

GIẢI PHÁP NÂNG CAO KHẢ NĂNG ỨNG XỬ AN TOÀN TRÊN KHÔNG GIAN MẠNG CỦA HỌC SINH - SINH VIÊN TRONG THỜI ĐẠI 4.0

Nguyễn Thị Thu Hương, Nguyễn Thị Huỳnh Giao, Bùi Thị Thu Hoài, Lưu Thị Huệ Nương
Trường Cao đẳng Sư phạm Kiên Giang

Tóm tắt: Bài viết này bàn về công nghệ và các loại tội phạm công nghệ cao, tác động của công nghệ - tội phạm công nghệ cao đến tâm sinh lý học sinh – sinh viên và đề ra một số giải pháp giúp học sinh – sinh viên biết cách ứng xử an toàn trên không gian mạng, nhằm tận dụng những ưu thế của kỷ nguyên số trong việc học tập, nghiên cứu và giải trí.

Từ khoá: Ứng xử an toàn trên không gian mạng, học sinh, sinh viên, thời đại 4.0.

SOLUTIONS TO IMPROVE STUDENTS' ABILITY TO BEHAVE SAFELY ON THE INTERNET IN THE 4.0 ERA

Nguyen Thi Thu Huong, Nguyen Thi Huynh Giao, Bui Thi Thu Hoai, Luu Thi Hue Nuong
Kien Giang College of Education

Abstract: This article discusses technology and high-tech crimes, the impact of technology - high-tech crimes on the psychology of students and proposes some solutions to help students know how to behave safely in cyberspace, in order to take advantage of the advantages of the digital age in learning, research and entertainment.

Keywords: Safe behavior in cyberspace, students, 4.0 era.

Nhận bài: 22/04/2025

Phản biện: 20/05/2025

Duyệt đăng: 25/05/2025

I. ĐẶT VẤN ĐỀ

Trong thời đại công nghệ 4.0, giới trẻ ngày nay được tiếp cận với Internet từ sớm và rất thành thạo trong việc sử dụng các thiết bị công nghệ nhất là học sinh-sinh viên (HSSV). Không gian mạng (KGM) đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày như: trao đổi thông tin, cung cấp không gian học tập tiện lợi, mở ra tài nguyên học tập phong phú, tạo cơ hội tiếp xúc với đa dạng nguồn kiến thức, giúp HSSV dễ dàng kết nối, trao đổi với bạn bè. Tuy nhiên, dù mang lại nhiều lợi ích, công nghệ cũng là nơi tiềm ẩn nhiều rủi ro mà nhà trường, cha mẹ học sinh và xã hội cần nhận biết và giáo dục trẻ cách nhận diện, ứng xử an toàn với môi trường KGM.

Nhận thức được tầm quan trọng của công nghệ và việc giúp HSSV nắm bắt rõ kiến thức về an toàn KGM, cũng như nâng cao kỹ năng công nghệ trong thời đại số. Ngoài việc trang bị các kiến thức duyệt web an toàn, người lớn cần giúp trẻ nhận diện các loại hình tội phạm mạng phổ biến hiện nay, đồng thời hướng dẫn các biện pháp phòng ngừa và đối phó với những nguy cơ mà các em có thể gặp phải trên KGM, từ đó nâng cao nhận thức và kỹ năng bảo vệ bản thân trước các mối đe dọa tiềm ẩn và xây dựng một môi trường học tập an toàn, lành mạnh trên môi trường mạng.

II. NỘI DUNG NGHIÊN CỨU

2.1. Thực trạng môi trường mạng và những mối đe dọa tiềm ẩn ảnh hưởng đến sự phát triển tâm, sinh lý học sinh-sinh viên

2.1.1. Thực trạng môi trường mạng

Trong những năm gần đây, các nền tảng mạng xã hội như Facebook, Instagram, X (Twitter), Telegram, Zalo, Wechat, TikTok... đã tạo ra một mạng lưới kết nối toàn cầu mạnh mẽ, lượng người truy cập Internet tăng thần tốc. “Tính đến năm 2023, hơn 5 tỉ người trên toàn cầu sử dụng Internet, chiếm 60% dân số thế giới. Trong đó, tỉ lệ người Việt Nam sử dụng Internet đã đạt hơn 75% dân số” [1], các nền tảng này không những giúp người dùng chia sẻ thông tin, phục vụ nhu cầu giao tiếp cá nhân mà còn trở thành công cụ mạnh mẽ trong truyền thông, quảng bá thương hiệu, tiếp thị và quảng cáo.

