

XÂY DỰNG VĂN HÓA AN TOÀN THÔNG TIN TẠI CÁC CƠ SỞ GIÁO DỤC TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

Đỗ Mạnh Dũng

Khoa Công nghệ Thông tin và Ngoại ngữ - Trường Cao đẳng Lào Cai

Tóm tắt: Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ, các cơ sở giáo dục ngày càng phụ thuộc vào hệ thống công nghệ thông tin và dữ liệu số. Tuy nhiên, bên cạnh những lợi ích lớn, môi trường số cũng đặt ra các nguy cơ an toàn thông tin ngày càng phức tạp, đặc biệt liên quan đến hành vi người dùng và văn hóa tổ chức. Bài báo này tập trung phân tích vai trò của văn hóa an toàn thông tin trong giáo dục; làm rõ các thành tố cấu thành văn hóa an toàn thông tin; đánh giá thực trạng nhận thức, thái độ và hành vi của giáo viên, học sinh – sinh viên trong bối cảnh số hóa; từ đó đề xuất các giải pháp xây dựng và phát triển văn hóa an toàn thông tin tại các cơ sở giáo dục. Các giải pháp bao gồm nâng cao nhận thức, hoàn thiện quy tắc ứng xử số, xây dựng chính sách nội bộ, hình thành đội ngũ đại sứ an toàn thông tin và xây dựng môi trường số minh bạch, nhân văn. Kết quả nghiên cứu góp phần cung cấp cơ sở khoa học cho các trường học trong quá trình triển khai chuyển đổi số an toàn và bền vững.

Từ khóa: an toàn thông tin; văn hóa số; văn hóa an toàn thông tin; giáo dục; chuyển đổi số.

BUILDING AN INFORMATION SECURITY CULTURE AT EDUCATIONAL INSTITUTIONS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract: In the context of rapid digital transformation, educational institutions are increasingly dependent on information technology systems and digital data. Despite the significant benefits, the digital environment also poses complex cybersecurity risks, particularly those arising from user behavior and organizational culture. This paper analyzes the role of cybersecurity culture in education, identifies key components of cybersecurity culture, and examines the current awareness, attitudes, and behaviors of teachers and students in the digital era. Based on these insights, the study proposes several solutions to develop a strong cybersecurity culture in educational institutions, including raising awareness, establishing digital codes of conduct, developing internal policies, building cybersecurity ambassadors, and fostering a transparent and ethical digital environment. The findings aim to provide scientific foundations for schools to implement safe and sustainable digital transformation.

Keywords: cybersecurity; digital culture; cybersecurity culture; education; digital transformation.

Nhận bài: 20/10/2025

Phản biện: 19/11/2025

Duyệt đăng: 23/11/2025

I. ĐẶT VẤN ĐỀ

Chuyển đổi số đang trở thành xu thế tất yếu trong lĩnh vực giáo dục, góp phần đổi mới phương pháp dạy – học, thúc đẩy quản trị nhà trường hiện đại và nâng cao chất lượng đào tạo. Các hệ thống quản lý học tập (LMS), học liệu số, dữ liệu số hóa hồ sơ học sinh – sinh viên, nền tảng dạy học trực tuyến và các công cụ tương tác số ngày càng được sử dụng rộng rãi. Tuy nhiên, cùng với sự mở rộng của không gian số, các nguy cơ mất an toàn thông tin cũng gia tăng cả về mức độ lẫn phạm vi. Nhiều sự cố như rò rỉ dữ liệu cá nhân, xâm nhập tài khoản, lừa đảo trực tuyến hoặc vi phạm đạo đức số cho thấy an toàn thông tin đã trở thành thách thức đáng quan tâm đối với các cơ sở giáo dục.

Thực tế cho thấy phần lớn các rủi ro an toàn thông tin trong nhà trường không chỉ xuất phát từ các lỗ hổng kỹ thuật mà còn liên quan trực tiếp đến nhận thức, hành vi và thói quen của người dùng. Giáo viên, học sinh – sinh viên là nhóm sử dụng thường xuyên các thiết bị và nền tảng số nhưng đa số chưa được trang bị đầy đủ kỹ năng an toàn thông tin. Việc chia sẻ mật khẩu, sử dụng phần mềm không rõ nguồn gốc, truy cập liên kết

lạ hay thiếu thận trọng khi bảo vệ dữ liệu cá nhân vẫn diễn ra phổ biến. Bên cạnh đó, nhiều cơ sở giáo dục chưa xây dựng được bộ quy tắc ứng xử số, chưa có cơ chế quản trị an toàn thông tin thống nhất, dẫn đến khó khăn khi triển khai chuyển đổi số an toàn.

