NÂNG CAO HIỆU QUẢ PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG CHO SINH VIÊN TẠI TRUNG TÂM GIÁO DỤC QUỐC PHÒNG VÀ AN NINH ĐẠI HỌC THÁI NGUYÊN TRONG BỐI CẢNH MỚI

Nguyễn Huy Hoàng
Giảng viên, Trung tâm Giáo dục quốc phòng và An ninh, Đại học Thái Nguyên

Tóm tắt: *Nghiên cứu đánh giá thực trạng và đề xuất định hướng nâng cao hiệu quả phòng, chống vi phạm pháp luật trên không gian mạng cho sinh viên tại Trung tâm Giáo dục quốc phòng và an ninh Đại học Thái Nguyên. Dữ liệu được thu thập bằng bảng hỏi ẩn danh; từ 788 phản hồi ban đầu, 781 phiếu hợp lệ được sử dụng để phân tích. Kết quả cho thấy nhận thức pháp luật và an toàn số của sinh viên ở mức cao (ĐTB = 4,05/5), hành vi an toàn ở mức cao (4,06/5), trong khi hành vi nguy cơ ở mức thấp (2,05/5). Tuy nhiên, năng lực ứng phó thực tế chưa tương xứng: mức tự tin xử lý sự cố chỉ đạt 3,19/5; 63,6% từng gặp tin nhắn/cuộc gọi giả mạo hoặc yêu cầu chuyển tiền và 50,4% từng gặp đường link lừa đảo, trang giả mạo hoặc tệp độc hại. Từ khoảng cách giữa "biết" và "làm được", nghiên cứu đề xuất chuyển trọng tâm từ tuyên truyền kiến thức sang giáo dục dựa trên tình huống, mô phỏng, kênh cảnh báo - hỗ trợ rõ ràng và cơ chế đánh giá định kỳ.*

Từ khóa: *không gian mạng; vi phạm pháp luật; sinh viên; giáo dục quốc phòng và an ninh; an toàn số.*

IMPROVING THE EFFECTIVENESS OF PREVENTING AND COMBATING LEGAL VIOLATIONS IN CYBERSPACE AMONG STUDENTS AT THE CENTER FOR NATIONAL DEFENSE AND SECURITY EDUCATION, THAI NGUYEN UNIVERSITY, IN THE NEW CONTEXT

Abstract: *This study examines the current state of, and proposes directions for, improving the prevention of legal violations in cyberspace among students at the Center for National Defense and Security Education, Thai Nguyen University. Data were collected through an anonymous questionnaire. Of 788 initial responses, 781 valid questionnaires were retained for analysis. The findings indicate high levels of legal and digital-safety awareness (M = 4.05/5) and safe online behavior (M = 4.06/5), while self-reported risky behavior remained low (M = 2.05/5). Nevertheless, practical response capacity did not fully correspond to these positive indicators: students' confidence in handling cyber incidents was only moderate (M = 3.19/5); 63.6% had encountered impersonation messages/calls or requests to transfer money, and 50.4% had encountered phishing links, fake websites, or malicious files. On the basis of this knowledge-to-action gap, the study recommends shifting from predominantly knowledge-oriented communication toward scenario-based education, simulations, clearly communicated warning and support channels, and periodic evaluation.*

Keywords: *cyberspace; legal violations; students; national defense and security education; digital safety.*

