INTERNET SECURITY LITERACY ENHANCEMENTS MODEL FOR COLLEGE STUDENT IN GUANGXI

LONG YIFEI

A thesis submitted in partial fulfillment of the requirements for
the Degree of Doctor of Philosophy Program in
Digital Technology Management for Education
Academic Year 2024

Thesis Title Internet Security Literacy Enhancements Model for College Student in Guangxi

Author Mrs.Long Yifei

Thesis Committee

..... Chairperson
(Associate Professor Dr. Sombat Teekasap)

..... Committee
(Dr.Nainapas Injoungjirakit)

..... Committee
(Assistant Professor Dr. Prapai Sridama)

Accepted by Bansomdejchaopraya Rajabhat University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Digital Technology Management for Education

..... Dean of Graduate School
(Assistant Professor Dr. Nukul Sarawong)

..... President
(Assistant Professor Dr. Kanakorn Sawangcharoen)

Defense Committee

..... Chairperson
(Professor Dr.Apichart Pattaratuma)

..... Committee
(Associate Professor Dr.Supawat Lawanwisut)

..... Committee
(Associate Professor Dr.Duang-arthit Srimoon)

Thesis	**Internet security literacy enhancements model for college student in Guangxi**
Author	**Long Yifei**
Program	**Digital Technology Management for Education**
Major Advisor	**Associate Professor Dr.Sombat Teekasap**
Co-advisor	**Dr.Nainapas Injoungjirakit**
Co-advisor	**Assistant Professor Dr.Prapai Sridama**
Academic Year	**2024**

ABSTRACT

Internet security is of great significance in modern society, but college students face many problems and challenges when using the internet. As an important group of internet users, their lack of awareness of internet security and inadequate education have made them the main victims of issues such as online fraud. The objectives of this study include: 1) to investigate the current situation of internet security literacy among college students in Guangxi, China; 2) to construct a model to enhance the internet security literacy of college students; and 3) to evaluate the model to enhance the internet security literacy of college students. This study is based on the latest research results, with a sample of college students and experts in the field of internet security in Guangxi universities. The research methods used include expert investigation, Delphi pre - and post test experiments, and expert evaluation.

The research results found that:

Firstly, conduct a survey of experts in the field of internet security to fully understand the current situation, existing problems, and suggestions of college students' internet security literacy are generally at a lower than average level and require further improvement.

Secondly, design a training model that revolves around five dimensions of internet security literacy, combines online and offline to enhance the internet security

literacy of college students, and use the Delphi method to solicit opinions and adjust the model.

Thirdly, Apply the model and verify its implementation effectiveness through pre - and post testing experiments, combined with expert CIPP evaluation opinions. The model for improving the score of internet security literacy test of college students, which has been unanimously recognized by experts and successfully evaluated through experiments.

This study provides strong support for improving the internet security literacy of college students and promoting the smooth achievement of internet security education goals.

Keywords: Internet Security Literacy, College Student, Improve Model Construction, Guangxi Universities

Acknowledgements

As this doctoral dissertation is about to be completed, I would like to express my deep gratitude. The completion of this doctoral dissertation is not only the result of my personal perseverance and hard work, but also the result of everyone's help, care and support.

First of all, I would like to express my sincere gratitude to my major advisor, Associate Professor Dr.Sombat Teekasap, and two Co-advisor, Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama. Your outstanding academic achievements, rigorous academic attitude and selfless dedication have always been my role models for academic pursuits. From topic selection, research design, data collection to the writing and revision of the thesis, you have given me meticulous guidance and help, gradually helping me find my own direction on the academic road and constantly break through myself in the research process.

Secondly, I would like to thank my dearest classmates and family. In a foreign country, in countless days and nights of struggle, we encouraged each other, made progress together, and spent many unforgettable times. Your company has made my doctoral life more colorful and made me no longer lonely on the road of scientific research.

At the same time, I would like to especially thank the experts and scholars who participated in the research of my doctoral dissertation. Thanks to Bansomdejchaopraya Rajabhat University. Bansomdejchaopraya Rajabhat University has provided me with a good academic environment and resources. During my time at school, I have listened to many wonderful courses from teachers and participated in a variety of academic activities, which have given me the opportunity to contact cutting-edge academic research and outstanding scholars, which have greatly enriched my experience.

Once again, I would like to express my most sincere thanks to all those who have given me help and support! In the future, I will continue to uphold a rigorous and realistic scientific attitude and make unremitting efforts to achieve more results in the academic field, give back to society, and live up to everyone's expectations.

Long Yifei

Contents

Contents (Continued)

List of Figures

List of Tables

List of Tables (Continued)

Chapter 1
Introduction

Rationale

Internet security is of great significance in social development. The development of society cannot be separated from the Internet. While the world is experiencing Internet driven changes and achieving prosperity, it is also suffering from problems caused by the Internet, which has caused negative impacts. Computer viruses, online fraud, spread of online rumors, illegal theft of internet accounts, poor quality and service of e-commerce products, malicious online evaluations and other phenomena continue to emerge, which directly affect the security of individuals, enterprises, units, organizations, and countries.

There are many problems for college students when using the internet. College students are an important group who use the internet and are closely related to it in their studies and daily lives. In recent years, due to the weak awareness of Internet security among college students, there have been many moral and legal issues, which have affected their physical and mental health. According to the "Research Report on the Governance of Telecom Internet Fraud under the New Situation (2020)", more than 70% of internet fraud cases are currently caused by young netizens' weak awareness of internet prevention, leading to serious leakage of personal confidential information, and this proportion is continuously increasing.

There is a certain degree of deficiency in internet security education. The internet has characteristics such as virtuality, openness, and flexibility, which bring difficulties to internet security education. Most universities currently do not have a scientific education and training model for college students' Internet security education, or the education methods are not suitable for the needs of the internet era and the characteristics of college students. The low level of Internet security education has led to slow progress in improving Internet security literacy.

It is necessary to enhance the internet security literacy of college students. As an elite group in society, college students are the driving force for national development and the main reserve force for Internet security talents. As an important force in promoting national economic and social development, their Internet security literacy will directly affect the smooth progress of national information development goals. Therefore, it is urgent to improve the internet security literacy of college students.

Research Question

How to improve the Internet security literacy enhancements for college students in Guangxi ?

Objectives

1. To study the current situation of improve the Internet security literacy enhancements for college students in Guangxi.

2. To design a model of improve the Internet security literacy enhancements for college students in Guangxi.

3. To evaluate the internet security literacy enhancements model for college student in Guangxi.

Scope of the Research

Population, Samples, and Variables

For objective 1, in the research on the current status of college students' Internet security literacy:

Population

300 experts in the field of internet security in Guangxi universities.

Sample group

21 experts with over 10 years of work experience in the field of internet security in Guangxi universities.

The five selected universities are representative universities of different levels and cities in Guangxi, including Guangxi Minzu University, Guangxi University of

Finance and Economics, Guangxi Vocational University Of Agriculture, Guangxi Vocational and Technical College, and Guangxi Polytechnic of Construction.

Variable

Independent variable: the internet security literacy of college students.

Dependent variables: By reviewing the relevant literature of this study, the characteristics mentioned in the internet security of college students were counted, and the five aspects of awareness, knowledge, skills, morality and psychology were selected as the variables of this study.

1. Have awareness of internet security; (Emphasize internet security and have awareness of preventing internet security)

2. Ability to master internet security knowledge; (mastery of internet knowledge and relevant laws and regulations)

3. Ability to prevent and respond to internet security risks; (protection of personal privacy, public internet connection habits, installation of protection software, etc.)

4. Standardize the moral behavior ability of internet security; (standardize internet messages and messages, infringement of internet intellectual property rights, and non-standard browsing of websites)

5. Establish the ability of internet psychological security. (Prevent Internet dependence addiction and dealing with Internet risk shocks).

For objective 2, design a model to enhance college students' Internet security literacy:

Population:

Experts in the field of internet security in Guangxi universities.

Sample group

21 experts with over 10 years of work experience in the field of internet security in Guangxi universities.

The following conditions are required: 1) Have a certain understanding and research in the field of Internet security literacy among college students; 2) More than 10 years of work experience in the field of education; 3) A manager with a deputy senior professional title or above.

For objective 3, in the study of evaluating and improving the internet security literacy model of college students:

Population:

1. College students in Guangxi

2. Experts in the field of Internet security in Guangxi

Sample:

1. Select 28 students from Class 1 of Big Data Enterprise Management as experimental samples for pre - and post test experiments.

2. Based on the actual situation of internet security literacy among college students in Guangxi, 5 experts were selected to evaluate the model for improving the internet security literacy of college students.

Research content

This article draws on and references the research results on internet security literacy at home and abroad, analyzes the current situation of internet security literacy among college students in Guangxi, China, and constructs a model to enhance college students' internet security literacy from multiple dimensions, thereby evaluating the model to enhance college students' internet security literacy.

Time

The time scope of this study is from June 2023 to June 2024

Geographic scope

The field category of this study is college students in Guangxi, China.

Advantages

1. Investigation and sorting out the current situation of college students' internet security awareness, knowledge, skills and morality, which can find out the problems of the internet security literacy of college students and analyze the causes.

2. Through the deconstruction and analysis of college students ' internet security literacy, and based on relevant theoretical research, scientific, complete and appropriate evaluation indicators are selected to build a generally applicable evaluation index system of college students' internet security literacy.

3. Provide data support for the education administrative departments to master the internet security awareness of college students and the internet security behavior of college students. Combined with the evaluation results, on the basis of the present situation and the analysis of specific ideas and targeted countermeasures, not only can make the government and education department more practical grasp the current status of college students' internet security literacy, for colleges and universities to carry out students in the internet security education, the government regulation and national related system also has certain reference significance.

Definition of Terms

Literacy

This study defines literacy as the basic ability of an individual to unleash their potential, learn, understand, and apply knowledge, skills, and attitudes, achieve their desired goals, and make correct value judgments and choices through interpersonal communication and interaction, in order to adapt to social life. It includes three levels: cognition, emotion, and skills.

Internet security

In this study, it mainly refers to the ability to take necessary measures to prevent attacks, intrusion, interference, destruction, illegal use, and accidents on the internet, maintain stable and reliable operation of the internet, and ensure the integrity, confidentiality, and availability of internet data. An internet system is not threatened or infringed upon, and can achieve resource sharing function normally.

Internet literacy

In this study, it refers to the ability to use computer and internet resources to locate, organize, understand, evaluate, and analyze information. Internet literacy is a comprehensive manifestation of internet related abilities, ranging from being proficient in basic internet tools such as search engines and email, to being able to classify, organize, and compare internet information, and then participating in internet co construction.

Internet security literacy

The ability to safely and reasonably utilize computer and internet resources to locate, organize, understand, evaluate, and analyze information. This study believes that Internet security literacy is divided into 5 parts, including awareness, the ability to master Internet security knowledge, the ability to prevent and respond to Internet security risks, the ability to regulate ethical behavior in Internet security, and the ability to establish Internet security psychology.

Ability to master internet security knowledge

In this study, it refers to the level of mastery of internet security common sense and knowledge of internet security related laws and regulations.

Ability to prevent and respond to internet security risks

In this study, it refers to the ability to respond to internet security issues, whether personal privacy can be protected on the internet, whether public internet connection habits are good, and whether protective software is installed in place.

Standardize the ethical behavior ability of internet security

In this study, it refers to the ability to have a strong awareness of internet security, consciously regulate one's words and actions on the internet, and abide by morality. Such as whether online messages and messages are standardized, whether there are violations of online intellectual property rights, and whether there are non-standard website browsing behaviors.

Establishing the ability to ensure internet psychological security

In this study, it refers to the ability to scientifically and reasonably avoid excessive dependence on the internet during daily internet use, maintain a healthy psychological state after internet security issues occur, respond to internet danger shocks, and adjust mindset in a timely manner.

