

FROM AWARENESS TO BEHAVIOR: THE EFFECTIVENESS OF EDUCATIONAL INTERVENTIONS IN PREVENTING ONLINE KIDNAPPING AMONG HIGH SCHOOL STUDENTS – A CASE STUDY OF PHU THIEN COMMUNE, GIA LAI PROVINCE, VIETNAM

Nguyen Hoang Anh Thu^{1*}, Do Quynh Giao², Hoang Thi Dieu Loan³

Tran Quoc Tuan High School, Phu Thien Commune, Gia Lai Province, Vietnam.

*Corresponding Author

Nguyen Hoang Anh Thu

Tran Quoc Tuan High School, Phu Thien Commune, Gia Lai Province, Vietnam.

Article History

Received: 02.11.2025

Accepted: 19.12.2025

Published: 12.01.2026

Abstract: In the context of the increasing use of the Internet and social networking platforms among high school students, the risk of online kidnapping—commonly associated with online grooming leading to abduction or extortion—has emerged as a serious threat. This study aims to identify the characteristics of online kidnapping behaviors, examine the current level of awareness among high school students in Phu Thien Commune, Gia Lai Province, and propose effective preventive educational interventions.

A survey was conducted with 715 students and 71 teachers from two high schools in the area. The results reveal that 76.2% of students had little or no understanding of online kidnapping, nearly 70% had interacted with strangers online, and almost 50% had shared personal information on the Internet. Furthermore, 43.2% of students reported handling online threats on their own or confiding only in peers, rather than seeking assistance from adults.

Based on these findings, the study designed and implemented a comprehensive intervention framework, including awareness campaigns, the development of a digital safety handbook, the establishment of student clubs, the use of artificial intelligence (ChatGPT) for scenario-based simulations, and the integration of online safety topics into school curricula. Experimental results demonstrate significant improvements: students' awareness of online kidnapping increased from 23.8% to 97%, while safe response skills and the tendency to seek adult assistance improved markedly, with the reporting rate rising from approximately 40% before intervention to 87% after intervention. Notably, 93.5% of students evaluated ChatGPT as highly useful in recognizing early signs of online fraud and grooming.

The study concludes that combining digital safety education with AI-based tools and fostering collaboration among schools, families, and communities constitutes an effective approach to preventing online kidnapping among high school students.

Keywords: online kidnapping; digital safety; high school students; online grooming; fraud prevention; self-protection skills; educational intervention; ChatGPT; artificial intelligence (AI); Gia Lai (Phu Thien).

Cite this article:

Thu, N.H.A., Giao, D.Q., Loan, H.T.D., (2026). FROM AWARENESS TO BEHAVIOR: THE EFFECTIVENESS OF EDUCATIONAL INTERVENTIONS IN PREVENTING ONLINE KIDNAPPING AMONG HIGH SCHOOL STUDENTS – A CASE STUDY OF PHU THIEN COMMUNE, GIA LAI PROVINCE, VIETNAM. *ISAR Journal of Arts, Humanities and Social Sciences*, 4(1), 31-38.

1. Introduction

The rapid development of the Internet and social networking platforms has brought significant benefits for learning and social connectivity; however, it has also introduced new risks for students. *Online kidnapping*—often referred to as *online grooming leading to abduction or cyber-kidnapping*—can be understood as a form of crime in which offenders exploit digital environments to deceive or lure victims, primarily children and students, through psychological manipulation with the intent to arrange face-to-face meetings for malicious purposes or to extort money.

According to the Vietnamese Ministry of Education and Training (2025), citing information from the Ministry of Public Security, recent cases have emerged in which criminals impersonated police officers or prosecutors and contacted students by phone, falsely accusing them of being “involved in criminal cases.” Victims were subsequently threatened and instructed to demand ransom payments from their families. This sophisticated form of fraud has caused severe anxiety among students and parents alike and has been officially identified as *online kidnapping*—a new manifestation of cybercrime that capitalizes on students’ lack of experience and limited risk awareness.

Prior to the 2025–2026 academic year, the Government Information Portal issued warnings about the increasingly sophisticated nature of online kidnapping schemes, highlighting a case in which a female student in Dong Nai Province was coerced into demanding a ransom of 300 million VND from her family via online messages. Fortunately, timely intervention by the police prevented further harm. Such incidents underscore the seriousness of online kidnapping and emphasize the urgent need for proactive prevention by schools and society at large.