Nhận bài: 22/09/2026 *Phản biện: 22/10/2026* *Duyệt đăng: 25/10/2026*

I. ĐẶT VẤN ĐỀ

Không gian mạng mở rộng cơ hội học tập, kết nối của sinh viên nhưng cũng gia tăng nguy cơ lừa đảo, giả mạo, tin sai lệch, xâm phạm dữ liệu và bắt nạt trực tuyến. Vì vậy, phòng, chống vi phạm pháp luật cần kết hợp giáo dục, phòng ngừa, cảnh báo, hỗ trợ và ứng phó. Luật An ninh mạng số 116/2025/QH15, có hiệu lực từ 01/7/2026, và Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, có hiệu lực từ 01/01/2026, đặt ra yêu cầu cập nhật giáo dục pháp luật theo tình huống thực tế. Các nghiên cứu cho thấy nhận thức tích cực chưa bảo đảm hành vi an toàn (Alharbi & Tassaddiq, 2021), hiểu biết pháp lý còn hạn chế (Ayyoub và cộng sự, 2022), đồng thời nhận thức pháp luật có liên hệ với hành vi (Alhadidi, Nweiran & Hilal, 2024). Tại Việt Nam, bảo mật thông tin cá nhân của sinh viên cũng chịu ảnh hưởng của nhiều yếu tố nhận thức và hành vi (Lê Như Ý, Nguyễn Minh Hiếu & Nguyễn Thị Ngọc Linh, 2023). Trung tâm Giáo dục quốc phòng và an ninh Đại học Thái Nguyên tập trung sinh viên từ nhiều cơ sở trong thời gian nhất định, thuận lợi cho giáo dục thống nhất nhưng đòi hỏi giải pháp ngắn gọn, thiết thực. Trong phạm vi tài liệu khảo cứu, chưa có nghiên cứu đồng thời đánh giá nhận thức, hành vi, trải nghiệm rủi ro và hoạt động phòng, chống tại Trung tâm trên mẫu lớn. Nghiên cứu trả lời hai câu hỏi: (1) mức độ nhận thức, hành vi an toàn, hành vi nguy cơ và năng lực ứng phó của sinh viên; (2) nội dung cần ưu tiên để nâng cao hiệu quả phòng, chống. Qua đó, bài viết làm rõ khoảng cách giữa nhận thức và ứng phó thực tế, cung cấp căn cứ lựa chọn giải pháp.

II. NỘI DUNG NGHIÊN CỨU

2.1. Tổng quan và khung phân tích

2.1.1. Phòng, chống vi phạm pháp luật trên không gian mạng trong môi trường giáo dục

Nghiên cứu tiếp cận phòng, chống vi phạm pháp luật trên không gian mạng theo nghĩa rộng, gồm giáo dục pháp luật, kỹ năng an toàn, chuẩn mực ứng xử, cảnh báo rủi ro, hỗ trợ sự cố, tiếp nhận phản ánh, đánh giá và phối hợp lực lượng. Mục tiêu là tăng khả năng tự bảo vệ, quyết định đúng và tìm kiếm hỗ trợ. Hiệu quả được xem xét qua bốn tầng: nhận thức quyền, nghĩa vụ và hành vi bị cấm; kỹ năng xử lý tình huống; duy trì hành vi an toàn; tiếp cận cảnh báo, tư vấn và báo cáo. Chỉ đo hiểu biết pháp luật chưa phản ánh đầy đủ khả năng xử lý giả mạo, yêu cầu chuyển tiền, chiếm quyền tài khoản hoặc phát tán dữ liệu.

2.1.2. Khoảng cách giữa nhận thức và hành động

Đánh giá nhận thức cần gắn với tình huống sử dụng Internet, thiết bị (Alharbi & Tassaddiq, 2021), vì hiểu biết chung chưa bảo đảm nắm được thủ tục và cách ứng xử pháp lý (Ayyoub và cộng sự, 2022). Alhadidi và cộng sự (2024) nhấn mạnh quan hệ giữa nhận thức pháp luật và hành vi; Bhandari (2025) đề cao chính sách, giáo dục và phòng ngừa trong đại học. Từ đó, nghiên cứu sử dụng khung "nhận thức – hành vi – tiếp xúc rủi ro – năng lực ứng phó – hỗ trợ thể chế". Với thời gian đào tạo tập trung có giới hạn, chương trình cần giúp sinh viên chuyển từ hiểu quy định sang kiểm chứng thông tin, nhận diện giả mạo, bảo vệ tài khoản, lưu bằng chứng, ngừng tương tác đáng ngờ và báo cáo đúng đầu mối.