Từ nhu cầu ngày càng mở rộng của người dùng và sự phát triển mạnh mẽ của công nghệ, ngoài việc thỏa mãn nhu cầu giải trí, thời đại công nghệ 4.0 còn đòi hỏi sự tiện ích, nhanh chóng, dễ tiếp cận, giá cả cạnh tranh. Chính những điều này đã tạo tiền đề cho các sản phẩm giao dịch điện tử như Lazada, Amazon, Shopee, Tiki, Taobao... xuất hiện và đã trở thành bộ phận quan trọng trong nền kinh tế tiêu dùng.

Ngoài ra, nhu cầu mạnh mẽ của việc giảng dạy và học tập trực tuyến, nhất là trong bối cảnh đại dịch COVID-19 đã làm thay đổi nhận thức của công dân toàn cầu, họ nhận ra vai trò to lớn của Internet và do đó nhu cầu sử dụng, tương tác trên KGM ngày càng trở nên phổ biến.

Môi trường mạng tác động sâu rộng đến toàn xã hội, tạo ra nhiều cơ hội mới cho giáo dục, kinh doanh, giao tiếp, kết nối bạn bè, các nền tảng trực

tuyển còn mở ra cơ hội học tập và làm việc từ xa, góp phần thúc đẩy sự phát triển của nền kinh tế số và cải thiện chất lượng cuộc sống. Ngoài việc mang lại nhiều lợi ích, nó còn lộ ra những mặt hạn chế vô cùng nguy hiểm như: lừa đảo qua mạng, bắt nạt trực tuyến, hạn chế khả năng giao tiếp trực tiếp và nghiện mạng xã hội, những nguy cơ này đặt ra nhiều thách thức không những cho nhà giáo dục, cha mẹ học sinh mà còn cho toàn xã hội, bởi vì tác hại của nó đối với sức khỏe và đạo đức xã hội. HSSV rất dễ bị ảnh hưởng bởi các xu hướng tiêu cực trên mạng, bất chước, cuồng tín người nổi tiếng, dẫn đến các vấn đề như trầm cảm, lo âu và cô lập xã hội. Sự phụ thuộc mạnh mẽ vào các nền tảng mạng xã hội có thể dẫn đến cảm giác thiếu kết nối thực sự, giảm chất lượng các mối quan hệ xã hội và nhất là khả năng đối mặt với tội phạm mạng, bởi lẽ các em có kiến thức về kỹ thuật nhưng chưa có kinh nghiệm sống đầy đủ, tội phạm mạng có thể gây ra những tác động nghiêm trọng đến đời sống cá nhân, học tập và phát triển tâm lý.

2.1.2. Các mối đe dọa từ môi trường mạng đối với học sinh-sinh viên

Một là, lừa đảo trên mạng

Tội phạm mạng ngày càng tinh vi, thường lợi dụng sự thiếu kinh nghiệm và tâm lý cả tin của học sinh, sinh viên (HSSV). Các hình thức phổ biến gồm email/phishing, trang web giả, và cuộc gọi mạo danh. Chúng giả danh tổ chức tín dụng, thương hiệu uy tín, kêu gọi đầu tư hoặc nhận thưởng, nhằm lấy thông tin cá nhân hoặc dụ chuyển tiền trước. Dấu hiệu lừa đảo gồm: yêu cầu cung cấp thông tin nhạy cảm, đưa ra lời mời hấp dẫn phi thực tế, gây áp lực thời gian, thiếu bảo mật, sử dụng tên lạ, và cảnh báo từ phần mềm an ninh.

