

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

Nguyen Thi Huyen Nhu¹, Nguyen Bao Nhu Y², Nguyen Ngọc Bao Tram³, Cu Hoang Dung⁴, Vo Ky Duyen⁵, Vu Xuan Huong^{6*}

^{1,2,3,4}Nguyen Binh Khiem High School, Ho Chi Minh City, Vietnam;

⁵Chau Thanh High School, Ho Chi Minh City, Vietnam;

⁶Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam;

ABSTRACT: The increasing integration of digital technologies into education and daily life has heightened adolescents' exposure to cyber risks, including online manipulation and exploitation. This study investigates Vietnamese high school students' awareness and preventive behaviors regarding “online kidnapping,” a behavioral phenomenon encompassing catfishing, sextortion, and digital coercion. Employing a quantitative research design, data were collected from 338 students at Nguyen Binh Khiem High School (Ho Chi Minh City) through an 11-item standardized questionnaire. Statistical analyses using SPSS 26.0, including descriptive statistics, Chi-square tests, and Pearson's correlation, revealed that only 25% of participants had a clear understanding of online kidnapping, while 68% had interacted with strangers online and 32% had shared personal or sensitive information. A significant positive correlation was found between awareness and preventive behaviors ($r = 0.62$, $p < 0.01$), indicating that higher cognitive understanding is associated with safer online practices. Grounded in Ajzen's Theory of Planned Behavior and Kolb's Experiential Learning Model, the study introduces the “360° Digital Shield”, a three-tier educational framework that integrates (1) school-wide awareness programs, (2) peer-led digital media campaigns, and (3) curriculum-based experiential learning modules. This model emphasizes continuous, participatory learning to build sustainable digital resilience. The research contributes to the growing body of evidence-based digital safety education and provides practical implications for policymakers and educators in promoting responsible digital citizenship among youth in developing contexts.

KEYWORDS: Digital literacy, online kidnapping, cyber safety education, adolescent behavior, Vietnam, quantitative research

1. INTRODUCTION

The rapid expansion of digital technology has fundamentally transformed the way young people communicate, learn, and interact. In the era of digital citizenship, the Internet serves as both an indispensable learning tool and a potential source of social and psychological risk. For adolescents, particularly high school students, daily engagement with social media platforms such as TikTok, Facebook, YouTube, and Zalo has become routine. However, this increased connectivity exposes them to various cyber threats, including deception, emotional manipulation, and exploitation through virtual interactions (Livingstone et al., 2011; Hinduja & Patchin, 2015). In Vietnam, the digitalization of education and social life is advancing rapidly. According to the Ministry of Labour, Invalids and Social Affairs (2023), over 93% of Vietnamese adolescents aged 14 - 15 are Internet users, yet many lack the necessary digital literacy skills to identify and respond to online risks. Reports from WeProtect Global Alliance (2023) indicate a global surge of over 360% in self-generated sexual content by minors, underscoring the growing prevalence of online coercion and extortion targeting youth. These findings highlight that online safety is not merely a technical issue but a socio-educational challenge requiring early, evidence-based interventions within the school context.

Despite increasing attention to cyberbullying and online privacy, research on “online kidnapping”, a term encompassing manipulative behaviors such as catfishing, sextortion, and digital coercion remains limited. Online kidnapping refers to deceptive online interactions in which offenders gradually gain victims' trust through emotional manipulation or impersonation, leading to information disclosure, blackmail, or offline encounters. The phenomenon reflects the intersection between technology, psychology, and social vulnerability. Unlike conventional cybercrime, online kidnapping exploits affective dimensions trust, empathy, and social belonging, making adolescents particularly susceptible due to their developmental stage and search for social validation.

In Vietnam, empirical research on students' understanding of such manipulative online behaviors is still scarce, especially at the high school level. While the Ministry of Education and Training (2024) has emphasized digital citizenship in its digital

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

transformation agenda, most school-based initiatives remain limited to short-term awareness sessions rather than systematic, data-driven programs. Consequently, students’ awareness of online risks often remains fragmented, and their behavioral responses hesitation to report, limited assertiveness, and emotional vulnerability reflect gaps in digital resilience training.

