

THIẾT KẾ VÀ VẬN DỤNG BỘ CÔNG CỤ TRỰC QUAN CÙNG MÔ HÌNH PHẢN XẠ SỐ TRONG GIÁO DỤC PHÒNG CHỐNG “BẮT CÓC TRỰC TUYẾN” CHO HỌC SINH TRUNG HỌC PHỔ THÔNG

VÕ THÚY KIỀU

Trường Trung học phổ thông Sa Đéc, tỉnh Đồng Tháp

Nhận bài ngày 05/7/2026. Sửa chữa xong 10/8/2026. Duyệt đăng 15/8/2026.

Abstract

In the digital era, cyber scams, particularly “virtual kidnapping,” have emerged as a serious threat to high school students. This study surveyed 661 students to identify gaps in their digital safety competencies. To address these educational needs, the author designed and implemented an integrated system of visual tools and digital reflex models, including a QR code-based digital platform, the “STOP LINK” sticker set, reminder keychains, the SAFE CODE reflex model, and the 4H rule. A pedagogical experiment conducted with class 12B1 (N = 41) and a control class, 12B3 (N = 43), at Sa Dec High School showed substantial improvements: the rate of correctly identifying manipulation-based scam scenarios increased from 44.2% to 87.8%; the “Stop” reflex before interacting with suspicious links increased from 32.6% to 82.9%; and proactive reporting to families and schools rose from 14.0% to 80.5%. The approach was also successfully implemented in class 11A9 and supported students in winning Second Prize in a provincial-level Science and Technology Competition. These findings suggest a practical approach to reinforcing digital safety skills through concrete, memorable, and experience-based educational tools in high school settings.

Keywords: Digital safety, experiential activities, SAFE CODE, STOP LINK sticker, virtual kidnapping, visual educational tools.

1. Đặt vấn đề

Sự bùng nổ của chuyển đổi số trong thế kỷ XXI đã biến không gian mạng thành một phần không thể thiếu đối với học sinh (HS) trung học phổ thông (THPT). Đi kèm với các cơ hội học tập là rủi ro an ninh phi truyền thống phức tạp đe dọa môi trường giáo dục. Chương trình Giáo dục phổ thông (GDPT) 2018 xác định việc hình thành năng lực số và kỹ năng tự vệ trực tuyến cho HS là yêu cầu cấp thiết (Bộ Giáo dục và Đào tạo, 2024). Để đạt hiệu quả, công tác chủ nhiệm lớp và Hoạt động trải nghiệm (HĐTN) cần không ngừng đổi mới phương pháp, thay thế lối truyền tải lý thuyết một chiều bằng các can thiệp trực quan sinh động. Một hình thức tội phạm công nghệ cao đặc biệt nguy hiểm gần đây là nạn “bắt cóc trực tuyến” (virtual kidnapping). Đây là thủ đoạn lừa đảo tinh vi lợi dụng sơ hở thông tin cá nhân và áp dụng trí tuệ nhân tạo (Deepfake giọng nói, hình ảnh) để thao túng tâm lý nạn nhân (Bộ Công an, 2024). Tội phạm không tiếp xúc vật lý trực tiếp nhưng giả danh cơ quan pháp luật hoặc người thân gặp tai nạn khẩn cấp, cưỡng ép HS ngắt liên kết hoàn toàn với gia đình và ẩn náu tại khách sạn. Khi HS bị cô lập trong sợ hãi, chúng sẽ tổng tiền phụ huynh (Bộ Giáo dục và Đào tạo, 2024). Thủ đoạn này đánh mạnh vào tâm lý lo sợ của HS và bản năng bảo vệ con cái của cha mẹ. Số liệu thực tế rất đáng báo động: Từ giữa năm 2024 đến tháng 8/2025, cả nước ghi nhận khoảng 50 vụ án bắt cóc trực tuyến liên quan đến HS, sinh viên, với 90% nạn nhân là nữ giới (Bộ Công an, 2024). Tại Thành phố Hồ Chí Minh, tính đến tháng 8/2025 có 28 HS, sinh viên sập bẫy lừa đảo này (Bảo Tuổi Trẻ Media, 2025). Tại tỉnh Đồng Tháp, riêng quý IV năm 2025 cũng ghi nhận ít nhất 04 HS THPT bị đe dọa tổng tiền dưới kịch bản bắt cóc ảo (Đài Phát thanh và Truyền hình Đồng Tháp, 2025). Thực tế đó cho thấy yêu cầu cấp bách phải xây dựng lá chắn bảo vệ chủ động cho HS ngay