Trong bối cảnh đó, xây dựng văn hóa an toàn thông tin – được hiểu là hệ thống các giá trị, chuẩn mực, thái độ và hành vi tích cực trong sử dụng công nghệ – trở thành yêu cầu cấp thiết đối với các cơ sở giáo dục. Văn hóa an toàn thông tin giúp hình thành thói quen sử dụng an toàn, nâng cao trách nhiệm cá nhân, thúc đẩy tuân thủ chính sách và tạo ra môi trường số lành mạnh trong nhà trường. Đây chính là nền tảng quan trọng để đảm bảo chuyển đổi số diễn ra hiệu quả, bền vững và an toàn.

II. NỘI DUNG NGHIÊN CỨU

2.1. Khái niệm an toàn thông tin và văn hóa an toàn thông tin

An toàn thông tin (Information Security) được hiểu là việc bảo vệ thông tin khỏi các nguy cơ bị truy cập trái phép, bị sửa đổi, phá hoại hoặc gián đoạn. Theo mô hình CIA, an toàn thông tin bao gồm ba yếu tố cốt lõi: tính bảo mật

(Confidentiality), tính toàn vẹn (Integrity) và tính sẵn sàng (Availability).

Văn hóa an toàn thông tin (Cybersecurity Culture) là tập hợp các giá trị, chuẩn mực, niềm tin, thói quen và hành vi của các thành viên trong tổ chức đối với vấn đề bảo vệ thông tin. Theo quan điểm của ENISA (EU), văn hóa an toàn thông tin không chỉ liên quan đến công nghệ mà còn bao gồm ý thức tự giác, thái độ tích cực, tinh thần trách nhiệm và khả năng ra quyết định an toàn trong môi trường số.

Trong bối cảnh giáo dục, văn hóa an toàn thông tin là nền tảng giúp mỗi thành viên – từ cán bộ quản lý, giáo viên đến học sinh – sinh viên – chủ động phòng ngừa rủi ro và hành xử đúng chuẩn mực khi sử dụng công nghệ.

2.2. Ý nghĩa của văn hóa an toàn thông tin trong cơ sở giáo dục

Văn hóa an toàn thông tin đóng vai trò then chốt trong việc đảm bảo sự phát triển bền vững của các cơ sở giáo dục trong bối cảnh chuyển đổi số. Khi các hoạt động dạy học, quản lý và tương tác đều diễn ra trên môi trường số, yếu tố con người trở thành mắt xích quan trọng nhất quyết định sự an toàn của hệ thống. Văn hóa an toàn thông tin không chỉ giúp giảm thiểu rủi ro mà còn nâng cao hiệu quả quản trị và chất lượng giáo dục. Ý nghĩa nổi bật của văn hóa an toàn thông tin thể hiện ở các khía cạnh sau:

Bảo vệ dữ liệu và quyền riêng tư của người học – người dạy: Cơ sở giáo dục lưu trữ nhiều loại dữ liệu quan trọng như hồ sơ cá nhân, kết quả học tập, thông tin sức khỏe, lịch sử tương tác trên môi trường số,... Đây là những dữ liệu nhạy cảm, dễ bị xâm phạm nếu người dùng thiếu ý thức bảo vệ. Văn hóa an toàn thông tin góp phần hình thành thói quen bảo mật thông tin, đảm bảo quyền riêng tư của giáo viên và học sinh theo đúng quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Giảm thiểu rủi ro từ yếu tố con người: Theo các nghiên cứu quốc tế, hơn 70% sự cố an toàn thông tin bắt nguồn từ lỗi chủ quan của người dùng: sử dụng mật khẩu yếu, chia sẻ tài khoản, mở email lạ, tải phần mềm không rõ nguồn gốc, kết nối Wi-Fi công cộng,... Văn hóa an toàn thông tin giúp mỗi cá nhân nâng cao nhận thức và trách nhiệm, từ đó hạn chế các hành vi rủi ro trong quá trình sử dụng công nghệ.

Đảm bảo hoạt động dạy học và quản lý không bị gián đoạn: Trong môi trường giáo dục số, sự cố an ninh mạng có thể dẫn tới ngừng trệ hệ thống LMS, gián đoạn bài giảng, mất dữ liệu học tập

hoặc làm tê liệt hệ thống quản lý trường học. Khi văn hóa an toàn thông tin được xây dựng vững chắc, nguy cơ sự cố giảm đáng kể, góp phần duy trì hoạt động dạy học và quản trị nhà trường thông suốt, hiệu quả.