High school students are in adolescence, a developmental stage characterized by psychological instability, curiosity, and limited life experience. As a result, they are particularly vulnerable to exploitation in digital environments. According to a UNICEF Vietnam report (2022), the proportion of children using the Internet on a daily basis in Vietnam is remarkably high, especially among those aged 14–15. Early and frequent exposure to online spaces without adequate digital safety skills places many students at heightened risk of grooming and online fraud.

In response, the Ministry of Education and Training has issued official warnings regarding criminal tactics that exploit social media to target students and has called for strengthened coordination among schools, families, and relevant authorities to protect learners. Similarly, the Ministry of Information and Communications released the *Handbook on Protecting Children in Cyberspace* (2023), providing guidance for parents and educational institutions in creating safer online environments. These policy initiatives demonstrate that online safety for students has become a national priority in Vietnam.

Phu Thien Commune, located in Gia Lai Province, is an area with relatively convenient transportation links connecting the Central Highlands with neighboring regions. While such connectivity facilitates social and economic interaction, it also poses potential challenges to social security in the context of rapid digital transformation, thereby making the issue of online safety for high school students particularly salient in this locality.

Based on the study, the authors find that students’ awareness of online kidnapping remains significantly limited. A survey of **715 high school students** in the locality reveals that nearly **70%** have added or communicated with strangers online, more than **30%** are unable to recognize signs of online fraud, and almost **50%** have shared sensitive personal information on the Internet. These alarming figures reflect the inadequacy of students’ digital safety skills, creating vulnerabilities that can be exploited by malicious actors.

Accordingly, the study highlights the urgent need to enhance students’ awareness and skills in preventing online kidnapping. This research seeks to address the following questions: *What is online kidnapping? How well do students currently understand this phenomenon? What roles have families and schools played in protecting students? Can technological tools, particularly artificial intelligence (AI), be applied to detect early signs of online grooming in digital communication? What are the consequences of online kidnapping, and which educational, technological, and behavioral interventions can effectively help students prevent such risks?*

On this basis, the primary objective of the study is to systematize knowledge of online grooming and fraud schemes targeting high school students, analyze their underlying causes and potential consequences, and, most importantly, propose a set of concrete and feasible interventions to prevent online kidnapping among high school students in the local context. The study is expected to contribute to raising awareness, equipping students with self-protection skills, and providing an evidence-based foundation for coordinated action among schools, families, and relevant authorities to ensure student safety in the digital environment.

1.2. Theoretical Framework / Literature Review

Definition of Online Kidnapping

The term *online kidnapping* refers to criminal behaviors in which offenders use digital platforms—such as social media, messaging applications, and online games—to approach victims, establish familiarity and trust, and subsequently deceive them. Victims are typically children or adolescents, and the ultimate purposes of such acts include sexual exploitation, coercion, or financial extortion. Unlike traditional kidnapping, which relies on direct physical force, online kidnapping occurs covertly within cyberspace. Perpetrators often impersonate trusted individuals, such as friends, relatives, or public officials, to manipulate victims psychologically.

A common tactic involves criminals posing as police officers or judicial authorities who contact victims by phone or online messaging, falsely accusing them of involvement in criminal cases. Victims are then threatened and instructed to demand ransom payments from their families. In such cases, no physical abduction initially takes place; instead, the crime manifests as online deception and financial extortion, targeting both victims and their families.

Online kidnapping can therefore be conceptualized as a hybrid form of cyber fraud and child exploitation. Its impacts extend beyond financial loss to include severe psychological harm, such as anxiety, fear, and a diminished sense of personal safety. In more serious cases, victims may be lured into face-to-face

meetings, posing direct threats to their physical safety and even their lives.

At the global level, child protection agencies have documented a significant rise in *online enticement* and *grooming* cases targeting minors. For example, the National Center for Missing & Exploited Children (NCMEC) reported receiving more than 518,000 cases of online enticement or suspicious communications within the first six months of 2025, representing a sharp increase compared to the same period in 2024 (Missing & Exploited Kids, 2025). These alarming figures serve as a global warning regarding the escalating severity of cybercrime targeting children and adolescents.

Situation in Vietnam: Along with the widespread use of the Internet, cases related to online kidnapping have begun to emerge in Vietnam. In addition to the previously mentioned tactic of impersonating police officers, various other schemes have been reported, including impersonating friends or relatives online to request in-person meetings, luring victims with virtual gifts or rewards, and approaching students through online games.