Ngoài việc mất tiền, HSSV có thể bị lợi dụng cho các hành vi phạm pháp, ảnh hưởng tâm lý và học tập. Tội phạm mạng thường tiếp cận qua mạng xã hội, giả danh với hình ảnh hấp dẫn, tán tỉnh, hứa hẹn tình cảm hoặc lợi ích, rồi dọa nạt, tống tiền bằng thông tin thu thập được.

Hai là, Lừa tuyển cộng tác viên online:

Tội phạm mạo danh sàn thương mại điện tử uy tín (Shopee, Tiki...) tuyển cộng tác viên, hứa hẹn thu nhập cao, dễ dàng, không cần kỹ năng. Sau đó yêu cầu nạn nhân cung cấp thông tin cá nhân hoặc nộp tiền cọc để “tạo tài khoản” hay “mua đơn hàng”, rồi chiếm đoạt tiền.

Ba là, cho vay qua app và việc làm thu nhập cao trừ nợ app

Tội phạm quảng cáo các ứng dụng vay tiền “siêu tốc, không cần thế chấp” để dụ người vay

cung cấp thông tin cá nhân và danh bạ. Sau khi giải ngân, chúng đe dọa khủng bố tinh thần để đòi nợ, hoặc gợi ý làm việc trừ nợ. Công việc thường là gọi điện lừa đảo người khác, giả danh công an, tòa án, ngân hàng... nhằm chiếm đoạt tài sản. Lương được dùng để cân trừ khoản vay.

2.1.3. Tác động của công nghệ số và tội phạm mạng đối với học sinh, sinh viên

Thứ nhất, bạo lực, đe dọa và bắt nạt trực tuyến

Mạng xã hội (MXH) và các nền tảng trực tuyến là không gian giúp trẻ giải trí, kết nối với mọi người nhưng cũng có thể trở thành nơi phát triển các hành vi bạo lực, đe dọa và bắt nạt. Theo báo cáo nghiên cứu của Quỹ Nhi đồng Liên Hiệp Quốc (UNICEF), cứ 5 trẻ em và thanh thiếu niên thì có 1 trẻ em bị bắt nạt trên mạng. Đáng lo ngại, 3/4 trong số đó không biết tìm kiếm sự giúp đỡ ở đâu. (Nguồn: Báo Thanh Niên).

Bắt nạt trực tuyến là một trong những vấn đề nghiêm trọng mà HSSV thường gặp phải. Với sự phát triển mạnh mẽ của công nghệ, các nền tảng trực tuyến cung cấp đầy đủ các công cụ giao tiếp như gọi video, nhắn tin sms, nhắn tin thoại, đăng trạng thái... đã làm cho các hình thức bắt nạt trực tuyến trở nên đa dạng, phổ biến và khó kiểm soát hơn. Những lời khích bác, chế giễu, lăng mạ, đe dọa, hoặc phát tán hình ảnh riêng tư một cách công khai có thể gây ra những tổn thương nặng nề về mặt tâm lý, đặc biệt là khi thời gian các em tiếp xúc với MXH đang tăng lên mỗi ngày. Hiện nay, tại một số trường Trung học cơ sở và Trung học phổ thông có hiện tượng học sinh lập nhóm zalo tẩy chay, cô lập, phi báng bạn học. Nạn nhân của những trường hợp bắt nạt trực tuyến thường rơi vào trạng thái lo âu, trầm cảm, tự ti, sợ đi học và trong nhiều trường hợp nghiêm trọng, các em có thể có ý định tự tử. Sự lan truyền nhanh chóng của thông tin xấu trên mạng khiến cho những tổn thương này càng trở nên nghiêm trọng và kéo dài hơn.

