PHÒNG NGỪA TỘI PHẠM LỪA ĐẢO BẰNG CÔNG NGHỆ CAO ĐỐI VỚI SINH VIÊN TRƯỜNG ĐẠI HỌC BÌNH DƯƠNG

Nguyễn Trương Thanh Thảo*, Đỗ Thái Như, Phạm Trần Trung Kiên, Lê Minh Nhựt
Trường Đại Học Bình Dương, *Email: nttthao@bdu.edu.vn

Tóm tắt:

Trong bối cảnh chuyển đổi số nhanh chóng và sự phổ biến rộng rãi của internet cùng các nền tảng mạng xã hội, tội phạm lừa đảo sử dụng công nghệ cao ngày càng gia tăng cả về số lượng lẫn mức độ tinh vi, đặc biệt trong nhóm sinh viên đại học. Nghiên cứu này xem xét thực trạng lừa đảo công nghệ cao nhắm vào sinh viên Trường Đại học Bình Dương thông qua dữ liệu khảo sát và phân tích định tính. Kết quả cho thấy khoảng 90% sinh viên thường xuyên sử dụng điện thoại thông minh và các nền tảng mạng xã hội như Facebook, TikTok và Zalo, khiến họ trở thành nhóm dễ bị tổn thương trước các hành vi lừa đảo trực tuyến. Đáng chú ý, 70% người tham gia khảo sát cho biết đã từng là nạn nhân của lừa đảo trên mạng, với các hình thức phổ biến bao gồm lừa đảo việc làm trực tuyến, giả mạo cơ quan nhà nước hoặc tổ chức tài chính, và các mô hình đầu tư gian lận liên quan đến tiền mã hóa. Trên cơ sở đó, nghiên cứu đề xuất các giải pháp phòng ngừa toàn diện như nâng cao năng lực số, tăng cường giáo dục pháp luật, đẩy mạnh các hoạt động tuyên truyền trong môi trường đại học, và cải thiện sự phối hợp giữa nhà trường với các cơ quan nhà nước.

Từ khóa: *tội phạm công nghệ cao; sinh viên đại học; lừa đảo trực tuyến; kiến thức kỹ thuật số; phương tiện truyền thông xã hội; nhận thức về an ninh mạng*

DOI:

Preventing Fraud Crime Using High Technology For Students Of Binh Duong University

Abstract:

In the context of rapid digital transformation and the widespread use of the internet and social media platforms, cyber-enabled fraud has become increasingly prevalent and sophisticated, particularly among university students. This study examines the current situation of high-tech fraud targeting students at Binh Duong University through survey data and qualitative analysis. The findings reveal that approximately 90% of students frequently use smartphones and social media platforms such as Facebook, TikTok, and Zalo, making them highly vulnerable to online scams. Notably, 70% of respondents reported having been victims of online fraud, with common forms including online job scams, impersonation of authorities or financial institutions, and fraudulent investment schemes involving cryptocurrencies. Based on these findings, the study proposes comprehensive preventive measures, including enhancing digital literacy, strengthening legal education, promoting awareness campaigns within universities, and improving coordination between educational institutions and state authorities.

Keywords: *high-tech crime; university students; online scams; digital literacy; social media; cybersecurity awareness*

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, công nghệ thông tin, internet và các nền tảng mạng xã hội đã và đang trở thành những yếu tố không thể tách rời trong đời sống của sinh viên. Các hoạt động học tập, giao tiếp, giải trí cũng như tìm kiếm cơ hội việc làm ngày càng được thực hiện chủ yếu trên môi trường số. Tuy nhiên, song song với những lợi ích to lớn mà công nghệ mang lại, không gian mạng cũng tiềm ẩn nhiều nguy cơ, đặc biệt là sự gia tăng của các hành vi lừa đảo sử dụng công nghệ cao với thủ đoạn ngày càng tinh vi và khó nhận diện. Trong số các nhóm người dùng, sinh viên được xem là đối tượng có mức độ tiếp cận công nghệ cao nhưng lại chưa có đầy đủ kinh nghiệm và kỹ năng phòng vệ cần thiết, do đó dễ trở thành

mục tiêu của các đối tượng lừa đảo. Thực tế cho thấy nhiều sinh viên đã và đang bị ảnh hưởng bởi các hình thức lừa đảo trực tuyến như giả mạo tổ chức, lừa đảo việc làm, hoặc kêu gọi đầu tư tài chính trên nền tảng số.

Xuất phát từ thực tiễn đó, nghiên cứu này được thực hiện nhằm phân tích một cách hệ thống thực trạng lừa đảo công nghệ cao đối với sinh viên Trường Đại học Bình Dương, đồng thời làm rõ các hình thức phổ biến, mức độ ảnh hưởng và những hạn chế trong nhận thức của sinh viên. Trên cơ sở đó, nghiên cứu hướng tới đề xuất các giải pháp phù hợp nhằm nâng cao hiệu quả phòng ngừa trong môi trường giáo dục đại học.

2. Đặt vấn đề

2.1. Tính cấp thiết của đề tài

Sự phát triển nhanh chóng của công nghệ số trong những năm gần đây đã tạo điều kiện thuận lợi cho các hành vi phạm tội trên không gian mạng, trong đó lừa đảo trực tuyến đang trở thành một vấn đề nổi cộm tại Việt Nam. Theo báo cáo của Cục An toàn thông tin, số vụ lừa đảo trực tuyến trong 6 tháng đầu năm 2023 đã tăng 64,78% so với cùng kỳ năm trước, phản ánh xu hướng gia tăng đáng kể cả về quy mô và mức độ phức tạp của loại tội phạm này (Văn Hoa và Hải Đăng, 2023). Đồng thời, thống kê của Bộ Công an cho thấy hơn 1.500 vụ án liên quan đến lừa đảo công nghệ cao đã được xử lý trong năm 2023, cho thấy tính chất nghiêm trọng và mức độ lan rộng của vấn đề trong xã hội (Báo Chính phủ, 2024).

Trong bối cảnh đó, sinh viên là nhóm đối tượng có nguy cơ cao do đặc điểm thường xuyên sử dụng internet và mạng xã hội trong nhiều mục đích khác nhau, từ học tập, giao tiếp đến tìm kiếm việc làm và tham gia các hoạt động tài chính trực tuyến. Tuy nhiên, phần lớn sinh viên vẫn còn hạn chế về kiến thức pháp luật, kỹ năng nhận diện rủi ro cũng như kinh nghiệm xử lý các tình huống lừa đảo trên không gian mạng.

Thực tiễn tại Trường Đại học Bình Dương cho thấy các hình thức lừa đảo như giả mạo cơ quan nhà nước, tuyển dụng trực tuyến với thu nhập cao, hay các mô hình đầu tư tài chính và tiền mã hóa đang ngày càng phổ biến và có xu hướng gia tăng. Những hành vi này không chỉ gây thiệt hại về tài sản mà còn tác động tiêu cực đến tâm lý, kết quả học tập và môi trường giáo dục của sinh viên

Từ những phân tích trên có thể thấy rằng, việc nghiên cứu thực trạng lừa đảo công nghệ cao đối với sinh viên, xác định các nguyên nhân và đề xuất giải pháp phòng ngừa phù hợp là yêu cầu mang tính cấp thiết cả về lý luận và thực tiễn, góp phần nâng cao năng lực tự bảo vệ của sinh viên trong môi trường số hiện nay.

2.2. Mục tiêu nghiên cứu

Mục tiêu của nghiên cứu là làm rõ các vấn đề lý luận và thực tiễn liên quan đến tội phạm lừa đảo sử dụng công nghệ cao trong bối cảnh chuyển đổi số hiện nay. Trước hết, nghiên cứu tập trung phân tích khái niệm, đặc điểm và các phương thức, thủ đoạn phổ biến của tội

phạm lừa đảo trên không gian mạng, đồng thời làm rõ cơ sở pháp lý điều chỉnh loại tội phạm này theo quy định của pháp luật Việt Nam, đặc biệt là các quy định của Bộ luật Hình sự và Luật An ninh mạng.

Trên cơ sở đó, nghiên cứu tiến hành khảo sát và đánh giá thực trạng sinh viên Trường Đại học Bình Dương bị tác động bởi các hành vi lừa đảo công nghệ cao, bao gồm mức độ tiếp xúc, hình thức lừa đảo phổ biến, mức độ thiệt hại và nhận thức của sinh viên đối với loại tội phạm này. Thông qua việc phân tích thực trạng, nghiên cứu nhằm nhận diện những nguyên nhân, hạn chế và nguy cơ dẫn đến việc sinh viên trở thành nạn nhân của các hành vi lừa đảo trên môi trường số.

Cuối cùng, dựa trên kết quả nghiên cứu lý luận và dữ liệu thực tiễn, đề tài đề xuất các giải pháp phòng ngừa có tính khả thi, phù hợp với đặc thù của môi trường đại học và đối tượng sinh viên, góp phần nâng cao hiệu quả công tác phòng, chống tội phạm lừa đảo công nghệ cao trong môi trường giáo dục.

2.3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của đề tài là các hành vi lừa đảo sử dụng công nghệ cao trên không gian mạng, đặc biệt là các phương thức lừa đảo có ứng dụng công nghệ số, trí tuệ nhân tạo và các nền tảng truyền thông xã hội, đồng thời tập trung phân tích sinh viên Trường Đại học Bình Dương với tư cách là nhóm đối tượng có nguy cơ cao trở thành nạn nhân của loại tội phạm này.

Về phạm vi nghiên cứu, đề tài được triển khai trong môi trường Trường Đại học Bình Dương, tập trung vào các hoạt động học tập, giao tiếp và sử dụng internet của sinh viên. Phạm vi thời gian nghiên cứu được xác định từ năm 2022 đến năm 2026, nhằm đảm bảo việc thu thập và phân tích dữ liệu phản ánh đúng thực trạng các hình thức lừa đảo công nghệ cao trong giai đoạn gần đây.

2.4. Phương pháp nghiên cứu

Để đạt được mục tiêu nghiên cứu, đề tài sử dụng kết hợp nhiều phương pháp nghiên cứu khác nhau nhằm đảm bảo tính toàn diện và khách quan của kết quả nghiên cứu.