A preliminary observation conducted at Nguyen Binh Khiem High School in Ho Chi Minh City revealed that most students spend between three and five hours online daily, primarily for entertainment or social networking. Many have encountered deceptive messages, impersonation attempts, or requests for private information. While the school has organized occasional seminars on online safety, these activities lack continuity, practical engagement, and measurable outcomes. This highlights an urgent need for research that empirically assesses students’ awareness and behaviors and translates findings into sustainable educational frameworks.

To address this gap, the present study adopts a quantitative approach to investigate high school students’ cognitive understanding, preventive behaviors, and educational needs concerning online kidnapping. The study is grounded in Ajzen’s Theory of Planned Behavior (1991), which posits that behavior is shaped by individual attitudes, perceived control, and social norms, and Kolb’s Experiential Learning Model (1984), emphasizing that durable behavioral change occurs through experience, reflection, and practice. By integrating these frameworks, this research assumes that higher awareness leads to stronger preventive behaviors, and that experiential education can effectively foster digital resilience among adolescents.

The study pursues three core objectives:

- 1) To assess the current level of awareness and preventive behaviors related to online kidnapping among high school students;
- 2) To examine the relationship between awareness and behavioral responses, identifying demographic or contextual differences (e.g., grade level, gender, daily Internet use);
- 3) To develop an evidence-based educational framework, the “360° Digital Shield” model that integrates awareness, peer engagement, and curriculum-based experiential learning to enhance digital safety education.

This research makes several contributions to the field of educational technology and digital citizenship studies. Empirically, it provides one of the first quantitative datasets on Vietnamese adolescents’ perceptions of online kidnapping, expanding the conceptual understanding of cyber victimization beyond conventional categories like bullying or fraud. Theoretically, it links behavioral psychology and experiential pedagogy, offering a multidimensional explanation for how awareness translates into protective behavior. Practically, it proposes a replicable and low-cost educational model tailored to developing-country contexts, aligning with national goals for digital transformation and child protection in cyberspace.

In doing so, the study aligns with the broader global agenda for sustainable digital citizenship education. It underscores the importance of *evidence-based, participatory learning* rather than passive information delivery. By equipping students with cognitive, emotional, and practical competencies, schools can cultivate a generation of learners who are not only digitally competent but also ethically grounded and socially responsible in the online environment. Ultimately, this research seeks to contribute to both academic discourse and educational practice by highlighting that digital safety is not solely a technological issue, it is an educational imperative. Through systematic assessment, data-driven intervention, and the “360° Digital Shield” model, the study demonstrates how schools can transform awareness into empowerment, fostering informed, resilient, and compassionate digital citizens capable of navigating the complex realities of cyberspace.

2. LITERATURE REVIEW

2.1. Conceptualizing “Online Kidnapping” and Adolescent Vulnerability

The concept of “*online kidnapping*” is an emerging construct that integrates elements of digital deception, emotional manipulation, and behavioral coercion. While the term itself remains underdeveloped in mainstream academic discourse, it captures a growing range of online behaviors that exploit trust and identity for harmful purposes. These include catfishing (false identity deception for emotional or financial gain), sextortion (coercive demands based on intimate content), and online grooming leading to physical exploitation (Hinduja & Patchin, 2015; WeProtect Global Alliance, 2023). Such phenomena represent a continuum of digital risks where psychological influence precedes overt victimization.

Adolescents are particularly vulnerable to these threats due to their developmental characteristics - high emotional responsiveness, strong social validation needs, and limited cognitive control (Livingstone et al., 2011). The convergence of these factors makes them more likely to engage impulsively with strangers online, underestimate risk, and disclose sensitive information. Studies have shown that adolescents’ perceived invulnerability and peer influence play a key role in shaping unsafe online behaviors (Vandoninck et al., 2013). Hence, understanding the psychosocial mechanisms underpinning online victimization is crucial for designing preventive interventions.

In the Vietnamese context, the prevalence of Internet use among youth has surged over the past decade, yet corresponding safety education remains fragmented (Ministry of Labour, Invalids and Social Affairs, 2023). Existing research often focuses on *cyberbullying* or *digital addiction*, while manipulative behaviors such as catfishing and sextortion remain understudied. The lack of conceptual clarity and empirical data has led to limited policy attention, even as anecdotal evidence suggests a rise in emotional

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

exploitation cases through social media. Addressing this research gap is critical to establishing a theoretical and practical foundation for school-based digital resilience programs.

