NĂNG LỰC AN TOÀN SỐ CỦA SINH VIÊN DÂN TỘC THIỂU SỐ TẠI TRƯỜNG ĐẠI HỌC SƯ PHẠM, ĐẠI HỌC THÁI NGUYÊN

NGUYỄN THỊ HUỆ
Viện Nghiên cứu Con người, Gia đình và Giới

Nhận bài ngày 15/7/2026. Sửa chữa xong 20/8/2026. Duyệt đăng 25/8/2026.

Abstract

This article examines the digital safety competence of ethnic minority students at Thai Nguyen University of Education in the context of digital transformation. Based on a survey of 200 ethnic minority students, the findings indicate that although the participants demonstrate a relatively high level of awareness of digital safety, they remain exposed to various risks in cyberspace. On this basis, the article proposes several recommendations for strengthening digital safety competence among ethnic minority students.

Keywords: *Digital safety, ethnic minorities, students.*

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số ở Việt Nam, sự phát triển nhanh của Internet, trí tuệ nhân tạo và các nền tảng mạng xã hội (MXH) đã tái định hình sâu sắc cách con người giao tiếp, học tập và tương tác. Không gian mạng đã trở thành một môi trường thiết yếu, đặc biệt đối với sinh viên (SV). Không gian mạng là "mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian" (Quốc hội, 2018). Trong không gian đó, SV đang phải đối mặt với nhiều nguy cơ và rủi ro về an toàn, khiến họ trở nên đặc biệt dễ bị tổn thương (Dương Thị Thu Hương, Nguyễn Thế Duy Long, 2024). Để chủ động ứng phó với những thách thức từ không gian mạng, Thủ tướng chính phủ đã ký quyết định phê duyệt Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 và Chương trình "Giáo dục lý tưởng cách mạng, đạo đức, lối sống văn hóa cho thanh niên, thiếu niên, nhi đồng trên không gian mạng giai đoạn 2022-2030" nhằm trang bị cho SV những năng lực số cần thiết để đảm bảo an toàn trên không gian mạng (Thủ tướng Chính phủ, 2022a, 2022b).

2. Phương pháp nghiên cứu

Nghiên cứu sử dụng phương pháp điều tra bằng bảng hỏi làm công cụ thu thập dữ liệu chính bên cạnh phỏng vấn sâu học sinh và giáo viên. Khảo sát thực địa được triển khai vào tháng 6 năm 2026 tại tỉnh Thái Nguyên. Mẫu khảo sát gồm 200 SV dân tộc thiểu số (DTTS) tại Trường Đại học Sư phạm, Đại học Thái Nguyên. Dữ liệu thu về được xử lý và phân tích bằng phần mềm SPSS.22. Cơ cấu mẫu khảo sát được phân bổ tương đối đồng đều theo các tiêu chí nhân khẩu học, đảm bảo độ tin cậy của dữ liệu nghiên cứu, được thể hiện tại bảng 1.

Email: huexhh@gmail.com

Bảng 1: Đặc điểm mẫu khảo sát

Tiêu chí		Số lượng	Tỷ lệ %	Tiêu chí		Số lượng	Tỷ lệ %
Giới tính	Nam	81	40,5	Nơi sinh sống trước khi học đại học	Miền núi	95	47,5
	Nữ	119	59,5		Nông thôn	70	35,0
	Tổng	200	100,0		Đô thị	35	17,5
Năm học	Năm thứ nhất	74	37,0		Tổng	200	100,0
	Năm thứ hai	64	32,0	Điều kiện kinh tế gia đình	Nghèo, cận nghèo	48	24,0
	Năm thứ ba	36	18,0		Trung bình	149	74,5
	Năm thứ tư	26	13,0		Khá giả	3	1,5
	Tổng	200	100,0		Tổng	200	100,0

Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

3. Kết quả nghiên cứu

3.1. Nhận thức về an toàn số

Luật Bảo vệ dữ liệu cá nhân (Luật số 91/2025/QH15) quy định về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan; có hiệu lực thi hành từ ngày 01/01/2026. Khung năng lực số dành cho người học xác định an toàn là một miền năng lực tập trung vào việc bảo vệ dữ liệu, thiết bị, sức khỏe và môi trường số; bao gồm các kỹ năng như bảo mật thông tin cá nhân, quản lý rủi ro mạng, sử dụng công nghệ số an toàn, bảo đảm sức khỏe tâm lý và thể chất khi tương tác trong môi trường số và thúc đẩy trách nhiệm bảo vệ môi trường kỹ thuật số (Bộ Giáo dục và Đào tạo, 2025).

Bảng 2: Năng lực bảo vệ thiết bị và dữ liệu cá nhân của SV DTTS

STT	Biểu hiện của năng lực	Điểm trung bình (Mean)	Độ lệch chuẩn (SD)
1	Tôi nhận biết được các rủi ro/mối đe dọa trong môi trường số (như virus, mã độc, phần mềm độc hại…).	4.05	0.837
2	Tôi chủ động thực hiện các biện pháp an toàn, bảo mật thiết bị (như cài mật khẩu mạnh…).	4.44	0.793
3	Tôi tự mình thiết lập, điều chỉnh được các phương thức bảo vệ phù hợp cho thiết bị số của mình (như cập nhật phần mềm diệt virus, thiết lập trình duyệt web an toàn…)	3.80	0.989
4	Tôi luôn đọc kỹ các thông báo về "Chính sách Quyền riêng tư" khi đăng ký sử dụng các dịch vụ số hoặc ứng dụng mạng xã hội.	3.83	1.124
5	Tôi chủ động tìm hiểu và thực hiện các cách thức để bảo vệ dữ liệu cá nhân khi chia sẻ thông tin lên MXH	4.18	0.939
6	Tôi có khả năng đánh giá mức độ phù hợp và an toàn của một ứng dụng/dịch vụ số trước khi đồng ý cung cấp thông tin cá nhân cho họ.	3.90	0.866

Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Kết quả khảo sát tại bảng 2 cho thấy năng lực bảo vệ thiết bị và dữ liệu cá nhân của SV DTTS đạt mức khá tốt, với điểm trung bình tổng thể đạt . Cụ thể, SV thể hiện tính chủ động thực hiện các biện pháp an toàn, cài đặt mật khẩu mạnh () và bảo vệ dữ liệu cá nhân khi chia sẻ trên MXH (). Bên cạnh đó, mức độ nhận diện các rủi ro, mối đe dọa như virus, mã độc cũng được đánh giá ở mức khá tốt (). Mặc dù vậy, SV DTTS tự đánh giá năng lực tự thiết lập, điều chỉnh phương thức bảo vệ thiết bị, đọc kỹ các thông báo về "Chính sách quyền riêng tư" còn hạn chế.

Kết quả này tương đồng với Khung năng lực số châu Âu DigComp 2.2 của Vuorikari và cộng sự (2022) khi chỉ ra rằng người học thường tự tin ở mức thao tác người dùng cơ bản nhưng gặp nhiều rào cản khi chuyển dịch sang mức độ tự chủ kỹ thuật và quản trị rủi ro hệ thống. Đồng thời, xu hướng bỏ qua hoặc xem nhẹ các chính sách quyền riêng tư của sinh viên đã được Obar và Oeldorf-Hirsch (2020) giải thích rằng người dùng ngại đọc thông tin, thường bỏ qua và dễ dàng chấp thuận các điều khoản dịch vụ số.

