NHẬN DIỆN MỘT SỐ THỦ ĐOẠN LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG HIỆN NAY

ThS. NGUYỄN CHÍ LINH*
ThS. VŨ ĐỨC QUANG**

Tóm tắt: *Trong thời đại số hiện nay, hành vi lừa đảo trên không gian mạng đã và đang trở thành một vấn nạn nghiêm trọng, ảnh hưởng trực tiếp đến an toàn tài chính và thông tin cá nhân của người dùng. Cùng với sự phát triển của khoa học và công nghệ, các đối tượng phạm tội sử dụng các thủ đoạn lừa đảo ngày càng tinh vi, khó phát hiện. Tại Việt Nam, mỗi năm, các cơ quan chức năng đã ghi nhận hàng nghìn vụ lừa đảo chiếm đoạt tài sản trên không gian mạng, gây thiệt hại lớn về vật chất và tinh thần... Trên cơ sở nhận diện một số thủ đoạn lừa đảo chiếm đoạt tài sản phổ biến trên không gian mạng hiện nay, bài viết đề xuất một số giải pháp phòng ngừa và giảm thiểu rủi ro lừa đảo trên không gian mạng.*

Từ khóa: *lừa đảo chiếm đoạt tài sản; lừa đảo trên không gian mạng; tội phạm sử dụng công nghệ cao*

Ngày nhận: 15/5/2025 **Ngày phản biện:** 02/6/2025 **Ngày duyệt đăng:** 10/6/2025

1. Nhận thức chung về tội phạm lừa đảo chiếm đoạt tài sản và hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng

Chiếm đoạt tài sản được hiểu là hành vi chuyển dịch một cách trái pháp luật tài sản của người khác thành của mình. Theo Điều 174 Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017), tội phạm lừa đảo chiếm đoạt tài sản được hiểu là hành vi phạm tội mà người thực hiện sử dụng thủ đoạn gian dối, lừa gạt người khác để chiếm đoạt tài sản của họ, nhằm thu lợi bất chính cho bản thân. Chủ thể của tội lừa đảo chiếm đoạt tài sản là bất kỳ người nào từ đủ 16 tuổi trở lên, có năng lực trách nhiệm hình sự. Khách thể của tội lừa đảo chiếm đoạt tài sản là quyền sở hữu tài sản của người khác. Về mặt khách quan của tội phạm, đối tượng có các hành vi dùng thủ đoạn gian dối để chiếm đoạt tài sản. Cụ thể, đối tượng đưa ra thông tin giả (không đúng sự thật) nhưng làm cho người khác tin đó là thật và giao tài sản cho người phạm tội. Việc đưa ra thông tin giả có thể thực hiện bằng nhiều cách khác nhau như: bằng lời nói, bằng chữ viết (viết thư), bằng hành động và bằng nhiều hình thức khác như giả vờ vay, mượn, thuê để chiếm đoạt tài sản. Dấu hiệu

*, ** Học viện Cảnh sát nhân dân.

bắt buộc của tội lừa đảo chiếm đoạt tài sản nằm ở mục đích của hành vi. Người phạm tội dùng các thủ đoạn gian dối nhằm chiếm đoạt tài sản của người khác, làm cho chủ sở hữu hoặc người quản lý tài sản nhầm tưởng, tin vào các thông tin không đúng sự thật đó và tự nguyện chuyển giao tài sản cho người phạm tội. Đây là dấu hiệu quan trọng để định tội danh, phân biệt với các tội danh khác có đặc điểm về hành vi tương đương. Bên cạnh đó, giá trị của tài sản bị chiếm đoạt phải từ hai triệu đồng trở lên thì người thực hiện hành vi mới bị truy cứu trách nhiệm hình sự. Trong trường hợp giá trị tài sản dưới hai triệu đồng thì phải thuộc trường hợp gây hậu quả nghiêm trọng hoặc đã bị xử phạt vi phạm hành chính về hành vi chiếm đoạt hoặc đã bị kết án về tội chiếm đoạt tài sản chưa được xóa án tích mà còn vi phạm thì người thực hiện hành vi nêu trên mới phải chịu trách nhiệm hình sự về tội này. Về mặt chủ quan của tội phạm, tội lừa đảo chiếm đoạt tài sản được thực hiện với lỗi cố ý trực tiếp. Người phạm tội nhận thức rõ hành vi chiếm đoạt tài sản của người khác do mình thực hiện là hành vi gian dối, trái pháp luật. Đồng thời, thấy trước hậu quả của hành vi đó là tài sản của người khác bị chiếm đoạt trái pháp luật và mong muốn hậu quả đó xảy ra.

