

# MỘT SỐ GIẢI PHÁP NÂNG CAO NHẬN THỨC VỀ AN TOÀN THÔNG TIN, AN NINH MẠNG CHO SINH VIÊN TẠI CÁC TRUNG TÂM GIÁO DỤC QUỐC PHÒNG VÀ AN NINH

Nguyễn Viễn Đông

Trung tâm Giáo dục quốc phòng và an ninh Đại học Thái Nguyên

**Tóm tắt:** Trong thời đại công nghệ thông tin phát triển mạnh mẽ, không gian mạng trở thành môi trường học tập, giao tiếp và phát triển quan trọng của sinh viên. Tuy nhiên, cùng với đó là sự gia tăng các nguy cơ như: lộ lọt thông tin cá nhân, lừa đảo trực tuyến, tấn công mạng và các hoạt động chống phá trên không gian mạng. Sinh viên là lực lượng trẻ, năng động nhưng còn hạn chế về kinh nghiệm, dễ trở thành đối tượng bị tác động. Đối với sinh viên học tập tại các Trung tâm Giáo dục quốc phòng và an ninh, việc nâng cao nhận thức về an toàn thông tin, an ninh mạng không chỉ giúp bảo vệ bản thân mà còn góp phần hình thành ý thức trách nhiệm công dân trong bảo vệ an ninh quốc gia trên không gian mạng. Vì vậy, việc nghiên cứu đánh giá đúng thực trạng và đề xuất các giải pháp phù hợp là yêu cầu cần thiết trong giai đoạn hiện nay.

**Từ khóa:** Sinh viên, giảng viên, an toàn thông tin, an ninh mạng, giáo dục quốc phòng và an ninh.

## SOME SOLUTIONS TO IMPROVE AWARENESS OF INFORMATION SECURITY AND CYBER SECURITY FOR STUDENTS AT NATIONAL DEFENSE AND SECURITY EDUCATION CENTERS

**Abstract:** In the era of rapidly developing information technology, cyberspace has become an important learning, communication, and development environment for students. However, along with this comes an increase in risks such as: leakage of personal information, online fraud, cyberattacks, and subversive activities in cyberspace. Students are a young, dynamic force but have limited experience, making them vulnerable to such influences. For students studying at National Defense and Security Education Centers, raising awareness of information security and cybersecurity not only helps protect themselves but also contributes to forming a sense of civic responsibility in protecting national security in cyberspace. Therefore, researching and accurately assessing the current situation and proposing appropriate solutions is a necessary requirement in the present period.

**Keywords:** Students, lecturers, information security, cybersecurity, national defense and security education.

Nhận bài: 18/03/2026

Phản biện: 19/04/2026

Duyệt đăng: 24/04/2026

### I. ĐẶT VẤN ĐỀ

Sự phát triển của internet cùng các dịch vụ trên không gian mạng đã làm nên một cuộc “cách mạng” về mọi mặt từ kinh tế, văn hóa đến khoa học kỹ thuật, giáo dục và cả chính trị. Một trong những đối tượng ảnh hưởng rất nhiều từ internet đó là sinh viên trong xã hội toàn cầu hóa hiện nay. Việc sử dụng internet đúng mục đích sẽ giúp ích rất nhiều trong quá trình học tập, bởi hầu hết các tài liệu đều được cung cấp trên mạng. Với mạng internet các bạn sẽ dễ dàng: Tìm kiếm tài liệu học tập của hầu hết các quốc gia; Trao đổi tài liệu, bài học với nhau ở bất cứ đâu; Luyện thi, luyện học trên các trang web; Trao đổi, học tập, lưu trữ, tải dữ liệu, phần mềm phục vụ cho học tập; Giúp giải trí sau giờ học mệt mỏi; Hỗ trợ làm thêm online để kiếm thêm thu nhập và rất rất nhiều lợi ích khác do nhu cầu sử dụng của sinh viên. Bên cạnh những lợi ích to lớn trong học tập, nghiên cứu và kết nối xã hội, mạng Internet cũng tiềm ẩn nhiều tác động tiêu cực, đặc biệt đối với sinh viên (nhóm đối tượng sử dụng Internet với tần suất cao). Trước hết, vấn đề thông tin sai lệch và tin