Nghiên cứu được thực hiện thông qua phương pháp khảo sát bằng bảng hỏi đối với sinh viên Trường Đại học Bình Dương. Tổng số mẫu khảo sát là 137 sinh viên, được lựa chọn theo phương pháp chọn mẫu thuận tiện. Thời gian thu thập dữ liệu được tiến hành từ tháng 12 năm 2025 đến tháng 03 năm 2026.

Bên cạnh đó, nhóm tác giả còn thực hiện phỏng vấn sâu với khoảng 70 sinh viên nhằm làm rõ hơn các hành vi, nhận thức và trải nghiệm liên quan đến lừa đảo công nghệ cao. Dữ liệu thu thập được xử lý bằng phương pháp phân tích định tính đối với dữ liệu phỏng vấn, từ đó đánh giá thực trạng và đề xuất các giải pháp phòng ngừa phù hợp.

Phương pháp phân tích định tính được sử dụng để làm rõ bản chất, đặc điểm và tác động của tội phạm lừa đảo

công nghệ cao đối với sinh viên thông qua việc phân tích tài liệu, nghiên cứu lý luận và tổng hợp các báo cáo của cơ quan quản lý nhà nước.

Phương pháp phỏng vấn sâu được thực hiện đối với các sinh viên đã từng là nạn nhân hoặc suýt trở thành nạn nhân của lừa đảo công nghệ cao. Nhóm nghiên cứu đã tiến hành phỏng vấn sinh viên Trường Đại học Bình Dương trên cơ sở tự nguyện tham gia nghiên cứu và có trải nghiệm thực tế liên quan đến các hình thức lừa đảo trên môi trường mạng. Nội dung phỏng vấn tập trung vào các vấn đề như phương thức tiếp cận của đối tượng lừa đảo, các thủ đoạn công nghệ được sử dụng (ví dụ: giả mạo danh tính, deepfake, chatbot, website hoặc email giả mạo), cũng như phản ứng và nhận thức của sinh viên trong quá trình xảy ra vụ việc.

Phương pháp quan sát được sử dụng nhằm ghi nhận thực tế việc sử dụng mạng xã hội và các nền tảng giao tiếp trực tuyến của sinh viên trong môi trường học tập, từ đó đánh giá những yếu tố có thể tạo điều kiện cho hành vi lừa đảo phát sinh.

Phương pháp nghiên cứu tình huống được sử dụng để phân tích các vụ việc lừa đảo điển hình có liên quan đến sinh viên hoặc môi trường giáo dục, qua đó làm rõ thủ đoạn của đối tượng phạm tội, hậu quả pháp lý và rút ra các bài học kinh nghiệm phục vụ cho công tác phòng ngừa.

3. Cơ sở lý thuyết và cơ sở pháp lý về phòng ngừa tội phạm lừa đảo bằng công nghệ cao

3.1. Cơ sở lý thuyết nghiên cứu

Nghiên cứu này được xây dựng trên cơ sở kết hợp các lý thuyết tội phạm học và an ninh mạng nhằm giải thích hành vi lừa đảo công nghệ cao trong bối cảnh sinh viên – nhóm đối tượng có mức độ sử dụng internet cao nhưng còn hạn chế về kỹ năng bảo mật.

Trước hết, nghiên cứu vận dụng Lý thuyết Hoạt động Thường ngày (Routine Activity Theory) của Cohen và Felson (1979) [3], theo đó hành vi phạm tội xảy ra khi có sự hội tụ của ba yếu tố: (i) sự tồn tại của đối tượng phù hợp, (ii) sự hiện diện của kẻ phạm tội có động cơ, và (iii) sự thiếu vắng của cơ chế giám sát hiệu quả. Trong môi trường trực tuyến, sinh viên thường xuyên tham gia các hoạt động như sử dụng mạng xã hội, giao dịch trực tuyến và chia sẻ thông tin cá nhân, từ đó trở thành "đối tượng phù hợp". Đồng thời, sự thiếu hụt về kỹ năng nhận diện rủi ro và bảo mật thông tin đóng vai trò như sự "thiếu vắng người giám sát", tạo điều kiện thuận lợi cho các đối tượng lừa đảo thực hiện hành vi phạm tội.

Bên cạnh đó, nghiên cứu cũng tiếp cận từ góc độ lý thuyết social engineering và phishing, nhấn mạnh vai trò của yếu tố tâm lý trong các hành vi lừa đảo. Các cuộc tấn công phishing không chỉ dựa vào yếu tố kỹ thuật mà còn khai thác các đặc điểm nhận thức và hành vi của người dùng, như sự tin

tưởng, thiếu cảnh giác hoặc phản ứng nhanh trước các thông tin mang tính cấp bách (Vishwanath và cộng sự, 2011). Các kỹ thuật social engineering thường sử dụng các kịch bản giả mạo (ví dụ: giả danh cơ quan nhà nước, ngân hàng hoặc người quen) nhằm tạo áp lực tâm lý và thúc đẩy nạn nhân đưa ra quyết định nhanh chóng mà không kiểm chứng thông tin.

Ngoài ra, một số nghiên cứu quốc tế cho thấy thanh niên và sinh viên là nhóm dễ bị tổn thương trước các hình thức lừa đảo công nghệ cao do đặc điểm hành vi như sử dụng internet với tần suất cao, xu hướng chia sẻ thông tin cá nhân và thiếu kinh nghiệm trong việc xử lý các tình huống rủi ro trực tuyến. Điều này củng cố thêm lập luận rằng yếu tố cá nhân và bối cảnh sử dụng công nghệ đóng vai trò quan trọng trong việc gia tăng nguy cơ trở thành nạn nhân.

Trên cơ sở kết hợp các lý thuyết nêu trên, nghiên cứu xây dựng khung phân tích nhằm đánh giá mối quan hệ giữa mức độ nhận thức, hành vi sử dụng internet và nguy cơ bị lừa đảo công nghệ cao của sinh viên, từ đó đề xuất các giải pháp phù hợp nhằm nâng cao khả năng phòng ngừa.

3.2. Khái niệm và đặc điểm của tội phạm lừa đảo công nghệ cao

Theo thống kê từ báo cáo, nghiên cứu khảo sát an ninh mạng 2024 do Ban Công Nghệ, Hiệp Hội An Ninh mạng quốc gia thực hiện vào tháng 12/2024 có nêu như sau:

"Cứ 220 người dùng điện thoại thông minh thì có 1 người là nạn nhân của lừa đảo, thiệt hại ước tính trong năm 2024 lên đến 18.900 tỷ đồng"

Dựa trên các số liệu được công bố của Ban công Nghệ và Hiệp Hội An Ninh Mạng cho thấy: Cứ 220 người dùng điện thoại thì sẽ có 1 người bị lừa đảo, tổng thiệt hại 2024 lên đến 18.900 tỉ đồng. Một số liệu rất đáng quan ngại thể hiện được thực trạng đang ngày càng tăng mạnh ở phạm vi quốc gia. Xem xét số liệu thống kê ứng với tổng dân số quốc gia hiện tại là 101.112.656 người – đứng thứ 3 Đông Nam Á, thứ 16 thế giới (Tổng cục Thống Kê Việt Nam, 2024). Điều này cho thấy tầm quan trọng của vấn đề và cần phải được quan tâm và xem xét ngay. Bên cạnh đó, sự phổ biến của của thiết bị di động cũng là một trong những lý do dẫn đến tình trạng này, vì chúng như một thứ tất yếu của đời sống con người, do đó tạo nhiều cơ hội cho tội phạm lợi dụng để trục lợi cho bản thân. Do đó, cần đặt ra câu hỏi về nguyên nhân khiến các đối tượng phạm tội có xu hướng chuyển sang sử dụng công nghệ cao trong hoạt động lừa đảo.Và đáng lo ngại hơn môi trường mạng là nơi mà các bạn sinh viên tiếp xúc thường xuyên với mật độ cao, nếu như không cẩn trọng và thiếu đi kĩ năng giải quyết vấn đề thì sẽ dễ dàng trở thành nạn nhân của các đối tượng phạm tội.

Tội phạm lừa đảo công nghệ cao là hình thức tội phạm lừa đảo trên không gian kĩ thuật số, bằng cách sử dụng kĩ

thuật và công nghệ cao để xâm hại đến các mối quan hệ được pháp luật bảo vệ.

Căn cứ theo khoản 1 điều 3 Nghị định số 25/2014/NĐ-CP có quy định rõ về khái niệm của tội phạm sử dụng công nghệ cao như sau:

"Tội phạm có sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao" (Nghị định 25/2014)

3.3. Các dạng lừa đảo công nghệ cao phổ biến ở sinh viên

Dựa trên thời gian nghiên cứu và khảo sát, nhóm nghiên cứu nhận thấy rằng. Hiện nay tại Việt Nam có những dạng lừa đảo qua công nghệ cao nhắm vào đối tượng là sinh viên như sau:

Lừa đảo việc làm online

Lừa đảo chiếm đoạt tài sản mạng xã hội

Lừa đảo đầu từ tài chính – tiền ảo

Lừa đảo cơ quan nhà nước, ngân hàng, trường học.

a) Lừa đảo việc làm online

Về hình thức: Các đội tượng phạm tội thường có xu hướng giả danh thành các sàn để tuyển nhân viên cho các công việc nhẹ lương cao như tuyển cộng tác viên bán hàng – tiếp thị liên kết, mạo danh ngân hàng hoặc các công ty công nghệ để tuyển nhân viên hoặc đi làm nhiệm vụ online để kiếm hoa hồng…. Đặc điểm chung của những hình thức lừa đảo trên là đều sử dụng những yêu cầu đơn giản cùng những lợi nhuận cao để dẫn dụ nạn nhân vào bẫy như là "chỉ cần có điện thoại", "làm kiếm thêm không cần vốn"… và rồi các đối tượng sau khoảng thời gian trả thật sẽ bắt đầu yêu cầu những chi phí bên ngoài như là yêu cầu mua hàng trước hoặc nạp tiền để "đặt cọc trước" – đối với hình thức tuyển cộng tác viên bán hàng, còn đối với làm việc tại nhà kiếm thêm thì sẽ yêu cầu đóng tiền nhập nguyên liệu, phí vận chuyển trước (thường sẽ là gấp bao lì xì, dán tem, cắt tem mạc,…thường xuất hiện nhiều ở dịp Tết đến)

Về tâm lý: Về mặt chủ quan của nạn nhân, các bạn sinh viên – đặc biệt là tân sinh viên thường có tâm lý muốn tự lập sớm với nhiều lý do khách quan nhau như: muốn tự lập để giảm gánh nặng cho ba mẹ, muốn tự chủ tài chính để mua thứ mình thích, muốn tận dụng thời gian rảnh để kiếm tiền tiết kiệm hoặc là chạy theo thị trường và phong trào khi mang trên mình "hội chứng sợ bị bỏ lỡ" – tức FOMO. Qua đó những vấn đề tâm lý trên gián tiếp dùng các đối tượng lừa đảm tiếp cận và thực hiện hành vi vi phạm pháp luật.

