiết bị thông minh; bí mật điều khiển thiết bị thông minh của nạn nhân để ghi âm, chụp hình, ghi lại các thao tác của người dùng và gửi dữ liệu về cho đối tượng. Sử

dụng các thông tin chiếm đoạt được để kết hợp với các phương thức, thủ đoạn khác để thực hiện hành vi lừa đảo. Ngoài ra, bằng các thông tin thu thập được, các đối tượng còn có thể sử dụngđể chiếm đoạt tiền trong tài khoản ngân hàng; sử dụng thông tin nhạy cảm để đe dọa, tống tiền hay phục vụ nhiều mục đích bất hợp pháp khác.

(6) Các thủ đoạn để chiếm lòng tin người bị hại

Để dẫn dụ người dùng truy cập vào các liên kết hoặc tập tin chứa mã độc hoặc thực hiện theo các yêu cầu của đối tượng để thực hiện hành vi lừa đảo, các đối tượng sử dụng nhiều thủ đoạn trong đó có thể hệ thống một số cách thức chính như sau:

Lợi dụng vào tâm lý chung của người dùng để đưa ra các thông báo về nhận quà, trúng thưởng hoặc lợi dụng các thời điểm đặc biệt để đưa ra các lý do thuyết phục như: nhận tiền lì xì đầu năm, nhập quà nhân dịp ngày lễ, nhận quà khuyến mại... Lợi dụng vào các tình hình chính trị, kinh tế, xã hội mà dư luận, xã hội đang quan tâm, có liên quan đến đông đảo người dân, rao bán các mặt hàng thiết yếu, đang khan hiếm, kích thích trí tò mò của người dùng như đưa các thông tin liên quan đến dịch bệnh Covid-19, rao bán khẩu trang, thiết bị y tế, tiêm vắc xin phòng dịch; các chính sách về cách ly, phong tỏa; lợi dụng nhiều người đang gặp khó khăn để chào mời kiếm tiền online, sử dụng clip, hình ảnh nóng để dẫn dụ…

Đưa người dùng vào các tình trạng khẩn cấp về thời gian, đặt vào tình thế nếu không thực hiện ngay theo yêu cầu, hướng dẫn của các đối tượng thì sẽ bị ảnh hưởng quyền lợi. Do đó người dùng thường không kịp có thời gian để cân nhắc, kiểm chứng và dễ bị dẫn dụ theo thủ đoạn của đối tượng.

Sử dụng phần mềm (Voice over IP) giả số điện thoại, tạo các âm thanh giả để lừa đảo khi gọi điện thoại; sử dụng phần mềm giả mạo tin nhắn thương hiệu (brandname) của các cơ quan, doanh nghiệp nổi tiếng để tạo lòng tin cho người bị hại (trong năm 2021 đã phát hiện thủ đoạn giả mạo tin nhắn của các ngân hàng Vietcombank, Vietinbank, Sacombank để lừa đảo). Các trang website giả mạo có giao diện giống hoàn toàn với website thật, có đường link truy cập gần giống với đường link thật, tạo sự nhầm lẫn cho người dùng.

Lợi dụng tâm lý dễ bị dẫn dụ vào các hoạt động khi đã có nhiều người tham gia, các đối tượng tạo các khách hàng ảo, bình luận giả, tạo ra số lượng giao dịch ảo để tạo lòng tin cho người dùng. Điển hình như: để dẫn dụ người dùng vào các hoạt động kiếm tiền online, các sàn giao dịch chứng khoán, ngoại hối bất hợp pháp, các đối tượng đưa ra hàng loạt khách hàng ảo để bình luận, phỏng vấn đưa thông tin về các khoản lợi nhuận thu được...

Nghiên cứu đặc điểm, sở thích, nhu cầu, thói quen, các mối quan hệ của từng người dùng để đe dọa, lừa đảo; đồng thời các đối tượng không chỉ sử dụng một phương thức mà phối hợp sử dụng nhiều phương thức, thủ đoạn để tạo lòng tin cho nạn nhân. Đưa ra các chiến thuật riêng đối với từng loại người dùng như với học sinh, sinh viên, với phụ nữ, với người cao tuổi,....

