THỰC TRẠNG KỸ NĂNG SỬ DỤNG INTERNET AN TOÀN CỦA HỌC SINH THPT VIỆT NAM VÀ MỘT SỐ GIẢI PHÁP GIÁO DỤC

CURRENT STATUS OF SAFE INTERNET USAGE SKILLS OF VIETNAMESE HIGH SCHOOL STUDENTS AND SOME EDUCATIONAL SOLUTIONS

PHAN THỊ THÚY QUYÊN, *pttquyen@iemh.edu.vn*
Trường Cán bộ quản lý giáo dục Thành phố Hồ Chí Minh.

THÔNG TIN

Ngày nhận: 05/11/2025
Ngày nhận lại: 15/12/2025
Duyệt đăng: 18/12/2025
Mã số: TCKH-S05T12-2025-B03
ISSN: 2354 - 0788

TÓM TẮT

Trong bối cảnh chuyển đổi số đang định hình lại môi trường học tập, học sinh phổ thông sử dụng Internet với tần suất cao nhưng chưa được trang bị đầy đủ kỹ năng tự bảo vệ, dẫn đến gia tăng các rủi ro về an toàn thông tin và sức khỏe tâm lý. Bài viết tiếp cận vấn đề theo hướng kết hợp phân tích - tổng hợp các tài liệu chính sách, báo cáo quốc gia và quốc tế với khảo sát thực tế. Dữ liệu được thu thập từ 408 học sinh cùng phỏng vấn giáo viên, cán bộ quản lý tại một số trường phổ thông, và được xử lý bằng thống kê mô tả. Kết quả cho thấy học sinh có mức độ tiếp cận Internet rộng nhưng nhận thức rủi ro còn hạn chế; tình trạng bắt nạt mạng, tiếp cận nội dung độc hại và lừa đảo trực tuyến diễn ra phổ biến. Từ các phát hiện trên, bài viết đề xuất nhóm giải pháp tăng cường giáo dục kỹ năng số, chuẩn hóa nội dung an toàn mạng trong chương trình học và đẩy mạnh phối hợp giữa nhà trường, gia đình và xã hội.

Từ khóa:
An toàn internet, kỹ năng số, rủi ro mạng, chuyển đổi số, giáo dục.
Keywords:
Internet safety, digital literacy, cyber risks, digital transformation, education.

ABSTRACT

In the context of digital transformation reshaping the learning environment, high school students frequently use the Internet at high speed but are not fully equipped with protection skills, leading to increased risks to information security and mental health. The paper approaches the problem by combining analysis and synthesis of policy documents, national and international reports with field surveys. Data were collected from 408 students and interviews with teachers and administrators at a number of high schools, and analyzed using descriptive statistics. The results show that students have wide access to the Internet but limited risk awareness; cyberbullying, access to harmful content and online fraud are common. From the above findings, the article proposes a set of solutions to enhance digital skills education, standardize cyber security content in the curriculum and promote coordination between schools, families and society.

1. Introduction

In the context of strong digital transformation, the Internet has become an important learning and interaction environment for high school students. Many international studies have shown that using the Internet provides great opportunities for students to expand their knowledge. It also helps increase their self-learning ability and form digital competencies (OECD, 2021). However, along with the benefits, students also face increasing risks. These include cyberbullying, accessing harmful content, online fraud, and privacy violations. Such factors can have negative impacts on mental health, learning ability, and personality development (Livingstone & Third, 2017; UNICEF, 2022).

UNICEF (2022) shows that children and adolescents are the most vulnerable group in the digital environment due to limited ability to evaluate information, incomplete self-protection capacity, and easy manipulation in online interactions. In Vietnam, surveys by the Ministry of Information and Communications (2023) and MSD (2024) also recorded a rapid increase in the rate of students accessing the Internet, while the level of awareness about cyber safety is still low, leading to many risks of abuse or falling into unsafe online behaviors.

In that context, equipping high school students with skills to use the Internet safely and responsibly is not only an inevitable need but also a requirement of modern education, in line with the goal of developing digital citizens in the new general education program. However, many domestic and foreign studies have shown that the content of cyber safety education is still scattered, unsystematic and has not been implemented synchronously in schools (Hoang Thi Minh & Pham Quy Hoi, 2023; DQ Institute, 2022). Therefore, it is imperative that immediate and concerted action be taken to empirically analyze the current situation, address key challenges, and develop effective solutions to ensure the safety and growth of students in the digital era.

2. Overview and Research Methods

2.1. Theoretical Framework

This study is underpinned by an integrated theoretical framework drawing on three complementary perspectives to explain high school students' Internet usage behaviors and online safety risks in the context of digital transformation.

First, the Theory of Planned Behavior (Ajzen, 1991) posits that individual behavior is shaped by attitudes toward the behavior, perceived social norms and perceived behavioral control. This theory provides a useful lens for interpreting students' online behaviors, as frequent Internet use and risk-taking practices may reflect not only personal attitudes but also normative peer influence and limited perceived control over online risks.