Findings from our survey indicate that students are relatively capable of recognizing several common schemes: 75.6% were aware of free-gift fraud tactics, approximately 70% could identify impersonation of friends or law enforcement officers, and around 67% expressed caution toward invitations made through online games. However, more sophisticated strategies—such as psychological intimidation, emotional manipulation, or threats—were recognized by far fewer students, with notably low identification rates. This suggests that cybercriminals are increasingly employing complex and evolving tactics that exceed students' general awareness, thereby requiring educational interventions to keep pace with such developments.

A report by UNICEF (2022) on children and Internet use in Vietnam similarly highlights that children face multiple online risks, ranging from fraud and cyberbullying to sexual exploitation, and calls for strengthened digital skills education for adolescents. In response, the Ministry of Education and Training (MOET) issued official guidelines in 2022 on educating students in safe Internet use, requiring schools to integrate online safety content into teaching and extracurricular activities. These measures indicate that, from policy-level management to school-based practice, the urgency of protecting students in cyberspace has been widely acknowledged in Vietnam.

Related Studies: Internationally, a growing body of research has focused on detecting and preventing online grooming and child exploitation. For example, Leiva-Bianchi et al. (2025) conducted a meta-analytic review of 33 studies and demonstrated that machine learning-based approaches can detect grooming-related conversations with accuracy rates exceeding 90%. In several countries, artificial intelligence technologies have been piloted to automatically identify and block conversations exhibiting grooming indicators on social media platforms (Home Office & Priti Patel MP, 2020).

Beyond technological solutions, educational research has also emphasized the effectiveness of awareness-raising interventions. Studies indicate that when students are equipped with knowledge about common fraud and grooming tactics, they become more vigilant and better prepared to respond appropriately to online risks (NSPCC, 2023). In Vietnam, although systematic academic research on *online kidnapping* remains limited, official

guidance issued by the MOET (2022) and the Ministry of Information and Communications (2023) has outlined essential preventive skills, such as avoiding the disclosure of personal information, refraining from meeting online acquaintances offline, and promptly reporting suspicious situations to parents or teachers. These policy documents provide a foundational framework upon which the present study builds its intervention strategies.

1.3. Research Methodology

Research Design

This study adopts a mixed-methods approach that combines theoretical analysis with empirical research. First, the authors collected and analyzed relevant literature and reports on online fraud, online grooming, and existing prevention models proposed both internationally and in Vietnam.

The empirical component was conducted at Tran Quoc Tuan High School and Vo Van Kiet High School in Phu Thien Commune, Gia Lai Province—an area characterized by a rural population, a high proportion of ethnic minority students, and rapidly expanding access to the Internet. The empirical research consisted of three main components:

Questionnaire Survey:

Structured questionnaires were administered to students and teachers to assess students' initial awareness, Internet use behaviors, and readiness to respond to online kidnapping risks. A total of 715 students and 71 teachers participated in the baseline survey.

Interviews and Focus Group Discussions:

The research team conducted in-depth interviews with 20 parents and organized small-group discussions with teachers and students to gather qualitative insights into perceived causes of online risks and potential preventive solutions.

Educational Intervention (Experimental Study):

Based on the baseline survey results and expert consultations, the research team developed a set of intervention measures and implemented a pilot program over a three-month period (September–December 2025) at the two participating schools.

Intervention Measures:

During the experimental phase, students in the intervention group were exposed to a comprehensive set of preventive measures, including:

Awareness Campaigns and Training Workshops:

The study organized thematic seminars and extracurricular workshops on preventing online kidnapping, involving experts, teachers, and parents. The content focused on recognizing fraud and grooming tactics, developing self-protection skills, and responding appropriately to online threats.

Digital Safety Handbook:

A digital handbook in the form of e-books and infographics was developed, outlining common signs of online grooming and fraud, as well as step-by-step guidance on what to do when suspicious situations arise. Students could easily access the handbook via smartphones or computers for on-demand reference.

Online Safety Club:

An online safety club was established to promote peer learning and experience sharing. The club met regularly to discuss real-life cases, simulate risk scenarios, and practice response strategies. A dedicated social media fan page was also created to disseminate timely warnings and updates from relevant authorities.

ChatGPT-Based Scenario Simulation:

Artificial intelligence, specifically ChatGPT, was employed to simulate potentially dangerous online conversations (e.g., invitations from strangers to meet in person or offers of rewards through online games). Students interacted with the chatbot in realistic scenarios to practice recognizing risks and applying safe responses. More than 15 simulated scenarios and guiding prompts were developed to support student training.