2.2. Theoretical Frameworks: Behavioral and Experiential Learning Perspectives

The present study is grounded in two complementary theoretical perspectives: Ajzen’s Theory of Planned Behavior (TPB) and Kolb’s Experiential Learning Model (ELM).

1) According to TPB (Ajzen, 1991), human behavior is determined by three interrelated constructs: attitudes (individual evaluation of the behavior), subjective norms (social expectations), and perceived behavioral control (self-efficacy in executing the behavior). Applied to online safety, TPB suggests that students’ preventive behaviors such as verifying online identities or refusing to share private data depend on their awareness of digital risks, peer influence, and confidence in their ability to act safely. Empirical evidence supports this linkage; for instance, Yoon (2011) demonstrated that individuals with higher levels of digital ethics awareness and perceived behavioral control were significantly less likely to engage in unsafe or unethical online practices. This finding reinforces the principle that awareness, attitude, and self-efficacy operate interactively to shape responsible digital behaviors, thereby validating TPB’s relevance in the context of cyber safety education.

2) Kolb’s (1984) Experiential Learning Model complements TPB by emphasizing learning through action and reflection. Kolb conceptualizes learning as a cyclical process involving four stages: concrete experience, reflective observation, abstract conceptualization, and active experimentation. In digital safety education, this model implies that students must not only *know* what safe behaviors are but must *practice* and *reflect* on them through simulated or real scenarios. Research has shown that experiential interventions such as role-play, digital storytelling, and peer mentoring are more effective in developing long-term protective behaviors than one-time lectures (Li et al., 2020).

Together, TPB and ELM offer a robust theoretical foundation for understanding and improving students’ online safety behaviors. TPB explains *why* students act, while ELM elucidates *how* sustainable behavioral change occurs. Integrating these perspectives allows educators to design multi-layered interventions that target both cognition and practice, bridging the gap between awareness and action.

2.3. Empirical Studies on Digital Safety Education

A growing body of international research highlights the critical role of schools in promoting online safety and digital ethics. Livingstone and Haddon (2009) in the EU Kids Online project demonstrated that students with higher levels of parental mediation and school-based instruction exhibited more cautious online behaviors. Similarly, Mishna et al. (2010) reported that structured school programs on cyber-ethics significantly reduced exposure to online harassment among secondary students. Recent empirical studies also emphasize *participatory learning approaches* as key to effective digital citizenship education. Byrne et al. (2016) found that student-led campaigns such as peer-generated videos and social media content enhance engagement and knowledge retention compared to traditional instruction. Likewise, Lee and Chae (2007) demonstrated that combining media production activities with reflective discussions fosters both digital competence and empathy. These findings suggest that education models focusing solely on information dissemination are insufficient; instead, experiential, interactive, and collaborative approaches yield more sustainable behavioral change.

In Southeast Asia, however, implementation remains inconsistent. Research in Thailand (Wong, 2021) and cross-national studies in developing contexts (Livingstone, Byrne, & Carr, 2015) revealed that digital safety programs are often limited to policy-level awareness, lacking practical application and evaluation mechanisms. Vietnamese studies echo this pattern: school initiatives primarily consist of one-off seminars, with few empirical assessments of student learning outcomes. This absence of measurable frameworks has hindered policymakers’ ability to evaluate effectiveness and scalability, highlighting the need for evidence-based, contextually adapted digital safety education in schools.

2.4. The Need for Evidence-Based Education in the Vietnamese Context

In recent years, Vietnam’s Ministry of Education and Training has underscored the importance of integrating digital literacy into the national curriculum as part of the *Digital Transformation in Education Program 2021- 2025* (MOET, 2024). Yet, the transition from policy to practice remains challenging. Most schools still lack standardized assessment tools and context-specific curricula to address evolving cyber risks. Empirical evidence from Nguyen Binh Khiem High School illustrates these challenges. According to the survey analyzed in this study, only one in four students fully understood online kidnapping, while over two-thirds had interacted with strangers online and nearly one-third had shared private data. These statistics reveal not only informational gaps but also behavioral and emotional vulnerabilities. Moreover, although 63% of students had participated in at least one online safety session, the irregular frequency and lack of interactive pedagogy limited long-term impact.