Email: kieuvanlv1@gmail.com

tại trường học. Tuy nhiên, công tác giáo dục kỹ năng số học đường hiện nay vẫn bộc lộ nhiều hạn chế do thiếu các bộ công cụ trực quan dễ nhớ và quy trình phản xạ nhanh khi khủng hoảng xảy ra (Võ Thúy Kiều, 2026). Để khắc phục, nghiên cứu này tiến hành thiết kế và vận dụng đồng bộ hệ sinh thái thiết bị giáo dục mềm (quy trình phản xạ SAFE CODE, mô hình 4H) cùng các bộ công cụ trực quan hữu hình (Sticker STOP LINK, Móc khóa thông điệp) nhằm nâng cao năng lực tự vệ số và thúc đẩy tư duy nghiên cứu khoa học (NCKH) của HS tại trường THPT Sa Đéc (Võ Thúy Kiều, 2026).

2. Cơ sở lý luận

2.1. Khái niệm và bản chất của tội phạm bắt cóc trực tuyến

Bắt cóc trực tuyến là hình thức tống tiền lừa đảo công nghệ cao mà không có sự giam giữ vật lý thực sự đối với nạn nhân (Center for Cybercrime Studies, 2023). Tội phạm kết hợp các thủ thuật tâm lý xã hội (social engineering), thu thập thông tin đời tư từ mạng xã hội và sử dụng AI Deepfake để tái tạo giọng nói, hình ảnh người thân nhằm tạo dựng kịch bản khủng hoảng khẩn cấp. Nạn nhân bị đưa vào trạng thái hoảng loạn cảm tính và bị bắt buộc phải tự cắt đứt liên lạc với gia đình. Bản chất của loại tội phạm này là sự thao túng tâm lý có chủ đích, đánh vào lòng trắc ẩn và nỗi sợ hãi tột cùng để tống tiền (Bộ Công an, 2024).

2.2. Đặc điểm tâm lý học sinh trung học phổ thông trước các nguy cơ thao túng mạng

HS THPT (từ 15 đến 18 tuổi) đang ở giai đoạn nhạy cảm về tâm lý, dễ trở thành đối tượng bị thao túng trực tuyến bởi ba đặc điểm hành vi cốt lõi (Trường THPT Lê Hồng Phong Hà Nội, 2023):

Một là, khao khát khẳng định bản thân và tính tò mò cao khiến HS dễ tin tưởng mối quan hệ ảo và chia sẻ thông tin cá nhân tùy tiện.

Hai là, sự nhạy cảm cảm xúc cực lớn làm HS dễ rơi vào hoảng loạn khi bị đe dọa (như ghép ảnh nhạy cảm bằng AI), dẫn đến mất khả năng phản xạ lý trí và làm theo yêu cầu giữ bí mật tuyệt đối của kẻ xấu.

Ba là, sự thiếu hụt nghiêm trọng về kinh nghiệm sống và kỹ năng xử lý khủng hoảng số thực chiến (Trường THPT Lê Hồng Phong Hà Nội, 2023).