giả đang trở thành một thách thức lớn. Sinh viên thường xuyên tiếp cận lượng thông tin khổng lồ từ các nền tảng trực tuyến nhưng chưa được trang bị đầy đủ kỹ năng kiểm chứng, dẫn đến việc tiếp nhận và lan truyền thông tin không chính xác. Điều này không chỉ ảnh hưởng đến nhận thức cá nhân mà còn gây tác động tiêu cực đến môi trường học thuật. Thứ hai, nguy cơ mất an toàn thông tin cá nhân ngày càng gia tăng. Nhiều sinh viên có thói quen chia sẻ thông tin cá nhân một cách thiếu kiểm soát trên mạng xã hội, tạo điều kiện cho các hành vi lừa đảo, đánh cắp dữ liệu. Các hình thức tấn công mạng như giả mạo tài khoản, gửi đường link độc hại diễn ra ngày càng phổ biến và tinh vi. Một vấn đề đáng chú ý khác là tình trạng nghiện Internet và mạng xã hội. Theo một số khảo sát giả định, khoảng 65–75% sinh viên dành trên 4 giờ mỗi ngày cho Internet ngoài mục đích học tập. Việc sử dụng quá mức dẫn đến giảm hiệu quả học tập, rối loạn giấc ngủ và ảnh hưởng tiêu cực đến sức khỏe thể chất cũng như tinh thần. Ngoài ra, Internet còn tác động đến đạo đức và hành vi của

sinh viên thông qua việc tiếp cận các nội dung không phù hợp như bạo lực, phản cảm hoặc lệch chuẩn. Điều này có thể làm thay đổi nhận thức, lối sống và chuẩn mực hành vi của một bộ phận sinh viên nếu không được định hướng đúng đắn. Bên cạnh đó, hiện tượng bạo lực mạng cũng đang có xu hướng gia tăng trong môi trường học đường. Việc xúc phạm, công kích cá nhân trên mạng xã hội không chỉ gây tổn thương tâm lý mà còn ảnh hưởng đến danh dự, uy tín của người bị hại. Cuối cùng, việc lạm dụng Internet còn dẫn đến suy giảm tương tác xã hội trực tiếp. Nhiều sinh viên có xu hướng giao tiếp qua mạng nhiều hơn ngoài đời thực, làm giảm kỹ năng giao tiếp, khả năng làm việc nhóm và xây dựng các mối quan hệ xã hội bền vững.

Hiện nay môn học giáo dục quốc phòng và an ninh tại các Trung tâm Giáo dục quốc phòng và an ninh được giảng dạy theo Thông tư 05/2020/TT-BGDĐT của Bộ Giáo dục và Đào tạo về “Ban hành Chương trình giáo dục quốc phòng và an ninh trong trường trung cấp sư phạm, cao đẳng sư phạm và cơ sở giáo dục đại học”, trong học phần Công tác quốc phòng và an ninh có nội dung giảng dạy về an toàn thông tin và phòng chống một số loại tội phạm trên không gian mạng. Tuy nhiên, do nhiều yếu tố khách quan và chủ quan nên nội dung vẫn chưa làm cho sinh viên hiểu sâu về các vấn đề an toàn thông tin và an ninh mạng.

Từ những phân tích trên có thể thấy, mặt trái của Internet là vấn đề cần được nhận diện đầy đủ, để từ đó đề ra các giải pháp nâng cao nhận thức về an toàn thông tin, an ninh mạng cho sinh viên tại các Trung tâm Giáo dục quốc phòng và an ninh là hết sức cấp thiết, góp phần xây dựng môi trường mạng lành mạnh, an toàn, nâng cao chất lượng giáo dục cho sinh viên.

## II. NỘI DUNG NGHIÊN CỨU

### 2.1. Thủ đoạn và xu hướng của các loại tội phạm hiện nay về lĩnh vực an toàn thông tin và an ninh mạng

Cuộc sống hiện đại ngày nay đem đến cho con người đầy đủ về cả vật chất lẫn tinh thần. Xu hướng của thời đại công nghệ số được đẩy mạnh, nên con người phải thường xuyên sử dụng internet, phần không thể thiếu trong cuộc sống. Hiện nay các loại tội phạm công nghệ cao thường sử dụng nhiều thủ đoạn rất tinh vi. Đặc biệt các đối tượng thường sử dụng chiêu trò nhắm vào