This situation reflects what scholars term the *awareness-action gap*, a discrepancy between what individuals know and how they behave (Livingstone et al., 2011). Bridging this gap requires moving beyond theoretical instruction toward evidence-based education

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

that continuously measures learning outcomes and adapts content accordingly. Such data-driven pedagogy enables educators to identify which educational components - cognitive, emotional, or behavioral - most effectively improve students' digital safety.

2.5. Toward a Comprehensive Educational Framework

Synthesizing insights from global research and local realities, it becomes clear that effective digital safety education should operate at multiple levels: awareness, practice, and institutional integration. This aligns with multi-tiered behavioral models used in public health education (Bandura, 2001), where sustained change is achieved through reinforcement and environmental support. Building upon these theoretical and empirical foundations, the current study proposes the “360° Digital Shield” model, a holistic framework combining (1) school-wide awareness campaigns, (2) student-driven digital media engagement, and (3) curriculum-based experiential learning.

This structure aims not only to enhance cognitive understanding but also to cultivate agency and peer accountability in digital spaces. By embedding continuous assessment and feedback loops, the model contributes to both theoretical advancement in behavior-based digital education and practical implementation within Vietnam's educational system. In summary, prior literature underscores that adolescents' digital safety cannot be secured through isolated interventions. Instead, sustained behavioral change requires a combination of cognitive awareness, experiential practice, and institutional reinforcement. The integration of behavioral and experiential theories within an evidence-based educational framework offers a promising pathway to fostering resilient, responsible, and ethically aware digital citizens in the 21st century.

3. METHODOLOGY

3.1. Research Design

This study employed a quantitative descriptive–analytical design to examine the awareness and preventive behaviors of Vietnamese high school students toward online kidnapping. The quantitative approach was chosen for its ability to measure psychological and behavioral patterns across a large sample, ensuring objectivity and generalizability. Guided by Ajzen's Theory of Planned Behavior (1991) and Kolb's Experiential Learning Model (1984), the study explored how students' knowledge, attitudes, and perceived control shape their digital safety behaviors. The integration of behavioral and experiential perspectives enabled the research to move beyond mere awareness assessment, highlighting how cognitive understanding translates into real-world actions in cyberspace.

3.2. Participants

The study was conducted at Nguyen Binh Khiem High School in Ho Chi Minh City, a representative public school known for active technology integration and diverse student demographics. A total of 338 students from grades 10 to 12 participated, comprising 149 males (44.1%) and 189 females (55.9%), aged 15–18. The sample included 37.6% grade 10 students, 36.4% grade 11, and 26.0% grade 12. Participants were recruited through convenience sampling, an appropriate method in educational contexts that ensures accessibility while maintaining heterogeneity. Inclusion criteria required that students use the Internet daily and possess at least one active social media account. Participation was voluntary, with informed consent obtained from both students and school administrators.

3.3. Instruments

Data were collected using a structured self-administered questionnaire consisting of 11 items divided into four sections. The first section gathered demographic information such as age, gender, and daily Internet use. The second assessed students' awareness of online kidnapping behaviors, catfishing, sextortion, fake identities, and coercive messaging, measured on a 5-point Likert scale from “Never heard” to “Very familiar.” The third section evaluated behavioral responses to simulated online threats, including actions like verifying identity, refusing requests, or reporting incidents. The final section explored students' exposure to online safety education and their preferred learning formats, such as workshops, videos, or school clubs.

The instrument was developed based on prior international surveys (Livingstone et al., 2011; Mishna et al., 2010) and validated by three digital literacy experts for content accuracy. A pilot test with 30 students ensured clarity and linguistic suitability, leading to minor revisions. The internal consistency reliability achieved a Cronbach's alpha of 0.84, indicating high reliability for both awareness and behavioral scales. This rigorous validation process ensured that the instrument captured the intended constructs of perception and preventive action effectively.

3.4. Data Collection Procedures

Data collection took place over three weeks in October 2025 using Google Forms distributed via the school's digital learning network. Students completed the questionnaire during computer science classes or homeroom sessions, supervised by teachers to standardize administration. Participation was anonymous, and no personal identifiers were recorded. The final dataset included 338 valid responses, representing a response rate of 96.6%, which exceeds the standard threshold for social-behavioral research.