Bảng 3: Năng lực bảo vệ sức khỏe, an sinh số và môi trường của SV DTTS

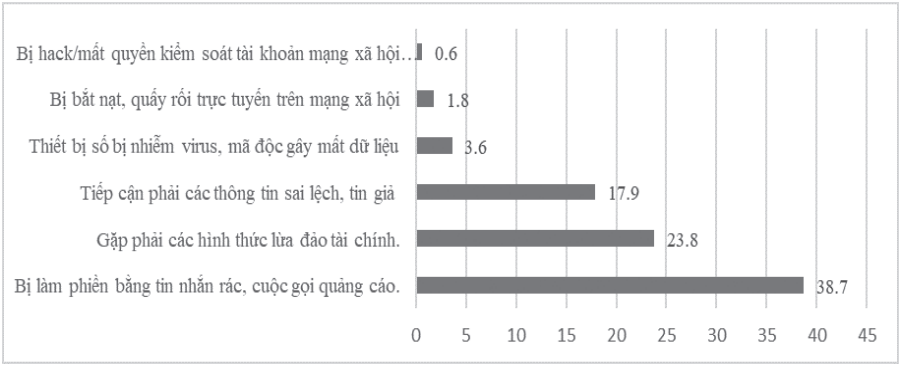
STT	Biểu hiện của năng lực	Điểm trung bình (Mean)	Độ lệch chuẩn (SD)
1	Tôi chủ động thực hiện các biện pháp để tránh rủi ro đến sức khỏe thể chất khi sử dụng thiết bị số (cài đặt thời gian vào mạng, độ sáng màn hình để tránh mỏi mắt,….	4.19	0.863
2	Tôi chủ động thực hiện các biện pháp để tránh rủi ro đến sức khỏe tinh thần (căng thẳng, nghiện mạng…) khi sử dụng thiết bị số	3.99	0.868
3	Tôi biết cách bảo vệ bản thân khỏi nguy cơ bị bắt nạt, quấy rối trực tuyến.	4.27	0.838
4	Công nghệ số giúp bảo tồn và lan tỏa văn hóa của dân tộc tôi	4.41	0.731
5	Công nghệ số giúp tăng cường sự gắn kết trong cộng đồng/xã hội	4.34	0.779
6	Tôi biết cách bật chế độ tiết kiệm pin, cài đặt thời gian tự động tắt màn hình khi không sử dụng điện thoại	4.44	0.900
7	Tôi có thói quen xóa các email rác, hủy đăng ký các bản tin không đọc, xóa bớt ảnh/video trùng lặp trên iCloud hoặc Google Drive để tiết kiệm dung lượng	3.83	1.208

Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Số liệu tại bảng 3 phản ánh năng lực bảo vệ sức khỏe, an sinh số và môi trường của SV DTTS ở mức khá tốt (). Đáng chú ý, SV thể hiện sự nhận thức cao về vai trò của công nghệ số trong việc bảo tồn, lan tỏa các giá trị văn hóa dân tộc () và thúc đẩy gắn kết cộng đồng (). Kết quả này củng cố quan điểm của Dyson và cộng sự (2015) khi nhấn mạnh rằng các phương tiện truyền thông số đóng vai trò là công cụ trao quyền mạnh mẽ, giúp thanh niên tái định hình và lan tỏa bản sắc văn hóa dân tộc trong không gian liên văn hóa. Bên cạnh đó, SV cũng tự tin trong việc phòng ngừa bắt nạt trực tuyến () và điều chỉnh thiết bị để tránh rủi ro đến sức khỏe thể chất (). Dù vậy, mức độ chủ động ứng phó với rủi ro sức khỏe tinh thần như căng thẳng hay nghiện mạng vẫn còn hạn chế (), phản ánh thách thức chung của người trẻ trước hội chứng sợ bỏ lỡ (FOMO) và quá tải kết nối (Twenge et al., 2018). Ở khía cạnh môi trường số, dù SV làm rất tốt các thao tác tiết kiệm pin cho thiết bị số (), thói quen giảm thiểu rác thải dữ liệu qua việc dọn dẹp và xóa thư rác lại đạt mức thấp nhất (). Kết quả này tương đồng với quan sát của Preist và cộng sự (2016) về sự thiếu hụt nhận thức của người dùng đối với dấu chân carbon do dữ liệu lưu trữ trực tuyến tạo ra. Điều này đặt ra nhu cầu cần nâng cao giáo dục an toàn số cho SV DTTS một cách toàn diện hơn. Đánh giá tổng thể, năng lực an toàn số tổng hợp được tạo ra từ 13 biến quan sát được trình bày ở trên đạt điểm trung bình . Giá trị độ lệch chuẩn thấp phản ánh sự đồng đều giữa các SV DTTS trong việc nhận thức an toàn số trên không gian mạng. Kết quả này cho thấy SV DTTS không chỉ nắm vững các thao tác kỹ thuật cơ bản để bảo vệ thiết bị và dữ liệu cá nhân mà còn thể hiện ý thức trách nhiệm cao đối với việc bảo vệ sức khỏe, an sinh số và môi trường sinh thái số.