Second, Social learning theory (Bandura, 1977) emphasizes that behaviors are acquired through observation, imitation, and social interaction. In school settings, students' online behaviors are strongly influenced by peers, teachers and digital communities. This framework helps explain the diffusion of both positive and negative online practices, such as information sharing, cyberbullying and unsafe interactions, among adolescents.

Third, Bronfenbrenner's Ecological Systems Theory (1979) situates student behavior within multiple, interacting environmental systems, including the individual, family, school and broader socio-digital context. From this perspective, online safety risks are not solely individual issues but outcomes of combined influences from home supervision, school policies, digital platforms and societal norms.

Together, these theories form a coherent conceptual framework that guides the research design, instrument development and interpretation of findings. They suggest that students' Internet

usage behaviors and safety risks are shaped by the interaction between personal dispositions, social learning processes and multi-level environmental conditions.

2.2. Research Design and Methods

Research design

The study adopts a descriptive–analytical research design, combining secondary document analysis with a cross-sectional mixed-methods field survey. This approach allows for both contextual understanding and empirical assessment of the current status of Internet use and online safety among Vietnamese high school students. Quantitative data provide an overview of usage patterns and risk prevalence, while qualitative data offer contextual insights from educators and school administrators.

Secondary document analysis

Document analysis was conducted on key policy documents and reports issued by the Ministry of Education and Training and the Ministry of Information and Communications, along with international and national studies by OECD (2021), UNICEF (2022) and the Management and Sustainable development institute (2020-2024). This method helped establish the policy context, identify prevailing issues related to student online behavior, and inform the construction of survey instruments.

Sampling and participants

The field survey was conducted in March 2025 at five public high schools in Vietnam, including three urban schools and two rural schools, to ensure contextual diversity. Schools were selected based on the following criteria: (i) implementation of the 2018 General Education Program; (ii) availability of basic digital learning infrastructure; (iii) institutional consent to participate in the study.

A cluster sampling technique was applied at both school and class levels. Within each selected school, intact classes from grades 10, 11, and 12 were randomly chosen and all students in these classes were invited to participate. The final quantitative sample consisted of 408 students, meeting the minimum requirement for descriptive and exploratory analysis.

In addition, 25 teachers (teaching Information technology, Civic education, Literature and related subjects) and 10 school administrators (principals, vice principals and heads of professional groups) were selected through purposive sampling for qualitative interviews, based on their direct involvement in student management and digital education practices.

Research instruments

The student questionnaire comprised 25 items, organized into three dimensions: Internet access and usage patterns (frequency, duration and purposes); Online behaviors and interactions (communication, social networking, content sharing); Exposure to online risks and safety incidents (cyberbullying, harmful content, online fraud, privacy violations).

Items employed nominal and Likert-type scales and were adapted from UNICEF's *Disrupting Harm* survey (2022) and relevant national studies to ensure content validity. The instrument was reviewed by two experts in educational management and pilot-tested with a small group of students to ensure clarity and appropriateness.

Semi-structured interview guidelines were developed for teachers and administrators, focusing on: (i) observed online behaviors and risks among students; (ii) current educational practices related to digital skills and online safety; (iii) institutional challenges and proposed solutions.

Data collection procedures

Student questionnaires were administered in classroom settings under researcher and teacher supervision, ensuring anonymity and voluntary participation. Interviews were

conducted face-to-face and recorded with participants' informed consent. Ethical principles, including confidentiality and the right to withdraw, were strictly observed throughout the data collection process.

Data analysis

Quantitative data were coded and processed using Microsoft Excel. Descriptive statistics (frequencies, percentages and distributions) were used to identify dominant patterns of Internet use and risk exposure. Cross-tabulation analyses were conducted to examine differences across grade levels and gender groups.

Qualitative interview data were analyzed using thematic content analysis, enabling triangulation with quantitative findings and strengthening the interpretive validity of the results.

Reliability and methodological limitations

Internal consistency of the questionnaire was assessed during pilot testing to ensure acceptable reliability. While the study primarily relies on descriptive and exploratory analyses and does not employ advanced inferential statistical testing, this limitation is acknowledged. Given the study's aim of assessing current practices and identifying prevalent risks, the applied methodological approach is considered appropriate, reliable and consistent with the research objectives.

3. Contents

3.1. Digital transformation context and impact on high school education

3.1.1. Digital transformation in the global context and in Vietnam

Digital transformation is rapidly reshaping education systems worldwide. According to the OECD (2021), digital technologies are altering the ways in which teaching, learning, assessment and educational management are conducted. In Vietnam, the National digital transformation program (Decision No. 749/QĐ-TTg, 2020) identifies education as a priority sector. The Ministry of Education and Training (2022) further emphasizes the development of digital learning resources, online teaching and learning, and learning management systems (LMS), as well as the enhancement of students' digital competencies. These factors have created favorable conditions for students to access the Internet more frequently and intensively.

