Research Article

INTERNET SECURITY LITERCY ENHANCEMENT MODEL FOR COLLEGE STUDENTS IN GUANGXI

Yifei Long[1], Sombat Teekasap[2*], Nainapas Injoungjirakit[3] Prapai Sridama[4] and Nisara Paethrangsi[5]

[1]Guangxi Vocational University of Agriculture, Nanning, China

[2, 3, 4]Bansomdejchaophaya Rajabhat University, Bangkok, Thailand

[5]Rajamangala University of Technology Thanyaburi

[*]E-mail: sombat.teekasap@gmail.com

Received: 2024-07-23

Revised: 2024-10-13

Accepted: 2024-10-30

ABSTRACT

Internet security is of great significance in modern society, but college students face many problems and challenges when using the network. As an important group of network use, the lack of Internet security awareness and the lack of education make them become the main victims of network fraud and other problems. The objectives of this study include 1) to study the current situation of the Internet security literacy of college students in Guangxi, China; 2) to build a model to improve college students' Internet security literacy; and 3) to evaluate a model to improve the Internet security literacy of college students. This study is based on the latest research results, and the research sample is college students in Guangxi and experts in the field of Internet security in universities in Guangxi. The research methods used include expert investigation, Delphi measurement experiment, and expert evaluation. A training model was designed to improve the Internet security literacy of college students, and the Delphi method was used to collect and adjust the opinions on the model. The model is applied, and the implementation effect of the model is tested through the test and after experiments, combined with the CIPP evaluation opinions of experts. Ultimately, professionals universally

acknowledge and successfully evaluate the Internet security literacy improvement strategy for college students through experiments. Through the investigation of experts in the field of Internet security, we can fully understand the current situation, existing problems, and suggestions for college students' Internet security literacy. To enhance college students' Internet security literacy and effectively advance Internet security education goals, strong assistance is required. The model for enhancing the internet security literacy of college students concentrating on five themes: psychology, ethics, knowledge, abilities, and awareness. To construct the complete training program from five perspectives: Training content, methodology, resources and tools, training time, and training evaluation improve college students' online security literacy.

Keywords: Internet security literacy; college students; promotion model construction; Guangxi universities

INTRODUCTION

Internet security is of great significance in social development. The development of society cannot be separated from the Internet. While the world is experiencing the change and prosperity driven by the Internet, it also suffers from the problems brought about by the Internet, which has caused negative effects. Computer viruses, telecom fraud, rumor spreading, illegal theft of accounts, poor product quality and services, malicious evaluation and other phenomena emerge in an endless stream, which directly affects the security of individuals, enterprises and units, organizations, and the country.

College students have many problems in the process of using the Internet. College students are an important group who use the Internet, and they are closely related to the Internet in their study and life. In recent years, due to the lack of strong awareness of Internet security, there are a lot of moral and legal problems, affecting the physical and mental health of college students. According to the "new situation of telecom network fraud management research report (2020)" data shows that more than 70% of the network fraud cases caused by the young Internet users network prevention awareness is not strong, leading in serious leakage of personal private information, and the proportion continues to rise.

The growing dependency on digital technologies and the internet has made

security education a critical need, especially in educational institutions. Despite the increasing importance of internet security, thereremains a notable gap in formal education about online security (Nguyen, 2020). The network has the characteristics of virtuality, openness, and flexibility, which brings difficulties to the Internet security education. Currently, most colleges and universities have not developed a scientific education and training model for Internet security education for college students. Additionally, existing education models often do not meet the needs of the digital age or align with the characteristics of college students. This low level of Internet security education results in slow progress in improving Internet security literacy.

It is very necessary to improve the Internet security literacy of college students (Jin & Hui, 2017). College students as the elite group of the society, college students are the new force of national development, but also the main reserve force of internet security talents, college students as an important force to promote the national economic and social development, their internet security literacy will directly affect the smooth progress of the national information development goals. Therefore, it is urgent to improve the internet security literacy of college students.