Curriculum Integration:

Online safety and fraud prevention content was integrated into relevant subjects such as civic and legal education, information technology, language arts, and homeroom activities. Teachers were provided with instructional materials to systematically embed digital safety education into regular classroom practice.

Evaluation of Effectiveness

To objectively assess the impact of the intervention measures, students were divided into two groups: an experimental group, which participated fully in all intervention activities (including ChatGPT interactions and club activities), and a control group, which did not participate or received only standard warning materials.

Both groups completed comparable questionnaires before and after the intervention period. Pre- and post-intervention

comparisons between the two groups enabled the measurement of changes in awareness and skills attributable to the intervention. In addition, qualitative feedback was collected from teachers, parents, and students regarding satisfaction, perceived usefulness, and the sustainability of the implemented activities.

Quantitative data were analyzed using descriptive statistical methods (e.g., percentage distributions and before–after comparisons), while qualitative responses were examined through content analysis to identify recurring themes and insights.

2. Findings

2.1. Students’ Initial Awareness and Behaviors Regarding Online Kidnapping

The baseline survey conducted at two high schools in Phu Thien Commune indicates that students’ overall awareness of *online kidnapping* remains highly limited. Specifically, 76.2% of students reported that they had either never heard of the concept or only had a vague understanding of it, while only 23.8% stated that they clearly understood what online kidnapping entails. These findings suggest that the majority of students have not fully recognized the seriousness and potential dangers of online grooming and fraud-related behaviors.

Regarding the ability to identify different forms of online kidnapping, students tended to demonstrate greater awareness of common and easily recognizable tactics frequently encountered on social media platforms. Approximately 68–76% of students reported being able to identify schemes such as fake prize or gift giveaways, impersonation of friends or relatives, impersonation of police officers or investigators, and luring through online games (Figure 1).

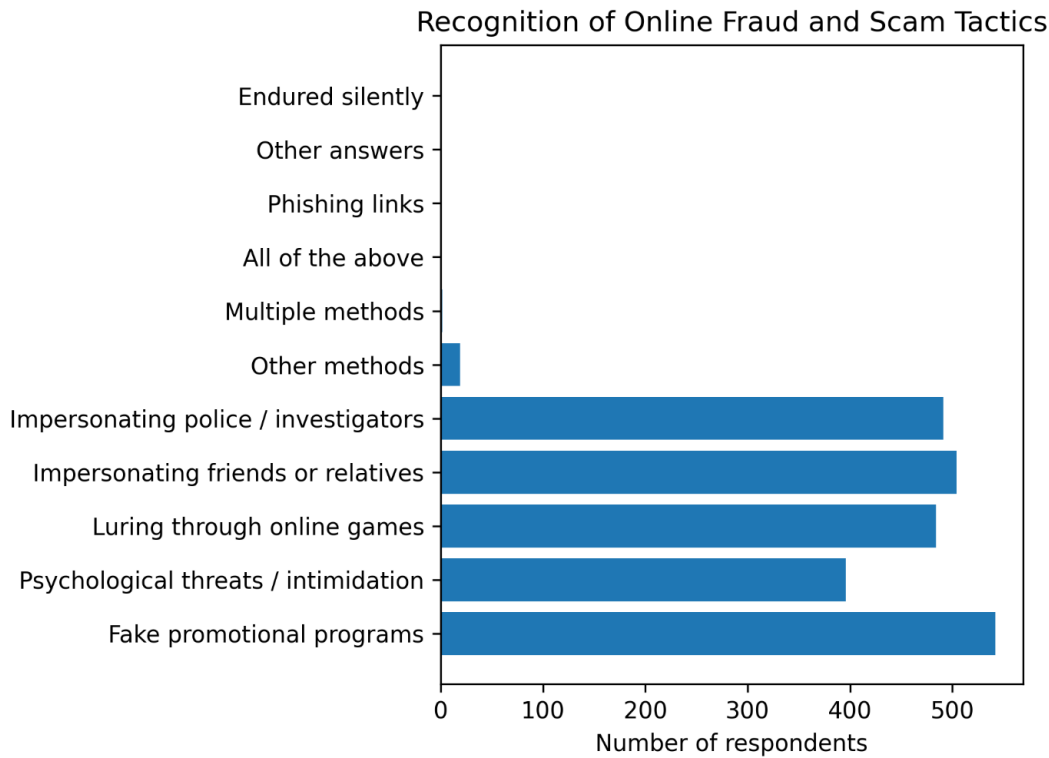


Figure 1. Students’ Awareness of Common Online Fraud and Grooming Tactics

However, more sophisticated tactics—such as threats, psychological intimidation, and emotional manipulation—exhibit considerably lower recognition rates. This indicates that students continue to face significant difficulties in identifying complex forms of online fraud, representing a critical vulnerability that cybercriminals can readily exploit.