sinh viên như: gọi điện rồi thông qua các trang mạng xã hội giới thiệu việc làm thêm nhưng phải chuyển tiền môi giới, sau khi nhận được tiền môi giới các đối tượng chiếm đoạt số tiền môi giới đó; Các đối tượng còn sử dụng điện thoại, AI giả danh công an, viện kiểm soát gọi điện thông báo cho các nạn nhân đang dính líu đến vụ án nào đó yêu cầu khai báo thông tin tài khoản, mật khẩu ngân hàng để chiếm đoạt số tiền trong tài khoản; hoặc chúng thực hiện hành vi tấn công mạng, chiếm quyền điều khiển tài khoản mạng xã hội để nhắn tin lừa đảo đến danh sách bạn bè vay tiền để chiếm đoạt; Không những vậy, các đối tượng thù địch còn sử dụng mạng xã hội để tuyên truyền, bôi nhọ Đảng và Nhà nước ta; ngoài ra một số loại đối tượng mới có xu hướng hack camera qua hệ thống camera gia đình hoặc máy tính cá nhân để quay lại sinh hoạt cá nhân, mà lực lượng sinh viên thường sử dụng máy tính cá nhân thường xuyên nên rất dễ bị các đối tượng lợi dụng... Tội phạm lừa đảo chiếm đoạt tài sản qua mạng có xu hướng gia tăng với nhiều thủ đoạn tinh vi, diễn biến phức tạp, có tính chất xuyên quốc gia, gây thiệt hại lớn và bức xúc cho nhân dân, hoạt động phát tán thông tin xấu, độc hại, thông tin sai sự thật trên không gian mạng tiếp tục tác động đến mọi mặt của đời sống xã hội; Ngoài ra hoạt động tổ chức đánh bạc qua mạng cũng là vấn đề đáng lo ngại. Thực tế cho thấy, sinh viên không chỉ là nạn nhân mà còn có thể trở thành các loại tội phạm công nghệ cao.

Khi bị các đối tượng tội phạm công nghệ cao lừa đảo, đánh cắp thông tin cá nhân, xâm phạm đời sống riêng tư... sinh viên thường có tâm lý hoang mang lo lắng, rất dễ rơi vào trạng thái tuyệt vọng. Một số sinh viên khi bị các đối tượng xâm phạm quyền riêng tư cá nhân thường có tâm lý lo sợ, hoảng loạn, xấu hổ, tự ti mất niềm tin vào bản thân và cảm giác bị cô lập... gây hậu quả xấu đến xã hội, kinh tế, tương lai nghề nghiệp có thể dẫn đến những điều tiêu cực, để lại hậu quả không nhỏ đến gia đình, nhà trường, bạn bè và người thân. Nhiều sinh viên khi vi phạm pháp luật trên không gian mạng có thể bị xử lý hình sự, ảnh hưởng lớn đến việc học hành cũng như danh dự của nhà trường, gia đình. Có thể thấy, từ những vấn đề trên đây, đòi hỏi chúng ta cần phải nâng cao nhận thức đội ngũ cán bộ giảng dạy, đặc biệt là sinh viên trong quá trình học tập tại Trung tâm.

## 2.2. Một số giải pháp nâng cao nhận thức về an toàn thông tin, an ninh mạng cho sinh viên tại các Trung tâm Giáo dục quốc phòng và an ninh

### 2.2.1. *Đẩy mạnh công tác tuyên truyền, giáo dục cho sinh viên có nhận thức đúng và sử dụng mạng internet an toàn*

Đẩy mạnh công tác tuyên truyền, giáo dục nhằm nâng cao nhận thức cho sinh viên về môi trường mạng Internet là một yêu cầu cấp thiết trong bối cảnh chuyển đổi số hiện nay. Nội dung tuyên truyền cần tập trung giúp sinh viên nhận diện các nguy cơ phổ biến như thông tin sai lệch, lừa đảo trực tuyến, xâm phạm dữ liệu cá nhân và các hành vi vi phạm pháp luật trên không gian mạng. Bên cạnh đó, cần chú trọng trang bị cho sinh viên các kỹ năng sử dụng Internet an toàn như: kiểm chứng thông tin, bảo mật tài khoản, ứng xử văn minh trên mạng xã hội và khai thác hiệu quả các nguồn tài nguyên phục vụ học tập. Thông qua các hình thức đa dạng như sinh hoạt chuyên đề, hội thảo, truyền thông trực tuyến và lồng ghép trong chương trình giảng dạy, hoạt động này góp phần hình thành ý thức tự giác, trách nhiệm của sinh viên trong việc xây dựng môi trường mạng lành mạnh, an toàn và văn minh.