Research Framework

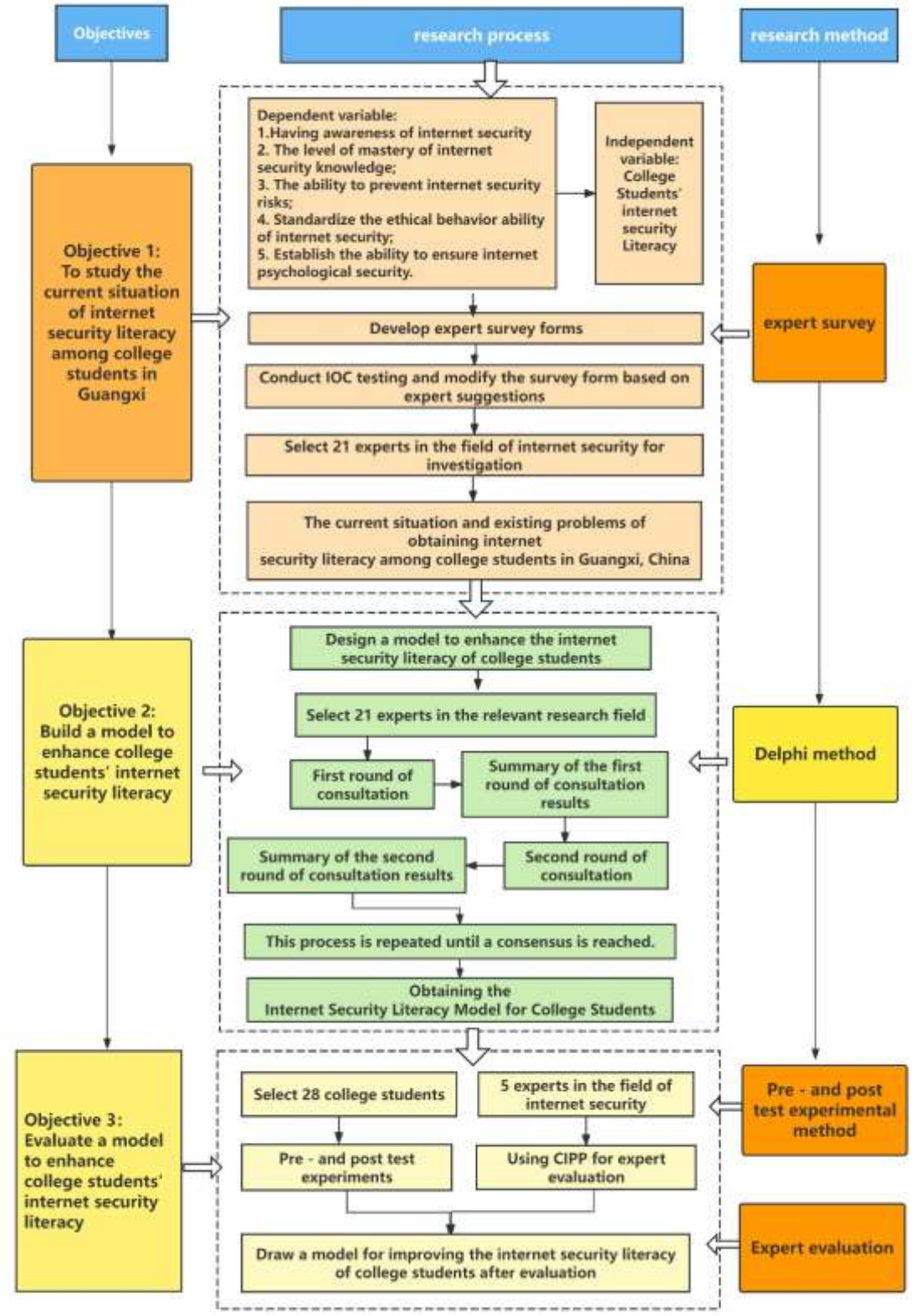

Figure 1.1 Research Framework

Chapter 2

Literature Review

This chapter will focus on the research objectives proposed in Chapter 1, summarize the main theoretical basis and relevant researchers of this study, and clarify the theoretical inheritance, improvement, and expansion relationship between this study and existing achievements. In order to study the theoretical basis of college students' internet literacy, this chapter elaborates on the following theories:

1. Internet Literacy
2. Internet Security Literacy
3. Current Situation of College Students' Internet Security Literacy
4. Models and Strategies for Improving College Students' Internet Security Literacy
5. Evaluating and Improving the Internet Security Literacy Model of College Students

Internet Literacy

The concept of internet literacy is constantly evolving along with the birth and development of Internet technology. In the early days of the development of the Internet, the Internet was known as the Web 1.0 era, and the internet was regarded as a tool to obtain information. People mainly obtained information and collect information in cyberspace, and the publication and acquisition of information was a one-way operation, and there was no real-time interaction between content publishers and users. Mc Clure (1994) In this period, the concept of internet literacy was put forward for the first time. He believed that internet literacy consists of two aspects, namely, knowledge and skills. Netizens should have certain internet knowledge, and can have certain internet use skills and technology. Some studies have also expanded the content of these two parts. Savolainen R (2002.) proposed that the level of internet literacy is reflected from the four main fields of "knowledge of available information resources on the Internet, skilled use of ICT tools to obtain

information, judging the relevance of information and communication". Have research more emphasis on the judgment and processing, internet literacy requires people can not only from complex information internet found, obtain and use effective information content, also requires people to critically process internet information, through the evaluation of information utility, filter out low quality, invalid information, Bu Wei in (2002) put forward the above points in the study.

With the progress of internet technology and the further development of the concept of "interconnection" in the internet, people have entered the Web 2.0 era. The internet is not only used as a means to obtain information, but also has become a new platform for human communication, and its social attributes are gradually prominent. This period of the use of the internet from a single access to information, into the information transmission between users, transfer mode from a single linear into mesh chain, information exponential growth, good and evil people mixed, good and bad are intermingled huge amounts of information to the Internet virtual and immediacy let the internet public opinion, internet violence gradually revealed. At the same time, the academic focus on internet literacy has also shifted from the perspective of skill use to the study of internet sociality. American scholar Art Silverblatt enriched the meaning of "internet literacy", and divides the internet literacy into seven levels: first, can determine their own internet consumption; second, have a better understanding of the basic principles of internet communication; third, is able to recognize the impact of the internet on individuals and society; fourth, has the ability to analyze internet information strategy; fifth, is good at interpreting internet information text and internet media culture; sixth, can well understand and appreciate the content of internet information; seventh, provide responsible and effective media information to the object of internet interaction. On the basis of the full study and analysis of the internet for human learning, knowledge dissemination, the interaction between people, and the construction of a lifelong learning system, Howard Rheingold (2012) summarizes the five aspects of internet literacy, namely, attention, garbage recognition, participation, collaboration, and intelligent internet people. As for garbage identification, he emphasized the retrieval ability of information retrieval, the process, the process of establishing personal

retrieval mechanism, the process of questioning information, and the process of verifying authenticity have improved people's information retrieval ability from multiple dimensions. In terms of intelligent internet people, he emphasizes the application of internet functions. He believes that the social internets supported by online internets have the structure of the general internet, but also have the characteristics of the human internet, and people have unique advantages and can quickly adapt to such a structure. Geng Yiqun Ruan Yan (2013) detailed analysis combed the 2000 to 2012 in the journal paper data research on internet literacy, during this period many scholars put forward the relevant definition is summarized, and selected 14 of the representative research results in-depth analysis, finally summarizes the evolution of internet literacy connotation is a dynamic process, with the continuous development of internet technology and the internet popularity, its concept connotation, the study of internet literacy in terms of discipline and coverage and local at the same time. The research finally suggests that internet literacy refers to people's ability to obtain specific information on the internet according to the current needs of themselves and social development, process, evaluate, use and create to help individuals solve related problems and improve the quality of human life.

After the birth and popularization of mobile Internet technology, people have entered the Web 3.0 era, and the development of the Internet presents two new trends.1. No longer limited by the time and space of the traditional PC terminal, people are online 24 hours a day (always online), and perceive the "acceleration" of the world, the relative "narrowing" of the world concept and the relative "amplification" of the world.2. The integration of people, time and space, mobile Internet makes mobile phone into a carrier of user identity, and people's social identity is simplified to a internet address. However, the intelligent and accurate identification of people by internet addresses cannot completely replace the social relations carried by the social identity in the past. Therefore, literacy education solely from the technical level can no longer meet the requirements of today's citizens living in cyberspace. In this period, the expansion of individual desire and the overall inclusiveness of the society are increasing; the simplification of the emergence of

social problems, and the phenomenon of "information cocoon", "enclosure" and "cultural barriers" brought the polarization of emotional perception. Yu Guoming (2017) There are several obvious expression orientations in the connotation of internet literacy. —— Internet literacy is a relatively independent concept category based on media literacy, digital literacy, information literacy, etc., plus social interaction, interactivity, openness and other internet characteristics. He analyzed the connotation of the internet literacy, combing the research of scholars on the above three concepts, finally from cognitive (internet contact habits to attention management), concept (value emotional orientation to critical thinking), behavior (from internet media involved in cooperation) three dimensions, formed the "cognitive —— concept —— behavior" evolution logic, to guide citizens' personal internet literacy. Ye Dingjian (2017) based on the basis of practice, in the study of the core internet literacy, five college students is: a high degree of internet security consciousness is the core, strong level of internet technology is the foundation, strict law-abiding self-discipline habit is the key, noble internet moral sentiment is fundamental, lead everyone to participate in the construction of the internet ability is the guarantee. Wang Weijun, Wang Wei, Hao Xinxiu (2020) Detailed the definition of internet literacy by Chinese and foreign scholars since 1994, and drew the Time Evolution of the Concept of Internet Literacy, which clearly presents the development and change process of this concept. On this basis, we propose that internet literacy is the comprehensive ability of internet survival and development, Is the ability to use the internet environment correctly, adapt well, develop healthily and explore the innovation, Refers to the comprehensive quality of individual internet survival and development, Mainly includes: (1) internet knowledge, It is the component of cognitive internet environment and application internet ability; (2) Dialectical thinking, That is to criticize and reflect on the dialectical treatment of internet information and the relationship between people and internet; (3) Self-management, That is, the restraint of self-behavior and avoid internet harm; (4) Self-development, That is, the application of a good internet to develop self-awareness and ability of components; (5) Social interaction, That is, the components of the interaction influence between

individuals and the internet society, It includes creation and rich information, ethics, and interaction with others.

Summary:

According to the existing analysis of achievements, there is still room for further research on internet literacy: (1) There is relatively little research on individual internet security literacy, and current research mostly focuses on functional and communication perspectives, mainly analyzing efficient use of the internet and dissemination of information. However, as a special space, individuals are already fully immersed in online activities, and their internet security issues are becoming increasingly prominent. (2) There is relatively little research on the psychological status of individuals in the internet. Whether from the perspective of skill enhancement or improving communication efficiency, the discussion focuses on the process of interaction between individuals and the outside world. However, in the process of individual participation in online activities, there is not only an output process, but also a psychological adjustment process such as regulating one's own negative emotions, which is worth further research.

Based on the comprehensive understanding of the above viewpoints, the author believes that internet literacy refers to a comprehensive and stable ability formed by people through online practical activities, with "internet thinking ability, internet knowledge and skills, learning and development ability, social interaction ability, legal and moral ability, and security protection ability" as the main content, which simultaneously affects society and oneself.

Internet Security Literacy

As an important part of the overall concept of internet literacy, internet security literacy has also experienced the continuous enrichment and development of its connotation under the influence of the development of internet technology from Web 1.0 to Web 3.0 technology. However, the replacement of technology is not the main clue of the development of the concept of complete internet security literacy. The author tries to sort out the existing research situation from the scope of the concept of internet security literacy determined by Chinese and foreign scholars.