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

3.5. Data Analysis

Data analysis was performed using SPSS version 26.0. Descriptive statistics, frequencies, percentages, and mean values were used to summarize student characteristics and general awareness. Chi-square tests (χ^2) examined differences in awareness and behavior across grade levels and gender, while Pearson’s correlation coefficient (r) assessed relationships between awareness and preventive actions. The significance level was set at $p < 0.05$. The analysis addressed three research questions: (1) What is the level of students’ awareness regarding online kidnapping? (2) How do demographic factors influence awareness and behavior? and (3) What is the relationship between awareness and preventive actions? The findings revealed a strong positive correlation ($r = 0.62$, $p < 0.01$) between awareness and safe behaviors, affirming the theoretical assumption that cognitive understanding drives preventive actions.

3.6. Validity and Reliability

To ensure methodological rigor, the study employed several validation strategies. Content validity was verified by expert review, while construct validity was supported through exploratory factor analysis, identifying two principal dimensions, awareness and behavior, explaining 68% of total variance. The reliability coefficient ($\alpha = 0.84$) further confirmed internal consistency across items. Statistical assumptions of normality, linearity, and homoscedasticity were tested and satisfied, ensuring robustness for correlation analysis. These procedures strengthened the validity and reproducibility of the study’s results.

3.7. Ethical Considerations

Ethical integrity was strictly observed following the ethical research guidelines of the Vietnam Ministry of Education and Training (MOET, 2024) and the American Psychological Association (APA, 2020). Participation was entirely voluntary, with no academic incentives or coercion. Each respondent was informed about the research objectives, data confidentiality, and their right to withdraw at any time. The study collected no personal identifiers and stored all data in encrypted, password-protected files. After completion, summarized findings were shared with the school to inform the design of digital safety education initiatives.

In sum, the study’s methodological design provided a robust and transparent framework for understanding the intersection between adolescent cognition, behavior, and digital safety. The integration of quantitative rigor, ethical compliance, and theoretical grounding ensured that the findings not only reflect empirical reality but also contribute to the growing discourse on evidence-based digital citizenship education. This methodological approach laid a solid foundation for the subsequent Results and Discussion sections, where the empirical data are interpreted to inform practical educational strategies, most notably the development of the “360° Digital Shield” model for sustainable online safety education in Vietnamese schools.

4. RESULTS AND DISCUSSION

4.1. Overview of Findings

The survey results provide a comprehensive overview of Vietnamese high school students’ awareness and preventive behaviors regarding online kidnapping. The findings reveal both encouraging progress and significant cognitive and behavioral gaps. Among 338 respondents, only 25% fully understood the concept of online kidnapping, while 53% had “heard about it” and 22% had “never encountered the term.” Despite the widespread use of the Internet—over 78% of students spending more than three hours online daily awareness of sophisticated online risks such as sextortion, catfishing, or coercive challenges remained limited.

Statistical analysis confirmed significant inter-grade differences ($\chi^2 = 12.43$, $p < 0.05$). Grade 12 students demonstrated higher awareness, likely due to age, digital exposure, and cognitive maturity. However, the overall awareness level across all grades was modest, indicating a lack of structured digital safety education within the school environment.

4.2. Behavioral Responses to Online Threats

When confronted with hypothetical online risks, students demonstrated partial competence and inconsistent protective behavior. When receiving a fake message from an impersonator requesting money, 53% stated they would verify identity via phone or video call, 27% would demand further proof, and 17% would block the contact. However, a concerning 3% admitted they would transfer money immediately, indicating lingering vulnerability to deception. Although most students recognized suspicious digital cues, their reluctance to report incidents or seek adult assistance revealed emotional barriers to action. Qualitative comments showed that many felt embarrassed or afraid of being blamed for online mistakes, reflecting low self-efficacy and fear of social judgment. This aligns with Ajzen’s (1991) Theory of Planned Behavior, suggesting that perceived behavioral control influences whether awareness translates into practice.

Gender patterns also emerged: female students tended to verify or block suspicious users, while males were more likely to “test” interactions, reflecting differing perceptions of risk. Additionally, peer influence shaped decision-making, as students often sought validation from friends before acting. These patterns highlight a persistent awareness–action gap (Livingstone & Haddon, 2009). Students understand online risks but lack confidence, experience, and institutional support to respond effectively. Addressing this requires experiential, peer-driven safety education that reinforces both knowledge and emotional resilience, empowering students to transform awareness into consistent, autonomous digital safety behaviors.