RESEARCH QUESTIONS

1. What is the current state of Internet security literacy among college students in Guangxi, China?

2. How can a model be developed to improve the Internet security literacy of college students in Guangxi?

3. How effective is the proposed model in enhancing the Internet security literacy of college students in Guangxi?

RESEARCH OBJECTIVES

1. To examine the current state of Internet security literacy among college students in Guangxi, China.

2. To develop a model aimed at enhancing the Internet security literacy of college students.

3. To evaluate the effectiveness of the proposed model in improving the Internet security literacy of college students.

LITERATURE REVIEW

Research on Internet security Literacy

Kamarulzaman et al (2022) proposed

that Internet information security literacy refers to the information security quality and ability that people have in carrying out network activities, as well as the awareness, attitude, knowledge, technology, and accomplishment of protecting their own and others' security (Ji et al, 2022) Based on existing research findings and Analytic Hierarchy Process (AHP), the network information security literacy of college students is decomposed into four principles: network information security prevention ability, network information security awareness, and network information legal ethics. Chen et al (2022) proposed in their research that the network information security literacy of college students in the perspective of platform society is the ability to face their own and others' information security when using the functions of various Internet platforms.

In terms of a comprehensive understanding of previous views, this study believes that internet security literacy refers to the comprehensive security ability formed by people in network practice activities, with "internet security awareness, internet security knowledge, internet security skills, internet security ethical standards, and internet security psychological adjustments" as the main content of internet security literacy. This study defines Internet security literacy as the comprehensive ability formed through network practice activities. It includes key components such as Internet security awareness, knowledge, skills, ethical standards, and psychological adjustments.

Research on the Current Situation of Internet Security Literacy among College Students

Que Fengyi (2022) found through investigation that the internet security literacy of college students is at a moderate level. The main problems include weak awareness of internet security, insufficient mastery of internet security knowledge and skills, lack of network learning ability, and frequent occurrence of network misconduct and violations. Yang Lu (2021) pointed out that there are problems such as adverse effects on the online environment, more dangerous behaviors on the internet, low attractiveness of online education in universities, and an inadequate internet security education system. Yao Ying (2021) through existing research and many cases, summarized those teenagers in the new era have weak Internet security awareness and increased Internet misconduct, mainly including increased Internet security

awareness and increased personal Internet security risks. The main reason is the lack of targeted educational content and a single educational form, which is the reason for insufficient educational technology support.

From the perspective of research methods, most scholars adopt the form of questionnaire surveys to study the current situation of internet security literacy among college students, using college students as samples, internet security literacy among college students as independent variables, and relevant factors as independent variables. This study will use expert survey methods to study the status of internet security literacy among college students and determine the problems and reasons for the existence of internet security literacy among college students.

Research on Models and Strategies for Improving College Students' Internet Security Literacy

Liu et al (2024) advocated for the establishment of a comprehensive Internet information security assurance system through the institutionalized and routine study of Internet information security rules and regulations. Yang Lu (2021) advocated for the continual enhancement of college students' safety literacy through the implementation of three-dimensional path innovation, content dimension innovation, and assurance dimension innovation. Yu Kun (2023) suggested that in constructing online security awareness education, it is imperative to thoroughly account for its diversity and the individualized distinctions among the learners.

Based on the above literature and other relevant research results, this study tends to focus on improving the education and teaching methods to enhance internet security literacy. By establishing a scientific and effective training program that emphasizes experiential training, it constitutes a model for enhancing the internet security literacy of college students.

Research on Evaluating and Improving the Internet Security Literacy Model of College Students

The methods that have a high proportion of evaluation and use for training models in the education field include the Kirkpatrick four level training evaluation model, the Delphi method, and so on. The Ke's Level 4 training evaluation model was developed by internationally renowned scholar Kirkpatrick (1998) proposed that it is the most widely used training evaluation tool in North America. It divides the training

effect into four progressive levels: reaction evaluation, learning evaluation, behavior evaluation, achievement evaluation, whether to evaluate, and the evaluation stage should be determined based on the importance of training (Wang Jinbo, 2012). Loop and feedback are the core of the Delphi method, which promotes the exchange of opinions among experts, encourages experts to learn from each other, inspires each other, and promotes the continuous deepening of expert understanding, thereby improving the scientific and reliability of the Delphi method (Wang Qi, 1986). Zhang et al (2022) embedded the CIPP model in the teaching evaluation system and constructed a teaching evaluation system with background input process outcome as the indicator (Chen et al, 2021)

Based on the above literature, different studies will choose different evaluation methods for how to evaluate the research model. Combining with the actual situation of this study, this article adopts the CIPP principle and selects the expert evaluation method and pre and posttest experiments to evaluate the improvement model of college students' internet security literacy. This method has stronger applicability in the field of education and training of college students' internet security literacy.