Thứ hai, xâm phạm quyền riêng tư

Với sự phát triển nhanh chóng của công nghệ và tính ứng dụng cao của các nền tảng xã hội, giúp người dùng đăng tải thông tin cá nhân và hình ảnh một cách nhanh chóng. Cũng chính vì tính đa dụng, kết nối nhanh chóng này đã tạo ra những mặt trái vô cùng nguy hiểm. Tội phạm mạng dễ dàng đánh cắp tài khoản để thu thập thông tin cá nhân như địa chỉ nhà, số điện thoại, thông tin tài chính và cả dữ liệu cá nhân, hình ảnh nhạy cảm, tin nhắn riêng tư... bằng các thủ thuật tinh vi thông qua các phần mềm gián điệp, tấn công lừa đảo

(phishing). Khi các thông tin cá nhân bị đánh cắp HSSV rất dễ trở thành nạn nhân của các vụ lừa đảo, tống tiền, quấy rối... Chính những hành động này đã tác động sâu sắc đến tâm-sinh lí HSSV do các em còn thiếu kinh nghiệm, dễ dàng lo âu, sợ hãi khi bị đe dọa. Xâm phạm quyền riêng tư là một loại tội phạm mạng đặc biệt nghiêm trọng và hậu quả rất khó lường.

Thứ ba, tiếp cận nội dung độc hại

MXH tuy ảo nhưng gây ra những hậu quả rất chân thực bởi vì không gian mạng chứa đựng kho thông tin khổng lồ, không những giúp HSSV gia tăng cơ hội tìm kiếm thông tin, cập nhật kiến thức mới, KGM càng phổ biến bởi sự phổ biến của học trực tuyến, các thiết bị như máy tính và điện thoại đã trở thành công cụ vô cùng quan trọng trong việc học tập nghiên cứu của HSSV. Tuy nhiên, chính các thiết bị này lại chính là mục tiêu dễ dàng cho các cuộc tấn công mạng như nhiễm virus, mã độc hoặc bị đánh cắp tài khoản học tập của các em, gây gián đoạn quá trình học tập hoặc nghiêm trọng hơn đó là mất toàn bộ dữ liệu-tài liệu học tập quan trọng làm ảnh hưởng đến quá trình và kết quả học tập. Chính những gián đoạn này sẽ ít nhiều tạo ra áp lực tâm lí của HSSV, đặc biệt là trong những giai đoạn ôn thi.

Sự phát triển nhanh chóng của công nghệ, đặc biệt là MXH, đem lại thông tin và hình ảnh phong phú, đa dạng nhưng đôi khi thiếu kiểm soát, khiến thanh thiếu niên dễ bị tác động từ các hành vi tiêu cực như bạo lực (game độc hại), khiêu dâm (game sex, sex game), các diễn đàn cực đoan (hội nhóm). “Mạng xã hội đưa thanh thiếu niên vào một không gian nơi các giá trị ảo, những hình mẫu phù phiếm là chuẩn mực sống. Ở đó, các em say mê với việc đếm số lượt thích, chia sẻ, và có thể thực hiện bất kỳ hành vi nào để có được những con số phù phiếm đó. Khi thiếu đi sự kiểm soát và hướng dẫn từ gia đình, nhà trường, các em dễ lạc vào vòng xoáy nguy hiểm, nơi mà việc thể hiện sai lệch nhiều khi lại trở thành cách để khẳng định bản thân” [2], dễ bị kích động, hùa theo những lời kêu gọi từ các hội nhóm, vô thức trở thành hung thủ của hàng loạt vụ án thương tâm gần đây. Ngoài ra, sự tiếp cận với nội dung độc hại có thể gây ra những vấn đề về tâm lí như lo âu, mất ngủ, mất cảm giác an toàn, rối loạn cảm xúc khác, thậm chí nghiêm trọng hơn là tác động tiêu cực đến tư duy, hành vi, nhân cách của các em. Các em có thể bị ảnh hưởng về mặt nhận thức dẫn đến hành vi sai trái, bạo lực hoặc phát triển những quan điểm lệch lạc về xã hội, con người và cuộc sống, các em

thường chỉ biết bản thân, quên trách nhiệm với gia đình-xã hội.