Some scholars believe that the concept of internet security literacy should closely follow the definition of internet literacy, and analyze the concept of security around the internet environment or field. Sun Liutao (2015) in the study of internet information security literacy refers to the people in internet activities of the quality and ability, information security is college students through computer and new media tools to carry out the process of internet behavior, has the safety of protecting themselves and others of consciousness, attitude, knowledge, technology, and accomplishment, including safety awareness, safety knowledge and skills, safety legal literacy and safety moral accomplishment, its connotation range stick to the definition of information literacy. In the perspective of social engineering analyzes the importance of the information security perspective, and put forward the good information security literacy is an important basis of information security management, the basic information security literacy is an effective means to resist internet security attacks, have a certain information security literacy is the basic requirement of members of the information society, Liu Feng (2010) The definition of internet security literacy comes from the concept of internet literacy, which refers to the internet information security literacy of people, is a part of the overall literacy of personnel, and is also one of the basic abilities of members of modern society to adapt to the work under the condition of information technology.

From the perspective of individuals, some scholars, in defining the concept of internet security literacy, put more emphasis on individual factors such as self-restraint, compliance with ethics and laws, and risk avoidance, so that this concept can be further used in the research of small, small samples or case analysis. For example, internet security literacy refers to the ability of college students to identify internet risks and protect their own security, specifically refers to the security awareness in the internet society and the ability to properly deal with relevant problems; at the same time, they have the awareness of avoiding risks and consciously stay away from internet activities that may infringe their privacy and property, which is Yang Mi and Zeng Dejin (2021) Definition of internet security literacy proposed in the monograph. Wang Ruili (2022, p.85-87), combined with the existing research results and hierarchical analysis method (Analytic Hierarchy Process, AHP)

divides the target layer (college students' internet information security literacy) into internet information security prevention ability, internet information security awareness, internet information security knowledge and internet information legal ethics four criterion layers, On the basis of the criterion layer, "can use commonly used internet security tools for analysis and defense", "understand the importance of internet security to campus and personal information" and "understand the traditional and the latest internet security threats" and other 25 specific indicators.

With the deepening of the study on internet security literacy, Chinese and foreign researchers are not satisfied with the definition of definition, the connotation of the latest research trends, more detailed internet security literacy standards, scale, system has become the mainstream research, these studies for the definition of internet literacy is more rich, perfect, form a complete system. Luo Li (2012) in the study of national information security literacy refers to the information, internet environment, the national understanding of information security, and information security of various comprehensive ability, including information security consciousness, information security knowledge, information ethics and information security ability such as specific content, and established the national information security literacy evaluation index system. The index system to information security consciousness, information security knowledge, information legal ethics, information security ability four elements as criterion layer, refine the on the basis of criterion layer "understand the important role of information security in the information society", "understand various viruses, Trojan hazards and the latest information security threats" 17 specific indicators. Gao Donghuai, Cai Hua, Dong Lipeng (2013) Referring to the evaluation indicators of domestic scholars on internet security literacy, information security literacy and information literacy, For example, the Student Internet Information Security Literacy Evaluation Program (Trial), Luo Li The National Information Security Literacy Evaluation Index System proposed, Gu Huaning, The Evaluation Standards for College Students' Information Literacy proposed by Zhang Xia, Fang Qun Research on information security in the elements of information literacy of military students in master's thesis and the Information Literacy Standards of Undergraduate Students in Military Colleges in Wang Yingying's thesis, At the same

time, combined with the actual situation of the students, And consulting 10 experts in related fields (3 information security, 3 computer internet terminal, 2 library and information science, 2 education technology), The students' internet information security literacy standards is divided into four dimensions: information security awareness, information security knowledge, information security skills and information security ethics, On this basis, the detailed "I think internet information security is more and more important to our study, scientific research, life, work", "I can correctly set windows, WiFi, office, E-mail and other passwords to prevent information theft" and other 28 specific problems. Chen Qi, Xiong Huixiang, Dai Qinquan (2022) in the research platform of college students' internet information security literacy refers to the people life and production practice gradually platform environment, college students in the use of all kinds of Internet platform function in the face of themselves and others information security consciousness, knowledge, ability, legal ethics and moral ability. Combined with the existing research and practice foundation, they try to build the platform of social threshold college students internet information security literacy evaluation index system, the system contains internet information security consciousness, internet information security knowledge, internet information security skills, internet information security legal and moral five level indicators, and refinement has been clear about the 32 secondary indicators.

Summary:

Based on the above literature and other relevant research results, there is still a lack of research on some issues. (1) There is relatively little research on online violence. At present, incidents of online violence have become common in the internet society, and some iconic forms of online violence have caused serious adverse consequences to the parties involved, even losing their lives. However, there is still a lack of results in the existing research on internet security literacy that incorporate factors of cyber violence into evaluation indicators and systems, which is not conducive to our research on how to respond to cyber violence and further improve the internet security literacy system. (2) There is relatively little research on the processing ability after encountering internet security incidents. At present, there is a lot of attention paid to the ability to prevent internet security in existing research

results. However, research on the ability of individuals to respond, handle, recover losses, and self-regulate after encountering internet security time is not sufficient. There are few results that consider relevant factors in the evaluation system of internet security literacy constructed by many scholars.

Table 2.1 Comprehensive results of internet security literacy research

Author **Internet security literacy**	Internet Security Awareness	Internet Security Skills	Internet Security Knowledge	Internet Security Responsibility and Ethics	Internet Security Risk Prevention Ability	Internet Security Legal Literacy	Internet Security Psychology
Sun Liutao (2015)	√	√	√	√		√	
Liu Feng (2010)	√	√	√				√
Yang Mi, Zeng Dejin (2021)	√	√	√	√	√		
Wang Ruili (2022)	√	√	√		√	√	
Luo Li (2012)	√	√	√	√		√	√
Gao Donghuai, Cai Hua, Dong Lipeng(2013)	√	√	√	√			√
Chen Qi, Xiong Huixiang, Dai Qinquan (2022)	√	√	√	√	√	√	
Wang Guangli (2020)	√	√	√	√			√
Que Fengyi (2022)	√	√	√	√			√
Wang Rui (2020)		√	√	√			
Yang Lu (2021)	√	√	√	√			
	10	**11**	**11**	**9**	**3**	**4**	**5**

Based on a comprehensive understanding of previous views, the author believes that Internet security literacy refers to the comprehensive ability that people develop in online practice activities, with "Internet security awareness, Internet security skills, Internet security laws and regulations, Internet security psychological debugging, and self-protection ability" as the main content, and continuously possess in the process of using online and offline activities.

Current Situation of Internet Security Literacy of College Students

From the perspective of research methods, most scholars take the form of questionnaire survey to study the current situation of college students 'internet security literacy, taking college students as samples, college students' internet security literacy as independent variables, and combining with related factors as independent variables. Que Fengyi (2022) Through the investigation, the internet security literacy of college students is at a medium level, and the main problems include the lack of strong awareness of internet security, the lack of internet security knowledge and skills, the lack of internet learning ability, internet misconduct and internet violations. Through analysis and research, it is found that the particularity of college students' age stage and the lack of attention to internet security problems, the universities have not formed a standardized long-term internet security education mechanism and the more severe internet security situation in the era of big data are the reasons for the results. Yang Lu (2021) Through the questionnaire survey, it is found that the internet security literacy of college students is at a medium level. The main problems of internet security include the construction of internet security environment, the basic awareness of internet security, the implementation of internet security education, and the guarantee of internet security regulations. The existing problems include the adverse influence of internet environment, many dangerous internet behaviors, the low attraction of internet education in colleges and universities, and the imperfection of internet security education system. The main causes are 1. Multiple challenges in education environment; 2. Students lack of safety awareness, lack of safety awareness and high dependence on internet; 3. Poor education content and methods, insufficient education content, insufficient theory

and practice, and single education mode, inadequate need to strengthen teachers, insufficient supervision, lack of communication and interaction with families.

For the main problems and reasons of college students' internet security literacy, relevant studies are as follows: Qiu Yueyan (2010) Students become the most vulnerable group to internet security risks, especially college students who have just left their parents and live independently as the main victims. From the perspective of classification, the security risks of college students mainly consof the following situations: first, the disclosure of personal information in the process of Internet access; second, various internet fraud, material and spiritual losses; third, the lack of security awareness of using internet equipment, resulting in the disclosure of sensitive information. Liu Feng (2010) proposed that there are many missing phenomena in information security literacy of college students, such as poor internet security awareness and relatively weak ability to resist bad information erosion, resulting in continuous campus internet crimes; little knowledge of information security, difficult to distinguish the truth of information, easy to violate the internet information security regulations; weak of information ethics and easy to be deceived. Wang Jianhui, Zhang Bei (2016) College students' awareness of information security needs to be improved. Although more and more people use the Internet and we media for communication, entertainment and learning, they mainly focus on how to get information from the Internet and less consider how to protect their own information in the internet environment. Talk that many students will publish their real materials on the Internet, encountered QQ password will be stolen, login password is too simple and other phenomena. College students 'information security knowledge and operation ability remains to be strengthened, although because of news propaganda, classroom education factors such as firewall, virus, but more complete internet information security management and prevention knowledge, some students won't install operating system, the configuration firewall, don't know need to regularly upgrade virus prevention and control products, don't know how to better configure their own computer, also did not master the basic skills to protect their own information security. Wang Rui (2020) from seven aspects proposed the youth group problems existing in the internet security consciousness, respectively is

the internet security consciousness cognitive overall insufficiency, internet physical and mental health security consciousness is weak, internet privacy security consciousness, internet privacy security consciousness is not strong, lack of legal security consciousness, internet property protection security consciousness, shortage of internet security application consciousness, internet education penetration is not high. It is believed that personal factors, social environment, law and system, internet technology and educational factors will affect the internet security awareness of youth groups. Wang Guangli (2020, p) contemporary college students 'internet security consciousness cultivation more fruitful, but at present, college students' internet security consciousness, family education operation co., LTD., low level of social resources utilization problem, and analyze the cause of the existing problems for college cultivation and management is not perfect, college students' own consciousness, family education and peer mutual assistance, internet environment management is not perfect. Yao Ying (2021) through the existing research and a large number of cases summarizes the existing problems of the new era youth internet security education, mainly internet security consciousness, internet anomie behavior increased, personal internet security risk increased three aspects, and the main education subject value degree is not high, education object internet security consciousness is not strong, the lack of education content, education form single, education technology support is not enough..59

Summary:

Based on the above literature and other relevant research results, most domestic and foreign scholars use questionnaire surveys and interviews to conduct research on the current situation of college students' internet security literacy. The research on the current situation of college students' internet security literacy is relatively sufficient, and based on different theoretical foundations and research methods of different disciplines, many problems and deficiencies in the current internet security literacy of college students have been proposed, such as a lack of overall awareness of internet security, weak awareness of internet security physical and mental health and safety Weak awareness of internet privacy and security, weak awareness of internet privacy and security, lack of awareness of internet legal

security, insufficient awareness of internet property protection and security, lack of awareness of internet security applications, and low popularity of internet education. In response to internet security issues that have a significant impact on individuals such as internet fraud and privacy information leakage, it is necessary to focus on researching and proposing educational guidance measures to help college students cope with the challenges of internet security.

This study will also adopt a structured interview method to study the current situation of college students' internet security literacy. By interviewing teachers in charge of internet security in universities, the problems and causes of college students' internet security literacy will be identified.