Hậu quả về phương diện tài chính, các hành vi lừa đảo có thể dẫn đến thiệt hại nghiêm trọng, trong nhiều trường hợp nạn nhân bị chiếm đoạt toàn bộ số tiền đã giao dịch.Qua đó kéo theo nhiều vấn đề khác như tâm lý bị ảnh hưởng gây ảnh hưởng rất lớn đối với những tân sinh viên lần đầu bước lên giảng đường đại học. Tiếp đến là kéo theo vấn đề xã hội khi người thân thì cãi vả, một số

trường hợp còn bị đe doạ khi chậm trễ. Và đáng lo ngại nhất là ở vấn đề an ninh. Nhiều tỉnh (Cần Thơ, TP.HCM, Bình Dương, Long An…) ghi nhận hàng trăm vụ sinh viên bị lừa, tổng thiệt hại hàng chục tỷ chỉ riêng hình thức CTV online.

b) Lừa đảo chiếm đoạt tài sản mạng xã hội

Về hình thức: Đây là hình thức lừa đảo mà đối tượng phạm tội sử dụng các thiết bị công nghệ cao để tấn công vào nhóm nạn nhân có khả năng nhận diện và cảnh giác công nghệ số thấp. Vì đặc thù của công nghệ rất phổ biến và khó kiểm soát được ngay từ những lần đầu sử dụng vì vậy ở đây nạn nhân của các đối tượng lừa đảo là rất lớn, trải dài ở mọi lứa tuổi, và là vì đặc thù trên môi trường công nghệ số nên gần như không có khó khăn về lãnh thổ và ngôn ngữ - cho nên nạn nhân có thể là người ngoại quốc định cư tại Việt Nam, qua đó gây ảnh hưởng đến hình ảnh và an ninh tổ quốc. Tuy nhiên, phổ biến nhất vẫn là đối với các đối tượng sinh viên. Bởi lẽ các bạn trẻ nói chung và sinh viên nói riêng là những đối tượng sử dụng các thiết bị di động công nghệ cao nhiều nhất (điện thoại di động, máy tính bảng, máy tính xách tay,..). Các đối tượng phạm tội có xu hướng sử dụng công nghệ cao nhằm chiếm đoạt quyền sử dụng với tài sản mạng xã hội với các thủ thuật như giả danh thành trai/gái với sự can thiệp của công nghệ để thực hiện hình thức lừa tình cảm (Romance scam). Sử dụng các lỗ hổng pháp lý về tiền mã hoá để lợi dụng các bạn sinh viên vào công việc đầu tư tiền ảo bằng cách tạo các nhóm, các diễn đàn ở mạng xã hội như Facebook, Telegram, X,… dụ dỗ nạp thêm tiền để đầu tư và lợi dụng để chiếm đoạt tài sản.

Về tâm lý: Xuất phát từ những tâm lý cơ bản nhất của con người trong từ khách quan khác nhau. Đối với các bạn sinh viên có thể sẽ mong cầu tình cảm trong một môi trường mới – đặc biệt là các bạn sinh viên nam dễ dàng trở thành nạn nhân của những chuyện "tình ảo" trên mạng xã hội rồi trở thành nạn nhân khi bị chiếm đoạt tài sản. Dưới tác động của nhu cầu tự chủ tài chính và kỳ vọng đạt được thu nhập cao trong thời gian ngắn, nhiều sinh viên có xu hướng tham gia sớm vào các hoạt động đầu tư tài chính như chứng khoán và tiền mã hóa. Tuy nhiên, do hạn chế về kiến thức chuyên môn và kinh nghiệm thực tiễn, họ dễ rơi vào trạng thái thiếu kiểm soát rủi ro và trở thành nạn nhân của các hành vi lừa đảo công nghệ cao.

Về hậu quả: Về kinh tế, mất trắng tiền mặt sau đó dẫn theo các tổn thương tâm lý sâu sắc – nhất là khi đang ở một môi trường một nơi mà không có gia đình ở gần. Về an ninh, nhiều bạn sinh viên khi đã dồn hết tất cả vào công cuộc đầu tư chứng khoán , tiền ảo để rồi bị lừa sẽ có thể dẫn đến trầm cảm và cực đoan hơn là có ý nghĩ thực hiện các hành vi gây hại đến bản thân trong những trường hợp nghiêm trọng , gây ra hậu quả về mạng người và an ninh khu vực nghiêm trọng.

c) Lừa đảo đầu tư tài chính – tiền ảo

Về hình thức: Đây là hình thức mà các đối tượng lừa đảo sẽ chủ động tạo các sàn giao dịch điện tử giả mạo, các dự án tiền ảo mang tính đa cấp và một hình thức đặc biệt khác là Romance scam kết hợp với lừa đầu tư tiền ảo qua đó thực hiện hành vi chiếm đoạt tài sản. Hình thức này tấn công vào mục tiêu cần giàu nhanh, giàu sớm của một bộ phận sinh viên trong thời buổi hiện nay. Do đó, không ít sinh viên đã trở thành nạn nhân của hình thức này.

Về tâm lý: Ngày này một số các bạn sinh viên, đặc biệt là tân sinh viên cố chạy theo phong trào xã hội, là nạn nhân của hội chứng "sợ bị bỏ lỡ" – FOMO. Điều này thúc đẩy các bạn có một động lực kiếm tiền nhanh - gọn - nhiều và từ đó thị trường Crypto trở thành nơi mà các đối tượng phạm tội nhắm tới để thực hành vi vi phạm pháp luật thông qua việc tấn công vào sự háo thắng và nền tảng kiến thức yếu kém về lĩnh vực tiền mã hoá mà các bạn sinh viên đang đua nhau đầu tư. Nhiều hình thức khác còn đánh vào tâm lý muốn được yêu như hình thức kết hợp Romance scam và lừa đầu tư tiền ảo/chứng khoán

Về hậu quả: Về kinh tế, mất trắng tiền mặt sau đó dẫn theo các tổn thương tâm lý sâu sắc – nhất là khi đang ở một môi trường một nơi mà không có gia đình ở gần. Về an ninh, nhiều bạn sinh viên khi đã dồn hết tất cả vào công cuộc đầu tư chứng khoán , tiền ảo để rồi bị lừa sẽ có thể dẫn đến trầm cảm và cực đoan hơn là có ý nghĩ thực hiện các hành vi gây hại đến bản thân trong những trường hợp nghiêm trọng, gây ra hậu quả về mạng người và an ninh khu vực nghiêm trọng.

d) Lừa cơ quan nhà nước, ngân hàng, trường học

Về hình thức: Đây là một hình thức có mức độ phổ biến cao, không chỉ tập trung vào sinh viên mà còn nhiều lứa tuổi khác. Đây là hình thức phổ biến không chỉ ở sinh viên mà gần như ở mọi lứa tuổi – đặc biệt là những nạn nhân có tâm lý sợ pháp luật và thiếu khả năng nhận dạng kiến thức hành chính, các đối tượng dễ dàng giả danh các đơn vị hành chính hay các cơ quan chức năng, ngân hàng, hay gần gũi nhất là chính trường đại học của sinh viên thì sẽ dễ dàng đưa nạn nhân vào bẫy để thực hiện hành vi vi phạm pháp luật.

Về tâm lý: Hình thức lừa đảo này tấn công vào điểm yếu của nạn nhân ở đây là khả năng nhận diện và nền tảng kiến thức pháp lý thấp, đặc biệt là kiến thức về thủ tục hành chính. Ngoài ra đó còn là tâm lý chủ quan và tâm lý sợ cơ quan nhà nước. Những điểm trên đã khiến cho hình thức này vô cùng nguy hại cho sinh viên khi phần trăm trở thành nạn nhân là rất cao.

Về hậu quả: Về kinh tế thì mất trắng hoàn toàn số tiền, ngoài ra còn dẫn thêm các tổn thương tâm lý dài hạn. Tuy nhiên hậu quả nghiêm trọng nhất, là đặc thù của hình thức này là sẽ khiến sinh viên nói chung và người dân không còn niềm tin vào các cơ quan nhà nước và các cơ quan hành chính. Qua đó hình thành tâm lý nghi ngờ cho xã hội, gây khó khăn

trong công tác ổn định xã hội của quốc gia.

3.4. Cơ sở pháp lý điều chỉnh

Trong quá trình nghiên cứu, nhóm tác giả nhận thấy, hành vi lừa đảo sinh viên bằng công nghệ cao được thực hiện dưới những hình thức như: lừa công việc làm online; lừa chiếm đoạt tài sản trên mạng xã hội , lừa đầu tư tài chính / tiền ảo, lừa giả danh cơ quan nhà nước, ngân hàng và trường học thì các đặc điểm tâm sinh lý của sinh viên chỉ đóng vai trò điều kiện, hoàn cảnh làm tăng tính dễ tổn thương, qua đó tạo thuận lợi cho việc thực hiện thủ đoạn gian dối để chiếm đoạt tài sản. Bên cạnh đó, khách thể của tội phạm hướng tới là quyền sở hữu tài sản của cá nhân hoặc tổ chức. Những hành vi, hình thức lừa đảo sinh viên bằng công nghệ cao thoả mãn cấu thành tội phạm Lừa đảo chiếm đoạt tài sản theo Điều 174 BLHS, vì những lí do sau:

Một là, đặc trưng của tội lừa đảo chiếm đoạt tài sản là người phạm tội sử dụng thủ đoạn gian dối (thông qua lời nói, hành động, việc làm, mối quan hệ, có thể sử dụng kết các công cụ, phương tiện khác,….) khiến cho bị hại tin tưởng nghĩ đó là sự thật và tự nguyện giao tài sản cho người phạm tội. Vì vậy khách thể xâm phạm ở đây là Quyền sỡ hữu tài sản của nạn nhân.