METHODOLOGY MATERIAL

Expert investigation

1. Review and analyze relevant documents, concepts, theories, and research on internet security literacy, and develop a survey questionnaire on the status of internet security literacy among college students.

2. Send the questionnaire to the thesis advisor and have 5 experts test the objective consistency index (IOC) of the questionnaire. Review and modify the content according to the suggestions.

3. Send the survey questionnaire on the status of college students' internet security literacy to 21 experts in the field of internet security, collect the questionnaire, eliminate invalid questionnaires, and organize the data. Through descriptive statistical analysis of the current situation of internet security literacy among college students, preliminary statistics are conducted on the frequency distribution, percentage, highest value, lowest value, etc. of each variable.

Delphi method

1. Based on the literature review and research objective 1, establish a training

model to enhance the internet security literacy of college students in Guangxi.

2. Using the Delphi method, solicit suggestions from 21 experts, who evaluate each strategy and choose "agree", "disagree", or "disagree". Agree = 1, disagree = -1, and uncertainty = 0. Compile expert suggestions and modify the training model to obtain Training Model 2

3. Conduct a second round of soliciting opinions from experts and compile their suggestions to develop training model 3;

4. A third round of opinion solicitation was conducted with experts, and all experts agreed. Finally, a training model was developed to enhance the internet security literacy of college students in Guangxi.

Pre - and posttest experiments

1. Conduct a pre-test on the students in the sample group and fill out the "College Student Internet Security Literacy Test Question".

2. Apply the internet security literacy model for college students, conduct experiments, and use the internet security literacy improvement model for college students to provide internet security literacy training to 35 students. Use test questions to conduct a post test on the students in the sample group.

3. Collect relevant results from pre - and posttests and organize the data and grades. Calculate the data of the highest, lowest, average, standard deviation, number of qualified individuals, and number of outstanding individuals in the pre - and post test scores and analyze them. If the post test data is higher than the pretest data, it indicates that after the implementation of training interventions, students' internet security literacy has significantly improved.

Expert verification

1. Select 5 experts to evaluate the model for improving the internet security literacy of college students.

2. Each expert evaluates the model for enhancing college students' internet security literacy around four aspects: Context, Input, Process, and Product.

3. Collect evaluation forms, organize whether experts agree and relevant opinions, and obtain evaluation results.

RESULTS

Part 1: Analysis of the Current Situation of Internet Security Literacy among College Students in Guangxi

1. College students have awareness of internet security. There are multiple

problems, among which the most prominent is the lack of awareness of regularly backing up information materials, with the highest agreement rate reaching 90.48%. This reflects that most college students have not developed the habit of regularly backing up information materials, which increases the risk of data loss and information security. The question with the lowest numerical value is "college students do not attach importance to the protection of personal online identity information", with a consent rate of 61.9%, which is relatively low among the four questions. This indicates that some college students can recognize the importance of protecting personal online identity information.

2. Regarding the acquisition and mastery of internet security expertise. A significant number of college students, when confronted with internet security concerns, lack the knowledge to adequately safeguard their rights, hence heightening the risk of further violations. For college students, the enthusiasm for actively learning and understanding internet security knowledge is not strong, and the approval rate is also as high as 95.24%. This reflects the lack of enthusiasm among college students in actively learning and understanding internet security knowledge, which may limit their effectiveness in mastering internet security knowledge. The lowest agreement rate among college students regarding the lack of understanding of basic knowledge such as the concept of internet security indicates that a small number of college students have some basic knowledge about internet security.