2.2. Phương pháp nghiên cứu

2.2.1. Thiết kế và công cụ nghiên cứu

Nghiên cứu mô tả cắt ngang, kết hợp phân tích tài liệu và khảo sát ẩn danh, không thu họ tên, mã sinh viên, số điện thoại hoặc tài khoản mạng xã hội. Bảng hỏi gồm thông tin nền, sử dụng Internet, nguồn kiến thức pháp luật; nhận thức pháp luật và an toàn số (NT); 5 tình huống xử lý; hành vi an toàn (AT), nguy cơ (NC); trải nghiệm rủi ro; tự tin ứng phó; đánh giá hoạt động phòng, chống (DG), hạn chế và mức cần thiết của giải pháp (GP). Các thang chính dùng Likert 5 mức. Từ 788 phản hồi thu ngày 16/7–11/8/2026, loại 6 trường hợp không đồng ý tham gia và 1 phản hồi trùng, còn 781 phiếu hợp lệ (99,1%). Mẫu gồm 607 nữ (77,7%), 167 nam (21,4%); 89,8% là sinh viên năm thứ hai. Do giới hạn địa bàn và cơ cấu giới, năm học không cân bằng, kết quả chủ yếu phản ánh bối cảnh Trung tâm, không suy rộng cho toàn bộ sinh viên Việt Nam.

2.2.2. Xử lý và phân tích dữ liệu

Các biến Likert được mã hóa từ 1 đến 5. Điểm nhóm được tính bằng trung bình các biến thành phần; riêng thang hành vi nguy cơ có hướng diễn giải ngược, điểm càng cao thể hiện tần suất hành vi nguy cơ càng lớn. Nghiên cứu sử dụng thống kê mô tả, tần suất, tỷ lệ phần trăm, điểm trung bình, độ lệch chuẩn và Cronbach's Alpha để kiểm tra nhất quán nội tại. Các câu hỏi nhiều lựa chọn được tính tỷ lệ trên N = 781 nên tổng tỷ lệ có thể vượt 100%. Kết quả định lượng được đối chiếu với câu trả lời mở để làm rõ trải nghiệm rủi ro. Các thang đo có Cronbach's Alpha từ 0,972 đến 0,991, cho thấy mức nhất quán nội tại rất cao. Tuy nhiên, hệ số quá cao cũng có thể phản ánh sự tương đồng lớn giữa một số biến, vì vậy bài viết không dùng Alpha như bằng chứng duy nhất về chất lượng thang đo mà đồng thời xem xét từng chỉ báo và phân bố câu trả lời. Đây là lựa chọn thận trọng nhằm tránh diễn giải quá mức dữ liệu tự báo cáo.

Bảng 1. Thống kê mô tả và độ tin cậy của các thang đo

Thang đo	Nội dung	Số biến	ĐTB	ĐLC	Alpha
NT	Nhận thức pháp luật	10	4,045	0,873	0,982
AT	Hành vi an toàn	8	4,060	0,749	0,972
NC	Hành vi nguy cơ	10	2,045	1,236	0,991
NN	Nhóm nguyên nhân	10	3,493	0,994	0,977
DG	Đánh giá hoạt động	10	4,015	0,804	0,986
GP	Mức cần thiết giải pháp	13	4,000	0,810	0,989

Nguồn: Xử lý dữ liệu khảo sát của nhóm nghiên cứu từ đề tài cấp Trung tâm, 2026.