Hai là, về chủ thể của tội Lừa đảo chiếm đoạt tài sản ở điều 174 BLHS là chủ thể phổ thông từ 16 tuổi trở lên không phân biệt về chức vụ, quyền hạn nhưng phải có năng lực hành vi dân sự đầy đủ. Mặt chủ quan của tội đây là lỗi cố ý trực tiếp vì nhận thức rõ hành vi gian dối, hành vi trái pháp luật, thấy trước hậu quả và mong muốn hậu quả xảy ra.

Ngoài ra, dấu hiệu bắt buộc của tội này là phải có hành vi gian dối thì mới cấu thành tội phạm để phân biệt với tội Lợi dụng tín nhiệm chiếm đoạt tài sản điều 175 BLHS. Giá trí tài sản là dấu hiệu định khung, nhưng vẫn thuộc mặt khách quan. Người phạm tội không cần phải là người trực tiếp nhận tài sản mà có thể để người khác nhận thay.

Theo quy định tại Điều 174 BLHS, tội lừa đảo chiếm đoạt tài sản được cấu trúc thành bốn khung hình phạt chính, với mức án được xác định chủ yếu dựa trên giá trị tài sản chiếm đoạt và các tình tiết định khung tăng nặng. Cụ thể, khoản 1 áp dụng khung cơ bản (cải tạo không giam giữ đến 03 năm hoặc tù từ 06 tháng đến 03 năm) đối với hành vi chiếm đoạt từ 2.000.000 đồng đến dưới 50.000.000 đồng (hoặc dưới 2.000.000 đồng nhưng thuộc một trong các trường hợp tái phạm, gây ảnh hưởng an ninh trật tự, hoặc tài sản là phương tiện kiếm sống chính của bị hại). Khung 2 (tù từ 02 đến 07 năm) dành cho các trường hợp có tổ chức, tính chất chuyên nghiệp, chiếm đoạt từ 50.000.000 đồng đến dưới 200.000.000 đồng, tái phạm nguy hiểm, lợi dụng chức vụ hoặc thủ đoạn xảo quyệt. Khung 3 (tù từ 07 đến 15 năm) áp dụng khi giá trị tài sản từ 200.000.000 đồng đến dưới 500.000.000 đồng hoặc lợi dụng thiên tai, dịch bệnh. Khung 4 (tù từ 12 đến 20 năm hoặc tù chung thân) dành cho hành vi chiếm đoạt 500.000.000 đồng trở lên hoặc lợi dụng hoàn cảnh chiến tranh, tình trạng khẩn cấp. Ngoài hình phạt chính, người phạm

tội còn có thể bị áp dụng hình phạt bổ sung là phạt tiền từ 10.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 đến 05 năm.

Trong thực tiễn xét xử tại các Tòa án nhân dân các cấp giai đoạn 2024–2026, mức hình phạt được áp dụng linh hoạt, chú trọng nguyên tắc cá thể hóa trách nhiệm hình sự theo các tình tiết tăng nặng (Điều 52 BLHS) và giảm nhẹ (Điều 51 BLHS). Các vụ án thuộc khung 1 thường được tuyên án từ 09 đến 24 tháng tù, trong đó nhiều trường hợp được hưởng án treo hoặc cải tạo không giam giữ nếu bị cáo thành khẩn, tự nguyện khắc phục hậu quả và bồi thường cho bị hại. Các vụ thuộc khung 2 và 3 chiếm tỷ lệ cao nhất, với mức án phổ biến từ 03 đến 08 năm tù, đặc biệt trong các vụ lừa đảo qua mạng, sử dụng công nghệ cao hoặc có tổ chức. Khung 4 chỉ áp dụng cho các vụ án đặc biệt nghiêm trọng, thường kết hợp với hình phạt bổ sung và buộc hoàn trả toàn bộ tài sản theo khoản 1 Điều 48 BLHS. Tuy nhiên, thực tiễn cũng cho thấy tỷ lệ thu hồi tài sản bị chiếm đoạt vẫn còn hạn chế, trong khi một số bất cập như mức định lượng tối thiểu 2.000.000 đồng chưa phù hợp với điều kiện kinh tế hiện nay dẫn đến tình trạng xử lý hình sự nhiều vụ án giá trị nhỏ, gây tốn kém nguồn lực tố tụng. Những phân tích trên cho thấy khung hình phạt của Điều 174 đã góp phần răn đe tội phạm, song cần tiếp tục hoàn thiện để nâng cao hiệu quả thực thi trong bối cảnh tội lừa đảo chiếm đoạt tài sản ngày càng tinh vi và phức tạp.

Một ví dụ điển hình là bản án số 01/2025/HS-ST của Tòa án nhân dân thành phố Bến Cát (nay là Tòa án nhân dân Khu vực 18 - Thành phố Hồ Chí Minh), trong đó bị cáo Trương Thanh Q đã thực hiện hành vi gian dối chiếm đoạt tài sản của bị hại trị giá 55.520.000 đồng. Hành vi này đủ yếu tố cấu thành tội "Lừa đảo chiếm đoạt tài sản"theo điểm c khoản 2 Điều 174 BLHS (chiếm đoạt tài sản trị giá từ 50.000.000 đồng đến dưới 200.000.000 đồng). Xét thấy bị cáo có tình tiết giảm nhẹ là thành khẩn khai báo (điểm s khoản 1 Điều 51 BLHS), Hội đồng xét xử đã tuyên phạt bị cáo 03 năm tù về tội danh trên. Đồng thời, căn cứ Điều 56 BLHS, Tòa án tổng hợp với hình phạt 06 năm tù của Bản án hình sự sơ thẩm số 33/2025/HS-ST ngày 24/02/2025 của Tòa án nhân dân huyện Định Quán (nay là Tòa án nhân dân Khu vực 7 - Đồng Nai), buộc bị cáo phải chấp hành hình phạt chung là 09 năm tù (Thư viện Pháp luật, 2025).

Vụ việc này phản ánh xu hướng áp dụng thực tiễn của Tòa án: dù thuộc khung hình phạt từ 02 đến 07 năm tù, mức án cụ thể vẫn được cá thể hóa phù hợp với mức độ nguy hiểm của hành vi, nhân thân bị cáo và khả năng cải tạo, đồng thời thể hiện việc kết hợp nhiều bản án khi bị cáo có tiền án. Việc buộc chấp hành hình phạt chung cũng góp phần đảm bảo tính nghiêm minh của pháp luật hình sự trong xử lý các trường hợp tái phạm hoặc phạm tội nhiều lần.

Ngoài ra, nhóm tác giả có nhận thấy được rằng hành vi lừa đảo sinh viên bởi các hình thức trên hoàn toàn có thể cấu thành tội Sử dụng mạng máy tính, viễn

thông để chiếm đoạt tài sản theo Điều 290 BLHS, vì những lí do sau

Một là, về khách thể xâm phạm. Đặc trưng của Tội Lừa đảo chiếm đoạt tài sản Điều 174 BLHS thì khách thể xâm phạm hướng tới là quyền sở hữu tài sản. Trong khi khách thể của Tội Sử dụng mạng máy tính, viễn thông để chiếm đoạt tài sản thì ngoài việc chiếm đoạt tài sản như Điều 174 BLHS, còn xâm phạm các hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, môi trường giao dịch điện tử, hoạt động thương mại điện tử, kinh doanh tiền tệ, huy động vốn tín dụng, mua bán và thanh toán cổ phiếu qua mạng.

Hai là, về hành vi khách quan của tội Sử dụng mạng máy tính, mạng viễn thông để chiếm đoạt tài sản được thể hiện ở một trong các hành vi sau:

"a) Sử dụng thông tin về tài khoản, thẻ ngân hàng của cơ quan, tổ chức, cá nhân để chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hoá, địch vụ:

b) Làm, tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả nhằm chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hoá, dịch vụ:

c) Truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản

d) Lừa đảo trong thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp hoặc giao dịch chứng khoán qua mạng nhằm chiếm đoạt tài sản

đ) Thiết lập, cung cấp dịch vụ viễn thông, Internet nhằm chiếm đoạt tài sản" (Bộ luật Hình sự, 2015)

Theo quy định tại Điều 290 Bộ luật Hình sự 2015 (sửa đổi, bổ sung năm 2017), tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản được cấu trúc với bốn khung hình phạt chính, áp dụng khi hành vi không thuộc tội trộm cắp tài sản (Điều 173) hoặc tội lừa đảo chiếm đoạt tài sản (Điều 174). Khung cơ bản (khoản 1) quy định mức phạt cải tạo không giam giữ đến 03 năm hoặc tù từ 06 tháng đến 03 năm. Khung 2 (tù từ 02 đến 07 năm) áp dụng đối với các trường hợp có tổ chức, tính chất chuyên nghiệp, tái phạm nguy hiểm, chiếm đoạt từ 50.000.000 đồng đến dưới 200.000.000 đồng hoặc gây thiệt hại tương ứng. Khung 3 (tù từ 07 đến 15 năm) dành cho trường hợp chiếm đoạt từ 200.000.000 đồng đến dưới 500.000.000 đồng hoặc gây thiệt hại lớn. Khung 4 (tù từ 12 đến 20 năm) áp dụng khi chiếm đoạt 500.000.000 đồng trở lên hoặc gây thiệt hại đặc biệt lớn. Ngoài hình phạt chính, người phạm tội còn có thể bị áp dụng hình phạt bổ sung là phạt tiền từ 20.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề từ 01 đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

Trong thực tiễn xét xử giai đoạn 2019–2023, tội phạm theo Điều 290 thuộc nhóm tội phạm công nghệ thông tin và mạng viễn thông có xu hướng tăng mạnh về số lượng vụ việc. Theo thống kê của Tòa án nhân dân tối cao, toàn quốc đã giải quyết 536 vụ với 1.133 bị cáo thuộc nhóm tội này, trong đó năm