3.1.2. Internet access level of high school students

International reports and recent studies indicate that Vietnamese children and adolescents have very high levels of Internet access. UNICEF's Disrupting Harm in Viet Nam report (2022) shows that the majority of children aged 12-17 use the Internet, with near-universal daily access among those aged 14 -17. A recent large-scale study on Vietnamese adolescents and young adults (aged 14-24) also reports extremely high rates of Internet and social media use, reflecting the strong diffusion of digital technologies among young people (Nguyen et al., 2025). Domestic media surveys further note that the Internet has become an essential medium for children and students, particularly through smartphones (VietnamNet, 2025).

Platforms such as YouTube, TikTok, Facebook, Zalo, Google Meet and Zoom have become integral to the educational ecosystem. Easy, ubiquitous access to the Internet provides a favorable condition for developing self-directed learning skills, critical thinking, and creativity. However, it also presents significant challenges regarding content moderation and the safeguarding of student safety (Ministry of Information and Communications, 2023).

3.1.3. Opportunities and challenges from the digital environment

The opportunities that the digital environment brings to high school education are substantial: expanding access to knowledge, personalizing learning, fostering enhanced collaboration among teachers, students and parents, and developing 21st-century skills such as teamwork, critical thinking and problem-solving. However, the challenges are

considerable, especially for students who lack adequate awareness and competence to protect themselves in cyberspace. Substantial threats such as exposure to age-inappropriate content, online enticement and scams, gaming and social media addiction, invasion of privacy and the lack of skills to discern credible from fabricated information are all risks that seriously affect students' psychological well-being and holistic development in the absence of appropriate educational methods (OECD, 2021). The data presented in this subsection are drawn from secondary sources, serving as contextual and comparative references for the subsequent analysis based on primary survey data.

3.2. Current status of Internet usage among high school students

3.2.1. Popular trends in Internet usage among students

Given the increasing and easy access to digital devices such as smartphones, tablets, and laptops among high school students, Internet usage has become an integral part of their daily academic and personal lives. Recent surveys (UNICEF, 2022) show that students use the Internet for a variety of different purposes, specifically:

Online learning: Utilization of platforms such as Zoom, Google Meet, and Microsoft Teams for remote learning, particularly after the COVID-19 pandemic; Search for academic information: Searching for learning materials, lecture videos, and sample papers on Google, YouTube and specialized digital learning material websites; Entertainment: Watching videos on YouTube and TikTok; listening to music and playing online games; Social exchange: Using social networks such as Facebook, Instagram, Zalo and Discord for chatting, networking and content sharing; Content creation: some students tend to become content creators, sharing short videos, livestreaming and participating in forums. Internet use often extends beyond regular school hours and often involves prolonged, continuous engagement, particularly in the evenings and on weekends. The frequency and duration of use depend on age, family condition, and the degree of parental and school supervision.

A survey conducted by the Management and Sustainable Development Research Institute (MSD) illustrates the purposes of Internet use among Vietnamese youth, as shown in Figure 1.

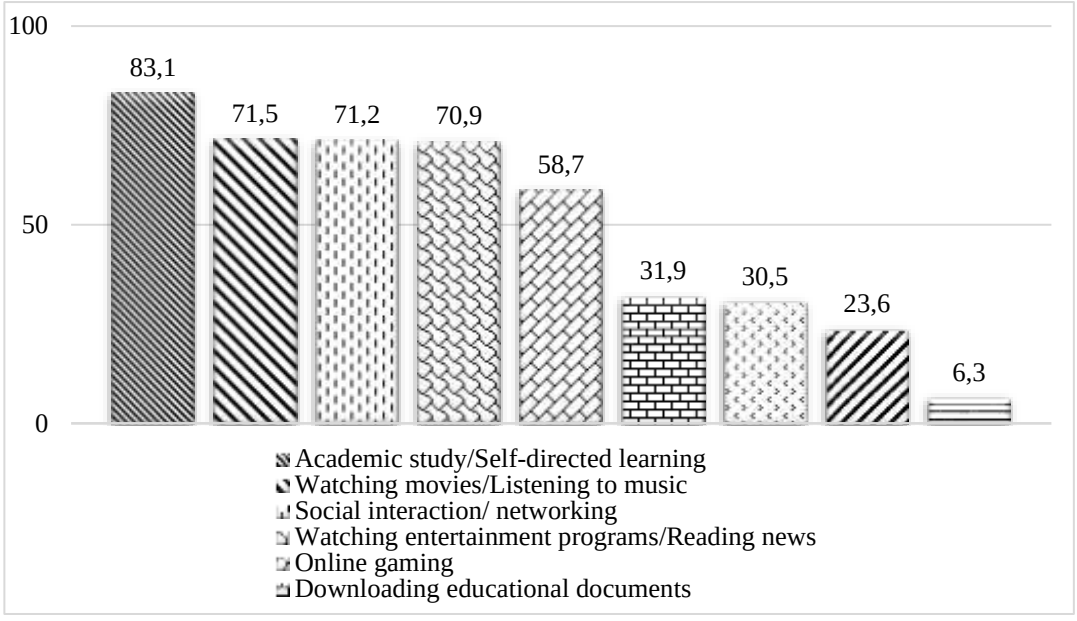


Figure 1. Purpose of Internet use by Vietnamese youth

(Source: MSD, Training material on child protection in the online environment, p.14)

High school students use the Internet for many different purposes: entertainment, study, news, making friends... UNICEF statistics (2022) show the online activities of this age group, as shown in table 2.