There are still certain deficiencies in the ability to prevent and respond to internet security risks. Especially in terms of improving firewall configuration and usage skills, configuring, and using antivirus software, and preventing network and telecommunications fraud, the problems are more serious. The three issues are particularly prominent, and the agreement rate of "not paying attention to the security of the electronic payment environment" is relatively the lowest compared to other issues, indicating that college students have a certain strengthening of their understanding of electronic payment security, but still need to pay more attention to the security of the online payment environment.

4. There are problems with the ability of college students to regulate and maintain internet security ethics. Especially regarding the issue of "the sense of responsibility

of college students in maintaining internet security needs to be improved", all experts agree, with the highest approval rate of 100%, indicating that college students lack a sense of responsibility in maintaining internet security and need to be further strengthened. Regarding the issue of "college students engaging in unverified dissemination or forwarding of false information", a consent rate of 80.95% was found, which is relatively low compared to other issues. This reflects that some college students do not verify whether information is false when publishing and forwarding, while a small number of college students are able to make necessary verifications and judgments about online information.

5. There are still shortcomings in cultivating and cultivating the ability of online psychological security among college students. 100% of the respondents agree with the issue that college students may experience psychological problems due to internet security incidents such as online violence and fraud. This indicates that internet security incidents do have a negative impact on the psychology of college students and reflects that the frequency of internet security incidents among college students may be higher. The consent rate of college students who lack the ability to self-regulate and intervene when encountering internet security psychological problems and the ability to seek professional counseling and assistance when encountering internet security psychological problems is relatively low, but it also reaches 90.48%, indicating that most college students lack effective coping strategies and seeking help when facing network psychologicalproblems.

In summary, the expert survey method has been used to draw the following conclusions: the overall internet security literacy of college students in Guangxi still has problems such as weak awareness of internet security, lack of understanding of basic knowledge of internet security, incomplete mastery of internet security response skills, insufficient sense of responsibility for maintaining internet security, and insufficient psychological adjustment ability for dealing with internet security. The overall level is below average and needs further improvement.

Part 2: Collect opinions through the Delphi method and obtain the model after three rounds of solicitation. Results of expert opinions on the first round of Delphi method:

In terms of training content, 17 experts chose to agree, with an average value of 0.90, close to 1, indicating that most people agreed with the design of the training content, with a mode of 1, further confirming the majority's recognition of this content. The IQR (interquartile range) is 0, indicating that the data distribution is relatively concentrated and there is no significant dispersion. In terms of training methods, 15 experts agreed, and 6 experts disagreed, with an average value of 0.43, indicating some differences in training methods. The mode is 1, indicating that although there are different opinions, there are still relatively more people who tend to agree with this training method. The IQR is 2, indicating a large degree of dispersion in the selection of training methods; In terms of training materials and tools, 15 experts agreed, 1 expert chose to be uncertain, and 5 experts chose not to agree. It is suggested to add some small games related to internet security to increase the fun of training and student participation. The average value is 0.48, indicating a certain degree of disagreement in training methods. The mode is 1, indicating that although there are different opinions, there are still relatively more people who tend to agree with this training method. The IQR is 1, indicating a certain degree of dispersion; In terms of training time, all 21 experts agree that the average value is 1 and the mode is 1, further confirming this point. The IQR is 0 and the data distribution is very concentrated. In terms of training evaluation, 20 experts agree, while 1 expert is uncertain, with a value of 0.95, close to 1, indicating that most people fully agree. The mode is 1, the IQR is 0, and the data distribution is very concentrated.

In summary, after the first round of expert opinion collection, all experts agreed on the training content, training time, and training evaluation. In terms of training methods, training materials, and tools, experts had different opinions and put forward suggestions. The comprehensive opinions include adding scenario simulation experience in the training methods section and adding game resources related to internet security in the training materials and tools.

