International Journal of Latest Research in Humanities and Social Science (IJLRHSS)
Volume 09 - Issue 08, 2026
www.ijlrhss.com || PP. 110-116

Guidelines for Enhancing Students' Cybersecurity at Nanning University

Wei Dan[1], Wichian Intarasompun[2], and Nuttamon Punchatree[3]
[1]*Educational Management and Learning Management Innovation Program*
[2]*Faculty of Education,*
[3]*Graduate School, Bansomdejchaopraya Rajabhat University*
1061, Israphap15 Road, Thonburi, Bangkok, Thailand

Abstract: The rapid development of the digital economy has brought unprecedented convenience to university students while simultaneously exposing them to escalating cybersecurity threats, such as online fraud, information leakage, and malicious attacks. This research aimed to 1) study the current level of students' cybersecurity at Nanning University, and 2) propose evidence-based guidelines for enhancing students' cybersecurity. The sample group consisted of 379 students selected by accidental random sampling from a population of 22,480 students at Nanning University, and five experts were purposively selected as key informants for structured interviews. The research instruments included a five-point Likert scale questionnaire and a structured interview guide. The questionnaire was validated by three experts with an IOC range of 0.60–1.00 and achieved a reliability coefficient of 0.85. Quantitative data were analyzed using frequency, percentage, mean, and standard deviation, while qualitative data from the interviews were analyzed using content analysis. The findings revealed that the overall level of students' cybersecurity at Nanning University was at a high level ($\bar{x}$ = 3.64, S.D. = 0.87). Among the five dimensions , Cybersecurity Behavior ranked highest ($\bar{x}$ = 3.86, S.D. = 0.82), followed by Cybersecurity Cognition ($\bar{x}$ = 3.75, S.D. = 0.85), Cybersecurity Awareness ($\bar{x}$ = 3.68, S.D. = 0.88), and Cybersecurity Literacy ($\bar{x}$ = 3.52, S.D. = 0.90), all of which were at high levels . Cybersecurity Risk Perception had the lowest mean score ($\bar{x}$ = 3.41, S.D. = 0.93) and was at a moderate level. Based on these findings and expert interviews, comprehensive enhancement guidelines were formulated across all five dimensions. These include practical training and continuous supervision for Cybersecurity Behavior; curriculum integration and online micro-courses for Cybersecurity Cognition; continuous promotion and diversified activities for Cybersecurity Awareness; case analysis and interdisciplinary learning for Cybersecurity Literacy; and real-life case analysis and risk simulation activities for Cybersecurity Risk Perception. This study provides actionable strategies for applied universities to cultivate digitally resilient graduates and offers practical references for enhancing cybersecurity education and digital governance in higher education.

Keywords: Students' cybersecurity, Cybersecurity awareness, Cybersecurity risk perception, Cybersecurity literacy, Higher education, Digital economy.

1. Introduction

With the rapid development of the digital economy, cybersecurity has become a global focus of attention. While digital technologies bring great convenience to people's lives, they also increase the risk of exposure to the dark side of the Internet (Rui et al., 2026). As of December 2025, the number of Internet users in China reached 1.067 billion, with an Internet penetration rate of 75.6% (Armas & Taherdoost, 2025). According to the Anti-Telecommunication and Internet Fraud Law of the People's Republic of China, telecommunication and Internet fraud refers to the act of defrauding public or private property through remote and non-contact methods using telecommunication and Internet technologies (Han, 2023).

University students represent a particularly significant demographic in this context. As an important force for the country's future development, college students' awareness of cybersecurity not only affects their own growth and development but also relates to the development and future of the country and the nation. The state attaches great importance to the cultivation of college students' cybersecurity awareness (Singh & Cheema, 2024). The relevant education authorities have issued the Implementation Outline for National Security Education and have repeatedly required colleges and universities to actively organize and carry out national cybersecurity publicity and education activities, aiming to enhance college students' awareness and skills in cybersecurity (Armas & Taherdoost, 2025).