Table 1. Online activities of children aged 12-17

Online activities	Total	12-13	14-15	16-17	Boy	Girl
Watching video	91%	85%	93%	94%	91%	91%
Using social media	88%	78%	91%	95%	85%	91%
Using text messaging applications	87%	73%	93%	95%	82%	92%
Doing school assignments	72%	69%	73%	75%	73%	72%
Reading news	70%	55%	72%	83%	68%	73%
Communicate with distant family members or friends.	65%	54%	70%	72%	59%	70%
Watching livestream	63%	58%	64%	66%	62%	64%
Follow celebrity or public figure on social media	52%	54%	53%	57%	46%	57%
Searching for new information	50%	37%	50%	60%	50%	49%
Playing online games	49%	47%	47%	53%	69%	33%
Seeking emotional support	45%	40%	44%	51%	49%	42%
Seeking information about career or studying opportunity	43%	41%	44%	45%	39%	47%
Participate in online web platforms centered around hobby sharing	36%	30%	33%	45%	35%	36%
Searching for health-related information	29%	19%	31%	37%	27%	31%
Searching for localized information and events	23%	20%	21%	28%	23%	23%
Creating personalized video and music content	9%	6%	9%	11%	6%	11%
Discuss political and societal issues	6%	8%	6%	6%	5%	7%
Creating blog or website	6%	7%	7%	6%	6%	7%

(Source: UNICEF, 2022, Preventing Harmful Behavior Project in Vietnam)

All students participating in the survey reported engaging in social networking activities across multiple platforms and for a variety of different purposes. This finding is also consistent with results from several other relevant surveys. The UNICEF (2022) report shows that 82% of Vietnamese children aged 12-13 use the internet daily, while the figure for 14-15 year olds is 93%. The MSD (2024) survey indicates that 83.9% of children used phones, and the rate of social networking use was 86.1%

Furthermore, 97% of children surveyed reported using phones for at least 1 hour per day, with nearly 27% using them for 5 hours or more daily. The dominant purpose was entertainment, cited by 86% of respondents, while the rates for academic study, information seeking and social networking were 75%, over 66% and over 57%, respectively (Information security department, 2024).

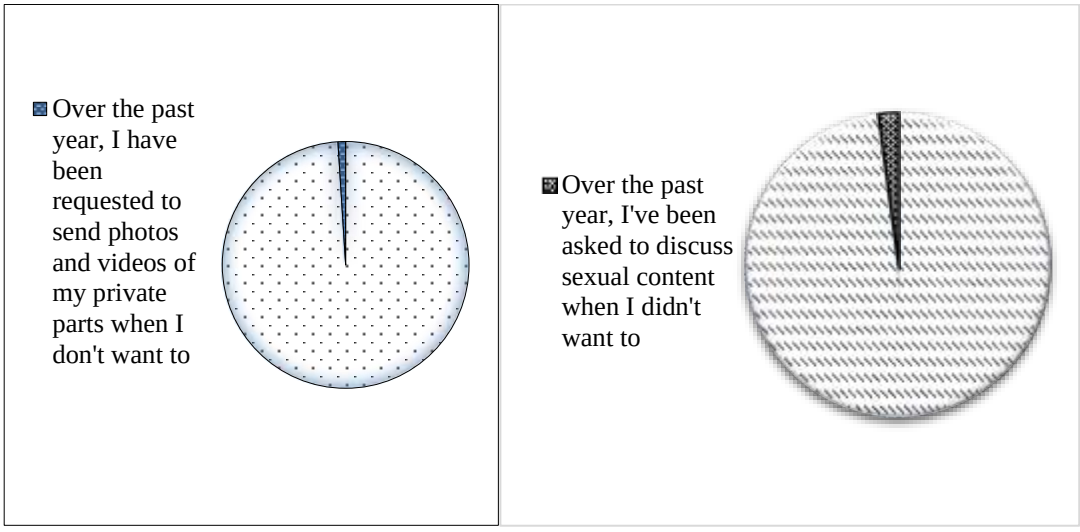
3.2.2. Risks and dangers from uncontrolled Internet use

Lack of knowledge and skills about online safety (UNICEF, 2022) makes students vulnerable to the following risks: Exposure to harmful content: Age-inappropriate content such as violence, pornography, gambling and superstition, remains widely accessible on digital platforms. Students may inadvertently or deliberately access this material, leading to adverse cognitive and behavioral consequences.

Internet addiction: Overuse of social media and online gaming leads to an imbalance between study and entertainment, resulting in academic performance decline, insomnia and psychological disorders.