2.3. Kết quả nghiên cứu và thảo luận

2.3.1. Nhận thức và hành vi: nền tảng tích cực nhưng chưa đủ

Kết quả cho thấy sinh viên có nền tảng nhận thức tương đối tốt. Điểm trung bình thang NT đạt 4,05/5; các biến thành phần dao động quanh mức cao. Ở 5 tình huống kiểm tra cách xử lý, điểm trung bình đạt 4,70/5 và 86,4% sinh viên trả lời

đúng cả 5 tình huống. Hành vi an toàn tự báo cáo đạt 4,06/5, trong khi hành vi nguy cơ chỉ 2,05/5. Nếu chỉ quan sát ba nhóm chỉ báo này, có thể kết luận môi trường hành vi của mẫu khảo sát khá tích cực. Tuy nhiên, kết luận đó cần được đặt cạnh dữ liệu về năng lực ứng phó. Mức tự tin khi xử lý sự cố chỉ đạt 3,19/5; 15,5% sinh viên cho biết ít hoặc hoàn toàn không tự tin. Một số kỹ năng như lưu bằng chứng và xác định kênh phản ánh thấp hơn nhóm kiến thức pháp luật cơ bản. Sự chênh lệch giữa điểm tình huống 4,70/5 và mức tự tin 3,19/5 cho thấy khả năng chọn đáp án đúng trong bảng hỏi chưa đồng nhất với cảm nhận có thể xử lý một sự cố thật. Đây là phát hiện quan trọng nhất của nghiên cứu. Kết quả này tương thích với hướng nghiên cứu quốc tế cho rằng nhận thức an ninh mạng cần được đánh giá cùng hành vi và năng lực thực hành (Alharbi & Tassaddiq, 2021). Nó cũng bổ sung một góc nhìn cho kết quả của Ayyoub và cộng sự (2022): người học có thể nhận biết tương đối tốt một vấn đề nhưng vẫn thiếu hiểu biết hoặc sự chắc chắn ở khâu xử lý cụ thể. Vì vậy, trong giáo dục phòng, chống vi phạm pháp luật trên không gian mạng, "biết đúng" nên được xem là điều kiện cần, còn "làm được" mới là chỉ báo gần hơn với năng lực phòng ngừa.

2.3.2. Mức tiếp xúc rủi ro cao tạo áp lực lên năng lực ứng phó

Dữ liệu trải nghiệm trong 12 tháng gần nhất cho thấy rủi ro không phải hiện tượng xa lạ. Có 497 sinh viên (63,6%) từng nhận tin nhắn/cuộc gọi giả mạo hoặc yêu cầu chuyển tiền; 394 sinh viên (50,4%) từng gặp link lừa đảo, trang giả mạo hoặc tệp độc hại. Các rủi ro khác gồm nội dung vi phạm bản quyền/phần mềm không rõ nguồn (21,0%), tin giả/xuyên tạc/kích động (20,5%), chiếm quyền hoặc truy cập trái phép tài khoản (14,6%), quấy rối/xúc phạm/bắt nạt trực tuyến (10,0%) và tự ý công khai hình ảnh/thông tin cá nhân (5,9%). Chỉ 18,6% cho biết chưa từng gặp tình huống nào được liệt kê.

Bảng 2. Một số rủi ro trực tuyến sinh viên đã gặp trong 12 tháng gần đây

Rủi ro	Số lựa chọn	Tỷ lệ (%)
Tin nhắn/cuộc gọi giả mạo hoặc yêu cầu chuyển tiền	497	63,6
Link lừa đảo, trang giả mạo hoặc tệp độc hại	394	50,4
Nội dung vi phạm bản quyền/phần mềm không rõ nguồn	164	21,0
Tin giả/xuyên tạc/kích động	160	20,5
Chiếm quyền/truy cập trái phép tài khoản	114	14,6
Quấy rối/xúc phạm/bắt nạt trực tuyến	78	10,0
Tự ý công khai hình ảnh/thông tin cá nhân	46	5,9
Chưa từng gặp tình huống nêu trên	145	18,6

Nguồn: Xử lý dữ liệu khảo sát của nhóm nghiên cứu, 2026.