Nanning University is an important applied undergraduate institution in Guangxi and one of the early pilot universities for applied technology education in China. The university offers multiple majors related to information technology and digital economy, with more than 2,000 students enrolled in these programs. Students at Nanning University generally possess strong abilities in digital technology application and innovative thinking, and they rely heavily on online platforms for learning, communication, and daily life.

However, the high frequency of Internet use also exposes students to increasing cybersecurity risks. While digital economy students demonstrate strong operational and technical skills, they often underestimate cybersecurity threats due to excessive dependence on digital tools and insufficient risk awareness (Singh & Cheema, 2024).

Enhancing college students' cybersecurity should start from the strategic overall situation of safeguarding national security, taking the issue of college students' cybersecurity as the orientation, and coordinating the basic points of technology and ideology in cyberspace (Han, 2023). This study, grounded in Cognitive Behavioral Theory and Social Learning Theory (Michaelsen & Esch, 2023), systematically investigates five core dimensions of students' cybersecurity: Cybersecurity Awareness, Cybersecurity Cognition, Cybersecurity Behavior, Cybersecurity Risk Perception, and Cybersecurity Literacy. By identifying specific weaknesses and gathering expert insights, this research aims to construct practical, multi-stakeholder enhancement guidelines tailored to the context of applied universities.

2. Research Objective

1. To study the current level of students' cybersecurity at Nanning University across five dimensions: Cybersecurity Awareness, Cybersecurity Cognition, Cybersecurity Behavior, Cybersecurity Risk Perception, and Cybersecurity Literacy.
2. To propose evidence-based guidelines for enhancing students' cybersecurity at Nanning University.

3. Research Methodology

This study adopts a mix of quantitative and qualitative methods. The questionnaire is designed to assess the level of students' cybersecurity at Nanning University across five dimensions: Cybersecurity Awareness, Cybersecurity Cognition, Cybersecurity Behavior, Cybersecurity Risk Perception, and Cybersecurity Literacy. Following the questionnaire, the study employs a structured interview to gain deeper insights into the guidelines for enhancing students' cybersecurity. The interviews are conducted with a selected group of participants, comprising five experts from Nanning University, chosen for their extensive experience and expertise in cybersecurity education, student management, and digital governance.

3.1 Population and Sample Group

This study involves a population of 22,480 students from Nanning University. A sample of 379 students was selected through accidental random sampling, utilizing Krejcie and Morgan's method (1970) for determining sample sizes. Additionally, qualitative insights were gathered through interviews with five experts from Nanning University, selected using purposive sampling based on the following criteria: at least five years of work experience in college, having extensive online teaching achievements in their field, and holding a master's degree or above. These informants were chosen to provide comprehensive guidelines for the development and optimization of students' cybersecurity enhancement.

3.2 Research instruments and Construction

The research instruments used in this study consisted of two types: a questionnaire and a structured interview guide. The questionnaire was distributed to 379 students at Nanning University. The survey was conducted online via the Wenjuanxing website (www.wenjuan.com) and disseminated through WeChat, QQ, Weibo, and other Internet software, with 379 valid responses received. Accidental random sampling ensured the representativeness of the sample. The questionnaire was designed based on the conceptual framework of students' cybersecurity and consisted of five dimensions with 24 items. It was divided into three parts: Part 1 collected personal information of respondents classified by gender and major; Part 2 contained items measuring the current level of students' cybersecurity using a five-point Likert scale; and Part 3 provided an optional section for suggestions and recommendations. The interpretation of scores followed the criteria proposed by Likert, where 4.50–5.00 indicated the highest level, 3.50–4.49 indicated a high level, 2.50–3.49 indicated a moderate level, 1.50–2.49 indicated a low level, and 1.00–1.49 indicated the lowest level. Additionally, reliability and validity tests were performed during the questionnaire design phase. The preliminary questionnaire was submitted to three experts in educational administration and related fields to evaluate its content validity using the Index of Item-Objective Congruence, with an IOC value of 0.60 or above considered acceptable. The revised questionnaire was then pilot-tested with 30 participants who were not included in the final sample, resulting in a Cronbach's Alpha coefficient of 0.85, confirming satisfactory internal consistency. The structured interview guide was designed based on the quantitative findings from Objective 1 and focused on the five dimensions of students' cybersecurity. The interview consisted of four parts: personal information of interviewees, questions and suggestions related to enhancement guidelines, review and revision according to the thesis advisor's recommendations, and the finalized guide used to conduct structured interviews with the