2023 ghi nhận cao nhất với 202 vụ và 449 bị cáo.Tù có thời hạn là hình phạt chính được áp dụng phổ biến nhất, chiếm 85,94% tổng số bị cáo (758/882 bị cáo). Cụ thể, khoảng 20,71% bị cáo được hưởng án treo; 39,58% bị tuyên tù dưới 03 năm; 15,04% bị tù từ 03 đến 07 năm; 21,9% bị tù từ 07 đến 15 năm; và 3,3% bị tù từ 15 đến 20 năm (sau khi tổng hợp hình phạt) (Bộ luật Hình sự, 2015). Tòa án thường chú trọng nguyên tắc cá thể hóa trách nhiệm hình sự theo Điều 51 và Điều 52 BLHS, ưu tiên áp dụng tình tiết giảm nhẹ (thành khẩn khai báo, tự nguyện khắc phục hậu quả), dẫn đến nhiều vụ thuộc khung 1–2 được tuyên án treo hoặc mức án thấp. Tuy nhiên, thực tiễn cũng cho thấy một số bất cập như ranh giới định tội giữa Điều 290 với Điều 174 chưa rõ ràng (đặc biệt với các vụ lừa đảo qua mạng), tỷ lệ thu hồi tài sản thấp do tính chất ảo của chứng cứ điện tử, cùng với số lượng vụ việc khởi tố tội phạm mạng năm 2023 khoảng 1.500 vụ. Những phân tích trên cho thấy khung hình phạt của Điều 290 đã góp phần răn đe tội phạm sử dụng công nghệ cao, song cần tiếp tục hoàn thiện để khắc phục chồng chéo định tội và nâng cao hiệu quả áp dụng trong bối cảnh tội phạm mạng ngày càng tinh vi và phức tạp.

Một ví dụ điển hình là bản án số 03/2025/HS-ST của toà án nhân dân khu vực thành phố Hà Nội (nay là khu vực 08 - Hà nội), tuyên án vào ngày 29/07/2025. Trong đó, bị cáo Đỗ Quốc V đã có hành sử dụng thiết bị di động của nạn nhân để truy cập vài tài khoản ngân hàng cá nhân mở tại Ngân hàng kỹ thương Việt Nam (Techcombank, TCB) để chiếm đoạt 2 lần với tổng số tiền là 210.00.000 đồng (trong đó với lần thứ 1 là 60.000.000 đồng, lần thứ 2 là 150.000.000 đồng). Hành vi nêu trên của V đã đủ yếu tố cấu thành tội Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi chiếm đoạt tài sản điều 290 BLHS. Cụ thể là điểm a khoản 3 điều 290 BLHS (Hiệp hội An ninh mạng quốc gia, 2025)

Các hành vi này còn cấu thành các tội về các hành vi bị nghiêm cấm ở không gian mạng theo điều 7 của Luật An ninh mạng. Thể hiện qua các giai đoạn tạo sàn giao dịch điện tử giả, xây dựng trang web giả đề tiếp cận sinh viên,…

Cùng với đó là những văn bản hướng dẫn và chính sách phòng chống tội phạm công nghệ cao được ban hành như:

Công điện số 139/CĐ-TTg ngày 23/12/2024: Về việc tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao, trên không gian mạng

Nghị định số 13/2023/NĐ-CP ngày 17/4/2023: Quy định về việc bảo vệ dữ liệu cá nhân

Nghị định số 356/2025/NĐ-CP ban hành ngày 31/12.2025: Quy định về việc các biện pháp thi hành luật bảo vệ dữ liệu cá nhân

Nghị định số 147/2024/NĐ-CP ban hành ngày 20/11/2024: Quy định về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, đóng vai trò quan trọng trong việc xác thực tài khoản mạng xã hội, giảm thiểu tài khoản rác sử dụng để lừa đảo.

Yêu cầu các bộ, ngành, địa phương đẩy mạnh phòng ngừa, xây dựng mô hình phối hợp liên ngành (Bộ Công an chủ trì), xây dựng cơ sở dữ liệu tài khoản nghi vấn lừa đảo (hoàn thành quý I/2025), cảnh báo kịp thời, thu hồi tài sản. Đây là văn bản nền tảng được nhắc lại và triển khai xuyên suốt 2025-2026.

Công điện số 29/CĐ-TTg ngày 03/4/2025: Về đẩy mạnh công tác phòng ngừa, xử lý hoạt động sử dụng công nghệ cao trên không gian mạng để lừa đảo chiếm đoạt tài sản.

Yêu cầu thực hiện nghiêm Công điện 139, tăng cường tuyên truyền, phối hợp ngân hàng phong tỏa tài khoản nghi vấn, xử lý SIM rác, tài khoản ảo dùng lừa đảo. Nhấn mạnh khắc phục tình trạng lừa đảo tinh vi hơn.

4. Thực trạng lừa đảo công nghệ cao đối với sinh viên trường Đại học Bình Dương

4.1. Thực trạng nhận thức của sinh viên

Hiện nay tại trường đã xuất hiện những thông tin sai sự thật, không chính thống của quý nhà trường, tuy nhiên vẫn ghi nhận được trường hợp sinh viên bị lừa đảo chứng tỏ một thực trạng cần được quan tâm. Điều đó cho thấy rằng, không chỉ là sinh viên đối với trường đại học Bình Dương. Sinh viên là nhóm đối tượng dễ bị ảnh hưởng do thói quen sử dụng mạng xã hội cao (TikTok, Facebook, Zalo), ít kinh nghiệm tài chính, và tâm lý mong muốn kiếm tiền nhanh hoặc dễ tin vào cơ hội "lương cao online. Theo thống kê của Hiệp hội An ninh mạng quốc gia Việt Nam, chỉ riêng trong năm 2024 đã ghi nhận hơn 1.200 vụ lừa đảo trực tuyến nhắm tới đối tượng học sinh, sinh viên, cho thấy nhóm người trẻ đang trở thành mục tiêu phổ biến của các đối tượng phạm tội trên không gian mạng[10]. Các hoạt động tuyên truyền tại các trường đại học (như Đại học Cần Thơ, UEH, Đại học Công nghiệp TP.HCM) thường xuyên được tổ chức để nâng cao nhận thức, nhưng thực tế cho thấy vẫn tồn tại "điểm mù nhận thức" ở nhóm trẻ.

Nguyên nhân đến từ mức độ hiểu biết và khả năng nhận diện, kiểm chứng thông tin trên nền tảng không gian mạng của sinh viên chưa được trang bị, cũng như là tâm lý non nớt và sự thiếu hiểu biết về an ninh mạng, thủ tục hành chính và kĩ năng sử dụng công nghệ còn yếu.

Dựa trên khảo sát của nhóm nghiên cứu, chúng tôi xin đưa ra những luận điểm như sau:

Thói quen tiếp xúc và rủi ro cao:

90% sử dụng chủ yếu điện thoại, nơi dễ tiếp nhận tin nhắn lừa đảo, link độc hại.

90% thường xuyên dùng TikTok, Facebook, Zalo (bao gồm trong công việc), chỉ 20% dùng email/Instagram – điều này khớp với thống kê quốc gia: hơn 70-80% lừa đảo đến từ mạng xã hội như Zalo/Facebook.

Tỉ lệ từng là nạn nhân và hình thức phổ biến

70% sinh viên từng bị lừa đảo – tỷ lệ cao hơn mức trung bình cộng đồng (khoảng 0,18-0,45% theo NCA), cho thấy sinh viên dễ bị ảnh hưởng hơn.

Trong số nạn nhân:

75% bị lừa "làm việc online" (lương cao, việc nhẹ) – hình thức phổ biến nhắm vào sinh viên do nhu cầu kiếm thêm. 25% bị lừa đầu tư tài chính/tiền ảo, chiếm đoạt tài khoản MXH, chuyển tiền.

Mức thiệt hại chủ yếu nhẹ: 80% dưới 1 triệu đồng, 15% 1-5 triệu, 5% trên 5 triệu – phù hợp với đối tượng sinh viên có thu nhập hạn chế, nhưng vẫn gây tổn thất tích lũy lớn.

Mức độ nhận thức và khả năng phòng ngừa

Hiểu rõ các hình thức lừa đảo công nghệ cao: 80% ở mức "Bình thường" (không sâu), 20% còn lại phân bổ đồng ý/không đồng ý → Nhận thức chung ở mức trung bình, chưa sâu sắc.

Khả năng nhận diện dấu hiệu lừa đảo: 70% "Bình thường", 20% đồng ý (tự tin), 10% không đồng ý (yếu) → Phần lớn tự đánh giá trung bình, nhưng thực tế vẫn dễ "sập bẫy" do thiếu kỹ năng thực hành.

Biết quy định pháp luật liên quan: 40% "Bình thường", 50% không biết, 10% biết (chủ yếu sinh viên học luật) → Đây là điểm yếu lớn, vì thiếu kiến thức pháp lý dẫn đến không biết cách xử lý khi bị lừa (báo công an, khóa tài khoản…).

Dựa trên các khảo sát của nhóm nghiên cứu thì có thể nhận rằng thực trạng cho thấy sinh viên tại Bình Dương nói riêng và sinh viên Việt Nam nói chung có mức độ tiếp xúc cao với rủi ro lừa đảo công nghệ cao, tỷ lệ từng là nạn nhân lớn (70%), nhưng nhận thức chỉ ở mức trung bình, đặc biệt về pháp luật và kỹ năng nhận diện sâu. Dù thiệt hại thường nhỏ lẻ, nhưng tích lũy gây ảnh hưởng tâm lý, tài chính và niềm tin xã hội. So với bối cảnh quốc gia (thiệt hại hàng nghìn tỷ, hình thức ngày càng tinh vi như deepfake), sinh viên cần được ưu tiên giáo dục hơn.