Không gian mạng là một môi trường ảo, được hình thành từ sự kết nối của hệ thống máy tính, mạng viễn thông và các thiết bị điện tử qua internet. Đây là nơi diễn ra các hoạt động như: trao đổi thông tin, giao tiếp trực tuyến, thương mại điện tử, học tập và các tương tác số khác. Không gian mạng không chỉ bao gồm các trang website và ứng dụng, mà còn liên quan đến các dịch vụ và dữ liệu được lưu trữ trên các máy chủ, với khả năng kết nối và tương tác qua hệ thống mạng internet toàn cầu. Như vậy, hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng là hành vi sử dụng các phương tiện công nghệ thông tin, mạng internet hoặc các dịch vụ trực tuyến để lừa đảo và chiếm đoạt tài sản của người khác. Các đối tượng thực hiện hành vi này thường sử dụng các thủ đoạn như giả mạo thông tin, tạo ra các website giả, lừa đảo qua email, tin nhắn hoặc mạng xã hội để thuyết phục nạn nhân chuyển tiền, cung cấp thông tin cá nhân, tài khoản ngân hàng, thẻ tín dụng... nhằm chiếm đoạt tài sản.

2. Thực trạng hoạt động lừa đảo chiếm đoạt tài sản trên không gian mạng tại Việt Nam trong thời gian qua

Trong những năm gần đây, lừa đảo chiếm đoạt tài sản trên không gian mạng tại Việt Nam đã trở thành một vấn đề ngày càng nhức nhối, ảnh hưởng không nhỏ đến an ninh mạng và gây thiệt hại lớn cho cá nhân, tổ chức. Các hình thức lừa đảo chiếm đoạt tài sản trên không gian mạng (lừa đảo trực tuyến) ngày càng trở nên tinh vi, đa dạng và phức tạp, chủ yếu diễn ra qua các kênh trực tuyến như email, mạng xã hội, website giả mạo và ứng dụng di động. Theo khảo sát của Hiệp hội An ninh mạng quốc gia tiến hành từ ngày 28/11/2024 đến ngày 14/12/2024 đối với trên 59.000 người dùng cá nhân, cứ 220 người dùng thì có 1 người là nạn nhân của lừa đảo trực tuyến[1]. Tổng thiệt hại do lừa đảo trực tuyến gây ra trong năm 2024 ước tính lên tới 18.900 tỷ đồng[2]. Lừa đảo chiếm đoạt tài sản trên không gian mạng không chỉ gây thiệt hại về mặt tài chính, mà còn ảnh hưởng nghiêm trọng

đến niềm tin của người dân vào các nền tảng trực tuyến và hệ thống bảo mật của các tổ chức. Nhiều cá nhân sau khi trở thành nạn nhân của các vụ lừa đảo đã mất lòng tin vào việc giao dịch trực tuyến. Đây là một trong những nguyên nhân chính gây cản trở sự phát triển của các nền tảng thương mại điện tử và các dịch vụ trực tuyến khác. Bên cạnh đó, việc bị mất tiền trong các vụ lừa đảo khiến nạn nhân rơi vào tình trạng hoang mang, lo lắng và đôi khi còn ảnh hưởng đến sức khỏe tâm lý, đặc biệt là những người cao tuổi. Hệ quả này không chỉ giới hạn trong phạm vi cá nhân, mà còn gây tổn hại đến hình ảnh và uy tín của các công ty, tổ chức bị giả mạo.