3. Một số biện pháp tăng cường phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng

Với những đặc điểm đặc trưng về phương thức, thủ đoạn phạm tội lừa đảo chiếm đoạt tài sản trên không gian mạng, trong thời gian tới, để nâng cao hiệu quả hoạt động phòng, chống loại tội phạm này, qua nghiên cứu, chúng tôi đề xuất một số

biện pháp sau:

Một là, các cấp, các ngành triển khai thực hiện nghiêm túc, hiệu quả các chủ trương của Đảng, pháp luật của Nhà nước liên quan đến công tác bảo đảm an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, trong đó có tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng. Đặc biệt là Nghị quyết số 29-NQ/TW, Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về "Chiến lược bảo vệ Tổ quốc trên không gian mạng và "Chiến lược bảo vệ An ninh mạng Quốc gia", Chỉ thị số 01/CT-Ttg ngày 18/02/2021 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh mạng, Chỉ thị số 21/CT-TTg ngày 25/5/2020 của Thủ tướng Chính phủ về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản, bảo đảm quyền và lợi ích hợp pháp của Nhà nước, tổ chức, doanh nghiệp và cá nhân trong sở hữu tài sản.

Hai là, tăng cường công tác thông tin, tuyên truyền, cảnh báo về hoạt động lừa đảo chiếm đoạt tài sản gắn với các vụ việc, vụ án điển hình. Nội dung tuyên truyền tập trung vào các nội dung như:

Phổ biến, cập nhật thường xuyên các phương thức, thủ đoạn lừa đảo; bảo vệ các thông tin cá nhân trên không gian mạng , hạn chế tối đa việc chia sẻ các thông tin cá nhân chia sẻ thông tin cá nhân, tâm tư, tình cảm, nguyện vọng của cá nhân trên không gian mạng, các mạng xã hội là trên các mạng xã hội (facebook, zalo, viber…) để các đối tượng khai thác thực hiện hành vi lừa đảo (nhất là những người sống độc thân, người già, hưu trí...); cảnh giác khi kết bạn với người nước ngoài, đặc biệt khi họ đưa ra các lời hứa về lợi ích vật chất. Thực hiện các biện pháp để bảo đảm an toàn như: Không thực hiện theo các hướng dẫn, yêu cầu trên mạng khi chưa có sự kiểm chứng; không truy cập vào các trang web, email lạ, không tải, mở các tài liệu, đường dẫn, ứng dụng khi chưa rõ nguồn gốc; cảnh giác với những lời giới thiệu, quảng cáo, chào mời các sản phẩm qua mạng; không cung cấp mã OTP do ngân hàng gửi cho bất kỳ ai, kể cả nhân viên ngân hàng;... Sử dụng các chương trình diệt virus có uy tín. Cập nhật bản trình duyệt, hệ điều hành và các chương trình sử dụng có bản quyền, cập nhật các bản vá lỗi thường xuyên [6].

Đề cao cảnh giác khi nhận các cuộc gọi đến bằng số điện thoại cố định, không giao dịch với số điện thoại đầu số lạ, người gọi tự xưng là cán bộ các cơ quan nhà nước, đặc biệt là lực lượng Công an để thông báo, yêu cầu điều tra vụ án qua điện thoại, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở... cho những người chưa rõ nhân thân lai lịch, không nghe lời của đối tượng chuyển tiền vào các tài khoản do các đối tượng chỉ định. Sàng lọc kỹ, kiểm tra kỹ thông tin quảng cáo, rao bán về hàng hóa, danh tính người bán hàng qua mạng, lựa chọn địa chỉ uy tín, hình thức thanh toán minh bạch. Không cho mượn, cho thuê các giấy tờ cá nhân có liên quan như căn cước công dân, thẻ ngân hàng, không nhận chuyển khoản hoặc nhận tiền chuyển khoản của các ngân hàng cho người không quen biết, không tin tưởng vào những chiêu trò nhận thưởng qua mạng mà yêu cầu nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Khi có thông báo trúng thưởng hoặc người gửi quà thì không nhận khi chưa xác định rõ lý do gửi và thông tin người gửi để xác nhận thông tin. Cảnh giác và thường xuyên kiểm tra đối với các dịch vụ cung cấp thông tin

qua tin nhắn trên điện thoại, yêu cầu tổng đài xóa bỏ các dịch vụ không cần thiết…