Các câu trả lời mở củng cố xu hướng này: sau khi loại câu trả lời không có nội dung thực chất, 456 ý kiến được mã hóa; nhóm từ khóa liên quan đến lừa đảo, giả mạo và chiếm đoạt xuất hiện trong khoảng 52,6% ý kiến có nội dung. Như vậy, mức hành vi nguy cơ tự báo cáo thấp không có nghĩa môi trường trực tuyến của sinh viên ít rủi ro. Ngược lại, phần lớn sinh viên đang hoạt động trong một môi trường có tần suất tiếp xúc đáng kể với các thủ đoạn lừa đảo và giả mạo. Phát hiện này làm thay đổi trọng tâm can thiệp. Nếu nguy cơ chủ yếu xuất phát từ việc sinh viên cố ý thực hiện hành vi không an toàn, giải pháp có thể tập trung vào nhắc nhở và kỷ luật. Nhưng khi sinh viên thường xuyên bị đặt trước các tình huống do tác nhân bên ngoài tạo ra, giáo dục cần ưu tiên năng lực nhận diện, phản ứng nhanh, lưu bằng chứng và tìm kiếm hỗ trợ. Đây cũng là lý do không nên đồng nhất "phòng, chống vi phạm" với "ngăn sinh viên vi phạm"; sinh viên đồng thời có thể là người có nguy cơ bị xâm hại trên không gian mạng.

2.3.3. Hoạt động hiện có được đánh giá tích cực nhưng còn thiếu tính thực hành

Sinh viên đánh giá hoạt động phòng, chống tại Trung tâm tương đối tích cực (DG = 4,02/5). Điều này cho thấy Trung tâm đã có nền tảng tổ chức và truyền thông có thể tiếp tục phát huy. Tuy nhiên, khi được hỏi về hạn chế, 41,5% cho rằng nội dung tuyên truyền còn chung chung; 34,4% cho rằng hình thức chưa hấp dẫn; 33,5% nhận thấy còn thiếu thực hành hoặc mô phỏng. Những tỷ lệ này giải thích một phần khoảng cách giữa nhận thức

cao và tự tin xử lý sự cố ở mức trung bình. Một điểm cần chú ý khác là kênh hỗ trợ. Có 23,8% sinh viên cho rằng trở ngại lớn nhất khi báo cáo là không biết báo cho ai hoặc báo bằng cách nào; 14,6% lo ngại lộ thông tin cá nhân. Trong phòng ngừa rủi ro số, sự chậm trễ ở khâu báo cáo có thể làm tăng thiệt hại, đặc biệt với chiếm quyền tài khoản, lừa đảo chuyển tiền hoặc phát tán dữ liệu. Vì vậy, hiệu quả của công tác phòng, chống không chỉ phụ thuộc nội dung giảng dạy mà còn phụ thuộc việc sinh viên có nhìn thấy, nhớ và tin tưởng một đầu mối hỗ trợ cụ thể hay không.

2.3.4. Mức độ cần thiết và thứ tự ưu tiên của giải pháp

Mười ba giải pháp được sinh viên đánh giá đều có điểm cần thiết xấp xỉ 4,0/5. Các giải pháp có điểm trung bình cao gồm thiết lập kênh thông tin chính thức (GP5 = 4,028), phổ biến quy tắc ứng xử (GP7 = 4,019), sử dụng tình huống, video, tương tác và mô phỏng (GP3 = 4,012), kênh tư vấn - phản ánh - báo cáo (GP6 = 4,012), và kết hợp biểu dương với nhắc nhở, xử lý (GP12 = 4,012). Chênh lệch điểm không lớn cho thấy nhu cầu mang tính hệ thống hơn là chỉ tập trung vào một biện pháp đơn lẻ. Khi được yêu cầu chọn tối đa ba giải pháp cần triển khai trước, kết quả phân hóa rõ hơn: GP1 - lồng ghép pháp luật và kỹ năng an toàn số vào bài giảng và GP3 - tăng cường tình huống, video, tương tác, mô phỏng cùng đạt 57,0%; tiếp theo là chuyên đề với cơ quan công an/chuyên gia (33,3%) và kênh thông tin chính thức (24,3%). Dữ liệu ưu tiên vì thế cung cấp căn cứ thực tế để sắp xếp lộ trình triển khai thay vì dàn trải nguồn lực.