2.3. Giải pháp ứng xử an toàn trên không gian mạng cho học sinh sinh viên trong thời đại 4.0

2.3.1. Vai trò của nhà trường trong việc nâng cao nhận thức và kiến thức về an toàn trên không gian mạng cho học sinh – sinh viên

KGM là nơi chứa đựng một kho kiến thức khổng lồ giúp học sinh tìm kiếm thông tin phục vụ cho việc học tập và phát triển bản thân. Nếu biết cách tương tác an toàn trên KGM sẽ mang lại rất nhiều lợi ích cho việc học tập và cuộc sống của HSSV như: các em dễ dàng kết nối, chia sẻ về tài liệu học tập, thiết lập các mối quan hệ bạn bè trên khắp các vùng miền, quốc gia...

Tuy nhiên, đối với lứa tuổi HSSV kinh nghiệm sống chưa nhiều, kiến thức tương tác an toàn trên KGM còn thiếu nên việc sử dụng mạng xã hội tiềm ẩn rất nhiều nguy cơ. KGM là không gian mở, dễ kết nối, là mảnh đất màu mỡ của nhiều đối tượng lừa đảo, các thông tin chưa được kiểm chứng, thông tin xấu độc, thông tin bẩn tràn lan. Thực tế đã có nhiều vụ việc đáng tiếc xảy ra như trẻ vị thành niên bị bắt cóc, lừa tiền, lừa tình, gây án mạng mà nguyên nhân chủ yếu bắt nguồn từ MXH. Không những thế, việc HSSV sử dụng internet nhiều đã dẫn đến tình trạng nghiện và phụ thuộc, làm ảnh hưởng đến sức khỏe thể chất và tinh thần như: bị các tật về mắt, các bệnh về xương khớp, chứng béo phì, ngại giao tiếp, mất ngủ, sức khỏe tinh thần không ổn định, nghiêm trọng hơn là ảnh hưởng trực tiếp đến kết quả học tập do các em bị phân tán thời gian.

Theo các chuyên gia, để giải quyết thực trạng này cần những giải pháp về đào tạo, giáo dục của nhà trường như: tích hợp an toàn mạng vào chương trình giảng dạy, tổ chức các hoạt động ngoại khóa về kĩ năng sử dụng mạng an toàn, đào tạo giáo viên chuyên trách về các vấn đề an toàn mạng, tập huấn kiến thức về công nghệ cho nhân viên nhà trường, lập tổ tư vấn tâm lí hỗ trợ HSSV, giải đáp các thắc mắc và tình huống khó xử khi tương tác trên KGM ...

Đưa kiến thức an toàn mạng vào giáo trình, chương trình học chính thức: bao gồm nội dung về các mối đe dọa mạng, tầm quan trọng của bảo mật thông tin cá nhân; các nguyên tắc cơ bản đảm bảo an ninh, an toàn thông tin người dùng trong việc sử dụng các phần mềm; các nguyên tắc áp dụng khi sử dụng ứng dụng quản lí mật khẩu như LastPass, KeePass, icloud Keychain, lưu trong trình duyệt, trong sổ tay...

Các khoá học chuyên biệt về an ninh mạng: nhà trường cần tổ chức các buổi học chuyên biệt về an ninh mạng cho viên chức, người lao động và HSSV, cung cấp các kiến thức sâu rộng về bảo mật mạng, cách ứng phó với các tình huống bị tấn công mạng, các kỹ thuật mã hoá dữ liệu hoặc quản lý bảo mật hệ thống.

Tích hợp nội dung kiến thức an toàn vào các môn học khác: ngoài việc đưa kiến thức an toàn mạng vào môn học chuyên biệt, nhà trường cần lồng ghép các nội dung về cách ứng xử an toàn trên KGM cho HSSV vào các môn học ưu thế như: Toán học, Khoa học máy tính, Giáo dục công dân, Kỹ năng sống và các giờ Hoạt động trải nghiệm, giúp các em nhận thức đúng, có kỹ năng ứng phó tốt với các tình huống xảy ra trên mạng để giảm bớt những nguy cơ rủi ro mất an toàn cho các em trước văn hóa độc hại trên mạng.