Từ kết quả khảo sát trên, có thể thấy nguy cơ sinh viên trở thành nạn nhân của lừa đảo công nghệ cao không chỉ xuất phát từ mức độ tiếp xúc cao với môi trường số mà còn chịu tác động tổng hợp của nhiều yếu tố. Trên cơ sở đó, nghiên cứu đề xuất khung phân tích gồm ba nhóm yếu tố chính: (i) nhận thức và hiểu biết pháp luật; (ii) hành vi sử dụng mạng xã hội và môi trường số; (iii) yếu tố tâm lý như nhu cầu tài chính và hội chứng sợ bị bỏ lỡ (FOMO). Các yếu tố này có mối quan hệ tương tác, trong đó nhận thức đóng vai trò nền tảng, hành vi là yếu tố trung gian và tâm lý là yếu tố thúc đẩy, qua đó làm gia tăng nguy cơ bị lừa đảo.

4.2. Thực trạng sinh viên bị tấn công

Nguyên nhân chủ yếu là do tâm lý muốn được tự chủ kinh tế, có bạn thì muốn giúp ba mẹ, có bạn thì muốn tự lập cũng như là tâm lý muốn tìm được một mức lương cao ổn định nên các bạn tự chủ động tìm đến những lời giới thiệu béo bở nhưng lại không có kĩ năng nhận diện và phòng tránh dấu hiện lừa đảo.

Các hình thức thường được gặp theo nhóm nghiên cứu phỏng vấn là lừa đảo công việc online, lừa đảo chiếm đoạt tài sản trên mạng xã hội. Các công nghệ được tiếp xúc nhiều nhất là thiết bị di động như điện thoại, máy tính xách tay.

Một trường hợp điển hình được ghi nhận thông qua phỏng vấn sâu là sinh

viên năm nhất bị lừa đảo thông qua hình thức tuyển dụng cộng tác viên bán hàng trực tuyến. Đối tượng lừa đảo tiếp cận nạn nhân thông qua mạng xã hội với lời mời công việc "việc nhẹ, thu nhập cao, không cần kinh nghiệm". Ban đầu, sinh viên được yêu cầu thực hiện các nhiệm vụ đơn giản như đặt đơn hàng ảo và được hoàn tiền kèm hoa hồng để tạo lòng tin. Sau một vài lần giao dịch thành công, đối tượng bắt đầu yêu cầu nạn nhân chuyển số tiền lớn hơn với lý do "mở khóa nhiệm vụ có giá trị cao hơn". Do đã tin tưởng vào hệ thống trước đó, sinh viên tiếp tục chuyển tiền nhưng sau đó không thể rút lại số tiền đã nạp và bị cắt liên lạc. Tổng số tiền thiệt hại tuy không lớn nhưng gây ảnh hưởng đáng kể đến tâm lý, khiến sinh viên mất niềm tin và lo lắng trong quá trình học tập. Trường hợp này phản ánh rõ thủ đoạn phổ biến của tội phạm lừa đảo công nghệ cao: tạo lòng tin ban đầu, khai thác tâm lý muốn kiếm tiền nhanh, sau đó từng bước gia tăng giá trị giao dịch để chiếm đoạt tài sản. Đồng thời, tình huống cũng cho thấy điểm yếu của sinh viên nằm ở việc thiếu kỹ năng kiểm chứng thông tin và dễ bị tác động bởi các yếu tố tâm lý.

Một trường hợp điển hình khác là sinh viên năm nhất (N.V.A) bị lừa đảo qua hình thức tuyển cộng tác viên bán hàng trực tuyến. Đối tượng tiếp cận nạn nhân qua mạng xã hội với lời mời "việc nhẹ, thu nhập cao, không cần kinh nghiệm". Ban đầu, nạn nhân được yêu cầu thực hiện các nhiệm vụ đơn giản như đặt đơn hàng ảo với số tiền nhỏ (500.000 VNĐ), sau đó được hoàn tiền kèm hoa hồng để tạo lòng tin. Sau vài lần giao dịch thành công, đối tượng yêu cầu nạn nhân nạp số tiền lớn hơn (5,2 triệu VNĐ) với lý do "mở khóa nhiệm vụ VIP". Do đã tin tưởng, nạn nhân tiếp tục chuyển tiền nhưng sau đó không thể rút vốn, bị đối tượng chặn liên lạc. Tổng thiệt hại khoảng 8 triệu VNĐ.

Nhóm nghiên cứu đã thực hiện công tác phỏng vấn chuyên sâu tại trường và khu vực lưu trú gần các cơ sở học tập của sinh viên Đại học Bình Dương, qua đó nhận được các kết quả như sau.

"Nhóm nghiên cứu: Em có thể kể lại cho anh/chị nghe về việc em bị lừa như thế nào không? Từ đầu đến cuối, em nhớ rõ nhất là gì?

Nạn nhân: Hồi đó em mới lên năm nhất, đang học online nhiều, tiền tiêu vặt cũng eo hẹp. Một hôm em lướt TikTok thì có một tài khoản nhắn tin cho em. Người ta tự xưng là 'chị quản lý nhân sự' của một shop bán mỹ phẩm online, bảo đang tuyển cộng tác viên bán hàng. Lương cao, làm tại nhà, không cần kinh nghiệm, chỉ cần dùng điện thoại là được. Em thấy hấp dẫn quá nên chat lại.

Nhóm nghiên cứu: Lúc đầu họ bắt em làm gì?

Nạn nhân: Ban đầu họ bảo em chỉ cần 'đặt đơn thử' để làm quen với hệ thống. Họ gửi link một trang web trông rất chuyên nghiệp, bảo em nạp 500 nghìn để đặt một đơn hàng ảo. Xong là họ sẽ hoàn lại tiền ngay và cộng thêm hoa hồng 100-150 nghìn. Em thử làm một lần, đúng là sau 15 phút tiền về tài khoản luôn, kèm tin nhắn chúc mừng 'Chúc mừng em hoàn thành nhiệm vụ đầu tiên'. Em mừng lắm, nghĩ thật sự có việc dễ kiếm tiền.

Lần thứ hai, thứ ba họ cũng cho em làm tương tự, mỗi lần hoa hồng cao hơn một chút. Lúc đó em tin hẳn, còn khoe với bạn cùng phòng là em kiếm được tiền online rồi.

Nhóm nghiên cứu: Sau đó mọi thứ thay đổi như thế nào?

Nạn nhân: Đến lần thứ tư, họ bảo em muốn mở 'nhiệm vụ VIP' để kiếm nhiều tiền hơn, phải nạp tối thiểu 5 triệu. Họ nói nếu hoàn thành sẽ được nhận ngay 7,5 triệu (gồm vốn + lãi + hoa hồng). Lúc này em đã tin họ lắm, nghĩ chỉ cần nạp lần này là có thể rút hết tiền ra luôn. Em vay mượn bạn bè thêm một ít, cộng với tiền học bổng vừa nhận được, em chuyển hẳn 5,2 triệu cho họ.

Xong rồi… họ bảo phải chờ 'xác nhận hệ thống' khoảng 30 phút. Nhưng sau đó họ bảo em phải nạp thêm 3 triệu nữa mới mở được lệnh rút tiền. Em hoảng quá, hỏi đi hỏi lại thì họ bắt đầu né tránh, nói chung chung. Em gọi điện thì họ tắt máy, nhắn tin thì block luôn. Em mới biết mình bị lừa."

Nạn nhân cho biết sau sự việc, bản thân rơi vào trạng thái lo lắng, mất tập trung học tập và giảm niềm tin vào các cơ hội kiếm tiền trực tuyến. Trường hợp này cho thấy thủ đoạn phổ biến của tội phạm lừa đảo công nghệ cao: xây dựng lòng tin dần dần, khai thác tâm lý muốn kiếm tiền nhanh của sinh viên, sau đó nâng dần giá trị giao dịch để chiếm đoạt tài sản.

Trên cơ sở nội dung phỏng vấn trong quá trình khảo sát, có thể nhận định rằng tình huống thực tiễn nêu trên thuộc dạng hành vi lừa đảo dưới hình thức "Lừa đảo làm việc Online", đã được đề cập ở phần trước. Cụ thể, chủ thể thực hiện hành vi đã chủ động tiếp cận nạn nhân thông qua môi trường mạng, đồng thời sử dụng các thủ đoạn gian dối như tạo lập trang web giả mạo có giao diện chuyên nghiệp, mạo danh vị trí "quản lý nhân sự" nhằm tạo dựng lòng tin. Trên cơ sở đó, nạn nhân bị dẫn dắt thực hiện việc chuyển giao tài sản một cách tự nguyện nhưng dựa trên thông tin sai lệch, qua đó làm phát sinh hậu quả chiếm đoạt tài sản. Hành vi này thỏa mãn các dấu hiệu pháp lý của tội "Lừa đảo chiếm đoạt tài sản" theo Điều 174 Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung), đặc biệt ở yếu tố sử dụng thủ đoạn gian dối nhằm làm cho bị hại nhầm lẫn và tự nguyện chuyển giao tài sản.

Các sinh viên được ghi nhận có dấu hiệu thụ động trong việc kiểm chứng thông tin và kiểm tra các thủ tục hành chính qua đó dẫn đến hậu quả là mất tiền do bị chiếm đoạt và để lại tổn thương tâm lý sâu sắc, qua đó còn tạo lên một sự nghi ngờ đối với các bên bị giả mạo như nhà trường, cơ quan hành chính hay các ngân hàng, gây mất chia rẽ liên kết của sinh viên với trường.

Kết quả nghiên cứu này có sự tương đồng với các nghiên cứu và báo cáo trước đây khi cho thấy sinh viên là nhóm đối tượng dễ bị tổn thương trước các hành vi lừa đảo công nghệ cao. Cụ thể, các chương trình truyền thông và cảnh báo từ Trường Đại học Kinh tế TP. Hồ Chí Minh (UEH) cho thấy sinh viên là nhóm đối tượng thường xuyên bị nhắm đến bởi các hình thức lừa đảo trực tuyến, hội thảo tại UEH đã chỉ ra nhiều hình thức lừa đảo trực tuyến phổ biến, đặc biệt trong môi trường mạng xã hội và

giao dịch tài chính (UEH, 2025). Vishwanath nhấn mạnh rằng hành vi của người dùng trong môi trường số không hoàn toàn dựa trên lý trí mà chịu ảnh hưởng lớn bởi các cơ chế nhận thức tự động (habitual processing) (Vishwanath và cộng sự, 2011). Chính sự phụ thuộc vào phản xạ nhanh và niềm tin chủ quan vào khả năng nhận diện rủi ro của bản thân đã khiến người dùng bỏ qua các dấu hiệu cảnh báo quan trọng, từ đó dễ dàng trở thành mục tiêu của các hình thức lừa đảo như phishing.