3.2. Thực trạng an toàn số

Hình 1: Tỷ lệ SV DTTS thường xuyên gặp phải các vấn đề an toàn số trong 6 tháng qua (%)

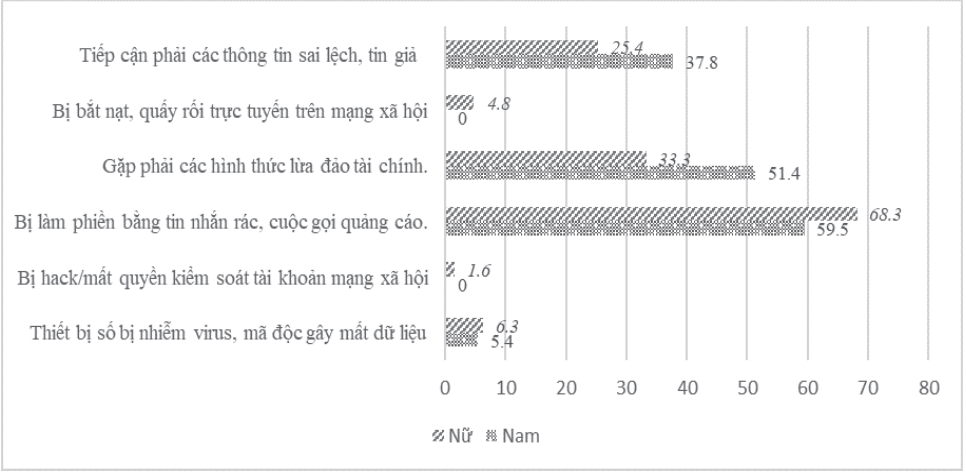


Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Có sự chênh lệch rõ rệt giữa các hình thức rủi ro an toàn số mà SV DTTS gặp phải trong 6 tháng qua. Nhóm rủi ro có tần suất xuất hiện cao nhất thuộc về hành vi bị làm phiền bởi tin nhắn, cuộc gọi rác (38,7%) và các bẫy

lừa đảo tài chính trực tuyến (23,8%). Kết quả này phản ánh xu hướng tương đồng với Báo cáo tình hình lừa đảo trực tuyến tại Việt Nam của Cục An toàn thông tin (2023), trong đó chỉ ra rằng người trẻ tuổi và SV là nhóm mục tiêu bị nhắm đến nhiều nhất bởi các thủ đoạn lừa đảo việc làm và mạo danh tài chính qua mạng xã hội do tâm lý tìm kiếm việc làm thêm và mức độ bảo mật số điện thoại cá nhân còn lỏng lẻo. Bên cạnh đó, có 17,9% SV gặp phải các vấn đề về thông tin sai lệch, tin giả cho thấy thực trạng về tiếp cận thông tin trong xã hội số. Kết quả này tương đồng với nghiên cứu của Đặng Vân Trang (2025), khi nhấn mạnh rằng SV Hà Nội có tỷ lệ cao gặp phải các thông tin sai lệch trên môi trường số. Ở chiều ngược lại, các rủi ro liên quan đến sự cố kỹ thuật và hành vi bắt nạt trực tuyến lại có tỷ lệ xuất hiện rất thấp: thiết bị nhiễm virus gây mất dữ liệu (3.6%), bị bắt nạt/quấy rối trực tuyến (1.8%) và mất kiểm soát tài khoản cá nhân (0.6%).