2.3. Vai trò của thiết bị giáo dục trực quan và điểm chặn thị giác

Trong khoa học sư phạm, trực quan hóa đóng vai trò then chốt trong việc định hình hành vi. Việc chuyển hóa các thông điệp giáo dục vô hình thành các vật phẩm vật lý hữu hình (Sticker cảnh báo dán sau điện thoại, móc khóa balo) được gọi là quá trình “Vật chất hóa thông điệp” (Cormack, 1994). Các vật phẩm này đóng vai trò như các “Điểm chặn thị giác” (visual blockers). Khi HS chuẩn bị thực hiện hành vi có nguy cơ rủi ro (như nhấp vào liên kết lạ hoặc gửi thông tin cá nhân), biểu tượng cảnh báo đập vào mắt sẽ kích hoạt ý thức cảnh giác (Cormack, 1994). Điểm chặn thị giác này giúp trì hoãn phản ứng bộc phát cảm tính, tạo ra khoảng dừng 5 giây để HS kích hoạt tư duy lý tính và kiểm chứng thông tin.

3. Phương pháp nghiên cứu

3.1. Thiết kế nghiên cứu và kiểm định công cụ

Nghiên cứu sử dụng phương pháp hỗn hợp kết hợp giữa khảo sát thực trạng định lượng diện rộng và thực nghiệm sư phạm có đối chứng (Nguyễn Thu Tuấn, 2015). Công cụ khảo sát chính là Phiếu khảo sát bảng hỏi (Phụ lục 5) gồm 16 câu hỏi đo lường nhận thức, hành vi và kỹ năng ứng phó rủi ro mạng. Để đảm bảo độ tin cậy và nhất quán nội tại trước khi tiến hành khảo sát diện rộng, tác giả đã kiểm định chất lượng thang đo bằng hệ số Cronbach's Alpha trên SPSS 20.0 (Lưu Hà Chi, 2024). Kết quả kiểm định đạt hệ số vô cùng lý tưởng: Thang đo Cơ hội nghề nghiệp đạt Cronbach's Alpha = 0.899; Gia đình và Xã hội đạt 0.917; Đặc điểm cá nhân đạt 0.885; Đặc điểm trường đại học đạt 0.925. Hệ số tương quan biến - tổng chọn đại diện nhỏ nhất đều lớn hơn 0.481, đạt tiêu chuẩn khoa học khắt khe để đưa vào đo lường thực tế (Lưu Hà Chi, 2024).

3.2. Mẫu khảo sát diện rộng

Đối tượng khảo sát diện rộng bao gồm 661 HS (321 nam, chiếm 48.6% và 340 nữ, chiếm 51.4%) tại trường THPT Sa Đéc và 2 trường lân cận trên địa bàn Phường Sa Đéc (Nguyễn Du và Nguyễn Đình Chiểu). Phân bố HS theo khối lớp đồng đều: Khối 10 có 213 em (32.2%), Khối 11 có 213 em (32.2%), Khối

12 có 235 em (35.6%). HS thực hiện khảo sát ẩn danh hoàn toàn qua Google Form bằng cách quét mã QR Code trực quan đặt tại lớp học.

3.3. Tiến trình nghiên cứu thực nghiệm và lộ trình chi tiết

Tiến trình thực nghiệm được triển khai theo quy trình 3 bước (Phụ lục 4):

Bước 1: Khảo sát thực trạng diện rộng bằng phiếu bảng hỏi và phỏng vấn sâu HS nòng cốt; *Bước 2:* Thiết kế hệ sinh thái bộ công cụ trực quan và báo cáo đề xuất tích hợp giải pháp phòng ngừa; *Bước 3:* Đưa giải pháp vào thực nghiệm tại lớp chủ nhiệm và đánh giá thông qua kết quả bồi dưỡng HS NCKH.

Lộ trình chi tiết gồm: Tháng 8/2025: Khảo sát thực trạng; Tháng 9/2025: Thiết kế và ra mắt hệ sinh thái truyền thông đa kênh tích hợp mã QR (Chatbot AI); Tháng 10/2025: Huấn luyện quy tắc SAFE CODE; Tháng 11/2025: Trao tặng Sticker STOP LINK và Móc khóa; Tháng 12/2025: Huấn luyện phản xạ 4H; Tháng 01/2026: Tổng kết, đối chiếu số liệu đối chứng lớp 12B3 và thực nghiệm 12B1, đồng thời đánh giá tính nhân rộng tại lớp 11A, Trường THPT Sa Đéc.