Cyberbullying: Many students become victims or perpetrators of harassment, insults, or the non-consensual sharing of inappropriate images in cyberspace, causing serious psychological trauma; Online Fraud: Adolescents are easily lured by prize-winning games, online shopping, malicious links, or risky online relationships; Invasion of privacy: Lack of security awareness makes it easy for students to disclose personal identifying information such as name, address, phone number, and personal photos, which can lead to significant adverse outcomes.

A UNICEF survey found that 5% of Vietnamese children who use the Internet had received unwanted sensitive images, and 8% have received inappropriate comments about themselves such as jokes, talk, or comments about children's bodies, appearance, or sexual activity (see Figure 2; UNICEF, 2022).



Background: Vietnamese youth aged 12–17 who use the Internet, n = 994

Figure 2. Percentage of Children Who Have Been Harassed Online in the 12–17 Age Group

(Source: UNICEF, 2022, Preventing Harmful Behavior in Vietnam Project)

A UNICEF survey found that 0.5% of the 994 children surveyed had created and shared self-generated sexual imagery. Which were repeatedly spread by the offender. However, the victims were afraid and hesitant to report the case, fearing that they could be considered criminalized for producing such content (see Figure 3; UNICEF, 2022).

A UNICEF survey found that 0.5% of the 994 children surveyed had taken or recorded nude videos of themselves and shared them, which were repeatedly spread by the offender, but they were afraid and did not report the incident, fearing that they might be considered guilty for producing such content (figure 3) (UNICEF, 2022). According to a UNICEF survey, approximately 0.5% of the 994 children surveyed reported having created and shared self-generated sexual images. These materials were subsequently repeatedly redistributed by perpetrators. The findings further indicate that affected children were reluctant to report the incidents, largely due to concerns about potential legal consequences or being perceived as responsible for the production of such content (see Figure 3; UNICEF, 2022).

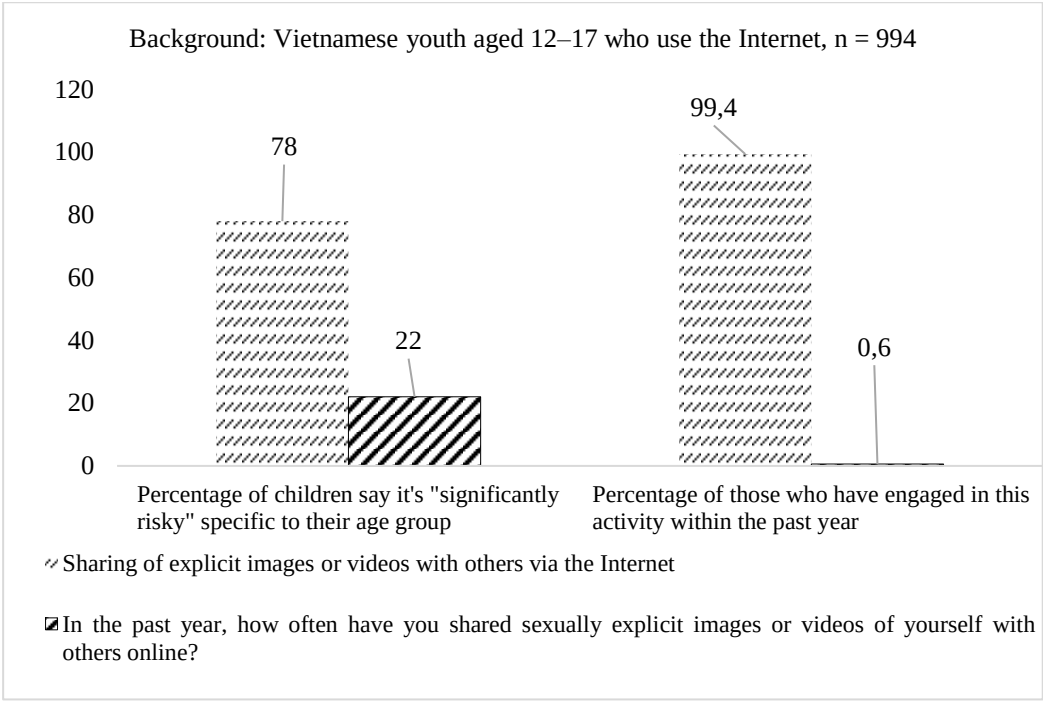


Figure 3. Percentage of children who have shared personal information on the Internet in the 12-17 age group

3.2.3. Shortage in digital skills and cybersecurity awareness

Although students are technically proficient in using the Internet (using applications, searching for information, communicating online), most of them have not been properly educated in specific digital skills: skills to identify false information (fake news); skills to secure personal information; skills to interact civilly online; skills to respond to internet safety. This is a significant gap in the current general education program, as the content on internet safety is often only briefly integrated, not systematic or mandatory. Parents also often lack sufficient knowledge to guide their children or are too busy to effectively monitor their children's Internet use, leading to students facing numerous risks and heightened insecurity. A survey of administrators and teachers regarding the risks of insecurity that students face when using the Internet reveals the following results (Figure 4).