Hình 2: Tỷ lệ SV DTTS thường xuyên gặp phải các vấn đề an toàn số trong 6 tháng qua theo giới tính (%)



Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Phân tích so sánh rủi ro an toàn số theo biến số giới tính cho thấy sự khác biệt đáng kể về loại hình nguy cơ mà SV nam và nữ DTTS phải đối mặt. SV nam thường gặp phải các vấn đề về lừa đảo tài chính trực tuyến (51,4% ở nam so với 33.3% ở nữ) và tiếp cận với thông tin sai lệch, tin giả (37.8% nam so với 25.4% ở nữ). Xu hướng này phản ánh sự năng động nhưng cũng tiềm ẩn nhiều rủi ro của nam giới trong các hoạt động giao dịch số và tương tác trên các diễn đàn mạng mở. Báo cáo "tình hình lừa đảo tại Việt Nam năm 2023" của Liên minh Chống lừa đảo toàn cầu cho thấy, lừa đảo đã gây ra tác động sâu sắc và để lại dấu ấn khó phai mờ trong lòng nạn nhân, không chỉ tổn thất về tài chính mà còn cả nỗi đau tinh thần (Liên minh Chống lừa đảo toàn cầu, 2023).

Ở chiều ngược lại, SV nữ thường gặp phải các rủi ro bị làm phiền bởi tin nhắn rác, cuộc gọi quảng cáo chiếm tới 68,3% (cao hơn mức 59,5% của nam). Đáng lưu ý, các nguy cơ về bạo lực mạng như bị bắt nạt, quấy rối trực tuyến (4,8%) và bị mất quyền kiểm soát tài khoản cá nhân (1,6%) chỉ được ghi nhận ở SV nữ, trong khi tỷ lệ này ở SV nam là 0%. Bắt nạt trực tuyến là việc bắt nạt trên các công cụ kỹ thuật số, có thể diễn ra trên phương tiện MXH, nền tảng nhắn tin, chơi game và điện thoại di động (Quỹ Nhi đồng Liên hợp quốc, 2021). Thực tế cho thấy, khi phụ nữ và trẻ em gái truy cập Internet, họ phải đối mặt với nguy cơ bị bạo lực thường xuyên hơn nam giới (UN Women, 2022). Khảo sát của UNICEF (2019) cho thấy, 21% thanh thiếu niên từng là nạn nhân của bắt nạt trên mạng. Điều này cho thấy, rủi ro trên không gian mạng không còn là nguy cơ tiềm ẩn mà đã trở thành một phần trải nghiệm của nữ SV, một bộ phận không nhỏ SV phải chịu đựng các tổn thương về mặt tâm lý và xã hội.

Bảng 4: Tỷ lệ SV DTTS thường xuyên gặp phải các vấn đề an toàn số trong 6 tháng qua theo năm học (%)

Tình huống rủi ro an toàn số	Năm thứ nhất	Năm thứ hai	Năm thứ ba	Năm thứ tư
Thiết bị số bị nhiễm virus, mã độc gây mất dữ liệu	6,3	5,6	6,7	5,9
Bị hack/mất quyền kiểm soát tài khoản MXH	3,1	0	0	0

Bị làm phiền bằng tin nhắn rác, cuộc gọi quảng cáo.	75	58,3	66,7	58,8
Gặp phải các hình thức lừa đảo tài chính.	18,8	47,2	53,3	52,9
Bị bắt nạt, quấy rối trực tuyến trên MXH	3,1	0	6,7	5,9
Tiếp cận phải các thông tin sai lệch, tin giả	25	22,2	33,3	52,9