Xây dựng môi trường số lành mạnh, văn minh: Văn hóa an toàn thông tin còn gắn liền với văn hóa ứng xử số và đạo đức số. Một môi trường số an toàn được tạo dựng khi giáo viên và học sinh tôn trọng quyền riêng tư, tuân thủ quy tắc chia sẻ thông tin, biết nhận diện và tránh xa các nội dung độc hại, lừa đảo hoặc vi phạm pháp luật. Điều này góp phần nâng cao chất lượng giáo dục nhân cách, đồng thời giúp học sinh – sinh viên phát triển kỹ năng sống trong thời đại số.

Tăng cường hiệu quả quản trị và chuyển đổi số của nhà trường: Chuyển đổi số đòi hỏi sự phối hợp đồng bộ giữa con người – quy trình – công nghệ. Một văn hóa an toàn thông tin mạnh giúp cán bộ quản lý dễ dàng triển khai các chính sách số, nâng cao mức độ tuân thủ, tối ưu hóa quy trình và tạo sự đồng thuận trong toàn trường. Đây là yếu tố quan trọng giúp nhà trường chuyển đổi số một cách bền vững, an toàn và hiệu quả.

Nâng cao uy tín và hình ảnh của cơ sở giáo dục: Trong thời đại dữ liệu là tài sản, một trường học có văn hóa an toàn thông tin tốt sẽ được phụ huynh, sinh viên và xã hội đánh giá cao về tính chuyên nghiệp và trách nhiệm. Điều này góp phần củng cố niềm tin của cộng đồng, hỗ trợ tuyển sinh, hợp tác và phát triển thương hiệu nhà trường.

2.3. Xây dựng văn hóa an toàn thông tin tại các cơ sở giáo dục trong bối cảnh chuyển đổi số

2.3.1. Nâng cao nhận thức và bồi dưỡng năng lực an toàn thông tin cho người học và cán bộ

Nâng cao nhận thức được xem là biện pháp cốt lõi vì yếu tố con người luôn là “mắt xích yếu nhất” trong chuỗi bảo mật. Nhiều sự cố an toàn thông tin trong môi trường giáo dục bắt nguồn từ hành vi thiếu thận trọng của người dùng như mở email lạ, chia sẻ mật khẩu, hoặc tải phần mềm không rõ nguồn gốc. Do đó, việc triển khai các chương trình bồi dưỡng ATTT cho cán bộ, giảng viên, sinh viên không chỉ giúp họ nhận diện nguy cơ mà còn thay đổi thái độ và hành vi sử dụng công nghệ.

Các hình thức truyền thông, tập huấn cần đa dạng, dễ hiểu, gắn với tình huống thực tế như mô phỏng tấn công phishing, phân tích sự cố rò rỉ dữ liệu hoặc thực hành bảo vệ tài khoản cá nhân. Ngoài ra, việc tích hợp ATTT vào môn Tin học, Kỹ năng số hay Giáo dục công dân sẽ giúp người

học hình thành tư duy bảo mật từ sớm. Sự thay đổi nhận thức không chỉ bảo vệ dữ liệu của bản thân người dùng mà còn góp phần tạo môi trường số an toàn chung cho toàn cơ sở giáo dục.

2.3.2. Hoàn thiện cơ chế, chính sách và quy trình quản lý an toàn thông tin

Một trong những rào cản lớn đối với việc xây dựng văn hóa an toàn thông tin trong các trường học là thiếu thống nhất về quy chế, quy định, dẫn đến sự lúng túng trong triển khai và xử lý sự cố. Việc hoàn thiện cơ chế, chính sách về ATTT giúp định hình các chuẩn mực hành vi, đưa việc bảo vệ thông tin trở thành trách nhiệm bắt buộc của mỗi cá nhân.

Các nhà trường cần ban hành quy định về quản lý dữ liệu, phân quyền truy cập, bảo mật tài khoản, sử dụng thiết bị cá nhân trong môi trường số, cũng như xác định rõ mức độ trách nhiệm và chế tài đối với vi phạm. Cơ chế xử lý sự cố cần được xây dựng theo các bước chuẩn: ghi nhận – phân loại – khoanh vùng – khắc phục – báo cáo – rút kinh nghiệm. Khi có một hệ thống văn bản đầy đủ, mọi thành viên có thể hành động thống nhất, giảm thiểu thiệt hại và tăng tính chủ động trong phòng ngừa.

Đặc biệt, quy định cần đi đôi với giám sát và đánh giá định kỳ nhằm đảm bảo văn hóa bảo mật không chỉ tồn tại “trên giấy” mà được thực thi thường xuyên và nghiêm túc trong đời sống nhà trường.