4. Kết quả nghiên cứu và thảo luận

4.1. Thực trạng nhận thức và hành vi trực tuyến tiềm ẩn nguy cơ của học sinh trung học phổ thông

Dữ liệu thực chứng thu được từ 661 mẫu khảo sát qua xử lý phần mềm SPSS chỉ ra lỗ hổng lớn về an toàn số học đường:

Thứ nhất, thời lượng sử dụng Internet và mức độ phơi nhiễm mạng cực kỳ lớn. Có tới 66.4% HS sử dụng Internet từ 3 giờ trở lên mỗi ngày, trong đó 30.9% online trên 5 giờ hàng ngày. Việc kết nối mạng liên tục làm gia tăng đáng kể nguy cơ tiếp xúc với các trang liên kết lạ, tài khoản giả mạo và các bẫy lừa đảo trực tuyến.

Thứ hai, nhận thức lỏng lẻo và hành vi trực tuyến tiềm ẩn nguy cơ cao. Mặc dù 68% HS đã từng nghe về “bắt cóc trực tuyến”, nhưng 87.3% chỉ nghĩ đến giai đoạn dụ dỗ gặp mặt trực tiếp ngoài đời thật, xem nhẹ các thủ đoạn tinh vi ban đầu như thu thập thông tin cá nhân (chỉ 42.3% biết) hay thao túng tâm lý (chỉ 40% nhận diện đúng). Khảo sát hành vi rủi ro thực tế cho thấy: 64.2% HS từng nhận lời mời/tin nhắn từ người lạ; 13.5% từng chia sẻ thông tin cá nhân nhạy cảm; 16.3% từng bị lôi kéo gặp mặt; và 74.6% chơi game trực tuyến cùng người lạ mà không cảnh giác (Võ Thúy Kiều, 2026). Khi gặp rủi ro, 6.5% HS lúng túng “không làm gì cả” và chỉ 21.9% chủ động báo cáo GV/Phụ huynh học sinh (PHHS). Đáng chú ý, nữ sinh có mức độ lo ngại cảm tính (66.1%) cao hơn nam sinh (33.9%), đặc biệt ở khối 10, đòi hỏi các giải pháp giáo dục phải mang tính cá nhân hóa và trực quan.

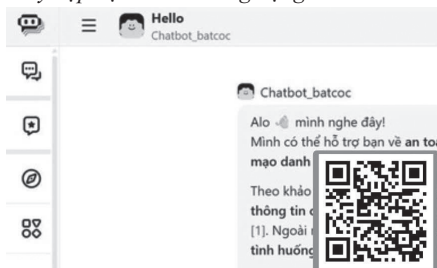
4.2. Thiết kế và vận dụng hệ sinh thái bộ công cụ trực quan và mô hình phản xạ số

Dựa trên các lỗ hổng nhận thức, tác giả thiết kế và đưa vào sử dụng hệ sinh thái 5 biện pháp tích hợp giữa công cụ trực quan hữu hình và quy trình phản xạ thực chiến:

4.2.1. Thiết lập môi trường Truyền thông số tương tác qua Câu lạc bộ “Thủ lĩnh An toàn mạng”

Để thay đổi phương thức truyền thông, Câu lạc bộ thiết lập mạng lưới ứng dụng số đồng bộ trên Facebook, TikTok, Website và hệ thống Chatbot AI (poe.com/Chatbot_batcoc). Toàn bộ cảm nang được đóng gói thành các mã QR Code trực quan nổi bật. Chatbot AI hoạt động như một chuyên gia tư vấn ảo hỗ trợ giải đáp thắc mắc, xử lý khủng hoảng ẩn danh cho HS 24/7 bằng ngôn ngữ trẻ trung của Gen Z, lồng ghép các hashtag tương tác để thu hút HS chủ động quét mã tham gia.