Expert opinion results of the second round of Delphi method:

In terms of training content, training time, and training evaluation, all 21 experts agreed, with an average value of 1.00 and a mode of 1, further confirming this point. The IQR is 0, the data distribution

is very concentrated, and opinions are highly consistent. In terms of training methods, 20 experts agreed, and 1 expert disagreed. It is recommended to increase the training method of psychological group counseling, with an average value of 0.90, close to 1, indicating that most people strongly agree. The mode is 1, indicating that most people agree. The IQR is 0, and the data distribution is very concentrated with highly consistent opinions. In terms of training materials and tools, 18 experts agreed, 2 experts disagreed, and 1 expert was uncertain. It is recommended to add an online learning app platform to facilitate students to learn and review online at any time, and to add props for psychological group counseling to make training activities more attractive. The average value is 0.76 and the mode is 1, indicating a certain degree of disagreement, but the majority still agree. The IQR is 0, and the data distribution is relatively concentrated, but there is still a certain degree of dispersion.

In summary, after the second round of expert opinion collection, all experts agreed on the training content, training time, and training evaluation. In terms of training methods, training materials, and tools, experts had different opinions and put forward suggestions. The comprehensive opinions include adding psychological group counseling training methods in the training methods and adding online learning platform "Xuetong" APP and group counseling props in the training materials and tools.

Expert opinion results of the third round of Delphi method:

21 experts agreed on the training content, training methods, training materials and tools, training time, and training evaluation. The average value is 1.00 and the mode is 1, further confirming this point. The IQR is 0, the data distribution is very concentrated, and opinions are highly consistent.

In summary, after soliciting opinions from experts in the first two rounds, the training model was adjusted twice. Through the third round of Delphi expert recommendations, all experts agreed on all aspects of the model, and the final Guangxi university student internet security literacy improvement model was determined.

Part 3: Implementation and Evaluation of the Internet Security Literacy Model Results for Guangxi University Students

Step 1: 28 students from a single

cohort of Big Data Enterprise Management at Guangxi Agricultural Vocational and Technical University were chosen for training. Administered a pre-test prior to the initiation of five training subjects and a post-test after each training session. After the training session was completed, a thorough examination was administered. The precise score data were as follows:

their performance, and at least no students have scored below 70. In the average score section: the pretest average score was 73, the posttest average score was 84, and the posttest average score was higher than the pretest, indicating a significant improvement in overall student performance. In terms of standard deviation: the pretest standard deviation is 10.8, and the posttest

Table 1 Analysis of Student Pre- and Post-Test Scores

(n = 28)

	highest score	lowest score	average score	standard deviation	qualified number (above 70 points)	excellent number (above 90 points)
Pre-Test	90	50	73	10.8	17	1
Post Test	95	70	84	8.4	28	12

From the analysis in Table 1, in the highest score section: the highest score in the pretest was 90, and the highest score in the post test was 95. The highest score in the post test was higher than that in the pretest, indicating a significant improvement in student performance in the post test. In the lowest score section: the lowest score in the pretest is 50, the lowest score in the post test is 70, and the lowest score in the post test is higher than that in the pretest, indicating that all students have improved

standard deviation is 8.4. The standard deviation measures the degree of data dispersion, while the posttest standard deviation is smaller than the pretest, indicating that the score distribution of students in the post test is more concentrated, that is, their performance is more consistent. In terms of the number of qualified students (above 70 points): the number of qualified students in the pretest was 17, and the number of qualified students in the post test was 28. The number of qualified students

in the post test was higher than that in the pretest, indicating that more students met the qualification criteria in the post test. In terms of the number of outstanding students (above 90 points): the number of outstanding students in the pretest was 1, and the number of outstanding students in the post test was 12. The number of outstanding students in the post test significantly increased compared to the pretest, indicating that more students achieved excellent results in the post test.

In summary, the overall performance of high school students in the post test has significantly improved, with not only an increase in average scores and the number of qualified students, but also a significant increase in the number of outstanding students. At the same time, the distribution of students' scores has become more concentrated. This means that the introduction of the training mode in this study has had a positive impact on the improvement of students' internet security literacy.

Step 2, invite experts to evaluate the model. Invite 5 experts with over 15 years of work experience to use expert evaluation methods to evaluate the CIPP of the model.