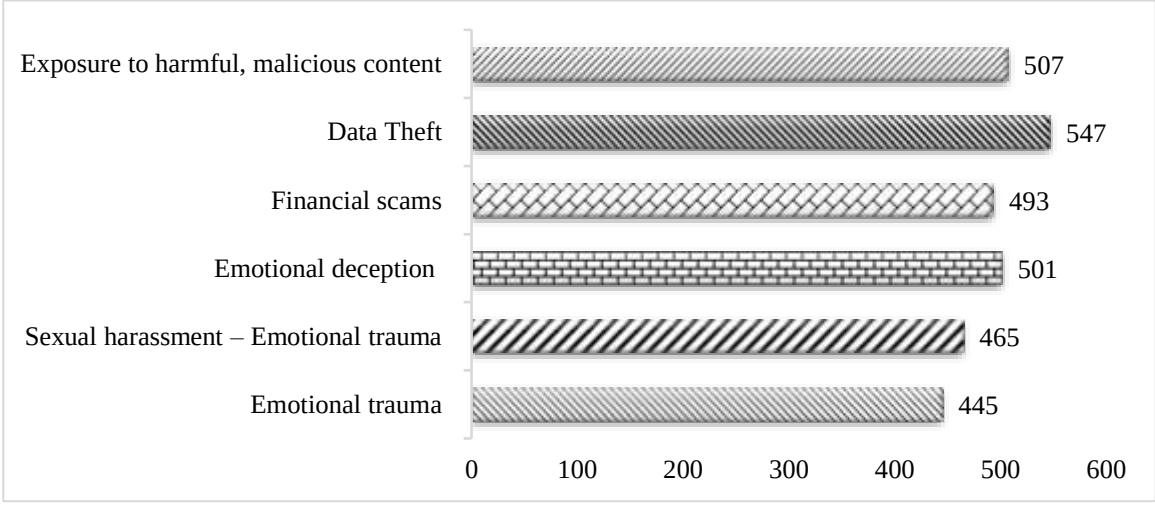


Figure 4. Cybersecurity risks faced by students when using the internet

In addition to the above prevalent risks, some opinions also cited other risks that may occur to students, such as: Being incited to do harmful acts; Being lured into doing illegal things; Forming distorted behaviors and perceptions; Being enticed to join evil groups; Being addicted to online games and social media. A separate survey of students about the risks and dangers that occur online revealed diverse responses, suggesting that they may have been victims of these behaviors (The results are shown in Table 2).

Table 2. Statistics on cyberbullying behavior related to deficiencies in digital competence

Behaviors	Option		% students participating in the survey		% by selection
	Yes	No	Yes	No	
Discrimination	314	94	77	23	12,6
Teasing	180	228	44,1	55,9	7,2
Provocation	227	181	55,6	44,4	9,1
Insult	349	58	85,5	14,5	14
Enticement	129	279	31,6	68,4	5,2
Intimidation	305	103	74,6	25,4	12,2
Disturbance	273	135	66,9	33,1	10,9
Suppression-control	239	169	58,5	41,4	9,6
Threats	318	90	77,9	22,1	12,7
Insinuation	164	244	40,2	59,8	6,5

Data from Table 2 shows that variables such as discrimination (12.6%), insult (14%), intimidation (12.2%), and threats (12.7%) all account for a high percentage. Insult (14%) accounts for the highest rate among these, with insult accounting for the highest percentage, showing the seriousness of verbal violence. Next are variables such as: provocation (9.1%), disturbance (10.9%), suppression - control (9.6%), ranging from 200 < 300 choices of students participating in the survey. The remaining variables are: teasing (7.2%), enticement (5.2%) and insinuation (6.5%), reaching levels below 200/408 students. However, considering the overall rates, we see that most of the variables selected for the survey are at the expected level, suggesting that these behaviors have been and are happening quite commonly among young people in schools today.

3.3. The role of education in ensuring cybersecurity for students

3.3.1. Digital skills education - An indispensable in the digital transformation era

In the digital age, technology-using skills are no longer an option but a mandatory condition for students to be able to learn, develop and integrate. However, "using technology proficiently" does not equate to "safe and responsible technology usage". Therefore, digital skills education-especially online safety skills-should be considered essential and mandatory educational components in the high school education curriculum (Hoang Thi Minh & Pham Quy Hoi, 2023).

The online environment contains both opportunities and risks. If students are not equipped with the skills to identify risks and protect themselves, they will become vulnerable, easily manipulated and dependent. On the contrary, if properly educated, students can become proactive, creative digital citizens who know how to protect themselves and respect the online community.

3.3.2. The role of stakeholders in online safety education

Cybersecurity education for students cannot be the sole responsibility of educational institutions but requires synchronous and sustained coordination among the family, the school and society.

The Educational Institution: The school provides formal knowledge and skills for students. It is necessary to integrate content on safe Internet usage skills into the curriculum, from subjects such as Information Technology and Citizenship Education, and through extracurricular activities. Organize seminars, discussions and digital skills practice sessions for students. Enhance teachers' professional capacity in instructing and advising on cybersecurity.