Hình 1: Tích hợp mã QR truy cập hệ sinh thái ứng dụng số đa nền tảng giáo dục an toàn mạng





4.2.2. Mô hình huấn luyện kỹ năng SAFE CODE và sơ đồ hóa phản xạ

Nhằm hình thành phản xạ tự vệ tức thời, tác giả thiết kế quy trình SAFE CODE tích hợp trực tiếp vào các giờ sinh hoạt HĐTN. Quy trình gồm 4 bước quyết định hành vi tự chủ:

- S - Stop (Dừng lại): Dừng mọi thao tác trước tin nhắn gây sốc hoặc yêu cầu khẩn cấp để lấy lại bình tĩnh trong 5 giây đầu.
- A & F - Ask & Find (Hỏi - Kiểm tra - Giữ lại): Đặt câu hỏi xác minh, tự kiểm tra qua các kênh chính thống và chụp màn hình điện thoại lưu giữ chứng cứ.
- E - Easy/Equal (Không làm một mình): Phá vỡ sự cô lập của tội phạm mạng bằng cách luôn chia sẻ, đồng hành cùng giáo viên, bạn bè hoặc cha mẹ.
- Code (Kết nối hỗ trợ): Kết nối nhanh đến các nguồn trợ giúp của nhà trường và cơ quan Công an.

Trong tiết HĐTN, giáo viên ứng dụng thiết bị trình chiếu để HS thực hành đóng vai xử lý trực tiếp 4 kịch bản bấy mạng thực tế sau:

Kịch bản 1: “Bẫy Link lạ từ tài khoản người quen”. Nhận được tin nhắn từ tài khoản bạn bị hack: “Vào xem clip bạn bị bôi xấu nè, xem nhanh kẻo bị xóa!”. HS thực hành SAFE CODE: Kiên quyết không bấm link (Stop), gọi điện thoại trực tiếp cho bạn để kiểm chứng (Ask & Find) và báo cáo giáo viên chủ nhiệm (GVCN) hỗ trợ.

Kịch bản 2: “Bẫy trúng thưởng và tổng tiền ngược”. Đối tượng giả shipper báo trúng iPhone 16 Pro Max, yêu cầu HS đọc OTP và địa chỉ nhà. Khi HS từ chối, chúng đe dọa tung tin bôi nhọ lên Fanpage trường. HS thực hành: Ghi âm cuộc gọi (Giữ lại), nhờ bạn bè chứng kiến (Không làm một mình) và lập tức chặn số (Hành động).

Kịch bản 3: “Bẫy Deepfake - Người thân gặp nạn”. Cuộc gọi video call hình ảnh nhòe từ mẹ khóc lóc báo tai nạn nguy kịch, đòi chuyển gấp 500 nghìn đồng vào số tài khoản lạ. HS áp dụng “Mật khẩu gia đình” để kiểm tra danh tính thật giả qua từ khóa bí mật (Hỏi/Kiểm tra) và liên hệ ngay người thân khác để định vị vị trí của mẹ (Kết nối hỗ trợ).

Kịch bản 4: “Bẫy đe dọa tung ảnh/clip nhạy cảm”. Kẻ xấu gửi tin nhắn chứa ảnh chân dung HS bị cắt ghép nhạy cảm bằng AI, đe dọa gửi cho bạn bè và giáo viên nếu không chuyển tiền. HS thực hành: Giữ bình tĩnh, không hoảng sợ thực hiện yêu cầu (Stop), báo cáo ngay với GVCN và cha mẹ để được hỗ trợ can thiệp pháp lý kịp thời (Ask & Find).

4.2.3. “Vật chất hóa” thông điệp giáo dục qua bộ Sticker STOP LINK và Móc khóa thông điệp

Tác giả chế tạo bộ Sticker “STOP LINK – Bộ thẻ cảnh báo chống lừa đảo” gồm 3 màu cảnh báo:

- STOP (Dừng lại trước khi bấm);
- 🔍 ASK (Hỏi người tin cậy);
- ⚠️ REPORT (Báo cáo nội dung xấu).