selected experts. The interview design featured structured yet open-ended questions, allowing respondents to elaborate on their experiences, views, and recommendations. For convenience and efficiency, the interviews were conducted either through online platforms or face-to-face, depending on the experts' availability, with the sessions recorded and transcribed for analysis.

3.3 Data Collection

The data was collected through a questionnaire survey designed based on research questions, literature review, conceptual framework, and relevant concepts pertaining to students' cybersecurity. The survey was distributed to students at Nanning University. The questionnaire was edited online via the Wenjuanxing website and distributed through various channels including WeChat, QQ, and Weibo. A total of 379 questionnaires were distributed, with 379 valid responses collected. Accidental random sampling was used to ensure a representative sample. During questionnaire design, reliability and validity tests were conducted to ensure robustness. The interview data was collected from five experts at Nanning University, selected using purposive sampling for their extensive experience and expertise in cybersecurity education, student management, and digital governance. The researcher made appointments with the selected experts and conducted individual interviews either through online platforms or face-to-face, depending on the experts' availability and convenience. The data from these interviews were meticulously transcribed and analyzed by content analysis, serving as a crucial component of the study's overall data collection process.

3.4 Data Analysis

The data analysis for this study was conducted in three distinct parts to ensure a comprehensive evaluation of both quantitative and qualitative data. In Part I, the demographic details of the respondents such as gender and major were statistically analyzed and presented as frequencies and percentages using statistical software to outline the general characteristics of the sample group. Part II involved a detailed analysis of responses to the Likert scale statements covering the five key dimensions: Cybersecurity Awareness, Cybersecurity Cognition, Cybersecurity Behavior, Cybersecurity Risk Perception, and Cybersecurity Literacy. The five-point Likert scale was utilized, with the ranges defined as: 4.50–5.00 indicating "the highest level," 3.50–4.49 as "high level," 2.50–3.49 as "moderate level," 1.50–2.49 as "low level," and 1.00–1.49 as "the least level," following the original interpretation by Likert. The analysis was performed using statistical software, and results were expressed in terms of means, standard deviations, and interpretations. Each dimension and sub-item were ranked from highest to lowest mean score to identify relative strengths and weaknesses, and the results were presented in structured tables. Part III complemented the quantitative analysis with a content analysis of the qualitative data obtained from the structured interviews. This involved an examination of the interview transcripts to identify and extract key themes, patterns, and recommendations related to improving cybersecurity awareness across the five dimensions. The interview data were analyzed to provide explanations and actionable recommendations for the identified weaknesses, and representative quotes from the interviewees were selected to illustrate the findings and provide evidence for the proposed enhancement guidelines.

3.5 Research Variable

Research variables are derived from previous literature review: 1) Cybersecurity Awareness; 2) Cybersecurity Cognition; 3) Cybersecurity Behavior; 4) Cybersecurity Risk Perception; 5) Cybersecurity Literacy. The dependent variable is the effectiveness of students' cybersecurity enhancement, which is defined as the level of students' cybersecurity competency and the perceived usability and effectiveness of the enhancement guidelines among students and experts at Nanning University regarding cybersecurity awareness and protective behaviors.