Tuy nhiên, điểm khác biệt của nghiên cứu này là đã đi sâu phân tích đặc điểm hành vi, mức độ nhận thức và các yếu tố tâm lý của sinh viên tại một cơ sở giáo dục cụ thể là Trường Đại học Bình Dương, qua đó bổ sung góc nhìn vi mô so với các nghiên cứu trước đây vốn chủ yếu tiếp cận ở phạm vi rộng hơn.

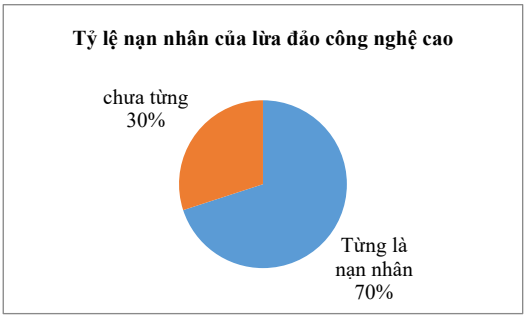
4.3. Nguyên nhân dẫn đến sinh viên trở thành nạn

Về mặt khách quan: Đại học là một môi trường mở và hoàn toàn mới – đặc biệt là các sinh viên xa nhà. Cùng với đó là sự tinh vi và chuyên nghiệp của tội phạm ngày càng phát triển hơn, môi trường mạng trực tuyến thì phát triển nhanh nhưng biện pháp bảo vệ thì chưa được theo kịp, hạn chế trong công tác giáo dục và tuyên truyền.

Về mặt chủ quan: Sinh viên đại học Bình Dương đang thiếu đi khả năng nhận dạng và kiểm chứng thông tin trên môi trường mạng kĩ thuật số, tâm lý còn non nớt và thiếu quyết đoán khi dễ bị lây động với các tác nhân bên ngoài như hiện tượng hội chứng "sợ bị bỏ lỡ" - FOMO, và đặc biệt là yếu kém trong nền tảng kiến thức pháp lý hành chính, đặc biệt là thủ tục hành chính khi dễ dàng bị dụ dỗ.

5. Giải pháp phòng ngừa tội phạm lừa đảo bằng công nghệ cao đối với sinh viên trường Đại học Bình Dương

Kết quả khảo sát sinh viên Trường Đại học Bình Dương cho thấy nguy cơ sinh viên trở thành nạn nhân của tội phạm lừa đảo bằng công nghệ cao đang ở mức đáng lo ngại. Trong tổng số sinh viên tham gia khảo sát, có 70% sinh viên từng là nạn nhân của lừa đảo trên không gian mạng, trong đó hình thức phổ biến nhất là lừa đảo việc làm online (75%), tiếp đến là lừa đảo đầu tư tài chính, chiếm đoạt tài khoản mạng xã hội và lừa đảo chuyển tiền (25%). Thực tế này cũng phù hợp với các cảnh báo của cơ quan chức năng về sự gia tăng của các hành vi lừa đảo trực tuyến thông qua mạng xã hội và các nền tảng số hiện nay (Tòa án nhân dân tối cao, 2025) .

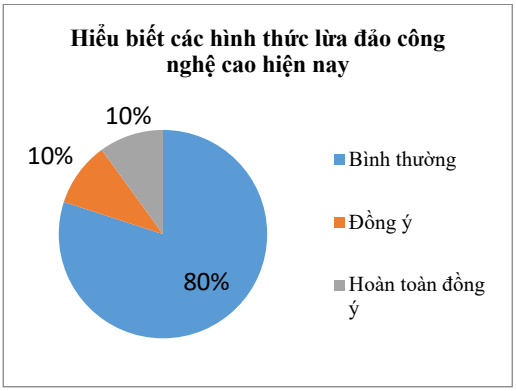


Hình 1: Biểu đồ tròn về tỷ lệ nạn nhân của lừa đảo công nghệ cao.

Đáng chú ý, 90% sinh viên sử dụng điện thoại thông minh làm thiết bị truy cập internet chính, đồng thời 90% thường xuyên sử dụng các nền tảng mạng xã hội như TikTok, Facebook, Zalo. Điều này cho thấy sinh viên có mức độ phụ thuộc cao vào môi trường

số, khiến họ trở thành nhóm đối tượng dễ bị các đối tượng phạm tội tiếp cận và thực hiện hành vi lừa đảo. Theo các nghiên cứu và cảnh báo truyền thông, nhiều hình thức lừa đảo phổ biến hiện nay thường lợi dụng các nền tảng mạng xã hội để tiếp cận người dùng với các nội dung hấp dẫn như việc làm online, đầu tư tài chính hoặc thông báo trúng thưởng nhằm đánh vào tâm lý của người trẻ (Hoài, 2023).

Bên cạnh đó, khảo sát cũng chỉ ra rằng 80% sinh viên chỉ hiểu biết ở mức "bình thường" về các hình thức lừa đảo công nghệ cao, trong khi 50% sinh viên cho biết không biết rõ các quy định pháp luật liên quan đến hành vi lừa đảo trên không gian mạng. Những số liệu này cho thấy khoảng trống đáng kể về kiến thức pháp luật và kỹ năng phòng vệ trên môi trường số của sinh viên. Trong bối cảnh đó, việc nâng cao nhận thức và xây dựng "tuyến phòng vệ đầu tiên" cho thanh thiếu niên và sinh viên trên không gian mạng được xem là giải pháp quan trọng nhằm hạn chế nguy cơ trở thành nạn nhân của tội phạm công nghệ cao (Linh và Vũ, 2026).



Hình 2: Biểu đồ tròn về sự hiểu biết các hình thức lừa đảo công nghệ cao hiện nay

Trên cơ sở đó, việc xây dựng các giải pháp phòng ngừa cần được thực hiện một cách đồng bộ từ phía nhà trường, sinh viên và cơ quan quản lý nhà nước, nhằm hạn chế tối đa nguy cơ sinh viên trở thành nạn nhân của các hành vi lừa đảo công nghệ cao.

5.1. Giải pháp từ phía nhà trường

5.1.1. Tăng cường tuyên truyền, giáo dục về phòng chống lừa đảo công nghệ cao

Kết quả khảo sát cho thấy phần lớn sinh viên chỉ có nhận thức ở mức trung bình về các hình thức lừa đảo công nghệ cao. Do đó, việc tăng cường tuyên truyền và phổ biến kiến thức về an toàn thông tin mạng là giải pháp cần thiết.

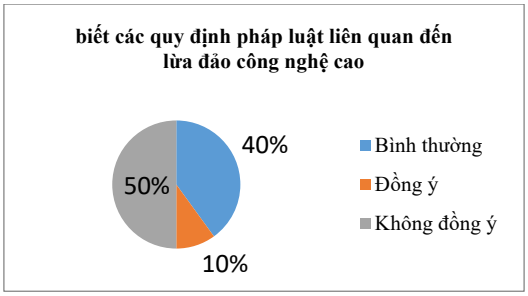
Nhà trường cần tổ chức các chương trình tuyên truyền định kỳ như: Hội thảo, tọa đàm về phòng chống tội phạm công nghệ cao. Chuyên đề phổ biến các thủ đoạn lừa đảo phổ biến trên mạng. Các buổi tập huấn kỹ năng nhận diện và xử lý khi gặp hành vi lừa đảo

Các nội dung tuyên truyền nên tập trung vào những hình thức lừa đảo phổ biến đối với sinh viên như: Lừa đảo việc làm online lương cao; Tin nhắn trúng thưởng; Giả danh cơ quan nhà nước hoặc ngân hàng; Mời gọi đầu tư tài chính hoặc tiền ảo

Việc tổ chức các hoạt động này không chỉ giúp sinh viên nâng cao nhận thức mà còn góp phần xây dựng văn hóa sử dụng internet an toàn trong môi trường đại học.

5.1.2. Lồng ghép nội dung phòng chống lừa đảo công nghệ cao vào chương trình đào tạo

Một trong những hạn chế được thể hiện qua khảo sát là 50% sinh viên không biết các quy định pháp luật liên quan đến lừa đảo công nghệ cao, trong khi chỉ khoảng 10% sinh viên (chủ yếu là sinh viên ngành luật) có hiểu biết về vấn đề này.



Hình 3: Biểu đồ tròn về sự hiểu biết các quy định pháp luật liên quan đến lừa đảo công nghệ cao ở sinh viên.

Do đó, nhà trường cần: Lồng ghép nội dung an toàn thông tin và phòng chống lừa đảo mạng vào các học phần như kỹ năng mềm, pháp luật đại cương hoặc giáo dục công dân.

Tổ chức các khóa học ngắn hạn hoặc chuyên đề ngoại khóa về an toàn số và bảo mật thông tin cá nhân.

Việc đưa các nội dung này vào chương trình đào tạo sẽ giúp sinh viên hiểu rõ: Các quy định pháp luật về tội phạm lừa đảo trên không gian mạng; Trách nhiệm pháp lý khi tham gia môi trường số; Các biện pháp tự bảo vệ trước nguy cơ bị lừa đảo; Qua đó góp phần nâng cao ý thức pháp luật và kỹ năng số cho sinh viên.

5.1.3. Xây dựng hệ thống cảnh báo sớm trong môi trường học đường

Do sinh viên sử dụng mạng xã hội với tần suất cao, các hình thức lừa đảo thường xuất hiện nhanh và thay đổi liên tục. Vì vậy, nhà trường cần xây dựng cơ chế cảnh báo sớm về các hình thức lừa đảo mới.

Cụ thể, nhà trường có thể: Cập nhật các thông tin cảnh báo trên website chính thức của trường; Gửi email cảnh báo đến sinh viên khi xuất hiện các hình thức lừa đảo mới; Đăng tải thông tin cảnh báo trên fanpage và các kênh truyền thông của trường.

Việc cảnh báo kịp thời sẽ giúp sinh viên nhận diện sớm các dấu hiệu lừa đảo và tránh trở thành nạn nhân.