Bộ Sticker được dán lên mặt sau điện thoại, laptop của HS tạo thành các “điểm chặn thị giác” nhắc nhở an toàn số thường xuyên. Đồng thời, móc khóa in thông điệp nhắc nhở được sản xuất làm phần thưởng, biến kỹ năng trừu tượng thành vật dụng gần gũi hàng ngày.

Khảo sát nhanh bằng Google Form sau 2 tuần triển khai bộ Sticker “STOP LINK” trên 60 HS lớp 12B1 và 11A9 phản hồi rất tích cực: 90% khẳng định biểu tượng giúp dễ nhớ và dễ áp dụng; 85% có thói quen chủ động kiểm tra nguồn liên kết trước khi nhấp chuột; 100% HS cho biết sự hiện diện thường trực của Sticker dán sau điện thoại giúp các em luôn tự kiểm soát hành vi số lý tính và văn minh.

4.2.4. Huấn luyện kỹ năng chuyên sâu theo mô hình “Phản xạ số 4H”

Mô hình 4H bao gồm: HỌC (Learn) - Nhận diện 3 tín hiệu đỏ (đòi giữ bí mật, đòi OTP/chuyển tiền, mạo danh cơ quan công quyền); HỎI (Consult) - Google Form ẩn danh phản hồi tình huống nguy hiểm trong 24 giờ; HÀNH ĐỘNG (Act) - Tổ chức cuộc thi quay video TikTok “Tập làm thám tử mạng” xử lý tình huống trong 5 giây; HỖ TRỢ (Support) - Mạng lưới nhóm nòng cốt phối hợp Đoàn trường kịp thời hỗ trợ đồng đẳng khi HS gặp sự cố.

4.2.5. Xây dựng mạng lưới “Lá chắn Gia đình” và bồi dưỡng học sinh nghiên cứu khoa học chuyên sâu

Tác giả hướng dẫn PHHS thiết lập “Mật mã gia đình” (Family Password) làm chốt chặn phi công nghệ vô hiệu hóa Deepfake AI giả dạng người thân tai nạn tổng tiền. Song song đó, tác giả trực tiếp hướng dẫn nhóm HS nòng cốt (Phạm Tấn Tài, Nguyễn Hoàng Quyên) sự phạm hóa dữ liệu thực nghiệm tại lớp 12B1 thành đề tài nghiên cứu Khoa học kỹ thuật và xuất sắc đạt Giải Nhì cấp Tỉnh năm học 2025-2026, khẳng định tính đúng đắn và hiệu quả lan tỏa của sáng kiến giáo dục.

4.3. Đánh giá hiệu quả thực nghiệm sự phạm và đồng áp dụng

Trải qua 6 tháng thực nghiệm đối chứng nghiêm túc tại trường THPT Sa Đéc, hệ thống các thiết bị giáo dục trực quan và mô hình phản xạ số đã mang lại sự chuyển biến định lượng vượt bậc về năng lực an toàn số của HS:

Bảng 1: So sánh các chỉ số năng lực an toàn số giữa lớp Đối chứng (12B3) và lớp Thực nghiệm (12B1)

Chỉ số đánh giá năng lực	Lớp 12B3 (Đối chứng - 43 HS)	Lớp 12B1 (Thực nghiệm - 41 HS)	Mức độ cải thiện
Nhận diện đúng bảy thao túng tâm lý	44,2% (19/43 HS)	87,8% (36/41 HS)	+ 43,6%
Phản xạ “Dừng lại” trước link lạ	32,6% (14/43 HS)	82,9% (34/41 HS)	+ 50,3%
Chủ động báo cáo với GV/PHHS	14,0% (6/43 HS)	80,5% (33/41 HS)	+ 66,5%