### 2.2.2. *Tiếp tục nâng cao năng lực, chất lượng đội ngũ giảng viên, cán bộ quản lý sinh viên về nội dung an toàn thông tin, an ninh mạng*

Đội ngũ giảng viên giữ vai trò then chốt trong việc truyền đạt kiến thức và định hướng nhận thức cho sinh viên về an toàn thông tin, an ninh mạng. Do đó, cần thường xuyên tổ chức các lớp tập huấn, bồi dưỡng chuyên môn, cập nhật kiến thức mới về công nghệ thông tin, an ninh mạng và các quy định của pháp luật liên quan. Nội dung bồi dưỡng cần gắn với thực tiễn, tập trung vào các xu hướng mới như tấn công mạng, lừa đảo trực tuyến, bảo mật dữ liệu cá nhân và kỹ năng ứng phó với các tình huống phát sinh trên không gian mạng.

Bên cạnh đó, cần khuyến khích giảng viên tự học, tự nghiên cứu, tham gia các khóa đào tạo trực tuyến, hội thảo chuyên đề để nâng cao trình độ, đổi mới phương pháp giảng dạy theo hướng hiện đại, tăng cường ứng dụng công nghệ thông tin. Đồng thời, nhà trường và Trung tâm cần có cơ chế hỗ trợ, tạo điều kiện về thời gian, kinh phí và tài liệu phục vụ công tác bồi dưỡng. Việc nâng cao năng lực đội ngũ giảng viên không chỉ góp phần nâng cao chất lượng giảng dạy môn học Giáo dục quốc phòng và an ninh mà còn đáp ứng yêu cầu

đào tạo nguồn nhân lực có nhận thức và kỹ năng số trong tình hình mới.

### 2.2.3. *Đổi mới phương pháp giảng dạy theo hướng tăng tính tương tác.*

Trong quá trình giảng dạy môn Giáo dục quốc phòng và an ninh, việc đổi mới phương pháp theo hướng phát huy tính tích cực, chủ động của sinh viên là yêu cầu cần thiết nhằm nâng cao hiệu quả giáo dục về an toàn thông tin, an ninh mạng. Giảng viên cần tăng cường sử dụng các phương pháp dạy học tích cực như thảo luận nhóm, học tập theo tình huống, mô phỏng các tình huống giả định liên quan đến hành vi vi phạm trên không gian mạng như lừa đảo trực tuyến, phát tán thông tin sai lệch, xâm phạm dữ liệu cá nhân.

Thông qua việc tham gia phân tích, xử lý tình huống, sinh viên không chỉ nắm vững kiến thức mà còn hình thành kỹ năng nhận diện, đánh giá và ứng phó với các nguy cơ trong thực tiễn. Bên cạnh đó, việc ứng dụng công nghệ thông tin trong giảng dạy như sử dụng video tình huống, nền tảng học trực tuyến, câu hỏi trắc nghiệm tương tác... góp phần tạo hứng thú học tập, nâng cao khả năng tiếp thu và ghi nhớ của sinh viên. Qua đó, từng bước hình thành năng lực tự bảo vệ bản thân và ý thức trách nhiệm khi tham gia môi trường mạng.

### 2.2.4. *Tổ chức các hoạt động ngoại khóa, chuyên đề về an toàn thông tin, an ninh mạng*

Bên cạnh nội dung giảng dạy chính khóa, việc tổ chức các hoạt động ngoại khóa, chuyên đề là giải pháp quan trọng nhằm nâng cao nhận thức cho sinh viên một cách trực quan, sinh động và hiệu quả. Trung tâm cần chủ động phối hợp với các cơ quan chức năng, đơn vị chuyên môn và lực lượng đảm bảo an ninh mạng để tổ chức các hội thảo, tọa đàm, diễn đàn trao đổi về các vấn đề nổi bật trong không gian mạng hiện nay như tin giả, lừa đảo trực tuyến, bảo mật thông tin cá nhân.