With regard to students' responses when encountering dangerous situations in the online environment, the survey results show that only 56% of students choose to seek assistance from parents, teachers, or other responsible adults, whereas 43.2% tend to handle the situation on their own or share it only with peers of the same age group (Figure 2). The lack of timely support from experienced adults entails substantial risks, as students are more likely to make poorly informed decisions and become susceptible to manipulation by malicious actors.

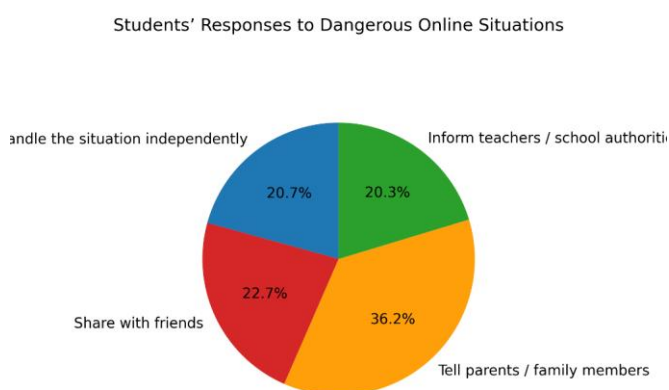


Figure 2. Students' responses when encountering dangerous situations in the online environment.

With regard to personal information protection behaviors, 77.7% of students are aware of the importance of securing their accounts and personal data; however, 23.3% of students still underestimate this issue (Figure 3). This finding indicates that a segment of students continues to lack sufficient knowledge and awareness of information security, which constitutes a critical factor in preventing online fraud and cyber-abduction behaviors.

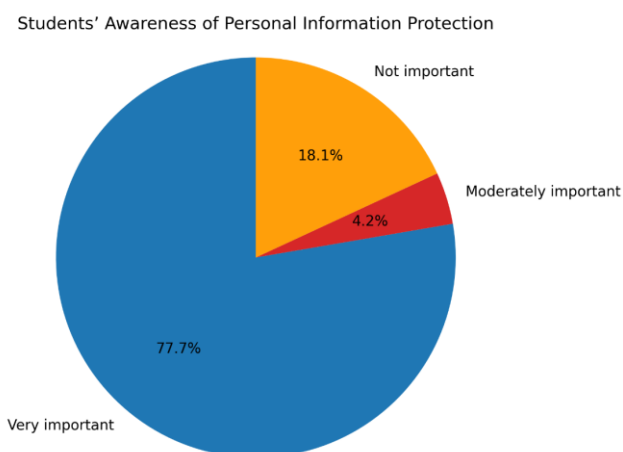


Figure 3. Awareness of personal information protection.

Notably, when examining students' awareness of the application of artificial intelligence (AI) in preventing online abduction, up to 61% of students reported that they had never heard of AI-based applications in this field, while only 23.8% demonstrated a certain level of understanding. These findings indicate that AI remains a relatively new concept for the majority of students. At the same time, they underscore the urgency of integrating AI-based solutions with digital safety education within schools in order to enhance students' capacity to prevent online abduction in the context of the rapidly expanding influence of social media (Figure 4).

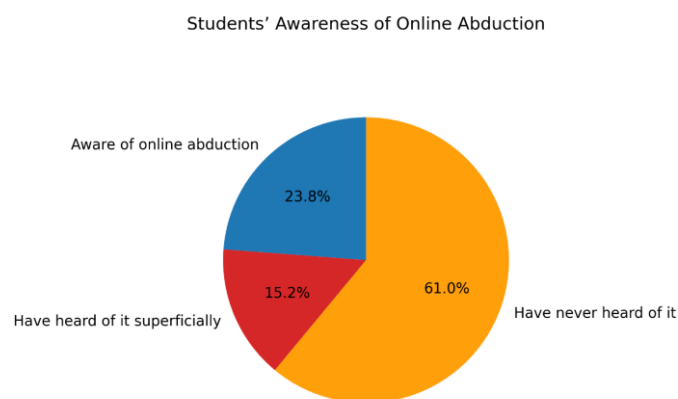


Figure 4. Students' level of awareness of online abduction and AI-based prevention.