Phân tích kết quả tại Bảng 1 cho thấy sự chênh lệch mang tính đột phá về năng lực phản xạ giữa hai lớp. Chỉ số nhận diện đúng bảy thao túng tâm lý ở lớp thực nghiệm 12B1 đạt tới 87.8% (36/41 HS) trong khi lớp đối chứng 12B3 chỉ đạt 44.2% (hiệu quả cải thiện +43.6%). Chỉ số phản xạ “Dừng lại” khi gặp liên kết lạ ở lớp 12B1 đạt 82.9% (34/41 HS), cao vượt bậc so với lớp đối chứng 12B3 chỉ đạt 32.6% (mức cải thiện +50.3%). Thành công lớn nhất thể hiện ở chỉ số chủ động báo cáo tức thời với GVCN/PHHS để phá vỡ sự cô lập: lớp thực nghiệm 12B1 đạt tỷ lệ rất cao là 80.5% (33/41 HS), trong khi lớp đối chứng 12B3 chỉ đạt tỷ lệ cực kỳ thấp là 14.0% (mức cải thiện +66.5%). Điều này minh chứng rằng mạng lưới hỗ trợ kết nối Gia đình - Nhà trường đã phát huy tác dụng bảo vệ an toàn tối ưu cho HS.

Bảng 2: Kết quả đồng áp dụng bộ giải pháp tại lớp 11A9 (Số: 42 HS)

Chỉ số đánh giá năng lực an toàn số	Trước khi áp dụng	Sau khi áp dụng	Mức độ cải thiện
Tỷ lệ HS nhận diện đúng bẫy lừa đảo mạng	35.7% (15/42 HS)	85.7% (36/42 HS)	+ 50.0%
Tỷ lệ HS thực hiện đúng phản xạ SAFE CODE	21.4% (9/42 HS)	78.6% (33/42 HS)	+ 57.2%
Tỷ lệ phụ huynh HS thiết lập “Mật mã gia đình”	14.3% (6/42 HS)	95.2% (40/42 HS)	+ 80.9%

Để khẳng định tính lan tỏa và khả năng nhân rộng bền vững của bộ giải pháp, kết quả đồng áp dụng tại lớp 11A9 do cô Trang Tuyết Hân làm GVCN cũng ghi nhận những chuyển biến vô cùng tích cực (Bảng 2). Kết quả thống kê chỉ ra tỷ lệ HS lớp 11A9 nhận diện đúng bẫy tăng vọt lên 85.7% (+50% cải thiện); tỷ lệ thực hiện đúng phản xạ kiểm chứng thông tin SAFE CODE đạt 78.6% (+57.2% cải thiện) và đặc biệt chốt chặn “Mật mã gia đình” phối hợp cùng PHHS đạt tỷ lệ thành lập tối ưu lên tới 95.2% (40/42 gia đình thực hiện thành công). Số liệu thực chứng này ở cả khối lớp 12 và khối lớp 11 khẳng định bộ giải pháp trực quan dân điện thoại dường như là một mô hình giáo dục kỹ năng số chuẩn mực, ổn định, mang tính thực tế rất cao và hoàn toàn khả thi để nhân rộng cho mọi đơn vị trường THPT.