The Family/Parents: The home is where students use the Internet most often, particularly in the evenings and on weekends. Parents need to be equipped with foundational digital literacy and skills to manage their children's Internet use. It is crucial to build a trusting, close relationship so that children feel safe to share when they encounter online problems. Apply appropriate parental monitoring tools and encourage the use of technology in a purposeful and constructive manner.

Society: Organizations, businesses and the media need to play a role in curating and disseminating positive content and building a safe online environment. Strengthen promotion and public awareness campaigns about online safety. Legal policies also need to be clear and timely to handle violations and child abuse in cyberspace.

3.3.3. Shortcomings in current cybersecurity education

Currently, in Vietnam, cybersecurity education content is only included in the curriculum in a fragmented manner or as non-mandatory recommendations, rather than being implemented as a mandatory, systematic skill set. Some schools organize seminars or invite experts to speak, but these initiatives lack adequate regularity and pedagogical depth.

In addition, the pedagogical competence of the teaching faculty in the field of cybersecurity is still limited. The absence of standardized curriculum documents and effective teacher training models leads to challenges in the practical implementation of cybersecurity education.

3.4. Proposed solutions for enhancing online safety education for high school students

Given the current status where students increasingly access the Internet early but lack the knowledge and skills to use it safely, the implementation of a synchronous, comprehensive, and feasible system of solutions is imperative. Below are some main groups of solutions:

3.4.1. Integrating online safety education into the formal curriculum

One of the important and fundamental solutions is to make online safety education content an official part of the high school education program, instead of just implementing it as an extracurricular activity or ad-hoc integration.

- At the primary education level, students need to be familiar with basic concepts: Internet function, definition of personal information, password security protocols, and recognizing online strangers.

At the lower secondary level, the content can be expanded to security practices, identifying online scams, media literacy (discerning false information) and responsible social media usage.

At the upper secondary level, it is necessary to raise awareness of privacy rights, laws related to online behavior, and the impact of the Internet on psychological well-being and personality development. Subjects such as Information Technology, Citizenship Education, and Experiential Activities should serve as the primary integration channels while designing interactive lessons and real-life situations to help students acquire applicable skills.

3.4.2. Enhancing teacher training and capacity building

Teachers are crucial to the direct implementation of cybersecurity education, hence they need to be equipped with the requisite knowledge, skills, and pedagogical methodologies. Some specific methods include: Organize regular professional development sessions for teachers of relevant disciplines; Provide standardized instructional materials compiled by the Ministry of Education and Training or accredited organizations; Encourage teachers to utilize digital learning platforms that integrate cybersecurity content; Facilitate a network for experience sharing among teachers at the local and national levels. In addition, the awareness of school administrators must be heightened to facilitate adequate instructional time, budgetary allocation and encourage innovation in digital skills education.

3.4.3. Strengthening the Role of Parents and the Family Unit

Parents need to be seen as essential partners in educating their children about online safety. However, many parents today lack information or adopt a parenting approach based on authoritarian control rather than collaborative partnership. Some recommendations: Organize digital skills workshops for parents, especially parents of primary and lower secondary school students; Develop a resource manual on safe Internet use at home for students and parents for mutual adherence; Encourage families to establish common rules for Internet use, set reasonable time limits, and place digital devices in common areas of the household; Facilitate seamless communication and collaboration between parents and schools through platforms like Zalo groups, regular online meetings and the sharing of digital resources and updates.

3.4.4. Application of Technology for Monitoring and Support

The advancement of technology serves as an effective tool for educating and safeguarding students in the online environment:

Utilization of software for Internet access management, harmful content filtering, and time control (e.g., Family link, Microsoft family safety).

Development of learning applications that integrate digital safety education, featuring reward systems and scenario-based questions to foster self-directed learning and self-assessment.

Leveraging AI and big data to analyze access behavior, enabling early detection and warning of anomalous behavior (e.g., a tendency to search for negative content, excessive frequency of use).

However, the use of monitoring technology needs to be accompanied by awareness education to avoid becoming counterproductive or eroding trust between students and adults.

3.4.5. Fostering Collaboration with Social Organizations and Enterprises

Many domestic and international organizations have implemented digital skills education programs for students (such as "YouSafe," "Think Before You Share," and "I am safer with Google," among others), but these initiatives have not been adequately scaled. Consequently, the following actions are required: Establishing cooperation between the Ministry of Education and Training and technology enterprises to build a national program on online safety education; Encouraging enterprises to provide financial resources, educational materials, and necessary software to schools; Connecting with social organizations and non-governmental organizations experienced in youth development, technology and media literacy to implement long-term community projects.

3.5. Discussion and Comparison with Previous Studies

The findings derived from the authors' primary survey indicate that Vietnamese high school students engage intensively with the Internet on a daily basis, mainly for entertainment, communication, and learning purposes. This pattern is consistent with secondary data reported by

UNICEF (2022) and the Ministry of Information and Communications (2023), which highlight near-universal Internet access among adolescents aged 12-17 in Vietnam. Compared with domestic studies, the results align with Hoang Thi Minh and Pham Quy Hoi (2023), who also reported high frequencies of Internet use among high school students. However, the present study records higher proportions of students experiencing online harassment, insults, threats, and intimidation, suggesting that cyber risks may be increasing and becoming more complex across different school contexts.