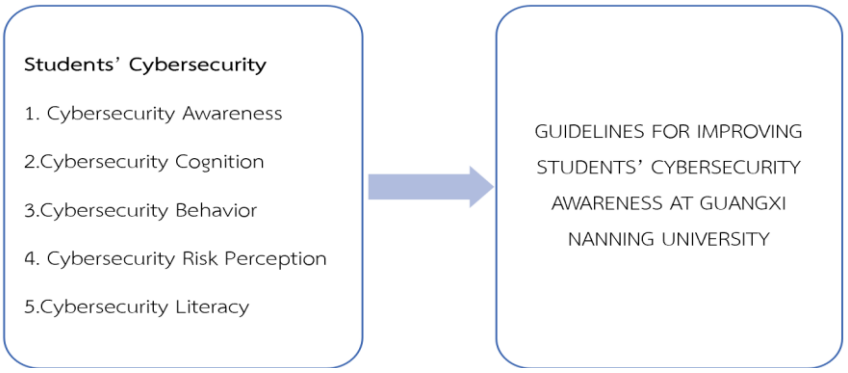

Figure 1: Research Framework

4. Research Findings

Part 1: Current Level of Students' Cybersecurity

The data on the current level of students' cybersecurity were analyzed using statistical methods by using frequency, percentage, mean, and standard deviation. Then the data was interpreted into levels and ordered into a ranking. To illustrate the current level of students' cybersecurity at Nanning University, in 5 dimensions: 1) Cybersecurity Awareness, 2) Cybersecurity Cognition, 3) Cybersecurity Behavior, 4) Cybersecurity Risk Perception, and 5) Cybersecurity Literacy. Data analysis was shown in Table 1

Table 1 The Mean ($\bar{x}$) and Standard Deviation (S.D.) the Current Level of Students' Cybersecurity Dimensions (n = 379)

Promotion Dimensions	$\bar{x}$	S.D.	Level	Ranking
1. Cybersecurity Behavior	3.86	0.82	High	1
2. Cybersecurity Cognition	3.75	0.85	High	2
3. Cybersecurity Awareness	3.68	0.88	High	3
4. Cybersecurity Literacy	3.52	0.90	High	4
5. Cybersecurity Risk Perception	3.41	0.93	Moderate	5
Total	**3.64**	**0.87**	**High**	**-**

As can be seen in Table 1, the overall mean of the level of students' cybersecurity at Nanning University is at a high level ($\bar{x}$ = 3.64, S.D. = 0.87). Among the five dimensions , the highest-ranking is "Cybersecurity Behavior" ($\bar{x}$ = 3.86, S.D. = 0.82), indicating a high level of effectiveness . This was followed by "Cybersecurity Cognition" ($\bar{x}$ = 3.75, S.D. = 0.85), "Cybersecurity Awareness" ($\bar{x}$ = 3.68, S.D. = 0.88), and "Cybersecurity Literacy" ($\bar{x}$ = 3.52, S.D. = 0.90), while "Cybersecurity Risk Perception" ($\bar{x}$ = 3.41, S.D. = 0.93) ranked fifth and was at a moderate level, indicating it is the lowest among all dimensions.

Part 2: Enhancement Guidelines

The following section presents interview analysis conducted with a diverse group of expert teachers and administrators from Nanning University. These interviews aimed to explore the various aspects of students' cybersecurity enhancement, specifically focusing on 1) Cybersecurity Awareness, 2) Cybersecurity Cognition, 3) Cybersecurity Behavior, 4) Cybersecurity Risk Perception, and 5) Cybersecurity Literacy. Showing the questions on the interview, the data were interpreted and supported by giving some examples of the interviewees.

1. The enhancement guideline for "Cybersecurity Behavior"

Experts suggested that students' cybersecurity behaviors should be improved through practical training, continuous supervision, and the development of daily security habits. The university should encourage students to participate in security behavior check-in programs involving password updates and security software installation. Campus network systems should provide security functions, including password change reminders and abnormal login alerts. Furthermore, the university can establish cybersecurity volunteer teams among students and cooperate with cybersecurity enterprises to provide practical learning opportunities.

2. The enhancement guideline for "Cybersecurity Cognition"

Experts suggested that cybersecurity cognition should be strengthened through curriculum integration and practical learning activities. The university should integrate cybersecurity knowledge into professional courses related to digital economy and financial technology, especially topics such as information reliability assessment, cybersecurity laws and regulations, and encryption principles. In addition, online micro-courses, cybersecurity knowledge competitions, and interdisciplinary seminars can provide students with continuous learning opportunities.