Table 2 Expert Evaluation Results

(n=5)

	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
C- Context Evaluation	✓	✓	✓	✓	✓
I- Input Evaluation	✓	✓	✓	✓	✓
P- Process Evaluation	✓	✓	✓	✓	✓
P- Product Evaluation	✓	✓	✓	✓	✓

Five experts gave positive feedback on all aspects of CIPP evaluation, indicating that the model is considered effective and appropriate in terms of background, input, process, and product. This is very positive feedback, indicating that the design and implementation of the model have been recognized by experts.

Part 3: Introduction to internet security Literacy Enhancement Model

The model for improving the internet security literacy of college students is divided into two parts. The first part is based on literature review and research status, focusing on five themes: awareness, knowledge, skills, ethics, and psychology. The first step is to enhance awareness, the second step is to improve knowledge, the third step is to improve skills, the fourth step is to improve psychological aspects, and the fifth step is to participate in moral aspects, setting up training programs around the above sequence. The second part of the model is the key part, designing the entire training from five aspects: training content, training methods, training materials and tools, training time, and training evaluation. The above two aspects comprehensively constitute an improvement model for enhancing the internet security literacy of college students.

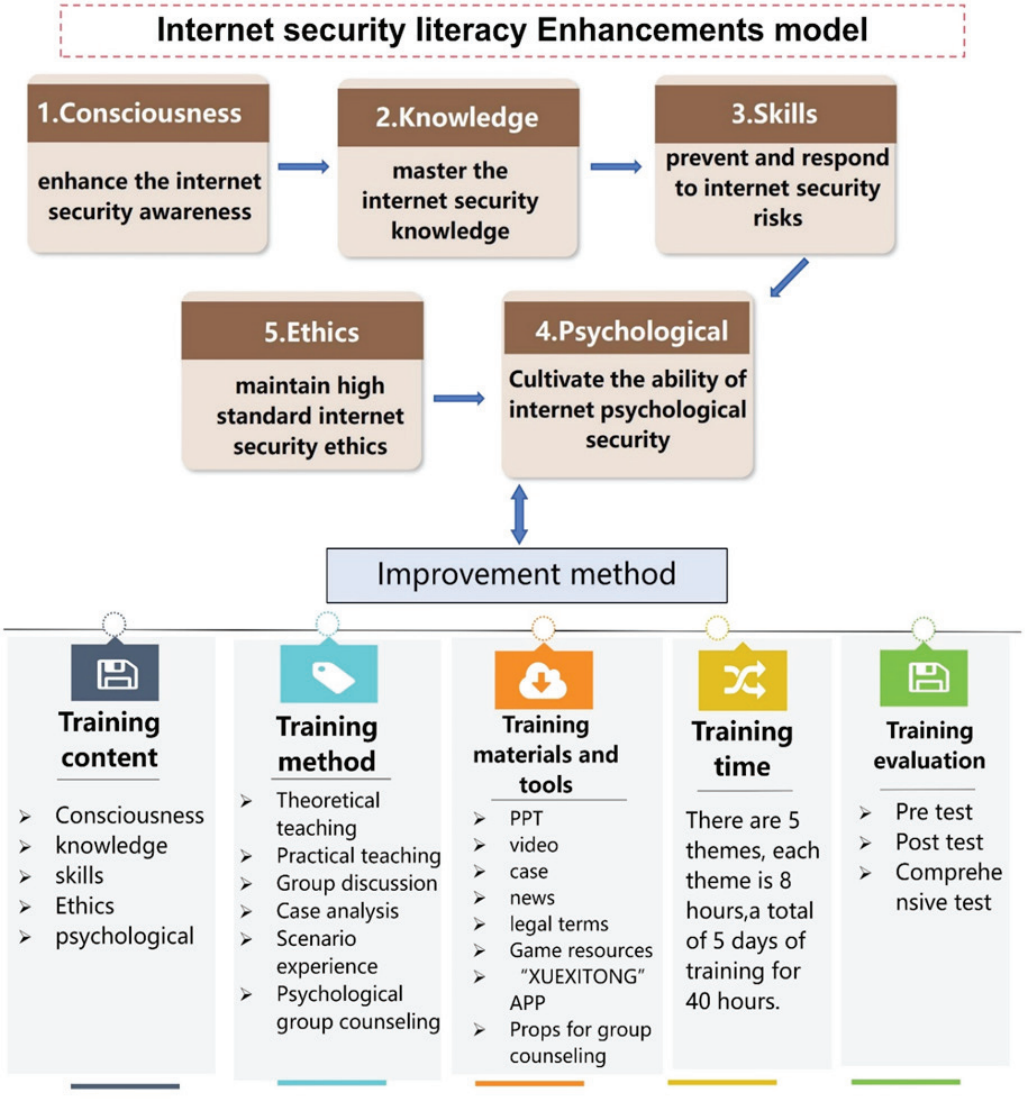

Figure 1 Internet security literacy enhancements model

CONCLUSION

The weak awareness of internet security literacy among college students in Guangxi is a significant concern, given the increasing reliance on digital platforms for academic, social, and personal activities. Many students exhibit limited understanding of the risks associated with online behaviors, such as sharing personal information, using weak passwords, or failing to recognize phishing attempts. This lack of awareness leaves them vulnerable to cyberattacks, identity theft, and privacy breaches. Factors contributing to this weakness

include inadequate formal education on cybersecurity, limited exposure to real-world cyber threats, and a general perception that such risks are minimal or distant. As internet usage continues to grow, this gap in security literacy presents a critical challenge that requires immediate attention through targeted educational initiatives and awareness campaigns. Without a stronger focus on building internet security literacy, students in Guangxi may continue to face significant cybersecurity risks in their academic and personal lives.

Insufficient training on improving the internet security literacy of college students. The coverage of training content is insufficient. Establish a systematic and scientific training model suitable for college students to enhance their internet security literacy.

A training model centering on five dimensions of Internet security literacy has been established, which combines online and offline training, and has been verified by experts in the field. It can better improve the Internet security literacy of college students.