Modes and Strategies to Improve College Students' Internet Security Literacy

Through the construction of the internet security system to improve the internet security literacy model. From the content and organization of information security awareness education, the improvement of information security literacy and building a complete internet information security guarantee system. Liu Feng (2010, p.88) that all college students must understand their most basic security responsibility, understand the information security threats faced by the campus internet, with good internet use habits to defend the campus internet risk and protect the information system. He proposed to use the advanced internet security technology to strengthen the information internet system, constantly formulate and improve the internet security management system, internet information security laws, regulations learning institutionalization, daily and other ways to build a complete internet information security system. Sun Liutao (2015) It is proposed to continuously improve the safety literacy of college students through implementation dimension innovation, content dimension innovation and guarantee dimension innovation. The implementation dimension emphasizes the strengthening of internet culture monitoring, the practical education of internet information security knowledge and skills, and the guidance of internet information security awareness; the content dimension emphasizes the cultivation of internet information security literacy, which

fits the campus culture and integrates into the contents of these campus culture; the guarantee dimension emphasizes the strengthening of system construction, hardware and software guarantee, and talent team guarantee.

By highlighting the core tasks of the subject. In his research, he proposed that in maintaining cyber security, in addition to strengthening security technology, teenagers should also be placed in an important position to maintain cyber security. Chen Gang zhu (2018) It is proposed that the main body of the use of the internet is people, and the maintenance of internet security should start from the young people and strengthen education. Internet security education can enable people to have a deeper understanding of internet security, have a stronger security awareness, improve the sense of social responsibility, and more effectively maintain internet security. But he also points out that either way, only makes the Internet relatively safe. He proposed that the internet security construction should be strengthened from the technical level and the institutional level. At the technical level, a protective wall needs to be built to filter out harmful and threatening information as much as possible to maintain internet security and provide a clean and healthy online environment for teenagers. At the institutional level, we should establish a system and mechanism of the state, society, families, schools and individuals, cultivate their internet security literacy at various levels, and help them use the Internet more happily and safely. At the individual level, he emphasized that teenagers should master the internet knowledge and skills, improve the identification ability, enhance the self-management ability and strengthen the self-discipline, observe the internet ethics and laws and regulations, and enhance the self-protection ability. With the cultivation path of college students' internet security consciousness as the core, Wang Guangli (2020) from the cultivation of internet security consciousness subject, cultivating object, cultivating body and cultivating platform four dimensions put forward contains strengthening internet security consciousness cultivating main body leading role, activate the internet security consciousness cultivating object initiative, rich internet security consciousness cultivating body, optimize the internet security consciousness cultivation platform construction of complete cultivation strategy. In order to gradually enhance the internet security

awareness of college students to ensure a good learning and growth environment for college students. Wang Rui (2020) proposed to improve the awareness of internet security, such as self-protection awareness and internet morality awareness; purify internet security environment continuously; improve the laws and regulations related to internet security to apply the current Internet security requirements, promote the popularization and application of internet security technology, and develop the high-level information security technology, antivirus software technology; strengthen internet security education, and take effective measures to enhance the internet security awareness of youth groups, so as to ensure the security of the internet environment of the whole society.

Establish the promotion mode through multi-party linkage. Dai Tiantian (2020) Measures to improve youth internet security literacy from three aspects of school, family and society. School education should attach great importance to cultivating teenagers internet literacy, in the internet security cognitive level stimulate students' learning interest and confidence, and according to the adolescent physical and mental growth rules and periodic characteristics of the Internet, construct the integration of internet literacy education system, school education to both technology education and literacy education, in the classroom more practical case illustrate specific measures, let students have relevant knowledge and practical ability. besides, The compilation of online literacy education materials should expand the knowledge of online sexual harassment, online bullying and bullying, online privacy protection and other aspects, Try to engage students in "cyber risk", Truly understand and understand the internet security; Parents' guidance to teenagers will become an important backing for cyber security assurance, Families should become the "second classroom" to cultivate teenagers' cyber security literacy, Parents should also reasonably guide their children to surf the Internet at home, Be the first "teacher" of internet literacy cultivation; besides, To ensure the internet security environment for teenagers, we need to improve the social legislation at the level of internet governance, Actively give full play to the guiding role of professional media, Form a media education system of social resources. Yao Ying (2021, p.41) Put forward the basic path of optimizing the youth internet security education in the new era, The

first is to strengthen the importance of education subjects to the internet security concept education, Form the educational force of school, family and society; The second is to enhance the internet security awareness of the education object, Improve the youth's internet security knowledge, morality, legal cultivation and self-prevention technology; Third, in the new era of youth internet security education content targeted promotion and the form of education is increasingly perfect and rich, To meet the physical and mental development needs of young people in the new era, Strengthen the practical links, So as to enhance its actual education effect; Finally, the development of information technology to build a strong defense line of internet security education, To provide strong technical support for the youth internet security education in the new era. Que Fengyi (2022) Combined with the internet governance theory, the age characteristics of college students and the historical background of big data, we propose countermeasures to improve the internet security literacy of college students from the three dimensions of society, school and individuals. According to the characteristics of college students in the new period, they should give full play to the role of the main channel of internet security education in colleges and universities, and give full play to the advantages of big data technology. At the same time, the power of other aspects of society is also very important, such as government supervision and management departments, we-media operation institutions, families, etc., and all sectors of society should form a joint force and multi-governance. In addition, we also need to pay attention to the internal cause is the fundamental, in the cultivation process, the key is to play the subjective initiative of college students themselves, so that they constantly improve their own awareness of internet security. Therefore, to improve the internet security literacy of contemporary college students requires the cooperation and joint efforts of college students, college students and all parties in the society. Chen Qi, Xiong Huixiang (2022) Several countermeasures and suggestions for the improvement of internet information security literacy from the national, university and individual students, combining the unified strategy of national literacy assessment with personalized education support; universities should build a "trinity" progressive and phased internet information security literacy education training system including talent training

construction, teacher team building and information security education environment, and follow the strategy of "attention-learning-experience-promotion".

The model of improving internet security literacy by improving education and teaching methods. Zhang Huanhuan, Wu Hao (2020) At present, the research on campus safety education at home and abroad is mainly offline classroom education. This way of education lacks systematization, continuity and communication, let cannot let students master safety knowledge and improve safety awareness in the first time. The campus safety education is presented in the form of "mobile class in the form of" mobile class on the palm of the hand ". Students are not limited by time and space, and can click to learn anytime and anywhere. By adding more intuitive teaching elements to the excellent course of safety education, such as case simulation and the appearance of the parties concerned, students can more intuitively and quickly obtain safety knowledge, so as to continuously improve students' safety awareness and improve the effect of safety education. Yang Lu (2021) From the three aspects of environment, individuals and universities, study the strategy of strengthening college students' internet security education. The first is to improve the education and teaching environment, in the internet can use internet education public video, public account and other mobile devices in the internet security events; the second is that college students should have the ability to identify all kinds of false and negative content in the internet, but also to get to the Internet, good at using Internet technology to obtain beneficial learning information. College students should exert a sense of responsibility in the process of internet use, strengthen self-supervision and self-discipline in internet behavior, establish the sense of rules, and maintain good internet behavior. In terms of internet security education, college students can promote practical teaching, college competition, seminar, promote the literacy of education workers, build institutional guarantee, develop the internet management mode on campus, expand exchanges and cooperation, and establish the linkage between college and family education. Yu Kun (2023, p.48) We should fully consider the diversity and the personalized differences of education objects in the teaching design of internet security awareness education. First, the combination of online and offline teaching mode. The virtual simulation project uses

the Web one-stop login to flexibly and independently realize the combination of online and offline teaching mode. The second is the combination of inside and after class. With the help of internet security awareness education in the virtual simulation experiment project, students can learn independently after class according to their own differences. Third, the combination of teaching and assessment, the process of the assessment and the result of the assessment combined. Fourth, the combination of publicity and competition, using virtual simulation experiment project resources to organize training, peer communication, online and offline competition, award publicity and other activities, combined with a variety of ways to improve students' professional ability and professional quality, through the campus internet news report.

Summary:

Scholars at home and abroad have proposed many ideas and models for internet security literacy education, mainly through building a internet security system, highlighting the core tasks of the subject, establishing improvement models through multi-party linkage, and improving education and teaching methods to enhance internet security literacy. However, there are still some shortcomings and gaps, and the practicality of internet security literacy education is not yet prominent. Many scholars have conducted research on improving safety awareness and strengthening safety thinking, and some have emphasized the importance of combining theory and practice in the education process. However, research on practical methods, content, and effectiveness is not sufficient.

Based on the above literature and other relevant research results, this study tends to improve the model of internet security literacy among college students by improving educational and teaching methods. By establishing a scientific and effective training program that highlights experiential training, it constitutes a model of enhancing college students' internet security literacy.

Evaluation To Improve the Internet Security Literacy Model for College Students

As for the way to improve the model of how to evaluate college students 'literacy, different scholars have selected different methods based on the actual research. The methods with a high proportion include Ke's four-level training evaluation mode, expert evaluation method and pre - and post test experimental method and Delphi method. The specific studies are as follows:

Four-level training assessment model

The training model of teacher managers is evaluated by using the training model of Ke's level 4 training evaluation model is evaluated by the international famous scholar Donald. L. Kirkpatrick is the most widely used training evaluation tool in North America. The training effect is divided into four progressive levels: response assessment, learning evaluation, behavior evaluation and achievement evaluation. These four levels of training evaluation are a process from low level to high level, the implementation is from easy to difficult, the evaluation significance is from small to large, and the cost is from low to high. Whether to evaluate and determine the stage of evaluation should be determined according to the importance of training (Wang Jinbo, 2012, p.78). Li Enjin (2014) proposed a quantitative evaluation index system for enterprise training through the four-level training evaluation mode, including (1) Response assessment (Reaction): assess the satisfaction of the trainees; (2) Learning assessment (Learning): determine the learning degree of the trainees; (3) behavior assessment (Behavior): investigate the knowledge application of the trainees; (4) achievement assessment (Result): estimate the economic benefits created by the training. It is proposed that the evaluation should adhere to the principles of training PDCA, closed-loop management, paying attention to the construction of enterprise training system, the comprehensiveness of training evaluation, and pay attention to the effectiveness of training evaluation.

Delphi method

Delphi method refers to the provisions according to certain procedures, by consulting the opinions of the experts, and will consult the results anonymous feedback to experts, adjust according to the results of the consultation, so several

rounds of anonymous feedback, the opinions of the experts gradually concentrated, finally form the expert's collective judgment results, anonymity, information feedback, convergence, statistics, diversity and other characteristics. With the continuous development of the Delphi method, this method has been given a broader definition, namely, the method to solve a complex problem by organizing an information processing team to treat an individual organization as a whole to obtain a conclusion about a problem (Guo Jia, 1985). Cycle and feedback are the core of Delphi law. Circulation and feedback promote the exchange of opinions between experts, promote experts to learn from each other, inspire each other, and promote the deepening of experts' understanding, thus improving the scientificity and reliability of Delphi method (Wang Qi, 1986).

Haynes David et al. (2023) conducted two rounds of Delphi studies to address priorities for addressing individual online risk. A literature corpus was created based on 69 peer-reviewed articles published between 2014 and 2019. Cluster analysis of the resulting text libraries using the Pearson correlation coefficient yielded seven broad themes. After two rounds of Delphi surveys with experts in information security and information literacy, the following topics were identified as priorities for further investigation: personalization and privacy, privacy responsibilities on social internets, measuring privacy risks, and the perception of impotence and the resulting indifference. The Delphi method provides clear conclusions about the research topic and has the potential as a tool to prioritize future research areas.