2.2. Effectiveness of the Experimental Intervention Measures

After the implementation of the intervention measures, the survey results reveal clear and substantial improvements in both awareness and behavioral responses among the student group participating in the project. From an initially limited level of knowledge, the majority of students developed a solid understanding of the concept of online abduction, the key indicators for identifying online fraud and grooming behaviors, and appropriate response strategies when encountering suspicious situations.

Regarding awareness of the concept of *online abduction*, prior to the intervention only 23.8% of students reported a clear understanding of this phenomenon. Following the intervention, this proportion increased sharply to 97%, indicating that nearly all participating students had acquired accurate and comprehensive knowledge. Correspondingly, the proportions of students who had merely "heard of it" or had "never heard of it" declined significantly, demonstrating the strong educational impact of the intervention activities.

In terms of skills for handling dangerous online situations, post-intervention results show that 87% of students indicated they would report suspicious incidents to parents, teachers, or school authorities, compared to approximately 40% before the intervention. This shift suggests a clear transition from a tendency toward self-handling to proactive help-seeking behavior involving responsible adults, thereby reducing the risk of manipulation by malicious actors. Many students also developed practical safety responses, such as preserving digital evidence, blocking suspicious accounts, and reporting incidents to relevant authorities.

With respect to personal information protection, the proportion of students who clearly understood the importance of not sharing sensitive information online increased to 93.5% after the intervention. This finding indicates a marked improvement in students' awareness of account security and personal data protection—skills that are essential in today's digital environment.

Concerning the application of ChatGPT and artificial intelligence (AI), survey results indicate that 93.5% of students positively evaluated the use of ChatGPT for simulating risky online scenarios. Students reported that this tool enabled them to identify fraudulent and grooming tactics at an early stage and to practice safe response strategies within a risk-free simulated environment. The experience of "interacting with AI in the role of a malicious actor" was perceived as novel, engaging, and highly effective in fostering digital safety skills.

In addition, feedback from teachers and parents demonstrates a high level of consensus regarding the effectiveness of the implemented measures. Approximately 95% of teachers identified behaviors that increase students' vulnerability to cybercrime, including excessive disclosure of personal information, befriending strangers online, and participation in unhealthy online gaming environments. Following the project, both teachers and parents highly rated the feasibility and effectiveness of the proposed solutions, such as extracurricular activities, the use of ChatGPT, and the establishment of school-based digital safety clubs.

Notably, when compared with the control group (which did not participate in the intervention activities), the experimental group exhibited significantly greater improvements across all indicators. The control group, which was only exposed to conventional warning materials, showed minimal changes in awareness and behavior. This comparative evidence further confirms the strong effectiveness of the integrated intervention framework proposed in this study.

3. Discussion

Analysis of underlying causes

Based on the initial survey results and expert opinions, the vulnerability of high school students to online grooming and abduction can be attributed to multiple interrelated factors.

First, student-related factors. Many students still lack adequate digital safety knowledge and skills, particularly in recognizing sophisticated tactics employed by cybercriminals. In addition, adolescent psychology—characterized by curiosity, trustfulness, and a strong desire to form new social connections—combined with limited communication with family members, creates favorable conditions for malicious actors to approach and manipulate them.

Second, family- and school-related factors. Parental supervision and guidance regarding students' Internet use remain insufficient in many cases. Some parents allow unrestricted access to digital devices without monitoring online content or interactions. At the same time, education on preventing online fraud and cyber-abduction has not been systematically integrated into the formal school curriculum, resulting in fragmented and inconsistent exposure to digital safety training.

Third, factors related to the online environment. Cyberspace is characterized by a high degree of anonymity, which enables offenders to conceal their real identities easily. Moreover, the

massive and heterogeneous volume of online information, coupled with the rapid advancement of technology—such as deepfake tools and fake or automated accounts—has made online scam and abduction scenarios increasingly sophisticated. Under these conditions, students face significant difficulties in distinguishing between authentic and deceptive interactions.

Taken together, the combination of knowledge gaps, adolescent psychological characteristics, and a complex digital environment constitutes the fundamental reasons why high school students represent a particularly vulnerable group in relation to online abduction.

Effectiveness and significance of the proposed solutions

The experimental results demonstrate that the proposed intervention measures exerted a positive and measurable impact on both students' awareness and behavior.