Discussion

The study of college students' internet security literacy employs literature review and expert survey methodologies to scientifically identify the characteristics and deficiencies in their internet security knowledge, thereby facilitating the development of targeted enhancement strategies. To enhance the online security literacy of college students in the study's objective 2, the Delphi method is employed to gather expert opinions over three rounds, thereby facilitating a more scientific collection of recommendations and refining the training model for more accuracy and rationality.

The emphasis on a multi-dimensional approach to internet security literacy is in accordance with the results of other studies that underscore the intricacy of cybersecurity education. Chen et al (2020) emphasized the necessity of addressing both cognitive and behavioral dimensions of cybersecurity in educational contexts, asserting that security encompasses not just technological concerns but also psychological and social elements. The integration of psychology and ethics in the proposed model corresponds with these findings, acknowledging that students must cultivate not only technical competencies but also the capacity to discern deceptive strategies and comprehend the ethical ramifications of their online conduct. This idea aligns with O'Brien,

McMahon, and Kelleher (2020) who suggested that a hands-on, skills-based approach is crucial for effective cybersecurity education, which is reflected in the proposed training program's focus on practical abilities, such as handling encryption and securing communications. Awareness of the ever-evolving nature of cyber threats is a critical factor in maintaining long-term security practices among students (Zhang, 2021)

SUGGESTIONS AND RECOMMENDATIONS

The teaching content and methods should keep up with the times. Today's society is undergoing rapid changes and testing still needs constant adjustment. The teaching content should be continuously adjusted according to the updates of internet security knowledge. The teaching methods will continue to be adjusted over time. In the teaching process, to achieve better teaching results, teaching methods will be continuously adjusted according to the teaching time.

Strengthen the construction of internet security teaching personnel and improve the quality of training. Experts with rich Internet security practices and teaching experience are selected as trainers to ensure the accuracy and practicality of the training content.

Strengthen cooperation with society. Network telecommunication companies and Internet security companies have more advantages in technology and prevention experience but lack a platform for communication and joint training with universities. Internet security technical experts and legal experts can be invited to the school for training to introduce cutting-edge Internet security protection knowledge and technology and enrich teaching resources.