Đồng thời, có thể tổ chức các cuộc thi tìm hiểu kiến thức về an toàn thông tin, an ninh mạng dưới nhiều hình thức như thi trắc nghiệm, sân khấu hóa, xử lý tình huống..., qua đó tạo sân chơi bổ ích, khuyến khích sinh viên chủ động tìm hiểu và nâng cao hiểu biết. Thông qua các hoạt động này, sinh viên không chỉ được củng cố kiến thức mà còn phát triển kỹ năng thực hành, khả năng phân biện và ý thức trách nhiệm khi tham gia môi trường mạng. Đây cũng là cơ hội để tăng cường sự gắn kết giữa lý thuyết và thực tiễn, góp phần nâng cao chất lượng giáo dục toàn diện trong nhà trường.

### 2.2.5. Xây dựng đội ngũ chuyên gia về an toàn thông tin, an ninh mạng nhằm hỗ trợ kịp thời cho sinh viên

Việc hình thành đội ngũ chuyên gia, cán bộ có trình độ chuyên môn sâu về an toàn thông tin, an ninh mạng là yêu cầu cần thiết nhằm nâng cao hiệu quả công tác giáo dục và hỗ trợ sinh viên trong môi trường số. Trung tâm cần chủ động xây dựng lực lượng nòng cốt gồm giảng viên, cán bộ công nghệ thông tin và các chuyên gia phối hợp từ các cơ quan, đơn vị chức năng để tư vấn, hỗ trợ, giải đáp các vấn đề phát sinh liên quan đến an toàn thông tin cho sinh viên.

Đội ngũ này có nhiệm vụ cung cấp thông tin cảnh báo sớm về các nguy cơ, hình thức lừa đảo mới trên không gian mạng; hướng dẫn sinh viên cách phòng tránh, xử lý khi gặp sự cố như bị đánh cắp tài khoản, lộ dữ liệu cá nhân hoặc bị tấn công mạng. Đồng thời, cần thiết lập các kênh hỗ trợ như đường dây nóng, hộp thư điện tử, nền tảng trực tuyến để tiếp nhận và xử lý kịp thời các phản ánh của sinh viên.

Bên cạnh đó, Trung tâm cần có cơ chế đào tạo,

bồi dưỡng, cập nhật kiến thức thường xuyên cho đội ngũ này, đồng thời tạo điều kiện về cơ sở vật chất, trang thiết bị phục vụ công tác chuyên môn. Việc xây dựng đội ngũ chuyên gia không chỉ giúp nâng cao năng lực ứng phó với các vấn đề an ninh mạng mà còn góp phần tạo dựng môi trường học tập an toàn, lành mạnh và hỗ trợ sinh viên một cách hiệu quả, kịp thời trong mọi tình huống.

### III. KẾT LUẬN

An toàn thông tin, an ninh mạng là vấn đề có ý nghĩa quan trọng trong bối cảnh hiện nay, đặc biệt đối với sinh viên – lực lượng sử dụng Internet thường xuyên và chịu nhiều tác động từ môi trường số. Việc nâng cao nhận thức và kỹ năng sử dụng Internet an toàn cho sinh viên tại các Trung tâm Giáo dục quốc phòng và an ninh là nhiệm vụ cần thiết và lâu dài.

Triển khai đồng bộ các giải pháp nêu trên sẽ góp phần nâng cao nhận thức, hình thành kỹ năng và ý thức trách nhiệm của sinh viên khi tham gia không gian mạng, qua đó xây dựng môi trường học tập an toàn, lành mạnh, đáp ứng yêu cầu giáo dục và bảo vệ Tổ quốc trong tình hình mới.

## TÀI LIỆU THAM KHẢO

- Bộ Giáo dục và Đào tạo (2023), *Chuyển đổi số trong giáo dục – cơ hội và thách thức*, NXB Giáo dục Việt Nam, Hà Nội.
- Bộ Thông tin và Truyền thông (2022), *Sổ tay hướng dẫn kỹ năng bảo đảm an toàn thông tin trên không gian mạng*.
- Chính phủ (2022), *Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ phê duyệt đề án “Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo trong giai đoạn 2022-2025, định hướng đến năm 2030”*, Hà Nội.
- Quốc hội (2018), *Luật An ninh mạng*, NXB Chính trị Quốc gia Sự thật, Hà Nội.
- Thông tư số 05/2020/TT-BGDĐT của Bộ Giáo dục và Đào tạo: Ban hành Chương trình giáo dục quốc phòng và an ninh trong trường trung cấp sư phạm, cao đẳng sư phạm và cơ sở giáo dục đại học.*