Có rất nhiều nguyên nhân dẫn đến sự gia tăng đáng lo ngại của những hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng tại Việt Nam trong thời gian qua như: sự thiếu hiểu biết về bảo mật, công nghệ và thiếu kỹ năng nhận diện các dấu hiệu lừa đảo của người dùng; sự phát triển của công nghệ và kỹ thuật tạo điều kiện thuận lợi cho các đối tượng thực hiện hành vi lừa đảo; sự phát triển mạnh mẽ của các nền tảng thương mại điện tử và mạng xã hội; thiếu quy định và giám sát chặt chẽ trên môi trường trực tuyến... Theo thông tin từ các chuyên gia, tội phạm mạng thường hoạt động có tổ chức, phối hợp giữa các đối tượng trong và ngoài nước và sử dụng nhiều chiêu thức lừa đảo tinh vi. Trước thực trạng trên, các cơ quan chức năng đã và đang tích cực tiến hành các hoạt động đấu tranh, phòng ngừa các vụ lừa đảo trực tuyến. Tuy nhiên, do tính chất phức tạp và tinh vi của các đối tượng phạm tội nên việc xác định và bắt giữ các nghi phạm gặp rất nhiều khó khăn. Hiện nay có rất nhiều các thủ đoạn lừa đảo chiếm đoạt tài sản trên không gian mạng, trong phạm vi bài viết, có thể nhận diện một số thủ đoạn phổ biến sau:

Thứ nhất, phishing (lừa đảo qua email và trang web giả mạo).

Phishing là một trong những thủ đoạn lừa đảo phổ biến nhất hiện nay. Các đối tượng thường giả mạo các tổ chức uy tín như ngân hàng, công ty hoặc các dịch vụ trực tuyến để đánh cắp thông tin cá nhân, tài khoản ngân hàng và mật khẩu của nạn nhân. Thủ đoạn này thường thực hiện qua email hoặc tin nhắn mạo danh kèm theo các liên kết giả mạo dẫn đến các trang web có giao diện tương tự các trang web chính thức. Ví dụ, một kẻ lừa đảo có thể gửi một email giả mạo từ ngân hàng, thông báo về vấn đề an ninh tài khoản hoặc yêu cầu người dùng xác minh thông tin qua một liên kết. Khi người dùng bấm vào liên kết, họ sẽ bị chuyển hướng đến một trang web trông giống hệt trang web của ngân hàng, nơi họ nhập thông tin tài khoản và mật khẩu mà không biết rằng mình đang cung cấp thông tin cho kẻ lừa đảo. Tại Việt Nam, năm 2022, một nhóm các đối tượng đã sử dụng thủ đoạn này để gửi các tin nhắn giả mạo từ ngân hàng BIDV yêu cầu khách hàng xác minh thông tin qua một trang web giả. Hàng nghìn khách hàng đã bị mất tiền khi đăng nhập vào trang web giả và cung cấp thông tin tài khoản ngân hàng của mình.

Thứ hai, lừa đảo qua mạng xã hội.

Lừa đảo qua mạng xã hội là thủ đoạn lợi dụng sự phổ biến của các nền tảng như Facebook, Instagram, Zalo... để thực hiện các hành vi lừa gạt. Kẻ lừa đảo tạo các tài khoản giả mạo hoặc các trang fanpage, các nhóm,

sau đó đăng bài kêu gọi mọi người tham gia vào các chương trình như: "quà tặng miễn phí", "trúng thưởng", "kêu gọi từ thiện"... Mục tiêu là dụ dỗ nạn nhân cung cấp thông tin cá nhân hoặc tham gia vào các giao dịch tài chính gian lận. Điển hình là vụ lừa đảo xảy ra trên Facebook vào năm 2021, khi một nhóm lừa đảo giả mạo các bài viết từ các cửa hàng nổi tiếng, thông báo người dùng có thể nhận được quà tặng miễn phí nếu chia sẻ bài viết và điền thông tin cá nhân. Sau khi người dùng thực hiện các yêu cầu này, họ không nhận được quà tặng mà thay vào đó, thông tin cá nhân của họ bị sử dụng để thực hiện các giao dịch gian lận. Kết quả là hàng trăm người dùng bị mất tiền và thông tin cá nhân.