3. The enhancement guideline for "Cybersecurity Awareness"

Experts suggested that students' cybersecurity awareness should be strengthened through continuous promotion, diversified activities, and university-family cooperation. The university should establish regular cybersecurity promotion activities, such as cybersecurity awareness months and thematic campaigns during important periods such as enrollment and scholarship application seasons. Safety reminders can be integrated into campus digital platforms. The university can also encourage students to participate in cybersecurity volunteer activities and establish online platforms for sharing cybersecurity news and risk warnings.

5. The enhancement guideline for "Cybersecurity Literacy"

Experts suggested that students' cybersecurity literacy should be enhanced through practical application, interdisciplinary learning, and professional development opportunities. The university should provide cybersecurity case analysis courses and organize cybersecurity solution design competitions. The university can also establish peer support programs, encourage interdisciplinary cooperation, and provide internship opportunities in cybersecurity enterprises. Furthermore, incorporating cybersecurity literacy into students' comprehensive evaluation systems can encourage continuous improvement.

6. The enhancement guideline for "Cybersecurity Risk Perception"

Experts suggested that students' cybersecurity risk perception should be enhanced through practical experiences, real-life case analysis, and continuous cybersecurity education. The university should organize cybersecurity fraud case-sharing activities, risk simulation experiences, and regular risk warning campaigns. Major-specific cybersecurity education should be provided for students in digital economy-related programs, allowing them to better understand risks such as data leakage, online fraud, and platform security issues related to their professional fields.

5. Conclusion and Discussion

The enhancement of students' cybersecurity at Nanning University is discussed as follows:

1. The overall level of students' cybersecurity at Nanning University across five dimensions was at a high level ($\bar{x}$ = 3.64, S.D. = 0.87). The analysis of the five dimensions revealed the following order : Cybersecurity Behavior ranked first ($\bar{x}$ = 3.86, S.D. = 0.82) and was at a high level, followed by Cybersecurity Cognition ($\bar{x}$ = 3.75, S.D. = 0.85), Cybersecurity Awareness ($\bar{x}$ = 3.68, S.D. = 0.88), and Cybersecurity Literacy ($\bar{x}$ = 3.52, S.D. = 0.90), which were also at high levels, whereas Cybersecurity Risk Perception ranked lowest ($\bar{x}$ = 3.41, S.D. = 0.93) and was at a moderate level. This study provides valuable insights into the current status and enhancement of students' cybersecurity within the context of higher education in China. The findings align with Cognitive Behavioral Theory, which emphasizes the critical role of individuals' cognitive processes in shaping their behaviors. The high levels of cybersecurity behavior and cognition indicate that students possess foundational knowledge and practices, but the moderate level of risk perception reflects a cognitive deficit that requires targeted intervention (Singh & Cheema, 2024).

2. Based on the quantitative survey outcomes and qualitative interview views from experts, the enhancement guidelines covering each dimension of students' cybersecurity are discussed below:

2.1. For Cybersecurity Behavior, experts suggested that students' cybersecurity behaviors should be improved through practical training, continuous supervision, and the development of daily security habits. The university should encourage students to participate in security behavior check-in programs and provide security functions such as password change reminders and abnormal login alerts. This situation reflects that although students demonstrate good basic cybersecurity behaviors, their proactive use of security protection measures remains insufficient. The experts' suggestions indicate a recognized need to shift from passive knowledge acquisition to active behavioral practice. This finding is consistent with Social Learning Theory, which posits that behavior formation is reinforced through observation, feedback, and reward mechanisms (Michaelsen & Esch, 2023). The research result of Bognár and Bottyán (2024) also supports this, emphasizing that the formation of standardized behavioral habits requires continuous education and reinforcement.