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

4.3. Educational Exposure and Preferences

The study also examined students' exposure to and preferences for online safety education, revealing both progress and gaps in implementation. A majority (63.4%) of respondents had participated in at least one digital safety session at school, though most described these as brief, one-time lectures. Only 26.3% reported receiving regular instruction or follow-up activities, while 10.3% indicated they had never been exposed to any form of structured online safety education. This inconsistency reflects the absence of a systematic, curriculum-based framework for digital safety within Vietnamese secondary schools. When asked about preferred learning formats, students showed a clear inclination toward interactive and participatory approaches. The most favored methods included workshops (24.9%), video-based modules (24.4%), online competitions (21.6%), and student clubs (19.8%). In qualitative feedback, many emphasized the appeal of “learning by doing,” particularly through multimedia projects, role-play activities, and peer mentoring programs. These findings confirm that traditional lecture-style instruction, often characterized by passive information transfer is no longer effective for “digital natives,” who thrive in dynamic, experiential learning environments. This preference aligns closely with Kolb's Experiential Learning Model (1984), which proposes that deep learning occurs through a continuous cycle of concrete experience, reflection, conceptualization, and experimentation. By engaging students in real-life scenarios and collaborative problem solving, schools can transform abstract safety concepts into practical digital habits. Therefore, integrating experience-based, media-supported, and peer-driven pedagogies is essential to strengthen both cognitive understanding and behavioral resilience. Such reforms would not only enhance the sustainability of online safety education but also promote digital citizenship as a core competency in 21st-century learning.

4.4. Correlation Between Awareness and Behavior

A key quantitative finding of this study is the strong and statistically significant positive correlation between students' awareness of online kidnapping and their preventive behaviors ($r = 0.62$, $p < 0.01$). This result demonstrates that students who possessed higher cognitive understanding of deceptive online tactics such as impersonation, sextortion, and data manipulation were also more likely to adopt cautious and self-protective actions. Specifically, these students reported a higher tendency to verify the sender's identity, refuse suspicious requests, and avoid disclosing personal information in online environments. The correlation indicates that awareness functions not only as a predictor but also as a behavioral catalyst, reinforcing the premise that digital safety is fundamentally a learned and practiced competence rather than a passive state of knowledge. This empirical relationship provides strong support for Ajzen's (1991) Theory of Planned Behavior (TPB), which posits that individuals' attitudes and perceived control over a situation directly influence their behavioral intentions and actions. In this context, students with greater awareness likely develop a stronger sense of perceived behavioral control, enabling them to act decisively when encountering online threats. In line with this theoretical framework, the findings highlight that knowledge enhancement is instrumental rather than merely informative, an essential cognitive foundation for shaping safe digital habits and moral responsibility in online interactions.

However, the data also reveal an important structural limitation: awareness alone does not guarantee consistent behavioral practice. Even among students with high awareness levels, occasional lapses in judgment such as delayed reporting or continued risky interactions suggest the presence of low self-efficacy and insufficient environmental reinforcement. This phenomenon echoes the “intention - behavior gap” observed in digital safety studies (Livingstone & Haddon, 2009), where students intellectually understand risks but fail to act upon them under emotional pressure or peer influence. The results therefore underscore the need for integrated educational interventions that bridge cognition and practice. Digital safety programs must move beyond knowledge dissemination toward behavioral training and psychosocial empowerment. This involves scenario-based exercises, peer collaboration, and simulated risk management activities that encourage reflective decision-making. Furthermore, institutional reinforcement through teacher modeling, consistent messaging, and reward systems can help translate awareness into habitual safe behavior. By combining cognitive understanding, experiential learning, and emotional resilience, schools can cultivate a culture of proactive digital citizenship where awareness consistently manifests as responsible online action.

4.5. Interpretation and Theoretical Alignment

The findings of this study align strongly with global research emphasizing the complex interplay between cognitive awareness, behavioral execution, and psychosocial factors in digital safety education. The positive correlation between awareness and preventive behavior confirms that knowledge serves as the foundation for digital self-protection, but also reveals that cognition alone is insufficient for consistent behavioral application. This echoes Ajzen's (1991) Theory of Planned Behavior (TPB), which posits that human action is guided by three determinants: attitude toward the behavior, subjective norms, and perceived behavioral control. Within this framework, students' understanding of online risks shapes their intentions to act safely, but whether those intentions translate into real behavior depends heavily on their self-efficacy and perceived social expectations.