Sự phối hợp này sẽ giúp sinh viên có kênh hỗ trợ chính thức khi gặp phải các hành vi lừa đảo trên mạng.

5.2. Giải pháp từ phía sinh viên

5.2.1. Nâng cao kỹ năng nhận diện các dấu hiệu lừa đảo

Kết quả khảo sát cho thấy 70% sinh viên chỉ đánh giá khả năng nhận diện lừa đảo của mình ở mức bình thường, cho thấy nhiều sinh viên vẫn còn thiếu kỹ năng phòng vệ trên không gian mạng.

Do đó, sinh viên cần chủ động trang bị cho mình các kỹ năng như: Kiểm tra nguồn gốc và độ tin cậy của thông tin; Xác minh danh tính người liên hệ trước khi thực hiện giao dịch; Không cung cấp thông tin cá nhân, mã OTP(One Time Password) hoặc tài khoản ngân hàng cho người lạ; Không truy cập các đường link lạ hoặc tải các ứng dụng không rõ nguồn gốc

Đây là những biện pháp đơn giản nhưng có hiệu quả cao trong việc phòng tránh lừa đảo.

5.2.2. Thận trọng trong các hoạt động việc làm online và đầu tư tài chính

Theo kết quả khảo sát, 75% sinh viên từng bị lừa đảo thông qua hình thức việc làm online, cho thấy đây là hình thức phổ biến nhất hiện nay.

Sinh viên cần đặc biệt cảnh giác với các lời mời như: Việc nhẹ lương cao;Làm việc online không cần kinh nghiệm; Kiếm tiền nhanh thông qua đầu tư tài chính hoặc tiền ảo

Trước khi tham gia các hoạt động này, sinh viên cần: Tìm hiểu kỹ thông tin về tổ chức hoặc cá nhân tuyển dụng; Không chuyển tiền đặt cọc hoặc phí tham gia công việc; Tham khảo ý kiến từ người thân hoặc giảng viên trước khi quyết định

5.2.3. Nâng cao hiểu biết pháp luật

Việc hiểu biết pháp luật giúp sinh viên nhận thức rõ hậu quả của các hành vi lừa đảo và biết cách bảo vệ quyền lợi của mình.

Sinh viên cần tìm hiểu các quy định pháp luật liên quan như: Quy định về tội lừa đảo chiếm đoạt tài sản; Quy định về tội sử dụng mạng máy tính, mạng viễn thông để chiếm đoạt tài sản; Quy trình tố giác tội phạm khi bị lừa đảo trên mạng.

Việc nâng cao hiểu biết pháp luật không chỉ giúp sinh viên tự bảo vệ bản thân mà còn góp phần nâng cao hiệu quả phòng chống tội phạm trong xã hội.

5.3. Kiến nghị đối với cơ quan quản lý nhà nước

Bên cạnh các giải pháp từ phía nhà trường và sinh viên, cơ quan quản lý nhà nước cũng cần có những chính sách hỗ trợ nhằm nâng cao hiệu quả phòng chống tội phạm công nghệ cao.

Cần tiếp tục hoàn thiện hệ thống pháp luật về phòng, chống tội phạm công nghệ cao, đồng thời tăng cường phát hiện và xử lý nghiêm các hành vi lừa đảo trên không gian mạng nhằm nâng cao tính răn đe của pháp luật. Bên cạnh đó, Nhà nước cần đẩy mạnh các chương trình giáo dục an toàn số cho thanh niên, sinh viên, góp phần nâng cao nhận thức và kỹ năng phòng tránh rủi ro trên môi trường mạng. Đồng thời, cần xây dựng các nền tảng tiếp nhận tố giác tội phạm trực tuyến thuận tiện, giúp người dân nhanh chóng báo cáo và được hỗ trợ kịp thời khi gặp phải hành vi lừa đảo.

6. Kết luận

Tội phạm lừa đảo bằng công nghệ cao đang trở thành một trong những thách thức nghiêm trọng đối với an ninh trật tự và an toàn xã hội trong bối cảnh chuyển đổi số hiện nay. Đối với nhóm sinh viên – đặc biệt là sinh viên Trường Đại học Bình Dương – kết quả nghiên cứu cho thấy đây là nhóm đối tượng có nguy cơ cao trở thành nạn nhân do đặc điểm sử dụng internet với tần suất lớn, mức độ phụ thuộc vào công nghệ cao, trong khi kỹ năng nhận diện và phòng tránh rủi ro còn hạn chế.

Trên cơ sở khảo sát thực tiễn, nghiên cứu ghi nhận một số phát hiện đáng chú ý. Thứ nhất, tỷ lệ sinh viên từng bị tiếp cận hoặc trở thành nạn nhân của các hình thức lừa đảo trực tuyến là tương đối cao. Thứ hai, mặc dù phần lớn sinh viên đã có nhận thức nhất định về các hình thức lừa đảo, nhưng khả năng nhận diện

tình huống cụ thể và phản ứng phù hợp vẫn còn hạn chế, đặc biệt trong các tình huống mang tính cấp bách hoặc có yếu tố tâm lý tác động. Thứ ba, các yếu tố như thiếu kinh nghiệm, tâm lý chủ quan và việc chia sẻ thông tin cá nhân trên không gian mạng là những nguyên nhân quan trọng làm gia tăng nguy cơ bị lừa đảo.

Về mặt lý luận, nghiên cứu đã vận dụng các khung lý thuyết như: Lý thuyết Hoạt động Thường ngày (Routine Activity Theory) và các lý thuyết về social engineering, phishing để giải thích mối quan hệ giữa hành vi sử dụng công nghệ và nguy cơ trở thành nạn nhân. Về mặt pháp lý, bài viết đã phân tích các quy định hiện hành liên quan đến tội phạm lừa đảo công nghệ cao, qua đó làm rõ cơ sở pháp lý cho các biện pháp phòng ngừa và xử lý.

Trên cơ sở đó, nghiên cứu đã đề xuất hệ thống giải pháp phòng ngừa mang tính khả thi, nhấn mạnh vai trò của nhà trường trong việc nâng cao nhận thức và kỹ năng cho sinh viên, sự chủ động của sinh viên trong việc bảo vệ thông tin cá nhân, cũng như sự phối hợp của các cơ quan chức năng trong công tác quản lý và xử lý hành vi vi phạm. Việc triển khai đồng bộ các giải pháp này không chỉ góp phần bảo vệ quyền và lợi ích hợp pháp của sinh viên mà còn hướng tới xây dựng môi trường học tập an toàn, lành mạnh trên không gian mạng.

Tuy nhiên, nghiên cứu vẫn còn một số hạn chế nhất định. Thứ nhất, phạm vi khảo sát chỉ tập trung tại địa phận trường đại học nên khả năng khái quát hóa chưa cao. Thứ hai, phương pháp thu thập dữ liệu chủ yếu dựa trên khảo sát và phỏng vấn định tính, chưa áp dụng các phương pháp phân tích định lượng chuyên sâu để kiểm định mối quan hệ giữa các biến số. Thứ ba, một số yếu tố như tác động của môi trường gia đình, bạn bè hoặc các yếu tố công nghệ cụ thể chưa được phân tích đầy đủ.

Do đó, trong thời gian tới, các nghiên cứu tiếp theo cần mở rộng phạm vi khảo sát sang nhiều trường đại học khác để tăng tính đại diện, đồng thời kết hợp các phương pháp nghiên cứu định lượng nhằm kiểm định mô hình lý thuyết một cách chặt chẽ hơn. Bên cạnh đó, cần tiếp tục nghiên cứu sâu hơn về các hình thức lừa đảo mới phát sinh trong bối cảnh chuyển đổi số và trí tuệ nhân tạo, từ đó đề xuất các giải pháp phòng ngừa hiệu quả và phù hợp với thực tiễn.

Tài liệu tham khảo

Baochinhphu.vn. (2024). *Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng năm 2024*. https://baochinhphu.vn/thiet-hai-do-lua-dao-truc-tuyen-uoc-tinh-18900-ty-dong-nam-2024-102241216153209577.htm

Chính phủ Việt Nam. (2014). *Nghị định số 25/2014/NĐ-CP*.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Hiệp hội An ninh mạng quốc gia (NCA). (2025). *Báo cáo/thông tin về an ninh mạng*. https://byvn.net/tozX

Hoài, T. (2023). *Cảnh giác 3 hình thức lừa đảo trực tuyến phổ biến*. *Tuổi Trẻ*. https://tuoitre.vn/canh-giac-

3-hinh-thuc-lua-dao-truc-tuyen-pho-bien-20231006123650927.htm

Khoản 1 Điều 290. (2015). *Bộ luật Hình sự*.

Kết quả một số chỉ tiêu điều tra dân số và nhà ở giữa kỳ năm 2024. (n.d.). https://byvn.net/tw1m

Linh, T., & Vũ, V. (2026). *Tăng cường "tuyến phòng vệ đầu tiên" bảo vệ thanh thiếu niên trên không gian mạng*. *Công an Nhân dân*.

Thư Viện Pháp Luật. (2025). *Bản án về tội lừa đảo chiếm đoạt tài sản số 01/2025/HS-ST*. https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-lua-dao-chiem-doat-tai-san-so-01-2025-hsst-370252

Tòa án nhân dân tối cao. (2025). *Bản án số 03/2025/HS-ST ngày 29/07/2025*. https://congbobanan.toaan.gov.vn/2ta1899021t1cvn/chi-tiet-ban-an

UEH. (2025). *Luật an ninh mạng và phòng chống gian lận trực tuyến*. https://byvn.net/lyt1

Văn Hoa, & Hải Đăng. (2023). *Lừa đảo trực tuyến tại Việt Nam trong 6 tháng đầu năm 2023 đã tăng 64,78%*. *Báo Dân tộc và Phát triển*. https://dantoctongiao.baodantoc.vn/lua-dao-truc-tuyen-tai-viet-nam-trong-6-thang-dau-nam-2023-da-tang-6478-1701343066503.htm

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability. *Decision Support Systems, 51*(3), 576–586.

Thông tin bài

Ngày nhận bài: 7/2/2026
Ngày hoàn thành: 20/3/2026
Ngày đăng bài: 25/3/2026
Tác giả liên hệ: Nguyễn Trương Thanh Thảo