REFFERENCES

Chen Qi, Xiong H, Dai Q & Gu J. (2022). Research on the evaluation and promotion strategy of college students' internet information security literacy ability under the platform society. **Library and Information work, 7,** 75-87.

Chen, Y. T., Shih, W. L., Lee, C. H., Wu, P. L., & Tsai, C. Y. (2021). Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan. **Computers & Education, 164**, 104131.

Chen, X., Zou, D., Cheng, G., & Xie, H. (2020). Detecting latent topics and trends in educational technologies over four decades using structural topic modeling: A retrospective of all volumes of Computers & Education. **Computers & Education, 151**, 103855.

Gao D, CAI H, Dong L, Shen X & Xu W. (2013). Design of students' internet information security literacy evaluation scale. **Chinese Medical Education Technology (02),** 173-177.

Gao G, Zhang L & Wang T. (2021). Construction of the online teaching quality evaluation index system based on the Delphi method. **Chinese Journal of Multimedia and internet Teaching, 01,** 32-34

Huang H & Wei M. (2018). Analysis on the application of easy class platform in the safety education of higher vocational colleges. **Liaoning Teachers' College (Natural Science edition) 04**, 61-63.

Ji, W., Wang, R., Tian, Y., & Wang, X. (2022). An attention based dual learning approach for video captioning. **Applied Soft Computing, 117,** 108332.

Jin, W., & Hui, Z. (2017, December). Embedding Information Security Literacy in College Education. In 2017 **International Conference on Social science, Education and Humanities Research** (ICSEHR 2017) (pp. 48-51). Atlantis Press.

Kamarulzaman, M. S., Shuhidan, S. M., & Wahid, K. A. (2022, September). The Moderating Role of Information Security Behaviour (ISB) on the Relationship between Digital Literacy (DL) and Information Security Culture (ISC): A Proposed Research Framework. **In Proceedings 82**(1), 35, MDPI.

Kirkpatrick, D.L. (1998). The Four Levels of Evaluation. In: Brown, S.M., Seidner, C.J. (eds) Evaluating Corporate Training: Models and Issues. **Evaluation in Education and Human Services, 46**. Springer, Dordrecht. https://doi.org/10.1007/978-94-011-4850-4_5

Luo Y. (2016). Research status and trend of internet literacy of college students in China Visual map analysis based on common word analysis method. **Modern Education Management 10,** 118-123.

Li R, Pan L, Hao J, Zhang H, Luo L & Wu Q. (2020). High accuracy of internet security awareness of individual assessment and group index construction method. **Journal of Beijing Institute of Technology, 09,** 1002-1008.

Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. **Humanities and Social Sciences Communications, 10**(1), 1-18.

Liu, J., Feng, X., Liu, J., & Yamaka, W. (2024). Digital Economy and Industrial Structure Transformation: Mechanisms for High-Quality Development in China's Agriculture and Rural Areas. **Agriculture, 14**(10), 1769.

Nguyen, C. T., Saputra, Y. M., Van Huynh, N., Nguyen, N. T., Khoa, T. V., Tuan, B. M., & Ottersten, B. (2020). A comprehensive survey of enabling and emerging technologies for social distancing—**Part I: Fundamentals and enabling technologies. IEEE Access, 8,** 153479-153507.

O'Brien, N. 2020. State of Mind Ireland: the design and evaluation of a positive mental health intervention among higher education students. **PhD Thesis**, University College.

Qiu Y. (2022). Discussion on the internet security awareness education of college students. **Technology Vision,34**, 42-46.

Qing, Y. & Kun, Y. (2023) Knowledge Sharing Behavior of Team Members in Blended Team-Based Learning: Moderating of Team Learning Ability. **The Asia-Pacific Education Researcher 33**(5), 1251-1263.

Wang J. (2019). Research on cultivating college students' self-management ability training in the Era of we-media. **Education modernization, 29**, 237-238.

Yu, Q., Yu, K., Li, B., & Wang, Q. (2023). Effectiveness of blended learning on students' learning performance: a meta-analysis. **Journal of Research on Technology in Education**, 1-22. https://doi.org/10.1080/15391523.2023.2264984