2.2. For Cybersecurity Cognition, experts suggested that cybersecurity cognition should be strengthened through curriculum integration and practical learning activities. The university should integrate cybersecurity knowledge into professional courses related to digital economy and financial technology. This situation reflects that students possess basic cybersecurity knowledge but lack the ability to evaluate information reliability and apply knowledge in academic contexts. The integration of cybersecurity into professional courses reflects an important shift from fragmented education to embedded learning. This finding is consistent with Cognitive Behavioral Theory, which highlights that cognitive understanding must be developed through systematic and contextualized learning experiences (Johnco et al., 2025). This also aligns with the research of Waqas et al. (2023), who argued that knowledge cognition serves as the cognitive foundation of cybersecurity awareness.

2.3. For Cybersecurity Awareness, experts suggested that students' cybersecurity awareness should be strengthened through continuous promotion, diversified activities, and university-family cooperation. The university should establish regular cybersecurity promotion activities and integrate safety reminders into campus digital platforms. This situation reflects that students demonstrate positive awareness in daily online activities but lack continuous attention to cybersecurity information and risk

warnings. The experts' suggestions emphasize moving from one-time training to continuous engagement. This finding is consistent with Social Learning Theory, which emphasizes that awareness and behavioral norms can be effectively strengthened through role modeling, peer influence, and collaborative learning (Michaelsen & Esch, 2023). This is also supported by Ukam et al. (2024), who emphasized that continuous and structured education is essential for forming stable cybersecurity awareness.

2.4. For Cybersecurity Literacy, experts suggested that students' cybersecurity literacy should be enhanced through practical application, interdisciplinary learning, and professional development opportunities. The university should provide cybersecurity case analysis courses and organize cybersecurity solution design competitions. This situation reflects that students possess basic cybersecurity knowledge and problem-solving abilities but lack the ability to apply cybersecurity knowledge in professional contexts. The experts' suggestions highlight the need to move from theoretical knowledge to practical application. This finding is consistent with Cognitive Behavioral Theory, which emphasizes that effective performance in digital environments depends on the integration of knowledge, perception, and action into a unified capability system (Cao &Iansiti, 2022). This is also aligned with Tessema (2025), who emphasized that cybersecurity literacy represents the transition from passive awareness to active risk management.

2.5. For Cybersecurity Risk Perception, experts suggested that students' cybersecurity risk perception should be enhanced through practical experiences, real-life case analysis, and continuous cybersecurity education. The university should organize cybersecurity fraud case-sharing activities and risk simulation experiences. This situation reflects that students underestimate the potential consequences of cybersecurity risks and lack awareness of their own vulnerability. This is the most critical area of deficiency. The experts' recommendations focus on making risks more personally relevant and concrete. This finding is consistent with Cognitive Behavioral Theory, which highlights that cognitive restructuring is more effective when individuals are exposed to realistic and experiential learning situations (Johnco et al., 2025). This also aligns with Singh and Cheema (2024), who argued that students in digital economy-related fields exhibit "overconfidence bias," leading them to underestimate cyber threats. The research of Rufat et al. (2025) further supports that individuals' subjective perception of risk plays a critical role in determining whether protective actions are taken.

6. Recommendations

6.1 Recommend for Implications

1) The research indicates that Cybersecurity Risk Perception is the weakest dimension of students' cybersecurity at Nanning University. Therefore, the university should organize cybersecurity fraud case-sharing activities, risk simulation experiences, and regular risk warning campaigns to help students recognize potential threats. Major-specific cybersecurity education should be provided for students in digital economy-related programs to help them better understand risks such as data leakage, online fraud, and platform security issues.
2) The research result indicates that students' proactive use of security protection tools is insufficient. Therefore, the university should encourage students to participate in security behavior check-in programs involving password updates and security software installation. Campus network systems should provide password change reminders and abnormal login alerts, and cybersecurity volunteer teams should be established among students.
3) The finding showed that students lack the ability to evaluate the reliability of online information. As a result, the university should integrate cybersecurity knowledge into professional courses related to digital economy and financial technology, especially topics such as information reliability assessment, cybersecurity laws and regulations, and encryption principles. Online micro-courses, cybersecurity knowledge competitions, and interdisciplinary seminars should also be provided.
4) The findings suggest that students lack continuous attention to cybersecurity information and risk warnings. Therefore, the university should establish regular cybersecurity promotion activities, such as cybersecurity awareness months and thematic campaigns. Safety reminders should be integrated into campus digital platforms, and student volunteer activities and online platforms for sharing cybersecurity news should be promoted.
5) The findings suggest that students lack the ability to apply cybersecurity knowledge in professional contexts. Therefore, the university should provide cybersecurity case analysis courses and organize cybersecurity solution design competitions. Peer support programs, interdisciplinary cooperation, and internship opportunities in cybersecurity enterprises should also be established. Cybersecurity literacy should be incorporated into students' comprehensive evaluation systems.