Ba là, làm tốt công tác hướng dẫn cơ quan, tổ chức, doanh nghiệp tham gia phòng ngừa vi phạm pháp luật trên không gian mạng trong đó có hành vi lừa đảo chiếm đoạt tài sản. Yêu cầu, thanh tra, kiểm tra việc chấp hành quy định của pháp luật về thời hạn bảo quản, lưu trữ, cung cấp thông tin, dữ liệu điện tử phục vụ công tác phòng chống tội phạm và vi phạm pháp luật khác xâm phạm an ninh mạng. Yêu cầu cơ quan, tổ chức, doanh nghiệp cung cấp thông tin, tài liệu, số liệu, chứng cứ liên quan cho cơ quan chuyên trách khi có yêu cầu theo quy định của pháp luật. Kiểm tra, giám sát hoạt động hợp tác với các tổ chức, doanh nghiệp cung cấp dịch vụ trên hạ tầng mạng, không cung cấp dịch vụ có nội dung lừa đảo; chủ động triển khai các biện pháp cảnh báo, hỗ trợ, bảo vệ người sử dụng. Thanh tra, kiểm tra, xử lý, giám sát các trang thông tin điện tử, tài khoản mạng xã hội của các tổ chức, cá nhân có các hoạt động có nguy cơ cao như huy động vốn, đầu tư trái phép, đổi tiền qua trung gian, quảng cáo mua bán hàng hóa, dịch vụ mua hộ hàng hóa... tích hợp trên các sản phẩm dịch vụ bưu chính, viễn thông, công nghệ thông.

Bốn là, nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng, xây dựng cơ chế để tăng cường quản lý, kiểm soát đối với các hoạt động thương mại điện tử, thanh toán điện tử. Các doanh nghiệp viễn thông, cung cấp dịch vụ Internet có cơ chế lưu giữ đầy đủ, chính xác, bảo mật thông tin cá nhân của người sử dụng dịch vụ; tăng cường quản lý các nội dung quảng cáo trên môi trường mạng, loại bỏ "sim rác". Rà soát, xác định những sơ hở, thiếu sót, những vấn đề gây vướng mắc trong công tác phòng ngừa, xử lý vi phạm, đặc biệt là những quy định về chứng cứ điện tử để phục vụ công tác điều tra, xử lý [7].

Năm là, tăng cường năng lực cho cơ quan chuyên trách trong phòng chống tội phạm công nghệ cao; trang bị các thiết bị, công cụ, phương tiện hiện đại; nâng cao kiến thức, kinh nghiệm về pháp luật, nghiệp vụ, kỹ thuật để đấu tranh với loại tội phạm này. Lực lượng Công an mở các đợt cao điểm tấn công, trấn áp tội phạm, trong đó có tội phạm lừa đảo chiếm đoạt tài sản, đặc biệt là tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng. Tập trung điều tra, khởi tố, xử lý các hành vi lừa đảo chiếm đoạt tài sản, triệt để thu hồi tài sản bị chiếm đoạt.

Sáu là, Ngân hàng Nhà nước Việt Nam ban hành các quy định đối với việc ứng dụng các phương tiện thanh toán mới, tiên tiến, bảo đảm chặt chẽ, an toàn; tăng cường kiểm tra, phát hiện kịp thời các hành vi gian lận, không đúng quy định pháp luật về hoạt động thanh toán, trung gian thanh toán, phòng ngừa đối tượng lợi dụng để thực hiện hành vi vi phạm pháp luật; khắc phục những sơ hở, thiếu sót trong các hoạt động như cho vay, thanh toán, chuyển tiền, nhận tiền... phối hợp xác minh, xử lý tội phạm; kịp thời có biện pháp phong tỏa, ngăn chặn việc tẩu tán tài sản trong các vụ việc, vụ án [10].