From an international perspective, OECD (2021) emphasizes that students often possess strong technical skills but lack sufficient competencies related to online safety, data protection and responsible digital behavior. The current findings support this observation, as students demonstrate frequent Internet use while exhibiting limited awareness and skills in managing online risks. Furthermore, the results are consistent with previous international research grounded in ecological and social learning perspectives (Livingstone & Third, 2017), which argue that online risks are shaped not only by individual behavior but also by peer influence, school practices, family supervision, and the broader digital environment. The similarities between the present findings and prior studies reinforce the validity of the results and underline the urgent need for systematic online safety education. Overall, while this study confirms key trends identified in earlier research, it also contributes updated empirical evidence on the growing exposure of Vietnamese high school students to cyber risks in the context of digital transformation.

4. Conclusion and Recommendations

4.1. Conclusion

The findings from 408 surveyed students show that Internet use is embedded in their daily routines. A total of 97% reported using the Internet every day, and nearly 27% used it for up to five hours, mainly for entertainment, learning, and information searching. This high level of engagement is accompanied by substantial risks. The data reveal high frequencies of harmful online behaviors, including insults (85.5%), threats (77.9%), discrimination (77%), intimidation (74.6%), harassment (66.9%) and coercion (58.5%). Other behaviors such as provocation, mocking, and manipulation, also occurred at notable levels.

These results suggest that although students are technologically proficient, they lack essential online safety skills, increasing their vulnerability to peer influence and negative digital interactions. Viewed through the Theory of Planned Behavior and Social Learning Theory, students' online behaviors appear strongly shaped by attitudes, perceived norms, and peer modeling. The Ecological Systems Theory further indicates that family, school and digital environments collectively contribute to the multilayered risks students encounter. Given this evidence, schools and policymakers should implement a structured and comprehensive online safety education program to protect students and support their healthy digital development amid ongoing digital transformation.

4.2. Recommendations

Based on the survey findings and subsequent analysis, several recommendations are proposed to enhance the effectiveness of safe Internet use education for high school students.

For the Ministry of Education and Training (MOET): Develop a systematic and mandatory cybersecurity skills curriculum for each level of education; issue standardized guidelines and conduct regular professional training for teachers and educational administrators; integrate digital literacy content into core subjects and formal educational activities.

For Schools: Proactively organize extracurricular activities, thematic workshops

and simulation exercises on online safety; utilize technological tools for monitoring and providing early warning of risky Internet usage; facilitate access for teachers to open educational resources and professional support communities.

For Parents: Proactively enhance awareness, acquire internet usage skills and utilize child monitoring technology; establish family rules for internet use, engage with children rather than resort to prohibition or neglect; encourage children to participate in online safety education activities at school and in the community.

For Organizations and Businesses: Cooperate with the education sector to implement systemic digital skills education programs; sponsor software, educational resources, open learning tools and platforms to support students in practicing digital skills; demonstrate social responsibility by actively censoring age-appropriate content on digital platforms.

For students: Students should actively develop self-protection skills online, including safeguarding personal information, verifying information sources, engaging respectfully in digital communication and promptly reporting harmful behaviors. They are encouraged to participate in school-led online safety programs and act responsibly in the digital environment.

REFERENCES

Ajzen, I. (1991). *The theory of planned behavior*. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Bandura, A. (1977). *Social learning theory*. Prentice Hall.

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design*. Harvard University Press.

Department of Information Security. (2024). *Handbook on protecting children in cyberspace*. Ministry of Information and Communications.

DQ Institute. (2022). *Digital intelligence (DQ) framework and global standards report*. DQ Institute.

Hoang.T.M & Pham.Q.H. (2023). *Digital skills for secondary school students: Opportunities and challenges. Journal of Educational Sciences, 39 (2), 44-55.*

Livingstone, S., & Third, A. (2017). *Children and young people's rights in the digital age: An emerging agenda*. New Media & Society, 19(5), 657–670.

Management and Sustainable Development Institute. (2018). *Training materials on child protection in the digital environment*.

Management and Sustainable Development Institute. (2024). *Survey on internet use among Vietnamese children in 2024*.

Ministry of Education and Training. (2022). *Digital transformation program for the education sector for the period 2022–2025*. Vietnam Education Publishing House.

Ministry of Information and Communications. (2023). *Summary report on cybersecurity in 2023.*

Organisation for Economic Co-operation and Development. (2021). *21st-century skills and education in the digital age*. OECD Publishing.

UNICEF. (2022). *Disrupting harm in Viet Nam: Evidence on online risks and harms faced by children.* UNICEF Innocenti.

VietnamNet. (2025). Vietnamese youth and internet usage trends. *VietnamNet Online Newspaper*.