CIPP evaluation mode

CIPP evaluation model was proposed by Daniel Leroy Stufflebeam, an American scholar, on the basis of his reflection on Taylor's behavior goal model in 1967. This model consists of Context Evaluation, Input Evaluation The four evaluation activities of Process Evaluation and Product Evaluation fully reflect the developmental function of evaluation., On the basis of clarifying the connotation of the CIPP model, Ge Li and Liu Zeyuan (2014) explained the appropriateness of the CIPP model and the evaluation of entrepreneurship education ability in universities from the perspectives of decision-making orientation, process orientation, and improvement function. Furthermore, analyze the composition of entrepreneurial education

capabilities in universities that match the CIPP model, and establish an evaluation index system for entrepreneurial education capabilities in universities based on CIPP, in order to enhance the basic capabilities of entrepreneurial environment based on background evaluation, entrepreneurial resource allocation capabilities based on input evaluation, entrepreneurial process action capabilities based on process evaluation, and entrepreneurial achievement performance capabilities based on outcome evaluation. Xu Xiangyun and Wang Jiajia (2022), based on the theoretical framework of the CIPP evaluation model, collected research samples through measurement tools (scales), and conducted project analysis, factor analysis, and reliability testing on the sample data, forming a stable four-dimensional structure of "background evaluation, input evaluation, process evaluation, and result evaluation". Zhang Wen (2022) took the compatibility between the CIPP model and the evaluation system of ideological and political education teaching as the starting point, embedded the CIPP model in the evaluation system of ideological and political education teaching, and constructed an evaluation system of ideological and political education teaching based on the indicators of "background input process results".

Pre - and post test experimental methods

Pre - and post experimental design refers to a design that compares the results of observations made on the subjects before experimental condition processing with the same observations made under experimental condition processing. That is, this type of design is a comparative design before and after the experiment (processing). Xin Chong, Zheng Chenna, and Zhu Chunhong (2024) selected 192 students from a certain university to conduct a 16-week PBL teaching experiment in a general education classroom. The research results indicate that compared with the control class, the learning motivation of the experimental class is significantly improved under the PBL teaching mode, with intrinsic motivation being the main driving force, the reinforcement effect of extrinsic motivation is enhanced, and the difference between intrinsic and extrinsic learning motivation is reduced. The research results provide further reference and guidance for the localization application of PBL teaching mode in general education courses and the improvement of student learning motivation. Based on the theory of positive psychology,

Liu Xiaoping (2023) explores the impact of using positive psychological intervention in the mental health education curriculum of public security colleges on the positive character and happiness index of college students. Select two classes of the same grade and major from a certain public security college as the experimental group and control group. The teaching design of the experimental group incorporates positive psychological intervention, while the control group has no intervention. The measurement results of the experimental group and the control group using the PERMA Happiness Index Scale and the Depression Anxiety Stress Self Rating Scale indicate that incorporating positive psychological concepts, theories, and application technologies into the mental health education of college students in public security colleges can improve their positive character and happiness index.

Summary:

Based on the above literature, different studies will choose different evaluation methods for how to evaluate research models, mainly including the Kirkpatrick four level training evaluation model and the Delphi method. Based on the actual situation of this study. This article is based on the CIPP principle and selects the use of expert evaluation method and pre - and post test method to evaluate the improvement model of internet security literacy of college students in Guangxi, China. This method has stronger research applicability in the field of college students' internet security literacy.

Chapter 3

Research Methodology

This study adopts a combination of quantitative and qualitative methods to analyze and study the improvement of internet security literacy among college students in Guangxi, China. It is divided into three stages:

In the first stage, in order to answer research objective 1, the current situation of internet security literacy among college students in Guangxi, China was studied, and the problems and reasons were analyzed.

In the second stage, in order to answer research objective 2, design a model to enhance the internet security literacy of college students.

In the third stage, in order to answer research objective 3, an evaluation was conducted on the model for improving college students' Internet security literacy.

In the First Stage, Corresponding Research Objective 1:

The Population

Experts in the field of internet security in Guangxi universities.

Sample Group

21 experts with over 10 years of work experience in the field of internet security in Guangxi universities.

Table 3.1 List of Distribution of Selected Research Samples

Number	Representative university	Experts
1	Guangxi Minzu University	3
2	Guangxi University of Finance and Economics	3
3	Guangxi Vocational University Of Agriculture	5
4	Guangxi Vocational and Technical College	5
5	Guangxi Polytechnic of Construction	5
	Total	**21**

The five selected universities are representative universities of different levels and cities in Guangxi, including Guangxi Minzu University, Guangxi University of Finance and Economics, Guangxi Vocational University of Agriculture, Guangxi Vocational and Technical College, and Guangxi Polytechnic of Construction.

Research Instruments

Research tools include Expert Survey Questionnaires and IOC tables

The survey questionnaire on the current status of Internet security literacy among college students is divided into three parts:

Table 3.2 Outline of the Expert Survey Questionnaires

Including parts	Content	Concrete content
Part 1	Conduct a survey on the basic information of the respondents	work experience, highest education level, professional title or position, and your workplace
Part 2	A survey on the current situation of internet security literacy among college students	1. Have awareness of internet security; 2. Ability to master internet security knowledge; 3. Ability to prevent and respond to internet security risks; 4. Standardize the moral behavior ability of internet security; 5. Establish the ability of internet psychological security.
Part 3	Conduct research on ways, effects, and suggestions for universities to enhance their internet security literacy	1.The ways and effects of universities to enhance the Internet security literacy of college students 2. Suggestions for improving the internet security literacy of college students

The first part is to investigate the basic information of the respondents;

The second part investigates the current situation of Internet security literacy among college students from five aspects. Based on the expert's understanding of the situation, determine "yes", "no", or "not sure" and choose the corresponding option. If the answer is "no" or "uncertain", ask the expert to briefly describe the reasons or suggestions based on past work experience.

The third part conducts research on the ways, effects, and suggestions for universities to enhance the internet security literacy of college students.

$$\text{IOC} = \frac{\sum \boldsymbol{R}}{\boldsymbol{N}}$$

$\sum R$ It is the sum of expert evaluation scores.

N is the number of expert personnel.

The scoring criteria are: 1=ensure that these contents are relevant to the theme, 0=uncertain whether these contents are related to the theme, -1=ensure that these contents are not related to the theme.

The criteria for determining the consistency between the problem and its content/definition/purpose are as follows:

If IOC>=0.50, then the question is consistent with the content/definition/purpose.

If IOC<0.50, then the issue is inconsistent with the content/definition/purpose. (Pérez-Rojo, 2019)

Data Acquisition

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

2. Soliciting opinions from schools and obtaining collection permits;

3. 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.

4. Send the "Survey on the Status of College Students' Internet Security Literacy" to 21 experts in the field of internet security.

5. Collect questionnaires, eliminate invalid questionnaires, and sort out data.

Data Analysis

1. This study through the form of consciousness, knowledge, skills, morality, psychology, the study of internet security literacy problems, the respondents of judgment "yes" "no" or "not sure" and choose the corresponding options, if the answer "no" or " not sure", then simple narrative reason or suggestion according to previous work experience.

2. By testing the reliability of the questionnaire and using the IOC test method, experts with more than 15 years of work experience in the field of internet security in Guangxi universities were invited for evaluation. Sort out the questionnaire results, check the integrity of the questionnaire, and sort out the valid questionnaire data;

3. The current situation of college students' internet security literacy was analyzed through descriptive statistics, and the frequency distribution, percentage, maximum value and minimum value of each variable were preliminarily calculated.

4.For the questionnaire set open-ended questions: What kind of training methods do you think can better improve the Internet security literacy of college students? Through summary, the most frequently mentioned suggestions are extracted.

Expected Output

The Current Status of Obtaining Internet Security Literacy of Guangxi University Students in China.

In the Second Stage, Corresponding Research Objective 2:

The Population

experts from Internet fields in Guangxi, China

Sample Group

21 experts in the field of internet security in Guangxi universities.

The following conditions are required:

1. Have a certain understanding and research in the field of Internet security literacy among college students;

2. More than 10 years of work experience in the field of education;

3. A manager with a deputy senior professional title or above.

Research Instruments

Internet security literacy improvement model of college students

According to the literature review, this paper puts forward the constituent elements of Internet security literacy and determines that college students' Internet security literacy includes 5 abilities, which are 1. Internet security awareness; 2. Internet security knowledge; 3. Internet security skills; 4. Internet security ethics; 5. Internet security psychology. According to the research objective 1, the problems obtained from the current research indicate that college students' Internet security literacy also has insufficient abilities in these five aspects, which is consistent with the reality. Through the comparison with others on the construction of improving Internet security literacy model. Establish a training model to improve the Internet security literacy of college students in Guangxi.

Data Acquisition

1. Based on the literature review and the current research of research objective 1, establish a training model for improving the Internet security literacy of college students1 in Guangxi;

2. The Delphi method is adopted to collect suggestions from 21 experts, who evaluate each strategy and choose "agree" or "disagree". If "disagree" is selected, reasons or suggestions need to be filled in, and the training model is modified after sorting out expert suggestions, and training model 2 is obtained;

3. Collected the second round of opinions from experts, and concluded the training model3 after sorting out the experts' suggestions;

4. The third round of opinion collection was conducted from experts, all of whom agreed, and the final training model for improving the Internet security literacy of college students in Guangxi was obtained.

Data Analysis

1. Experts evaluate each strategy and select "agree", "disagree" or "not sure", agree =1, disagree =-1, not sure =0.

2. Calculate and sort out the data of each round of Delphi method, including total, average, mode and quartile.

Average: A measure that represents the central tendency of a set of data. It is the sum of all the data in a set of data and then the number of the data in the set. It is an indicator of the tendency of data concentration.

Mode: Means that the mode is the data that occurs the most frequently in a set of data.

Mode = 1, majority agrees

Mode = -1, the majority disagrees

Mode = 0, majority uncertain

Interquartile Range (IQR):

The interquartile range can be used to analyze the concentration and distribution of expert opinions. This research adopts the consensus standards as outlined by Wu Jianxin (2014), as follows:

Interquartile range	Consensus Degree
0≤IQR≤1.8	High
1.8≤IQR≤2.0	Medium
IQR≥2.0	Low

Expected output

Get a designed model to improve the internet security literacy of college students in Guangxi.

In the Third Stage, Corresponding Research Objective 3:

Population

1. College students in Guangxi

2. Experts in the field of Internet security in Guangxi

Sample

1. Select 28 students from Class 1 of Big Data Enterprise Management as experimental samples for pre - and post test experiments.

2. Based on the actual situation of internet security literacy among college students in Guangxi, 5 experts were selected to evaluate the model for improving the internet security literacy of college students.

Research Instruments

"College Student Internet Security Literacy Test Questions" and "College Student Internet security Literacy Expert CIPP Evaluation Form"

The "Internet Security Literacy Test for College Students" assesses the Internet security literacy of college students from five aspects, namely the awareness of Internet security, the ability to master Internet security knowledge, the ability to prevent and respond to Internet security risks, the ability to regulate ethical behavior in Internet security, and the ability to establish internet psychological security.

By calculating scores

>=A score of 90 indicates a strong high level of Internet security literacy

>=80 points indicate a high level of Internet security literacy

>=A score of 70 indicates that Internet security literacy is at an intermediate level

>=A score of 60 indicates a low level of Internet security literacy

<50 points indicates that Internet security literacy is at an extremely low level

2. "Expert CIPP Evaluation Form for Internet security Literacy of College Students"

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

Data Collection

In the first stage, regarding the collection of pre - and post test experimental data:

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.

3. Use test questions to test the students in the sample group.

4. Collect relevant results from pre - and post tests, and organize the data and grades.

In the second stage, regarding the collection of expert evaluation data

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 and organize the results.

Data Analysis

1. Regarding data analysis of pre - and post test experiments: 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. There is a significant difference in the pre - and post test data. If the post test data is higher than the pre test data, it indicates that after the implementation of training interventions, students' Internet security literacy has significantly improved.

2. Analysis of expert evaluation data: Based on Context, Input, Process, and Product, organize whether the experts agree and provide relevant opinions to obtain the CIPP expert evaluation results.