First, thematic workshops and discussion sessions effectively attracted students' attention and raised awareness across the school community. The active involvement of teachers and parents contributed to the creation of a consistent educational environment, in which students perceived that both family and school took the issue seriously. This collective engagement encouraged students to approach digital safety learning with greater responsibility and commitment.

Second, the digital handbook proved to be a practical and user-friendly resource. Its visual design and concise content enabled students to access information at any time and to easily memorize key warning signs. Importantly, this material can be sustainably maintained, updated, and disseminated by schools to benefit successive cohorts of students.

Third, the establishment of a digital safety club created a healthy and interactive space where students could learn collaboratively and share experiences. Club activities fostered peer support and a sense of collective responsibility for online safety—an important factor, as peers may sometimes detect warning signs and alert one another before adults become aware. The club model also aligns well with broader educational goals related to life skills development and participatory school culture.

Fourth, the application of ChatGPT to simulate risky online scenarios represents a distinctive and innovative feature of the project. This AI-based tool provides a safe practice environment in which students can make mistakes and learn from them without real-world consequences. The results indicate that ChatGPT-enabled simulations helped students develop more effective reflexive responses compared to purely theoretical instruction. These findings highlight the considerable potential of AI technologies in education for preventing online exploitation. Teachers also expressed surprise at the realism and engagement of AI-generated scenarios and agreed that this approach merits further long-term application and study.

Fifth, integrating digital safety content into the formal curriculum ensures both sustainability and inclusiveness. Rather than relying solely on short-term projects, embedding these competencies—whether through integration across subjects or dedicated modules—ensures that all students acquire essential digital safety skills. This direction is consistent with national and international trends emphasizing digital literacy and online safety within general education systems.

Practical implications and limitations.

Building on its initial success, the proposed intervention model can be scaled up and applied in other high schools across Gia Lai Province and nationwide. The integrated approach—combining traditional education, modern technology, and extracurricular activities—has proven particularly effective and well suited to contemporary students' psychological characteristics. Moreover, the project strengthened collaboration among schools, families, and the wider community, thereby contributing to a more coherent and supportive digital safety environment for students.

Nevertheless, several limitations should be acknowledged. The experimental scope remains relatively small, involving only two schools over a three-month period, which restricts the ability to assess long-term impacts. In addition, the use of ChatGPT requires access to appropriate devices and stable Internet connectivity; therefore, implementation in disadvantaged areas would necessitate adequate infrastructural support. Some parents initially expressed concerns regarding the use of artificial intelligence, underscoring the need for communication efforts to clarify that AI functions as a supportive educational tool rather than a risk factor.

These limitations can be addressed in future research by expanding the scale and duration of interventions and by adapting implementation strategies to local conditions.

The research team conducted pre-intervention and post-intervention surveys to assess the effectiveness of the AI-supported application, with the results presented below.

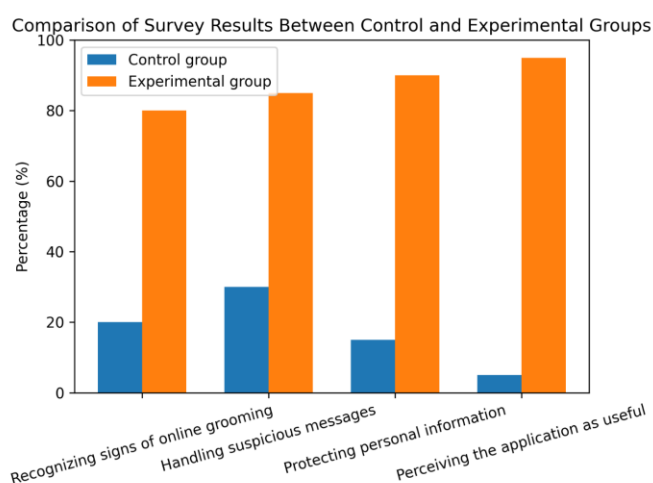


Figure 5. Comparison of survey results on application usage between the control group and the experimental group.

The comparison clearly indicates that students exposed to the AI-supported intervention achieved markedly higher outcomes across all indicators, whereas the control group—relying on conventional warning materials—showed only modest improvements.

Overall, the solutions proposed in this study not only address immediate local challenges but also open up a new direction for life skills education in the digital era. This approach emphasizes the integration of traditional educational methods with artificial intelligence-based technologies, while simultaneously promoting active community involvement in protecting adolescents within the online environment.