5. Kết luận

Nghiên cứu vận dụng hệ sinh thái bộ công cụ trực quan và mô hình phản xạ số trong công tác chủ nhiệm và Hoạt động trải nghiệm tại trường THPT Sa Đéc đã chứng minh tính đúng đắn và hiệu quả vượt trội trong thực tiễn. Việc “vật chất hóa” thông điệp giáo dục thành các sản phẩm nhân dân Sticker cảnh báo STOP LINK dán trực tiếp trên điện thoại và Móc khóa đeo balo mang theo hàng ngày đã tạo dựng thành công những “điểm chặn thị giác” đặc lực, buộc HS phải tri hoãn hành vi trực tuyến bộc phát cảm tính. Đồng thời, việc “quy trình hóa” kỹ năng số thông qua huấn luyện phản xạ SAFE CODE và quy tắc 4H đã giúp HS hình thành phản bản năng tự chủ, bản lĩnh tự vệ chủ động, phá vỡ thế cô lập sợ hãi để kết nối tức thời tìm sự trợ giúp của mạng lưới Gia đình - Nhà trường - Xã hội. Sự chuyển biến sâu sắc từ nhận thức cảm tính lo âu sang nhận thức lý tính tự chủ là minh chứng rõ nét nhất cho tính sư phạm và giá trị nhân văn của sáng kiến, hướng tới việc xây dựng những ngôi trường hạnh phúc và an toàn trong kỷ nguyên chuyển đổi số. Các trường THPT cần chủ động đưa chuyên đề huấn luyện quy tắc phản xạ SAFE CODE và trang bị bộ nhân dân Sticker cảnh báo STOP LINK tích hợp vào tuần sinh hoạt công dân đầu khóa cho HS khối lớp 10 mới chuyển cấp, nhằm trang bị sớm nhất “lá chắn tự vệ” cho HS suốt 3 năm học phổ thông dưới phương châm chủ động phòng bệnh hơn chữa bệnh. Các cơ quan quản lý giáo dục cần xem xét phát triển sáng kiến thành các chuyên đề sinh hoạt chuyên môn chuẩn mực cho Tổ chủ nhiệm lớp, khuyến khích GVCN ứng dụng công nghệ truyền thông đa kênh tương tác với HS và gia đình. Trong tương lai, các thủ đoạn lừa đảo của tội phạm mạng bằng công nghệ trí tuệ nhân tạo (Deepfake, AI) luôn thay đổi khôn lường hàng ngày, do đó nghiên cứu tiếp theo cần liên tục nâng cấp hệ thống kho học liệu cho Chatbot AI trực tuyến và phát triển thêm các bộ Sticker động (phiên bản số) để tăng tính tiếp cận sinh động và kịp thời hơn đối với HS.

Tài liệu tham khảo

- Báo Công an nhân dân (2024). “Bắt cóc online” – Vì sao học sinh, sinh viên dễ bị lừa? <https://cand.com.vn/phap-luat/bat-coc-online-vi-sao-hoc-sinh-sinh-vien-de-bi-lua-i775399/>.
- Báo Pháp luật Việt Nam (2024). Lá chắn mềm bảo vệ giới trẻ trước nguy cơ “bắt cóc online” – Bài 3: Chuyên gia an ninh mạng vạch trần thủ đoạn. <https://baophapluat.vn/la-chan-mem-bao-ve-gioi-tre-truoc-nguy-co-bat-coc-online-bai-3-chuyen-gia-an-ninh-mang-vach-tran-thu-doan.html>.
- Bộ Công an (2024). Bắt cóc online – Những con số cảnh báo. Báo Nhân Dân. <https://nhandan.vn/video-bat-coc-online-nhung-con-so-can-bao-post916970.html>.
- Bộ Giáo dục và Đào tạo (2024). Cảnh báo thủ đoạn “bắt cóc online” nhằm vào học sinh, sinh viên. VTC News. <https://vtcnews.vn/bo-gd-dt-can-bao-thu-doan-bat-coc-online-nham-vao-hoc-sinh-sinh-vien-ar959491.html>.
- Center for Cybercrime Studies (2023). Virtual kidnapping. <https://ccyber.org/ccrimetype/virtual-kidnapping/>.
- Đài Phát thanh và Truyền hình Đồng Tháp (2025). Cảnh báo thủ đoạn bắt cóc, đe dọa tổng tiền học sinh [Video]. YouTube. <https://www.youtube.com/watch?v=QPXBLaVFMcM>.
- Legal Service India. (2021). The concept of online kidnapping with reference to the Indian laws. <https://www.legalserviceindia.com/legal/article-3437-the-concept-of-online-kidnapping-with-reference-to-the-indian-laws.html>.
- Lưu Hà Chi (2024). Kiểm định chi bình phương SPSS: Khái niệm, mục đích & cách chạy. Luận văn Việt. <https://luanvanviet.com/kiem-dinh-chi-binh-phuong-spss/>.
- Trường THPT Lê Hồng Phong Hà Nội (2023). Tâm lý học sinh trung học phổ thông. <https://lehongphonghn.edu.vn/tam-li-hoc-sinh-trung-hoc-pho-thong/>.