6) The findings support that students' cybersecurity cultivation should be incorporated into the talent training system. Therefore, the university should establish a normalized education model of curriculum integration, activity immersion, and mechanism guarantee. Differentiated cybersecurity education should be carried out based on professional characteristics, and the form of education should be innovated by adopting more interactive methods such as case analysis, competitions, and practical training.

6.2 Future Research

1) Follow-up research can track the implementation effect of the enhancement guidelines proposed in this study, and observe the changes in students' cybersecurity awareness, cognition, and behaviors after relevant measures are put into practice.
2) Subsequent research can expand the sample scope to include students from different types of universities in Guangxi and across the country, conducting cross-university and cross-regional comparative studies to explore the differences in students' cybersecurity with different school-running orientations and professional backgrounds.
3) Further research can explore the internal correlations among the five dimensions using structural equation models to construct the path of action among dimensions, such as the impact of risk perception on safety behaviors and the promotion effect of cognition on literacy.
4) Mixed research methods combining quantitative data with in-depth interviews and focus group discussions can be introduced to more deeply explore the deep-seated reasons for the formation of students' cybersecurity shortcomings.
5) Researchers can further expand the research content to focus on new cybersecurity risks under the background of emerging technologies such as artificial intelligence and the metaverse, exploring their impact on students' cybersecurity and making the research more contemporary and forward-looking.

References

[1]. Al-Hashem, N., & Saidi, A. (2023). The psychological aspect of cybersecurity: understanding cyber threat perception and decision-making. International Journal of Applied Machine Learning and Computational Intelligence, 13(8), 11-22.
[2]. Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. Information, 16(5), 336.
[3]. Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. Education Sciences, 14(6), 588.
[4]. Cao, R., & Iansiti, M. (2022). Digital transformation, data architecture, and legacy systems. Journal of Digital economy, 1(1), 1-19.
[5]. Han, B. (2023). Individual frauds in China: exploring the impact and response to telecommunication network fraud and pig butchering scams University of Portsmouth Portsmouth, UK.
[6]. Johnco, C. J., Norberg, M., Wuthrich, V. M., & Rapee, R. M. (2025). Cognitive restructuring before exposure therapy or behavioral experiments? How the timing of expectancy violation and magnitude of expectancy change influence exposure therapy outcomes. Journal of consulting and clinical psychology, 93(5), 369.
[7]. Likert, R. (1932). A technique for the measurement of attitudes. archieves of psychology, 22 140, 1--55.
[8]. Michaelsen, M. M., & Esch, T. (2023). Understanding health behavior change by motivation and reward mechanisms: a review of the literature. Frontiers in Behavioral Neuroscience, 17, 1151918.
[9]. Rufat, S., Hudson, P., & Enderlin, E. (2025). Theoretical frameworks of risk perception and protective behaviour: an empirical comparison. Natural Hazards, 121(12), 14697-14767.
[10]. Singh, B., & Cheema, S. S. (2024). Psychological defenses in cyberspace: Unveiling the significance of cognitive shields in cybersecurity. International Journal of Advanced Networking and Applications, 16(1), 6291-6295.
[11]. Ukam, P. I., Onuh, P. A., Nnaji, D. I., Egbo, E. I., & Ugwu, C. O. (2024). How engagement in internet fraud impact academic activities of undergraduate students in Nigeria: A socio-legal study. Cogent Social Sciences, 10(1), 2280285.
[12]. Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. Sage Open, 13(4), 21582440231217720.