2.3.3. Phát triển hạ tầng kỹ thuật số an toàn – nền tảng để duy trì văn hóa ATTT

Hạ tầng kỹ thuật vừa là điều kiện vừa là công cụ để thực thi an toàn thông tin. Trong bối cảnh chuyển đổi số, các cơ sở giáo dục ngày càng phụ thuộc vào hệ thống quản lý học tập (LMS), cơ sở dữ liệu người học, kho học liệu số và các nền tảng quản lý đào tạo. Một khi những hệ thống này bị tấn công hoặc gián đoạn, toàn bộ hoạt động của nhà trường có thể bị ảnh hưởng nghiêm trọng.

Đầu tư vào hạ tầng bảo mật như tường lửa thế hệ mới, hệ thống chống mã độc, giải pháp phát hiện xâm nhập (IDS/IPS), sao lưu dữ liệu định kỳ và xác thực đa yếu tố (MFA) giúp giảm thiểu nguy cơ tấn công. Bên cạnh đó, các cơ sở giáo dục cần

triển khai hệ thống giám sát ATTT 24/7 để theo dõi, cảnh báo và ngăn chặn sớm sự cố. Đây là yếu tố mang tính “phòng ngừa chủ động” thay vì chỉ ứng phó bị động khi đã xảy ra rủi ro.

Việc phát triển hạ tầng kỹ thuật không chỉ bảo vệ hệ thống thông tin mà còn tạo môi trường tin cậy để giảng viên, sinh viên yên tâm giảng dạy – học tập trong không gian số, qua đó duy trì và củng cố văn hóa an toàn thông tin của nhà trường.

III. KẾT LUẬN

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ trong ngành giáo dục, việc xây dựng văn hóa an toàn thông tin trở thành yêu cầu cấp thiết nhằm bảo đảm sự ổn định, an toàn và bền vững cho các hoạt động dạy học, quản lý và phát triển nhà trường. Văn hóa an toàn thông tin không chỉ là tập hợp các quy định, chuẩn mực mà còn là sự kết hợp hài hòa giữa nhận thức, thái độ, hành vi của mỗi cá nhân với hạ tầng kỹ thuật và cơ chế quản lý của tổ chức.

Kết quả phân tích cho thấy bốn nhóm biện pháp trọng tâm – gồm nâng cao nhận thức và năng lực về an toàn thông tin; hoàn thiện cơ chế, chính sách và quy trình quản lý; phát triển hạ tầng kỹ thuật số an toàn; và hình thành thói quen, hành vi sử dụng công nghệ an toàn – giữ vai trò quyết định trong việc hình thành và duy trì văn hóa an toàn thông tin trong các cơ sở giáo dục. Trong đó, nhận thức và hành vi của người dùng là yếu tố then chốt; cơ chế, chính sách đóng vai trò định hướng; hạ tầng kỹ thuật bảo đảm nền tảng; và hành vi sử dụng công nghệ quyết định tính bền vững của văn hóa bảo mật.

Để văn hóa an toàn thông tin thực sự trở thành giá trị cốt lõi của các cơ sở giáo dục, cần sự phối hợp đồng bộ giữa nhà quản lý, đội ngũ kỹ thuật, giảng viên và người học. Các biện pháp cần được triển khai liên tục, được đánh giá và điều chỉnh phù hợp với sự thay đổi của công nghệ và các nguy cơ an ninh mạng mới. Việc phát triển văn hóa an toàn thông tin không chỉ bảo vệ dữ liệu và hệ thống của nhà trường mà còn góp phần hình thành kỹ năng số an toàn cho thế hệ học sinh – sinh viên, chuẩn bị nguồn nhân lực thích ứng tốt với môi trường số hiện đại.

TÀI LIỆU THAM KHẢO

- Bộ Thông tin và Truyền thông (2020). *Bộ quy tắc ứng xử trên mạng xã hội*. Hà Nội.
- Cục An toàn thông tin – Bộ TT&TT (2022). *Báo cáo hiện trạng an toàn thông tin Việt Nam*.
- Nguyễn Thành Trung (2021). “Xây dựng văn hóa an toàn thông tin trong các cơ quan, tổ chức.” *Tạp chí Công thương*, 23(5), 45–50.
- SANS Institute (2020). *Building a Security Awareness Program: Best Practices for Education Sector*.
- Kritzinger, E., & Smith, E. (2008). “Information security management: An educational framework for information security awareness.” *Computers & Security*, 27(1–2), 29–32.