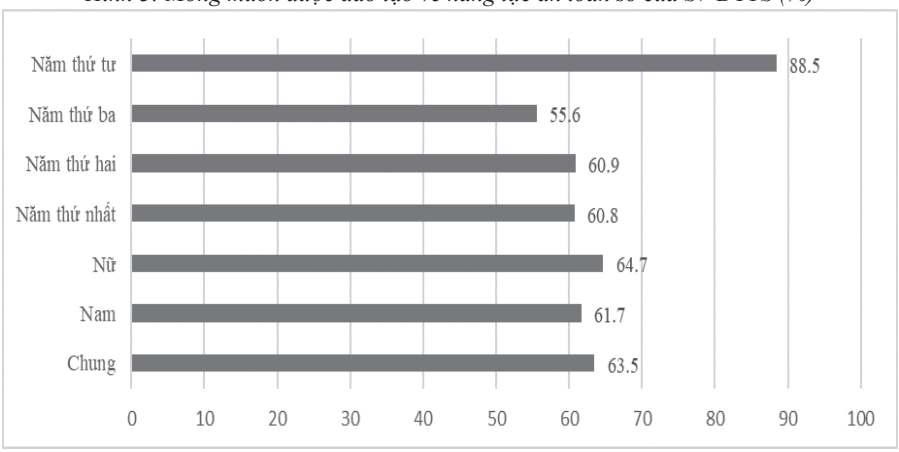
Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Phân tích so sánh theo tiến trình đào tạo tại bảng 4 cho thấy bức tranh về các rủi ro an toàn số của SV DTTS. Có xu hướng gia tăng hai loại hình rủi ro là bẫy lừa đảo tài chính trực tuyến và tiếp cận thông tin sai lệch/tin giả theo các năm học. Cụ thể, tỷ lệ SV thường xuyên gặp lừa đảo tài chính tăng từ 18,8% ở năm thứ nhất lên 47,2% ở năm thứ hai, 53,3% ở năm thứ ba và 52,9% ở năm thứ tư. Tương tự, tần suất tiếp cận tin giả ở SV năm cuối lên tới 52,9%, cao hơn gấp đôi so với SV năm nhất (25%). Sự gia tăng này có thể do các khóa cuối mở rộng tối đa các tương tác số phục vụ tìm kiếm việc làm, kiến tập, thực tập và mở rộng mạng lưới quan hệ xã hội.

Tin nhắn rác là tin nhắn quảng cáo mà không được sự đồng ý trước của người sử dụng, cuộc gọi rác là gọi điện thoại quảng cáo mà không được sự đồng ý trước của người sử dụng (Chính Phủ, 2020). Dù ở năm học nào, SV đều phải đối mặt với vấn đề nhận cuộc gọi và tin nhắn rác ở mức rất cao, phản ánh nguy cơ lộ lọt thông tin cá nhân ngay trong giai đoạn đầu nhập học.

Ở chiều ngược lại, các sự cố kỹ thuật và bạo lực mạng tiếp tục duy trì với tỷ lệ thấp, rủi ro thiết bị nhiễm mã độc từ 5,6% đến 6,7%; hiện tượng mất quyền kiểm soát tài khoản MXH đã hoàn toàn không xảy ra ở SV từ năm thứ hau đến năm thứ cuối. Điều đó cho thấy, khi SV có những trải nghiệm tích lũy thêm thâm niên học tập, được trang bị thêm các kinh nghiệm thì năng lực bảo vệ tài khoản được củng cố hơn.

Hình 3: Mong muốn được đào tạo về năng lực an toàn số của SV DTTS (%)



Nguồn: Kết quả khảo sát của nhiệm vụ, 2026

Số liệu tại hình 3 phản ánh nhu cầu cấp thiết và thực tế của SV DTTS đối với việc được đào tạo bài bản về an toàn số, với tỷ lệ mong muốn chung đạt tới 63,5%. Xét theo biến số giới tính, sự chênh lệch giữa SV nam (61,7%) và SV nữ (64,7%) là không đáng kể, khẳng định mong muốn được nâng cao năng lực an toàn số là mối quan tâm đồng đều của cả hai giới.