The data suggest that Vietnamese high school students often recognize the risks of online manipulation yet hesitate to respond assertively due to fear of judgment or uncertainty about institutional support. This phenomenon demonstrates limited perceived behavioral control, a key constraint in Ajzen's model. Without confidence in their ability to manage or report online threats, students remain vulnerable even when cognitively aware. Consequently, effective digital safety education must not only increase awareness

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

but also strengthen self-efficacy and create supportive environments that empower students to act. Kolb’s (1984) Experiential Learning Model (ELM) provides additional insight into this behavior–awareness dynamic. According to ELM, sustainable behavioral change occurs through a cyclical process of concrete experience, reflective observation, abstract conceptualization, and active experimentation. Applying this model to digital safety education implies that students must go beyond theoretical learning to actively experience, analyze, and reflect upon simulated online scenarios. When students engage in activities such as role-playing, case analysis, and peer-led discussions, they internalize protective behaviors more deeply, bridging the gap between cognition and action.

Furthermore, these interpretations resonate with prior studies (Livingstone & Haddon, 2009; Byrne et al., 2016), which found that participatory, experience-based learning fosters stronger retention of safety practices than traditional instruction. The theoretical alignment between TPB and ELM thus underscores a dual imperative for education: enhance knowledge to inform intention and foster experience to enable execution. Together, they frame digital safety as both a cognitive and behavioral competency, rooted in understanding but realized through action. In summary, the interplay between these theories illustrates that effective online safety education must target the whole learner: the mind (awareness), the heart (confidence and motivation), and the hand (practical action). Integrating these dimensions provides a theoretical and practical pathway for cultivating resilient, ethical, and empowered digital citizens.

4.6. Implications for Educational Practice

The findings of this study offer important insights for improving digital safety education in Vietnamese schools.

1) First, digital safety should be institutionalized as a core curricular component rather than an occasional event. One-off awareness sessions are insufficient to sustain behavioral change; instead, continuous integration into ICT and Civic Education subjects would ensure that all students regularly engage with online safety concepts;

2) Second, the results emphasize the need for experiential and participatory teaching methods. Digital-native learners respond better to interactive activities such as simulations, role-playing, and peer-led workshops than to traditional lectures. These approaches foster self-efficacy and align with Kolb’s Experiential Learning Model (1984), which highlights learning through action and reflection as key to internalizing behavioral change;

3) Third, the influence of peers suggests that student-led initiatives can serve as effective catalysts for promoting safe online conduct. Creating cyber safety clubs or appointing “digital ambassadors” can harness peer influence to normalize protective behaviors and support early reporting of risks;

4) Finally, teacher training and institutional support are essential to sustain this transformation. Educators need both technical knowledge and counseling skills to guide students through emotionally complex online challenges. Embedding these practices within school culture, supported by policy, parents, and communities can transform awareness into empowerment, cultivating a generation of responsible, resilient, and ethically aware digital citizens.

4.7. The “360° Digital Shield” Model: Integrating Awareness, Practice, and Sustainability

Building on the empirical findings and theoretical frameworks, this study proposes the “360° Digital Shield” model, a comprehensive educational framework designed to bridge the gap between awareness and action in adolescent digital safety. The model integrates behavioral theory, experiential pedagogy, and institutional practice to cultivate cognitive, emotional, and social resilience among students. It consists of three interrelated layers: Public Awareness, Digital Reinforcement, and Curricular Integration.

1) The Public Awareness Layer focuses on building foundational knowledge and collective consciousness. Schools can organize quarterly campaigns, workshops, and poster exhibitions using real-life case studies of online deception. These activities help normalize conversations about cyber risks and reduce stigma around reporting incidents. By embedding digital safety into school-wide events, students begin to perceive it as a shared responsibility rather than an individual issue.

2) The Digital Reinforcement Layer targets peer engagement and student agency. Through Cyber Safety Ambassador Clubs, students are trained to produce short videos, podcasts, or infographics addressing online risks. Peer-led digital content serves as a powerful medium for behavioral modeling, reflecting Bandura’s (2001) social learning principles that behavior is more effectively learned through observation and imitation. This layer enhances peer influence in a positive direction and transforms awareness into community-driven advocacy.