Thứ ba, lừa đảo đầu tư và tài chính.

Lừa đảo đầu tư là một trong những thủ đoạn rất tinh vi trên không gian mạng, đặc biệt là trong bối cảnh thị trường tài chính đang phát triển như ở Việt Nam. Các kẻ lừa đảo thường mời gọi các nhà đầu tư tham gia vào các dự án đầu tư "hấp dẫn", cam kết lợi nhuận cao mà không rõ nguồn gốc hoặc không có thông tin minh bạch. Các hình thức này thường bao gồm các sàn giao dịch ngoại hối, tiền điện tử hoặc các mô hình đầu tư đa cấp. Tất cả đều nhằm mục đích chiếm đoạt tiền của nhà đầu tư. Năm 2020, ở nước ta đã xảy ra vụ việc liên quan đến các đối tượng lừa đảo mời chào nạn nhân đầu tư vào các dự án tiền điện tử với lợi nhuận lên đến 50% mỗi tháng. Sau khi nạn nhân chuyển tiền vào các tài khoản được cung cấp, họ không thể rút tiền hoặc thu hồi vốn. Các sàn giao dịch này thường không có thực và không thể kiểm tra được, dẫn đến việc hàng nghìn nhà đầu tư mất trắng.

Thứ tư, lừa đảo qua phần mềm độc hại.

Lừa đảo qua phần mềm độc hại là một hình thức tấn công sử dụng phần mềm độc hại để xâm nhập vào thiết bị của nạn nhân và chiếm đoạt tài sản, thông tin cá nhân hoặc tài khoản ngân hàng. Các phần mềm này thường được phân phối qua các tệp đính kèm email, quảng cáo trực tuyến, hoặc các phần mềm tải miễn phí không rõ nguồn gốc. Một khi phần mềm độc hại được cài đặt, nó có thể ghi lại thông tin đăng nhập, theo dõi các hoạt động trực tuyến và thậm chí mã hóa dữ liệu yêu cầu nạn nhân phải trả tiền chuộc để lấy lại. Vào cuối năm 2019 và đầu năm 2020, nhiều tổ chức và doanh nghiệp tại Việt Nam, đặc biệt là các bệnh viện và công ty lớn đã bị tấn công bởi phần mềm độc hại dạng Ransomware. Các đối tượng đã sử dụng các email giả mạo để phát tán phần mềm độc hại, làm tê liệt hệ thống máy tính của các nạn nhân và yêu cầu tiền chuộc để khôi phục dữ liệu. Các cơ quan chức năng đã phát hiện ra rằng các tấn công này chủ yếu được thực hiện qua email lừa đảo và các liên kết chứa phần mềm độc hại.

Thứ năm, lừa đảo sử dụng công nghệ Deepfake và AI.

Deepfake và AI là những công cụ được sử dụng ngày càng phổ biến trong các hành vi lừa đảo trực tuyến. Deepfake là công nghệ sử dụng trí tuệ nhân tạo để tạo ra các video, hình ảnh hoặc âm thanh giả mạo với độ chân thực rất cao. Ví dụ, kẻ lừa đảo có thể tạo ra một video giả mạo giọng nói và hình ảnh của một người nổi tiếng để dụ dỗ người xem tham gia vào các chương trình đầu tư hoặc mua sản phẩm giả mạo. Những video này có thể tạo ra một mức độ tin cậy giả mạo rất cao, khiến nạn

nhân dễ dàng bị đánh lừa. Ngoài ra, AI cũng được sử dụng để tạo ra các tài liệu giả mạo như hợp đồng, email hoặc thông báo từ các tổ chức uy tín khiến nạn nhân dễ dàng bị lừa gạt khi không nhận thấy dấu hiệu của sự giả mạo. Các công nghệ này đang phát triển rất nhanh và có thể gây ra những hậu quả nghiêm trọng nếu không có các biện pháp bảo vệ hiệu quả.