In summary, the feasibility of college students' Internet security literacy can be more scientifically verified through the results of two evaluation methods, namely pre - and post test experiments and expert evaluation.

Expected Output

The training model for improving the Internet security literacy of college students is verified through pre - and post test experiments and expert evaluation.

Chapter 4
Data Analysis Results

The aim of this study is to investigate the improvement model of internet security literacy among college students in Guangxi, China. The research aims to: 1) the current situation of Internet security literacy among college students in Guangxi, 2) construct a model to enhance their Internet security literacy, and 3) evaluate the model to enhance their Internet security literacy. The research is conducted around the above three research objectives, and the results are divided into three parts.

Corresponding to Research Objective 1:

The main focus is on the current situation of Internet security literacy among college students in Guangxi. Using expert survey research methods, a survey questionnaire on the current situation of Internet security literacy among college students in Guangxi was developed. Data on the current situation of Internet security literacy among college students in Guangxi was collected and analyzed, and the problems in Internet security literacy among college students in Guangxi were identified. This part of the research is divided into three steps, and the specific introduction is as follows.

Step 1, prepare an expert survey questionnaire and conduct IOC testing. Based on the relevant content of the literature review, it is determined that Internet security literacy consists of 5 parts. Among them, 10 articles mention Internet security awareness, 11 articles mention Internet security knowledge, 11 articles mention Internet security skills, 9 articles mention internet security ethics, and 5 articles mention internet security psychology. Finally, it was determined that the internet security literacy of college students includes five aspects of abilities, which are ranked in order of importance: 1. Internet security awareness; 2. Internet security knowledge; 3. Internet security skills; 4. Internet security ethics; 5. Internet security psychology.

Based on the above content, a survey questionnaire on the current situation of internet security literacy among college students in Guangxi has been prepared. The questionnaire is divided into three parts, with a total of 30 questions. The first part is to fill in the basic information of experts, including age, work experience, education, professional title, etc.; The second part mainly investigates the problems of internet security literacy among college students in Guangxi, with approximately 4-6 questions for each part; The third part mainly investigates suggestions for improving internet security literacy, including 2 multiple-choice questions and 1 open-ended question. The specific content of the survey questionnaire on the current situation of internet security literacy among college students in Guangxi can be found in the appendix.

By testing the reliability of the questionnaire and using the IOC test method, experts with more than 15 years of work experience in the field of internet security in Guangxi universities were invited for evaluation. The specific process of IOC and the invitation letter for experts can be found in the appendix. After statistics, the data result shows that the highest IOC value is 1 and the lowest value is 0.6>=0.50, indicating that the questionnaire can be implemented.

Step 2, select 21 experts in the field of internet security. 21 experts with over 10 years of work experience in the field of internet security in Guangxi universities were selected, categorized by gender, age, education level, professional title, and work experience. The respondents are 11 males, accounting for 52%, and 10 females, accounting for 48%; The age distribution of the respondents is as follows: 10 people aged 30-40 account for 48%, 10 people aged 41-50 account for 48%, and 1 person aged 51-60 accounts for 4%; The educational qualifications of the respondents are as follows: 11 have a master's degree, accounting for 53%, and 10 have a doctoral degree, accounting for 47%; The job titles of the respondents are: 77 lecturers, accounting for 33%, 2 engineers, accounting for 10%, 10 associate professors, accounting for 47%, and 2 professors, accounting for 10%; The distribution of work experience among respondents is as follows: 17 people have worked for 10-20 years, accounting for 80%, and 4 people have worked for 21-30 years, accounting for 20%. The expert structure is scientifically reasonable, with broad representativeness, professionalism, and authority.

Table 4.1 Number and Percentages of Respondents

(n = 21)

	Personal information	**Number of people**	**Percentage (%)**
Gender	Male	11	52
	Female	10	48
	Total	21	100
Age	30-40 Years old	10	48
	41-50 Years old	10	48
	51-60 Years old	1	4
	Total	21	100
Educational background	Master's degree	11	53
	Doctor's degree	10	47
	Total	21	100
Professional ranks and titles	lecturer	7	33
	engineer	2	10
	adjunct professor	10	47
	professor	2	10
	Total	21	100
Work experience year	5-10 Years	2	10
	11-20 Years	17	80
	21-30 Years	2	10
	Total	21	100

Step 3, Conduct a survey on the current situation and analyze the data on the current status of internet security literacy among college students in Guangxi. This study through the form of consciousness, knowledge, skills, morality, psychology, the study of internet security literacy problems, the respondents of judgment "yes" "no" or "not sure" and choose the corresponding options, if the answer "no" or " not sure", then simple narrative reason or suggestion according to previous work experience. At the same time, the suggestions on how to improve the internet

security literacy of college students are collected. Researchers present the data by percentage. The survey results are as follows:

Table 4.2 Analysis of the Current Situation of Guangxi College Students Having and Improving internet security Consciousness

(n = 21)

Have and enhance internet security awareness	Yes	No	Not sure	Total
College students do not pay attention to the protection of personal network identity information	13	5	3	21
	61.9%	23.81%	14.29%	100%
College students do not pay attention to the protection of personal network activity information	16	2	3	21
	76.19%	9.52%	14.29%	100%
College students lack the awareness of regular backup of information and materials	19	2	0	21
	90.48%	9.52%	0	100%
College students lack the awareness to prevent online fraud	14	4	3	21
	66.67%	19.05%	14.29%	100%

According to Table 4.2, Having and enhance awareness of cyber security, For question 1, "college students do not pay attention to the protection of personal network identity information", 13 agreed to 61.9%, 5 people chose to disagree with 23.81%, The uncertain selection of 3 people accounted for 14.29%; For question 2, "college students do not pay attention to the protection of personal network activity information", 16 people agreed, accounting for 76.19%, 2 people chose to disagree with 9.52%, The uncertain selection of 3 people accounted for 14.29%; For question 3, "college students lack the awareness of regular backup of information", 19 agreed to 90.48%, 2 people chose to disagree with 9.52%, 0 people choose uncertain; For the question 4, "college students lack the awareness of preventing online fraud", 14 agreed to 66.67%, 19.05%, Uncertainty of 3 people accounted for 14.29%.

Conclusion: There are multiple issues among college students in terms of internet security awareness, the most prominent of which is the lack of awareness of regularly backing up information materials. The highest agreement rate is 90.48%, which reflects that the vast majority of 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.

According to Table 4.3, In the ability to learn and master cybersecurity knowledge, As for question 1, "College students lack understanding of internet security laws and regulations such as the Internet Security Law and the Personal Information Protection Law", 19 agreed to 90.48%, 41 chose to disagree with 4.76%, 1 uncertain choice accounted for 4.76%; For question 2, "college students lack of understanding of basic knowledge such as the concept of internet security", 17 agreed to 80.95%, 19.05%, 0 people choose uncertain; As for question 3, "college students do not understand how to protect their rights after encountering internet security problems", 20 agreed to 95.24%, 41 chose to disagree with 4.76%, 0 people choose uncertain; For question 4 "college students actively learn and understand internet security knowledge is not strong", 20 agreed to 95.24%, 41 chose to disagree with 4.76%, 0 people choose uncertain; For question 5, " College students have a single way to learn and master internet security knowledge, Poor learning results ", 18 agreed to 85.71%, 2 people chose to disagree with 9.52%, 4.76%.

Table 4.3 Status Analysis of the ability of Guangxi College students to learn and master internet security knowledge

(n = 21)

The ability to learn and master internet security knowledge	Yes	No	Not sure	Total
College students lack of understanding of internet security laws and regulations such as the Internet security Law and the Personal Information Protection Law	19	1	1	21
	90.48%	4.76%	4.76%	100%
College students lack of understanding of the basic knowledge such as the concept of internet security	17	4	0	21
	80.95%	19.05%	0	100%
College students do not understand how to protect their rights after encountering internet security problems	20	1	0	21
	95.24%	4.76%	0	100%
College students to learn and understand internet security knowledge is not strong	20	1	0	21
	95.24%	4.76%	0	100%
College students have a single way to learn and master the internet security knowledge, and the learning effect is not good	18	2	1	21
	85.71%	9.52%	4.76%	100%

Conclusion: There are multiple problems with the ability of college students to learn and master internet security knowledge. In question 3, "College students do not understand how to protect their rights after encountering internet security problems," the approval rate is as high as 95.24%, which is the highest among the five questions. This indicates that the vast majority of college students do not know how to effectively protect their rights when facing internet security issues, which increases

their risk of further infringement. For question 4, "College students have a low enthusiasm for actively learning and understanding internet security knowledge," the approval rate is also as high as 95.24%, which is the highest on par with question 3. 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 on the issue of lack of understanding of basic knowledge such as the concept of internet security is 80.95%, indicating that a small number of college students have some understanding of basic knowledge of internet security.

According to Table 4.4, In terms of the ability to prevent and respond to cybersecurity risks, For question 1, "College students need to improve their firewall configuration and use skills", 21 agreed to 100%, 0 People choose to disagree, 0 people choose uncertain; For question 2, "College students need to improve the configuration and use skills of anti-virus software", 21 agreed to 100%, 0 People choose to disagree, 0 people choose uncertain; For question 3, "college students need to improve their skills to prevent network telecom fraud", 21 agreed to 100%, 0 People choose to disagree, 0 people choose uncertain; For question 4, "College students have random links to the public network", 18 agreed to 85.71%, 2 people chose to disagree with 9.52%, 1 uncertain choice accounted for 4.76%; As for question 5, "College students do not pay attention to software rights management and privacy protection", 19 agreed to 90.48%, 41 chose to disagree with 4.76%, 1 uncertain choice accounted for 4.76%; As for the question 5, "whether college students do not pay attention to the safety of the electronic payment environment", 17 agreed to 80.95%, Three people chose to disagree with 14.29%, 4.76%.

Table 4.4 Analysis of the ability to prevent and respond to cybersecurity risks

(n = 21)

The ability to prevent and respond to cybersecurity risks	Yes	No	Not sure	Total
College students need to improve their firewall configuration and use skills	21	0	0	21
	100%	0	0	100%
College students need to improve the configuration and use skills of anti-virus software	21	0	0	21
	100%	0	0	100%
College students need to improve their skills to prevent online telecom fraud	21	0	0	21
	100%	0	0	100%
College students have the problem of random linking to the public network	18	2	1	21
	85.71%	9.52%	4.76%	100%
College students do not pay attention to software permission management and privacy protection	19	1	1	21
	90.48%	4.76%	4.76%	100%
College students do not pay attention to the security of the electronic payment environment	17	3	1	21
	80.95%	14.29%	4.76%	100%

Conclusion: There are still certain deficiencies in the ability of Guangxi university students to prevent and respond to internet security risks, especially in improving their skills in firewall configuration and use, configuring and using antivirus software, and preventing network and telecommunications fraud. The approval rate for all three issues is 100%, and the approval rate for "not valuing the security of the electronic payment environment" is the lowest compared to other issues, at 80.95%, It indicates that college students have a certain strengthening of their understanding of electronic payment security, but they still need to pay more attention to the security of the payment environment.

The first part is to investigate the basic information of the respondents;

The second part investigates the current situation of Internet security literacy among college students from five aspects. Based on the expert's understanding of the situation, determine "yes", "no", or "not sure" and choose the corresponding option. If the answer is "no" or "uncertain", ask the expert to briefly describe the reasons or suggestions based on past work experience.

The third part conducts research on the ways, effects, and suggestions for universities to enhance the internet security literacy of college students.