Mở trung tâm-tổ tư vấn tâm lý: ngoài việc hỗ trợ các em giải quyết các tình huống trong học đường và cuộc sống như tình cảm, mâu thuẫn cá nhân, cần hỗ trợ các em cách ứng phó với các nguy cơ mất an toàn mạng, các loại tội phạm công nghệ cao; nơi đủ chuyên nghiệp, độ tin cậy cao để các em yên tâm trải lòng; qua đó kịp thời can thiệp các tình huống có thể gây mất an toàn cho HSSV.

2.3.2. Phối hợp giữa nhà trường, cha mẹ học sinh và xã hội

Việc phối hợp giữa nhà trường, cha mẹ học sinh và xã hội trong việc định hướng ứng xử an toàn trên KGM cho học sinh là một yếu tố rất quan trọng nhằm bảo vệ học sinh trước những rủi ro từ môi trường mạng. Dưới đây là một số nội dung phối hợp cụ thể và thiết thực.

Một là, nhà trường giữ vai trò trung tâm trong việc giáo dục, định hướng và truyền đạt kiến thức về an toàn mạng cho học sinh. Lồng ghép nội dung giáo dục an toàn mạng vào các tiết học chính khóa hoặc hoạt động ngoại khóa. Tổ chức các buổi chuyên đề, hội thảo, mời chuyên gia chia

sẻ về cách nhận biết thông tin sai lệch, bạo lực mạng, lừa đảo trực tuyến... Xây dựng nội quy sử dụng internet, thiết bị di động trong trường học rõ ràng, có chế tài phù hợp. Phát hiện sớm và can thiệp khi học sinh có dấu hiệu bị ảnh hưởng tiêu cực từ MXH (ví dụ: trầm cảm, bị bắt nạt,...).

Hai là, gia đình là nơi hình thành thói quen và thái độ ban đầu của con đối với môi trường mạng. Tạo môi trường trao đổi cởi mở, quan tâm đến tâm lý và hành vi online của con cái. Giám sát nhưng không kiểm soát thái quá, giúp con hiểu sự nguy hiểm thay vì cấm đoán. Cha mẹ cần tự trang bị kiến thức về công nghệ, MXH để có thể hướng dẫn con hiệu quả, tạo môi trường trao đổi cởi mở về trải nghiệm trực tuyến. Đồng hành cùng con trong việc sử dụng MXH, ứng dụng học tập trực tuyến. Phối hợp chặt chẽ với nhà trường khi phát hiện những vấn đề bất thường từ con.

Ba là, các tổ chức xã hội, cơ quan truyền thông, công nghệ... cần tạo ra môi trường mạng an toàn và thân thiện. Xây dựng các nền tảng công nghệ lành mạnh, phù hợp với lứa tuổi học sinh. Truyền thông nâng cao nhận thức cộng đồng về an toàn mạng, nhất là qua các chiến dịch giáo dục. Xử lý nghiêm những hành vi xâm hại học sinh qua mạng, như bắt nạt, lừa đảo, xâm phạm đời tư... Phối hợp với công an, sở thông tin truyền thông để phổ biến pháp luật liên quan đến an toàn mạng. Khuyến khích các tổ chức đoàn thể (Đoàn Thanh niên, Hội phụ nữ, Hội khuyến học...) cùng tham gia hỗ trợ, giáo dục kỹ năng số cho học sinh.

III. KẾT LUẬN

Trong thời đại 4.0, khi học sinh – sinh viên là những công dân số “bẩm sinh”, việc nâng cao năng lực ứng xử an toàn trên KGM không chỉ là trách nhiệm của cá nhân mà cần sự phối hợp toàn diện từ nhà trường, gia đình và xã hội. Việc nâng cao khả năng ứng xử an toàn trên KGM là yếu tố cốt lõi để xây dựng một cộng đồng mạng lành mạnh, văn minh và sáng tạo.

TÀI LIỆU THAM KHẢO

1. TS. Nguyễn Hồng Quân (2024) *Nhận thức chung về an ninh mạng, tài liệu tập huấn, lưu hành nội bộ.*
2. <https://tienphong.vn/vu-quai-xe-dam-chet-nguoi-o-ha-noi-noi-dau-cua-xa-hoi-post1689107.tpo>