3. Một số giải pháp phòng ngừa, ngăn chặn các thủ đoạn lừa đảo chiếm đoạt tài sản trên không gian mạng

Một là, nâng cao nhận thức và kỹ năng công nghệ thông tin cho người dân. Việc trang bị cho người dân, đặc biệt là những người chưa quen với công nghệ những kiến thức cơ bản về an toàn mạng là bước đầu tiên trong việc phòng ngừa các mối đe dọa từ những hành vi lừa đảo trực tuyến. Các chương trình đào tạo về cách nhận diện các dấu hiệu của tội phạm, cách bảo vệ thông tin cá nhân và cách sử dụng mật khẩu mạnh đều rất quan trọng để giúp cho người dân phòng tránh được những nguy cơ từ các hành vi lừa đảo qua không gian mạng.

Hai là, tăng cường các biện pháp xác thực và mã hóa dữ liệu. Để bảo vệ thông tin cá nhân và tài sản của người dùng, việc áp dụng các biện pháp bảo mật mạnh mẽ như xác thực đa yếu tố (2FA) và mã hóa dữ liệu là vô cùng quan trọng. Xác thực đa yếu tố yêu cầu người dùng phải cung cấp thêm một lớp bảo mật ngoài mật khẩu. Ví dụ như mã OTP gửi qua điện thoại hoặc email. Đây là một giải pháp đơn giản nhưng hiệu quả, giúp ngăn chặn kẻ tấn công lợi dụng mật khẩu yếu để xâm nhập vào tài khoản nhằm thực hiện hành vi phạm tội. Bên cạnh đó, việc mã hóa dữ liệu cũng giúp bảo vệ thông tin quan trọng khỏi việc bị đánh cắp khi truyền qua mạng. Một số ứng dụng như WhatsApp, Signal đã áp dụng mã hóa đầu cuối (End-to-End Encryption) để bảo đảm rằng chỉ người gửi và người nhận mới có thể đọc được nội dung của cuộc trò chuyện.

Ba là, khuyến khích các biện pháp bảo mật mạng máy tính trong doanh nghiệp và tổ chức. Các doanh nghiệp và tổ chức có trách nhiệm lớn trong việc bảo vệ dữ liệu của khách hàng và đối tác. Cần áp dụng các biện pháp bảo mật nghiêm ngặt để bảo vệ thông tin khách hàng, tránh để xảy ra các vụ rò rỉ dữ liệu hoặc tấn công mạng. Các công ty cần triển khai các phần mềm bảo mật, thường xuyên cập nhật hệ thống và đào tạo nhân viên về các mối nguy hiểm tiềm ẩn trên không gian mạng. Đồng thời, các cơ quan chức năng cần tăng cường các chế tài xử phạt các tổ chức, doanh nghiệp, cá nhân cố tình tiết lộ trái phép thông tin của người dùng.

Bốn là, tăng cường ứng dụng công nghệ AI và dữ liệu lớn trong phát hiện những hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng. Công nghệ AI và dữ liệu lớn (Big Data) đóng vai trò quan trọng trong việc phát hiện và ngăn chặn các hành vi lừa đảo trên không gian mạng. Các hệ thống AI có thể phân tích lượng lớn dữ liệu để phát hiện các mẫu hành vi bất thường hoặc các dấu hiệu của lừa đảo. Các công nghệ này có thể nhanh chóng phát hiện các hoạt động đáng ngờ và cảnh báo cho người dùng hoặc tổ chức trước khi thiệt hại xảy ra. ◈

1, 2. Báo cáo tổng kết an ninh mạng năm 2024 (khu vực người dùng cá nhân) của Hiệp hội An ninh mạng quốc gia.