4. Conclusion and Recommendations

Conclusion

In the contemporary digital era, alongside the substantial benefits brought by the Internet, high school students are increasingly exposed to sophisticated forms of online grooming, fraud, and abduction. The study entitled *“Research and Proposal of Solutions to Prevent Online Abduction among High School Students in Phu Thien Commune, Gia Lai Province”* contributes to a comprehensive identification of this issue and the development of a system of solutions tailored to the practical conditions of local schools and students.

Through a combination of theoretical analysis and empirical surveys, the research reveals that students' levels of awareness and coping skills in relation to online abduction risks remain limited, while also identifying common behaviors that increase vulnerability to cybercrime, such as indiscriminate information sharing and befriending strangers online. On this basis, the project piloted a set of integrated interventions, including extracurricular education, the development of a digital handbook, AI-based scenario simulations using ChatGPT, the establishment of school safety clubs, and the integration of digital safety content into the curriculum.

The experimental results confirm the clear effectiveness of these solutions. Students demonstrated substantial improvements in knowledge and practical skills; teachers and parents also highly valued the feasibility and benefits of the proposed model. Following the intervention, students' ability to correctly identify dangerous online behaviors increased markedly, their responses to risky situations became more proactive and composed, and their awareness of personal information protection improved significantly. These positive changes contribute to the development of a safer and healthier school environment, aligned with the demands of today's digital society.

Recommendations

Based on the findings of this study, the authors propose the following recommendations:

- (1) Scaling up online abduction prevention education. It is recommended that the Department of Education and Training consider implementing extracurricular programs and digital safety handbooks across a wider range of high schools within the province. Schools should establish clubs or student-led task forces to sustain awareness-raising activities and peer-to-peer skill sharing.
- (2) Applying technology in monitoring and education. Law enforcement agencies and relevant authorities may explore the application of AI-based tools to monitor online platforms and detect early signs of child grooming and suspicious accounts. At the same time, the education sector should encourage the use of AI-driven simulations (such as ChatGPT) in life skills education, as these tools provide realistic, engaging, and experiential learning opportunities for students.
- (3) Strengthening coordination among the “three environments”. Families, schools, and society should work closely together to protect students in the online environment. Parents should receive training on emerging online risks in order to better supervise and communicate with their children; schools should regularly invite experts to update teachers on new cybercrime trends; and relevant

authorities should enhance community warnings when new scam tactics emerge.

(4) Policy and regulatory measures. It is recommended that the Ministry of Education and Training incorporate online safety education as a compulsory component of the revised general education curriculum. In parallel, stronger regulatory requirements should be imposed on social media platforms and service providers to enhance content moderation and cooperate with authorities in preventing the misuse of their platforms for criminal activities.

(5) Follow-up research. Future studies should expand this research model to other localities and conduct comparative analyses across regions, as well as assess the long-term effectiveness of the proposed solutions (e.g., after one to two years) to inform further refinement and improvement of online abduction prevention programs.

Overall, protecting students from the risk of online abduction is an urgent task that requires the collective efforts of the education system, families, and society as a whole. The positive outcomes of this study are expected to serve as a foundation for the wider implementation of effective solutions, contributing to the creation of a safer online environment for future generations.

References

1. Ministry of Education and Training. (2022). *Guidelines for communication and education on safe Internet use skills for students*. Hanoi, Vietnam.
2. Ministry of Information and Communications. (2023a). *Handbook on protecting children in cyberspace*. Information and Communications Publishing House.
3. Ministry of Information and Communications. (2023b). *Vietnam information security annual report 2023*. Authority of Information Security.
4. Home Office & Patel, P. (2020, January 9). *New AI technique to block online child grooming launched*. GOV.UK. <https://www.gov.uk/government/news/new-ai-technique-to-block-online-child-grooming-launched>
5. Leiva-Bianchi, M., Castillo, N., Astudillo, C. A., & Ahumada-Méndez, F. (2025). *Effectiveness of machine learning methods in detecting grooming: A systematic meta-analytic review*. *Scientific Reports*, 15, Article 9008. <https://doi.org/10.1038/s41598-024-83003-4>
6. National Center for Missing & Exploited Children. (2025, September 4). *Spike in online crimes against children: A "wake-up call"*. <https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call>
7. National Cyber Security Center. (n.d.). *NCSC official website*. Retrieved 2025 from <https://ncsc.gov.vn>
8. UNICEF Vietnam. (2022). *Children and the Internet: Awareness, behaviors, and risks in the online environment in Vietnam*. National research report.