Table 4.5 Analysis of the Current situation of College Students in Guangxi to regulate and Maintain Internet security Ethics

(n = 21)

Ability to regulate and maintain cyber security ethics	**Yes**	**No**	**Not sure**	**Total**
College students' sense of responsibility to maintain internet security needs to be enhanced	21	0	0	21
	100%	0	0	100%
College students publish or forward false information without confirmation	17	2	2	21
	80.95%	9.52%	9.52%	100%
College students lack the awareness of online intellectual property protection, such as using pirated software and not identifying copyright	20	1	0	21
	95.24%	4.76%	0	100%
College students participate in online gambling, part-time brush sheet, browsing bad websites and other network anomie behaviors	18	1	2	21
	85.71%	4.76%	9.52%	100%

According to Table 4.5, In the ability to regulate and maintain cybersecurity ethics, For question 1, "college students' sense of responsibility to maintain internet security needs to be improved", 21 agreed to 100%, 0 People choose to disagree, 0

people choose uncertain; As for question 2, "College students have an unverified behavior of publishing or forwarding false information", 17 agreed to 80.95%, 2 people chose to disagree with 9.52%, The uncertain choice of 2 people accounted for 9.52%; As for question 3, "college students lack the awareness of online intellectual property protection, such as using pirated software and not identifying copyright", 20 agreed to 95.24%, 41 chose to disagree with 4.76%, 0 people choose uncertain; As for question 4, "College students participate in online gambling, part-time brushing, and browsing bad websites", 18 agreed to 85.71%, 41 chose to disagree with 4.76%, The uncertain choice of 2 people accounted for 9.52%.

Conclusion: There are problems with the ability of college students to regulate and maintain internet security ethics, especially 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 further strengthening. 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.

According to Table 4.6, In cultivating and developing the ability of network psychological security, As for question 1, "college students are addicted to Internet addiction, such as online games and mobile phone separation anxiety", 20 agreed to 95.24%, 41 chose to disagree with 4.76%, 0 people choose uncertain; As for question 2, "college students will cause psychological problems due to cyber security incidents such as cyber violence and cyber fraud", 21 agreed to 100%, 0 People choose to disagree, 0 people choose uncertain; Regarding question 3, "college students lack the ability to self-regulate and intervene when they encounter psychological problems of internet security", 19 agreed to 90.48%, 41 chose to disagree with 4.76%, 1 uncertain choice accounted for 4.76%; For question 4, "College students lack the ability to seek professional counseling and help when they encounter psychological problems of

internet security", 19 agreed to 90.48%, 41 chose to disagree with 4.76%, 1 uncertain choice accounted for 4.76%;

Table 4.6 Analysis of the Current Situation of Cultivating and Cultivating the Network Psychological Security Ability of College Students in Guangxi

(n = 21)

Cultivate and develop the ability of network psychological security	**Yes**	**No**	**Not sure**	**Total**
College students are addicted to Internet, such as online games and mobile phone separation anxiety	20	1	0	21
	95.24%	4.76%	0	100%
College students will cause psychological problems due to internet security incidents such as network violence and network fraud	21	0	0	21
	100%	0	0	100%
College students lack the ability to self-regulate and intervene when encountering the psychological problems of internet security	19	1	1	21
	90.48%	4.76%	4.76%	100%
College students lack the ability to seek professional counseling and help when encountering psychological problems of internet security	19	1	1	21
	90.48%	4.76%	4.76%	100%

Conclusion: There are still shortcomings in cultivating and cultivating the ability of online psychological security among college students. Regarding the issue that college students may experience psychological problems due to online violence, fraud, and other internet security incidents, 100% of the respondents agree. This indicates that cybersecurity incidents do have a negative impact on the psychology of college students, and also reflects that the frequency of cybersecurity 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 the majority of college students lack effective coping strategies and ways to seek help when facing network psychological problems.

Table 4.7 Suggestion Analysis on improving the training mode of college students' internet security literacy

1. Enrich the content of internet security education and training courses
2. Introduce more practical cases into the training course
3. Establish an online learning platform to provide the latest internet security courses and resources
4. Practical and participatory learning methods, such as simulation exercises and cybersecurity competitions
5. Enhance students' awareness of independent learning internet security
6 Regularly invite internet security experts to give lectures
7. Combine online and offline publicity
8. Immersive experience, VR, Script experience, etc.
9. Visit the enterprises related to internet security
10. Organize debate competitions on hot issues on cyber security
11. Conduct group counseling on internet security psychology
12. Design the internet security test

According to Table 4.7, the questionnaire set open questions: What kind of training method do you think can better improve the internet security literacy of college students? By summary and induction, There are 12 improvement strategies, 1. Enrich the content of internet security education and training courses; 2. Introduce more practical cases into the training course; 3. Establish an online learning platform, Provide the latest internet security courses and resources; 4. Practical and participatory learning methods, Such as simulation exercises and cyber security competitions;

5. Enhance students' awareness of internet security in autonomous learning; 6. Regularly invite internet security experts to give lectures; 7. Carry out the combined online and offline publicity; 8. An immersive experience, VR, Script experience l, etc.; 9. Visit the enterprises related to internet security; 10. Organizing the debate competition on hot issues of cyber security; 11. Conduct group counseling on internet security psychology; 12. Design the internet security test. The above suggestions establish the foundation for the next step of building the internet security literacy improvement model of college students.

Corresponding Research Objective 2:

To construct an enhancement model, use the Delphi method to analyze strategies for improving the internet security literacy of Guangxi university students, and modify and improve the enhancement model.

According to the literature review, the constituent elements of internet security literacy were identified, and five aspects of abilities were identified for college students in cybersecurity literacy, namely: 1. Internet security awareness; 2. Internet security knowledge; 3. Internet security skills; 4. Internet security ethics; 5. Internet security psychology. According to the research objective 1, the current situation indicates that college students also have insufficient abilities in these five aspects of internet security literacy, which is consistent with the reality. Compare with others on building models to enhance cybersecurity literacy, the preliminary establishes improve Guangxi college students 'internet security literacy training mode 1, to 21 experts, modify the expert advice, training model, training model 2 to the second round of experts, experts, training model 3, to experts for the third round of opinions, experts agree, concluded that the final promotion of Guangxi college students' internet security literacy training model. The specific analysis results are shown as follows:

Round 1, In the first round, the training model 1 was distributed to 21 experts. The experts evaluated each strategy and chose "agree" or "disagree". If you chose "disagree", you needed to fill in the reasons or suggestions.

Table 4.8 Summary of Expert Opinion Results for the First Round of Delphi Method

(n = 21)

Model composition	Specific strategies	Agree (1)	Not sure(0)	Disagree(-1)	Total	Mean	Mode	IQR
Training content	Content revolving around five aspects of cybersecurity awareness, knowledge, skills, ethics, and psychology	19	2	0	19	0.90	1	0
Training methods	1. Theoretical teaching; 2. Practical teaching; 3. Group discussion; 4. Role playing 5. Case analysis	15	0	6	9	0.43	1	2
Training materials and tools	PPT, video, case, news, legal terms	15	1	5	10	0.48	1	1
Training time	There are a total of 5 themes, each lasting 8 hours, and a total of 5 days and 40 hours of training.	21	0	0	21	1.00	1	0
Training evaluation	Prepare test questions and evaluate the training effectiveness through scores before and after each theme training	20	1	0	20	0.95	1	0

According to Table 4.8, 17 experts chose to agree on the training content, with an average value of 0.90, close to 1, indicating that the majority of people agreed with the design of the training content, with a mode of 1, further confirming the majority's acceptance 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. It is suggested to increase training methods related to internet security scenario simulation experiences to encourage students to participate more actively in the training, resulting in a more realistic effect. The average value is 0.43, indicating a certain degree of disagreement in the 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, Indicates a significant degree of variability 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, 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 the majority of people fully agree. The mode is 1, the IQR is 0, and the data distribution is very concentrated.

Conclusion: After the first round of expert opinion collection, all experts agree on the training content, training time, and training evaluation. In terms of training methods, materials, and tools, experts have 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.

In the second round, the model will be modified based on the results of the first round, and Model 2 will be improved and distributed to 21 experts. The experts will evaluate each strategy and choose "agree" or "disagree". If "disagree" is selected, reasons or suggestions need to be filled in

According to Table 4.9, in terms of training content, training time, and training evaluation, all 21 experts agree, 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 the majority of people strongly agree. The mode is 1, indicating that the majority of 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.

Table 4.9 Summary of Expert Opinion Results for the Second Round of Delphi Method

(n = 21)

Model composition	Specific strategies	Agree (1)	Not sure(0)	Disagree(-1)	Total	Mean	Mode	IQR
Training content	Content revolving around five aspects of cybersecurity awareness, knowledge, skills, ethics, and psychology	21	0	0	21	1.00	1	0
Training methods	1. Theoretical teaching; 2. Practical teaching; 3. Group discussion; 4. Role playing; 5. Case analysis; 6. Scenario experience	20	0	1	19	0.90	1	0
Training materials and tools	PPT, video, case, news, legal terms, Game resources	18	1	2	16	0.76	1	0
Training time	There are a total of 5 themes, each lasting 8 hours, and a total of 5 days and 40 hours of training.	21	0	0	21	1.00	1	0
Training evaluation	Prepare test questions and evaluate the training effectiveness through scores before and after each theme training	21	0	0	21	1.00	1	0

Conclusion: 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. Based on the comprehensive opinions, the training method should include psychological group counseling, and the online learning platform "Xuexitong" APP and group counseling props should be added to the training materials and tools.

In the third round, the model will be modified based on the results of the second round, and the improved model 3 will be distributed to 21 experts. The experts will evaluate each strategy and choose "agree" or "disagree". If "disagree" is selected, reasons or suggestions need to be filled in.

Table 4.10 Summary of Expert Opinion Results for the Third Round of Delphi Method (n = 21)

Model composition	Specific strategies	Agree (1)	Not sure(0)	Disagree(-1)	Total	Mean	Mode	IQR
Training content	Content revolving around five aspects of cybersecurity awareness, knowledge, skills, ethics, and psychology	21	0	0	21	1	1	0
Training methods	1. Theoretical teaching; 2. Practical teaching; 3. Group discussion; 4. Role playing; 5. Case analysis; 6. Scenario experience; 7. Psychological group counseling	21	0	0	21	1	1	0

Table 4.10 (Continued)

(n = 21)

Model composition	Specific strategies	Agree (1)	Not sure(0)	Disagree(-1)	Total	Mean	Mode	IQR
Training materials and tools	PPT, video, case, news, legal terms, Game resources, "XUEXITONG" APP, Props for group counseling	21	0	0	21	1	1	0
Training time	There are a total of 5 themes, each lasting 8 hours, and a total of 5 days and 40 hours of training.	21	0	0	21	1	1	0
Training evaluation	Prepare test questions and evaluate the training effectiveness through scores before and after each theme training	21	0	0	21	1	1	0

According to Table 4.10, all 21 experts agree 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.

Conclusion: 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.