Bảy là, xây dựng phong trào toàn dân bảo vệ An ninh Tổ quốc trên không gian mạng, trong đó khuyến khích, hướng dẫn người dân tham gia các hoạt động phòng ngừa, đấu tranh với các hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng; kịp thời tố giác tội phạm, phối hợp chặt chẽ với các cơ quan chuyên trách, cung cấp thông tin, tài liệu phục vụ quá trình điều

tra, làm rõ, xử lý các đối tượng lừa đảo trên không gian mạng.

Tám là, tăng cường công tác hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao, trong đó có tội phạm lừa đảo qua mạng. Đặc biệt là phối hợp trong xử lý các đối tượng lừa đảo xuyên quốc gia. Liên kết với nước ngoài đào tạo, tập huấn nâng cao năng lực cho lực lượng chức năng về phối hợp tổ chức tập huấn kỹ năng thu thập, bảo quản, phục hồi và phân tích dữ liệu, chứng cứ điện tử tại Việt Nam; kỹ năng điều tra tội phạm sử dụng công nghệ cao.

4. KẾT LUẬN

Tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng là loại hình tội phạm đặc trưng phát sinh trong sự phát triển của thời kỳ Cách mạng công nghiệp 4.0, gây hậu quả nguy hiểm, tác động đến các cơ quan, tổ chức, cá nhân, gây nhiều hệ lụy cho xã hội. Đây cũng là loại tội phạm có sự kết hợp giữa tội phạm truyền thống (lừa đảo chiếm đoạt tài sản) với tội phạm phi truyền thống (tội phạm công nghệ cao), phương thức thủ đoạn rất đa dạng, tinh vi sử dụng yếu tố tâm lý và các yếu tố về kỹ thuật công nghệ, dẫn đến công tác phòng ngừa, đấu tranh, ngăn chặn có nhiều khó khăn, phức tạp. Do đó, đòi hỏi các cấp, các ngành, các lực lượng chức năng cần có sự vào cuộc quyết liệt cùng với sự nâng cao tinh thần cảnh giác, ý thức trách nhiệm của mỗi công dân trong việc chấp hành các quy định của pháp luật cũng như sự phối hợp, hỗ trợ lực lượng chức năng để từng bước ngăn chặn, đẩy lùi loại tội phạm này, xây dựng không gian mạng lành mạnh, an toàn phục vụ cho sự phát triển kinh tế xã hội và sự an ninh, an toàn cho mỗi người dân ./.

TÀI LIỆU THAM KHẢO

1. Hiệp hội Thương mại điện tử Việt Nam VECOM (2021), Báo cáo chỉ số thương mại điện tử Việt Nam 2021 ngày 20/04/2021.

2. Trần Văn Hòa (2012), *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, NXB Công an nhân dân

3. L. Hiệp (2021), *Cảnh báo các hình thức lừa đảo trong lĩnh vực tài chính ngân hàng*, Cổng thông tin điện tử Bộ Công an, https://cand.com.vn/Ban-tin-113/canh-bao-6-hinh-thuc-lua-dao-trong-linh-vuc-tai-chinh-ngan-hang-i623000/, ngày 05/8/2021.

4. Học viện Cảnh sát nhân dân (2014), *Kỷ yếu hội thảo khoa học "Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo",* Hà Nội.

5. Nguyễn Minh Đức (2020), *Điều tra tội phạm sử dụng công nghệ cao để thực hiện hành vi chiếm đoạt tài sản - những vấn đề lý luận và thực tiễn*, Học viện Cảnh sát nhân dân.

6. Trần Thị Lâm Thi, Nguyễn Anh Tuấn (2020), *Một số vấn đề cơ bản của Luật An ninh mạng*, NXB Công an nhân dân.

7. Hoàng Phước Thuận (2019), *Công tác bảo vệ an ninh mạng của lực lượng Công an nhân dân trong tình hình hiện nay*, NXB Công an nhân dân.

8. Quốc hội và Luật số 12/2017/QH14 ngày 20/6/2017 của Quốc hội sửa đổi, bổ sung một số điều của Bộ luật Hình sự;

9. Quốc Hội (2017), Bộ luật Hình sự số 100/2015/QH13 ngày 27/11/2015 của

10. Thủ tướng Chính phủ (2020), *Chỉ thị số 21/CT-TTg ngày 25/5/2020 về Tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản*.