Xét theo năm học, trong khi tỷ lệ có nhu cầu đào tạo duy trì ổn định từ năm thứ nhất đến năm thứ ba (từ 55,6% đến 60,9%), thì con số này tăng vọt lên mức 88,5% ở SV năm thứ tư có lẽ do SV năm cuối là nhóm đối diện nhiều nhất với các nguy cơ lừa đảo tài chính và tin giả do nhu cầu tìm kiếm việc làm. Hơn nữa, với tư cách là giáo viên tương lai, SV sư phạm năm cuối ý thức sâu sắc rằng năng lực an toàn số không chỉ là công cụ bảo vệ cá nhân, mà còn là chuẩn năng lực nghề nghiệp cốt lõi để xây dựng môi trường học đường số an toàn cho học sinh sau này. Kết quả này đặt ra yêu cầu cấp thiết cho nhà trường trong việc thiết kế các chuyên đề bồi dưỡng, tập huấn an toàn số chuyên sâu, đặc biệt ưu tiên tích hợp vào giai đoạn rèn luyện nghiệp vụ sư phạm trước khi SV ra trường.

4. Kết luận

Bài viết đã phác họa một bức tranh đa chiều về năng lực an toàn số của SV DTTS. Kết quả cho thấy, không gian mạng vừa là một môi trường trao quyền, cung cấp công cụ học tập và kết nối, vừa là một không gian đầy rủi ro, nơi họ phải đối mặt với các nguy cơ từ lừa đảo, mất an toàn dữ liệu đến quấy rối và bắt nạt trực tuyến. Các rủi ro mà SV DTTS phải đối mặt không đồng nhất mà thay đổi theo từng năm học, cho thấy sự cần thiết của các chương trình đào tạo được thiết kế chuyên biệt dành cho SV. Từ những phát hiện trên, để nâng cao năng lực an toàn số cho SV DTTS, bài viết đề xuất khuyến nghị như sau.

Đối với Nhà trường và Phòng Đào tạo - Công tác SV, tích hợp chuyên đề an toàn số vào chương trình đào tạo nghiệp vụ sư phạm, xây dựng các mô-đun bồi dưỡng bắt buộc hoặc tín chỉ tự chọn về an toàn số, đặc biệt chú trọng đào tạo thực hành các kỹ năng phòng chống tội phạm công nghệ cao, nhận diện bẫy lừa đảo tài chính và xác thực thông tin số. Đồng thời thực hiện tuyên truyền an toàn số có yếu tố nhạy cảm giới, thiết kế các cẩm nang, diễn đàn tư vấn phòng ngừa quấy rối trực tuyến và bảo vệ quyền riêng tư cá nhân hướng tới nữ SV; đẩy mạnh cảnh báo rủi ro lừa đảo tài chính, việc làm online cho nam SV.

Đối với sinh viên, tích cực tự học các phương thức bảo vệ thiết bị số và dữ liệu cá nhân, tạo thói quen kiểm tra và đọc kỹ các chính sách bảo mật trước khi chấp thuận các điều khoản dịch vụ. Bên cạnh đó, SV cần rèn kỹ năng tư duy phản biện thông tin, thực hành thói quen kiểm chứng chéo nguồn tin trước khi chia sẻ trên MXH; hình thành thói quen định kỳ dọn dẹp không gian lưu trữ đám mây và xử lý rác thải điện tử đúng quy chuẩn môi trường.

Tài liệu tham khảo

Bộ Giáo dục và Đào tạo (2025). *Thông tư số 02/2025/TT-BGDĐT quy định Khung năng lực số cho người học*.

Chính phủ (2020). *Nghị định số 91/2020/NĐ-CP về chống tin nhắn rác, thư điện tử rác, cuộc gọi rác*. https://vanban.chinhphu.vn/default.aspx?docid=200773&pageid=27160.