Bảng 3. Các giải pháp được sinh viên lựa chọn ưu tiên triển khai

Mã	Nội dung rút gọn	Số lựa chọn	Tỷ lệ (%)
GP1	Lồng ghép pháp luật và kỹ năng an toàn số	445	57,0
GP3	Tình huống, video, tương tác và mô phỏng	445	57,0
GP2	Chuyên đề với cơ quan công an/chuyên gia	260	33,3
GP5	Kênh thông tin chính thức	190	24,3
GP4	Học liệu số ngắn gọn	145	18,6
GP6	Kênh tư vấn, phản ánh và báo cáo	100	12,8

Nguồn: Xử lý dữ liệu khảo sát của nhóm nghiên cứu, 2026.

Cần phân biệt mức độ cần thiết với tính khả thi. Phiếu sinh viên đo trực tiếp mức cần thiết và thứ tự ưu tiên, không có thang riêng về tính khả thi. Vì vậy, nghiên cứu không suy diễn rằng sinh viên đã đánh giá tính khả thi của giải pháp. Tính khả thi khi triển khai cần được Trung tâm xem xét riêng theo nguồn nhân lực, chi phí, hạ tầng, mức phụ thuộc phối hợp bên ngoài và khả năng duy trì. Việc tách hai loại bằng chứng này giúp bảo đảm tính minh bạch phương pháp.

2.3.5. Định hướng nâng cao hiệu quả trong bối cảnh mới

Thứ nhất, chuyển trọng tâm từ phổ biến quy định sang phát triển năng lực ứng phó. Nội dung pháp luật vẫn cần thiết, nhưng nên được tích hợp vào chuỗi tình huống gần với trải nghiệm của sinh viên: tin nhắn mạo danh người thân hoặc cơ quan chức năng, yêu cầu chuyển tiền, trang đăng nhập giả, tài khoản bị chiếm quyền, phát tán ảnh cá nhân, tin sai lệch và nội dung vi phạm bản quyền. Mỗi tình huống cần yêu cầu người học thực hiện quy trình: nhận diện dấu hiệu - dừng tương tác - kiểm chứng - bảo vệ tài khoản/dữ liệu - lưu bằng chứng - báo cáo. Cách tổ chức này trực tiếp xử lý khoảng cách giữa điểm nhận thức cao và mức tự tin ứng phó trung bình. Thứ hai, tăng cường mô phỏng và học liệu số ngắn. Với đặc thù đào tạo tập trung, các mô-đun 5-10 phút, video tình huống, câu hỏi lựa chọn có phản hồi và bài mô phỏng nhận diện giả mạo phù hợp hơn những chuyên đề dài, nặng thông tin. Mô phỏng cần bảo đảm an toàn, không sử dụng đường link độc hại thật và không thu thập dữ liệu nhạy cảm. Kết quả thực hành có thể được dùng để điều chỉnh nội dung theo từng khóa học. Thứ ba, thiết lập một kênh cảnh báo - tư vấn - phản ánh dễ nhớ và có quy trình phản hồi. Đầu mối này cần được giới thiệu ngay đầu khóa, xuất hiện trên nền tảng chính thức và quy định rõ loại sự cố nào cần báo, thông tin tối thiểu cần cung cấp, cách lưu bằng chứng và nguyên tắc bảo vệ dữ liệu cá nhân. Với 23,8% sinh viên chưa rõ báo cho ai/bằng cách nào, việc làm rõ đầu mối có thể tạo tác động thực tế nhanh hơn so với việc bổ sung thêm một lượng lớn nội