3) The Curricular Integration Layer embeds online safety into formal instruction, particularly within ICT and Experiential Learning subjects. Using simulations, problem-solving exercises, and reflective discussions, students practice real-world decision-making aligned with Kolb’s Experiential Learning Model (1984). Periodic assessments track behavioral improvements and sustain accountability at the institutional level.

Together, these three layers create a continuous, 360-degree cycle of learning awareness informs action, action reinforces understanding, and institutional support sustains progress. The “360° Digital Shield” model thus provides a scalable, evidence-based

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

approach to digital citizenship education, ensuring that students not only know how to stay safe online but are also empowered to advocate for a safer, more ethical digital community.

4.8. Summary and Reflection

Overall, the study reveals that while Vietnamese adolescents exhibit moderate awareness of online risks, their behavioral defenses remain fragile. The positive correlation between awareness and preventive behavior confirms the necessity of cognitive education but also highlights the limits of information-based approaches. Sustainable digital resilience requires experiential, interactive, and data-driven education that continuously engages students, teachers, and parents. By combining behavioral theory with experiential learning, the “360° Digital Shield” model provides a pragmatic pathway for schools to cultivate safe, responsible, and empowered digital citizens. These findings extend the literature on adolescent digital safety in Southeast Asia and contribute to the global discourse on evidence-based cyber education where prevention begins not with technology, but with understanding, practice, and shared responsibility.

5. CONCLUSION

This study examined high school students’ awareness and preventive behaviors toward online kidnapping, a digital phenomenon involving deception, manipulation, and coercion in online environments. The findings revealed that while most students frequently engage in digital communication, their understanding of complex online risks remains limited. Only a small proportion could accurately identify forms of online kidnapping, and many demonstrated inconsistent or hesitant responses when facing potential threats. The statistical evidence confirmed a strong relationship between awareness and preventive behavior, indicating that knowledge and understanding are key factors influencing digital safety practices. The study also highlighted the importance of developing both cognitive and emotional competencies. Students with higher confidence and practical experience were more capable of applying safe online behaviors consistently. This suggests that digital safety education should go beyond theoretical instruction to include experiential learning and psychosocial support that empowers students to act decisively when confronted with risks. To support this transformation, the proposed “360° Digital Shield” framework emphasizes a holistic approach that integrates awareness-building, peer collaboration, and experiential learning within the school environment. This model encourages continuous engagement and community participation, creating a culture of shared responsibility for online safety. In conclusion, digital safety must be positioned as a fundamental component of education in the digital era. Fostering informed, confident, and responsible online behavior among adolescents requires coordinated efforts from schools, families, and society to prepare young people for a secure and ethical digital future.

REFERENCES

- 1) Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
- 2) Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52, 1-26.
- 3) Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). *Global Kids Online Research Synthesis, 2015-2016*. UNICEF Office of Research.
- 4) Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155-159.
- 5) Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications.
- 6) Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Thousand Oaks, CA: Corwin Press.
- 7) Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Englewood Cliffs, NJ: Prentice Hall.
- 8) Lee, S. J., & Chae, Y. G. (2007). Children’s Internet use in a family context: Influence of family relationships, parental mediation, and Internet parenting style. *Computers in Human Behavior*, 66, 107-115.
- 9) Livingstone, S., Byrne, J., & Carr, J. (2016). *One in three: Internet governance and children’s rights*. Global Commission on Internet Governance Paper Series No. 22. Centre for International Governance Innovation and Chatham House.
- 10) Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final Report 2009*. London: LSE.
- 11) Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children*. London: EU Kids Online, LSE.
- 12) Mishna, F., Cook, C., Gadalla, T., Daciuk, J., & Solomon, S. (2010). Cyber bullying behaviors among middle and high school students. *American Journal of Orthopsychiatry*, 80(3), 362-374.
- 13) Ministry of Education and Training (MOET). (2024). *Circular No. 06/2024/TT-BGDDT on the Regulation of Scientific Research in Secondary Education*. Hanoi: MOET.

Online Kidnapping Awareness and Preventive Education among Vietnamese High School Students: A Quantitative Study and the “360° Digital Shield” Model

- 14) Ministry of Labour, Invalids and Social Affairs. (2023). *Safer Internet Day 2023: Sustaining a safer online world for children*. Government Portal, Hanoi.
- 15) WeProtect Global Alliance. (2023). *Global Threat Assessment 2023: Child sexual exploitation online*. London: WeProtect.
- 16) Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of Business Ethics*, 100(3), 405–417.