Cục An toàn thông tin (2023). *Báo cáo tổng hợp tình hình an toàn thông tin và lừa đảo trực tuyến tại Việt Nam năm 2023*. Bộ Thông tin và Truyền thông.

Đặng, V. T. (2025). *Rủi ro trong tiếp cận thông tin trên mạng xã hội của sinh viên Hà Nội*. Đối thoại Phát triển. https://www.doithoaiphattrien.vn/vi/news/van-de-hom-nay/rui-ro-trong-tiep-can-thong-tin-tren-mang-xa-hoi-cua-sinh-vien-ha-noi-12323.html.

Dương, T. T. H., & Nguyễn, T. D. L. (2024). Những nguy cơ mất an toàn trong sử dụng mạng xã hội trên không gian mạng của sinh viên hiện nay. *Tạp chí Lý luận Chính trị và Truyền thông*. https://lyluanchinhtrivatruyenthong.vn/nhung-nguy-co-mat-an-toan-trong-su-dung-mang-xa-hoi-tren-khong-gian-mang-cua-sinh-vien-hien-nay-p28604.html.

Dyson, L. E., Grant, S., & Hendriks, M. (Eds.). (2015). *Indigenous people and mobile technologies* (1st ed.). Routledge. https://doi.org/10.4324/9781315759364.

Global Anti-Scam Alliance, & Chống Lừa Đảo (2023). *Thực trạng lừa đảo ở Việt Nam 2023*. https://chongluadao.vn/blog/VietNamScamReport2023.pdf.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870.

Preist, C., Schien, D., & Blevis, E. (2016). Understanding and mitigating the effects of device and cloud service design decisions on the environmental footprint of digital infrastructure. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 1324–1337). Association for Computing Machinery. https://doi.org/10.1145/2858036.2858378.

Quốc hội (2018). *Luật An ninh mạng (Luật số 24/2018/QH14)*.

Thủ tướng Chính phủ (2022a). *Quyết định số 311/QĐ-TTg phê duyệt Chương trình "Giáo dục lý tưởng cách mạng, đạo đức, lối sống văn hóa cho thanh niên, thiếu niên, nhi đồng trên không gian mạng giai đoạn 2022–2030"*.

Thủ tướng Chính phủ (2022b). *Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030*. https://vanban.chinhphu.vn/?docid=206362&pageid=27160.

Twenge, J. M., Martin, G. N., & Campbell, W. K. (2018). Decreases in psychological well-being among American adolescents after 2012 and links to screen time during the rise of smartphone technology. *Emotion, 18*(6), 765–780. https://doi.org/10.1037/emo0000403.

UN Women (2022). *Bạo lực phụ nữ và trẻ em gái qua mạng và công nghệ thông tin–truyền thông trong đại dịch COVID-19*. https://vietnam.un.org/vi/download/108826/186080.

UNICEF Việt Nam (2019). *Bắt nạt trẻ nhỏ trên mạng và những tác động đến tâm lý trẻ em*. https://www.unicef.org/vietnam/vi/th%C3%B4ng-c%C3%A1o-b%C3%A1o-ch%C3%AD/b%E1%BA%AFt-n%E1%BA%A1t-tr%E1%BA%BB-nh%E1%BB%8F-tr%C3%AAn-m%E1%BA%A1ng-v%C3%A0-nh%E1%BB%AFng-t%C3%A1c-%C4%91%E1%BB%99ng-%C4%91%E1%BA%BFn-t%C3%A2m-l%C3%BD-tr%E1%BA%BB-em.

UNICEF Việt Nam (2021). *Bắt nạt trực tuyến là gì – Làm thế nào để ngăn chặn điều này?* https://www.unicef.org/vietnam/vi/bat-nat-truc-tuyen-la-gi-lam-the-nao-de-ngan-chan-dieu-nay.

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens—with new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/115376.