dung lý thuyết. Thứ tư, tổ chức phối hợp theo chu trình thay vì theo sự kiện. Trung tâm, cơ sở đào tạo có sinh viên học tại Trung tâm, tổ chức Đoàn - Hội và cơ quan chức năng cần chia sẻ cảnh báo, học liệu và quy trình hỗ trợ theo phạm vi trách nhiệm. Mỗi năm nên có một vòng đánh giá gồm rà soát rủi ro mới, cập nhật tình huống, kiểm tra mức biết kênh báo cáo, tổng hợp sự cố và điều chỉnh hoạt động. Việc duy trì đều đặn quan trọng hơn tổ chức nhiều hoạt động ngắn hạn nhưng không theo dõi kết quả. Thứ năm, đánh giá hiệu quả bằng chỉ báo năng lực thay vì chỉ đếm hoạt động. Bên cạnh số buổi tuyên truyền hoặc số tài liệu phát hành, cần theo dõi tỷ lệ sinh viên nhận diện đúng tình huống giả mạo, biết các bước xử lý ban đầu, biết đầu mối báo cáo, có khả năng lưu bằng chứng và duy trì hành vi bảo vệ tài khoản. Đây là cách đưa công tác phòng, chống từ logic "đã triển khai" sang logic "người học đã làm được gì".

III. KẾT LUẬN

Khảo sát 781 sinh viên tại Trung tâm Giáo dục quốc phòng và an ninh Đại học Thái Nguyên cho thấy một bức tranh hai mặt. Một mặt, nhận thức pháp luật, kết quả xử lý tình huống trên bảng hỏi và hành vi an toàn đều ở mức tích cực; hành vi nguy cơ tự báo cáo ở mức thấp. Mặt khác, sinh viên tiếp xúc thường xuyên với các rủi ro trực tuyến, đặc biệt là giả mạo, yêu cầu chuyển tiền và đường link/trang giả; mức tự tin xử lý sự cố mới ở mức trung bình và một bộ phận chưa biết rõ kênh phản ánh. Khoảng cách giữa "biết" và "làm được" vì vậy là vấn đề trung tâm cần giải quyết. Từ bằng chứng khảo sát, bài viết đề xuất ưu tiên lồng ghép pháp luật với kỹ năng an toàn số; sử dụng tình huống và mô phỏng; xây dựng học liệu ngắn, kênh thông tin và kênh hỗ trợ chính thức; tăng phối hợp và đánh giá định kỳ dựa trên năng lực ứng phó. Những giải pháp này phù hợp với lựa chọn ưu tiên của sinh viên và đặc thù đào tạo tập trung của Trung tâm. Tuy nhiên, nghiên cứu dựa chủ yếu trên dữ liệu tự báo cáo, mẫu có cơ cấu giới và năm học không cân bằng và chưa sử dụng thiết kế thực nghiệm trước - sau. Các nghiên cứu tiếp theo nên bổ sung bài kiểm tra hành vi thực hành, so sánh giữa nhóm sinh viên và đánh giá tác động của mô-đun mô phỏng sau can thiệp.

TÀI LIỆU THAM KHẢO

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of cybercrime and legal awareness on the behavior of University of Jordan students. Heliyon, 10(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23. https://doi.org/10.3390/bdcc5020023

Ayyoub, H. Y., AlAhmad, A. A., Al-Serhan, A., Al-Abdallat, M. F., Al-Muheisen, E., Boshmaf, H., Abu-Taleb, Y. A., Alqudah, Y. O., & Alshamaileh, Y. (2022). Awareness of electronic crimes related to e-learning among students at the University of Jordan. Heliyon, 8(10), e10897. https://doi.org/10.1016/j.heliyon.2022.e10897

Bhandari, B. (2025). Cybersecurity awareness amongst university students: Legal remedies and policies to mitigate risks. Unity Journal, 6(1), 120–135. https://doi.org/10.3126/unityj.v6i1.75557

Bộ Thông tin và Truyền thông. (2021). Quyết định số 874/QĐ-BTTTT ngày 17/6/2021 về việc ban hành Bộ Quy tắc ứng xử trên mạng xã hội.

Chính phủ. (2024). Nghị định số 147/2024/NĐ-CP ngày 09/11/2024 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

Quốc hội. (2013). Luật Giáo dục quốc phòng và an ninh số 30/2013/QH13 ngày 19/6/2013.

Quốc hội. (2025a). Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025.