The content of the Guangxi University Student Internet Security Literacy Enhancement Model is as follows:

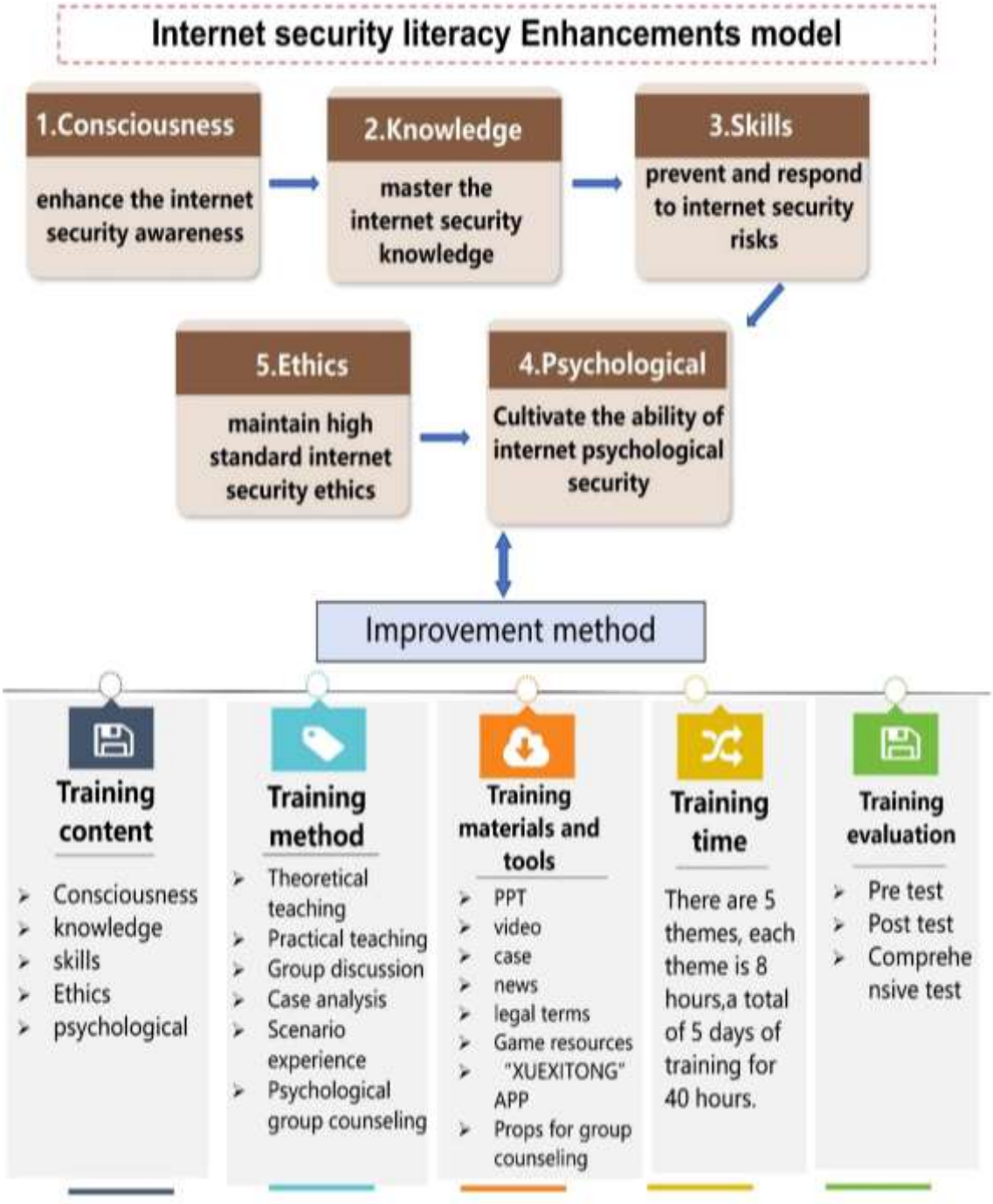

Figure 4.1 Internet Security Literacy Enhancement Model

The model of improving college students' internet security literacy is a multi-dimensional and gradual education system, which is carefully divided into two core parts. Firstly, on the basis of in-depth analysis of literature review and current research status, the model closely around the five key themes of consciousness, knowledge, skills, ethics and psychology, constructs a comprehensive and systematic training framework.

Part I: theory construction and theme deepening

1.Enhance awareness: as a starting point, through vivid case analysis, shocking review of network security events and interactive lectures, arouse college students' attention to network security, make them deeply aware of the significant impact of network security on personal information security, property security and even social stability, so as to establish a strong awareness of internet security.

2.Improve knowledge: on the basis of consciousness awakening, through systematic course learning, cover the basic concepts, principles, laws and regulations, common threat types and preventive measures of network security, so as to build a solid internet security knowledge system for college students. Make use of online courses, textbooks, video tutorials and other teaching resources to ensure the comprehensiveness and timeliness of knowledge.

3.Improve skills: skills are the key to meet the challenges of internet security. Through practical projects such as simulated attack and defense drills, security vulnerability mining and repair practices, and personal information protection strategy formulation, college students can exercise and improve their network security skills in real or simulated situations. At the same time, teach them to use practical software such as firewall, anti-virus software and password management tools to enhance their self-protection ability.

4.Improve psychology: network security is not only about technology, but also about psychology. Through psychological counseling, stress management training and other ways, help college students establish a healthy internet security mentality, learn to keep calm and rational in the face of network fraud, information leakage and other crises, and effectively deal with psychological pressure.

5.Participation morality: emphasize the importance of internet ethics and guide college students to establish a correct network security morality. By organizing network security ethics seminar, moral dilemma case analysis and other activities, let them deeply understand the moral principles of respecting others' privacy, not participating in internet attacks, maintaining a healthy internet environment, and actively participate in internet security volunteer activities to spread positive energy.

The second part, as a key component of the model, its carefully designed training program provides a solid support for improving college students' internet security literacy. The following is a detailed and rich exposition of these five aspects:

1. training content: The training content is designed closely around the five themes of consciousness, knowledge, skills, ethics and psychology to ensure full coverage of all aspects of the field of network security. The content includes not only basic theoretical knowledge, such as the basic concept of internet security, laws and regulations, common threat types, but also practical operation skills, such as the use of security software, attack defense technology, data backup and recovery, etc. At the same time, it also pays attention to psychological education and moral guidance to help college students establish a correct concept of internet security and morality.

2. training methods: Adopt diversified training methods to meet the needs of different learners. In addition to the traditional lecture teaching, interactive teaching methods such as case analysis, group discussion, role play and simulation exercise are also introduced to enhance the interest and effectiveness of learning. Using modern information technology means, such as online learning platform, virtual reality technology, etc., to provide learners with more rich and intuitive learning experience.

3. training materials and tools: Provide high-quality and diversified training materials and tools to support the smooth implementation of teaching activities. These materials include teaching materials, courseware, video tutorials, simulation software, etc., designed to help learners systematically master internet security knowledge and skills. At the same time, learners are encouraged to use Internet resources for autonomous learning and extended learning to continuously improve their internet security literacy.

4. training time: Reasonably arrange the training time to ensure that learners have enough time for in-depth study and practice. According to the training content and difficulty, formulate a detailed training plan and schedule, and clarify the learning objectives and tasks of each stage. At the same time, considering the individual differences and learning progress of learners, flexible learning time and personalized learning support are provided.

5. training evaluation: Establish a scientific and comprehensive training evaluation mechanism to objectively and accurately evaluate the training effect. Through knowledge test, skill assessment, project evaluation, psychological test and other ways, comprehensively investigate the learners' learning achievements and ability level. According to the evaluation results, timely adjust the training contents and methods to ensure the smooth realization of training objectives. At the same time, pay attention to the establishment of feedback mechanism, encourage learners to put forward opinions and suggestions, and constantly improve and perfect the training program.

To sum up, the second part provides strong guarantee and support for improving college students' internet security literacy through careful training content design, diversified training methods, rich training materials and tools, reasonable training schedule and scientific training evaluation mechanism.

These two aspects complement each other and together constitute an improvement mode to improve college students' internet security literacy. The specific display training program is as follows:

Topic 1: Enhance the awareness of personal internet security

Training objectives:

1. Enhance the awareness of protecting personal identity information when going online

2. Enhance the awareness of protecting personal activity information when going online

3. Enhance the awareness of regular backup of network information and materials

4. Enhance the awareness of preventing online fraud

5. Enhance the awareness of preventing non-performing online loans

Training preparation:

1. Preparation of teaching resources, including multimedia classrooms, the Internet, books, videos, etc.

2. Understand the basic information of the training students Pre -testing

Training process:

The whole training process is divided into 8 hours and 5 parts. The training. The training methods include theoretical teaching, case presentation, group discussion, practical teaching, interactive questions and answers. The training materials and tools mainly include PPT, related cases, operation manuals, and videos, etc. The specific contents are as follows:

Table 4.11 Enhance the awareness of personal internet security

Problems that need to be addressed	Training content	Training method	Training materials and tools	Time-share
Enhance the awareness of protecting personal identity information when going online	1. What is personal identity information. Including identity, contact information, property status, etc.; 2. Consequences of personal information leakage on the Internet. Identity theft, property loss and personal privacy leakage; 3. How to avoid having personal identity information leaked on the Internet. Use privacy protection tools, such as virtual private network (VPN), privacy browser, encrypted communication software.	Lecture with essential Examples	PPT, related information and cases of personal information protection	2 Hours

Table 4.11 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	Time-share
Enhance the awareness of protecting personal activity information when going online	1. What is the personal network activity information. Browse records, search history, online shopping records, etc. 2. Consequences of personal activity information leakage on the Internet. For business analysis, advertising push, etc. 3. How to avoid having personal identity information leaked on the Internet. Be careful when publishing information on social media to avoid leaking excessive personal information, such as location and birthday information.	panel discussion	Cases related to the protection of personal activities	1 Hour

Table 4.11 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	Time-share
Enhance the awareness of regular backup of network information and data	1. The importance of data backup. Prevent data loss, especially in the case of hardware failures, natural disasters, malicious attacks, etc. 2. Methods of data backup. 3. Cycle and frequency of data backup.	Lecture practical	Operation manual on how to perform an effective data backup	1 Hour
Enhance the awareness of preventing online fraud	1. The concept and type of network fraud. Such as phishing fraud, false advertising, social media fraud, impersonating identity fraud, etc. 2. Common cases of preventing online fraud. In recent years, the typical cases of network fraud in college students, understand the means of fraudsters and the process of victims.	Case explains	And network fraud related videos, cases	2 Hours

Table 4.11 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	Time-share
Enhance the awareness of preventing non-performing online loans	1. Risk of non-performing online loans. Falling in the interest trap, violent collection of repayment. 2. Methods to prevent the risk of non-performing online loans. Set up a scientific concept of consumption, learn to check the qualification of lending institutions, understand the loan interest rate and fees.	Interactive Q & A	PPT	2 Hours
			amount to	8 Hours

After-school arrangements and references:

1. Students are required to review the classroom content and requirements according to their own actual situation to improve the effectiveness of the training

2. Arrange the test to enhance the internet security awareness, and analyze and compare the data before and after the test.

Topic 2: Improve the ability to master the knowledge of internet security

Training objectives:

1. Master the important laws related to cyber security

2. Master the basic knowledge related to internet security

3. Understand how to protect the rights after encountering internet security problems

4. Improve the enthusiasm of active learning and understanding of internet security knowledge

Training preparation:

1. Preparation of teaching resources, including multimedia classrooms, the Internet, books, videos, etc.

2. Understand the basic information of the training students

Training process:

The whole training process is divided into 8 hours and four parts. The training methods include theoretical teaching, case presentation, group discussion, role playing, interactive games. The training materials and tools mainly include PPT, related cases, news materials, video animation, etc. The specific contents are as follows:

Table 4.12 Improve the ability to master the knowledge of internet security

Problems that need to be addressed	Training content	Training method	Training materials and tools	time-share
Master the important laws related to cyber security	1. Study the important provisions of the Cyber Security Law 2. Study the important provisions of the Personal Information Protection Law	Theory teaching	PPT, showing the specific terms of the law	2 Hours
Master the basic knowledge related to internet security	1. The concept of internet security 2. What is cyber security literacy 3. What are the common internet security problems are	panel discussion	PPT shows basic knowledge of internet security; writing tool used for panel discussion results	2 Hours

Table 4.12 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	time-share
Understand how to protect their rights after encountering internet security problems	1. How to collect the evidence 2. Which departments can you report your problems to	playing	Cases of rights protection after encountering internet security problems; related news materials; Guiding Opinions on Further Strengthening the Reporting of Network Tort Information	2 Hours
Enhance the initiative of active learning and understanding of internet security knowledge	Show animations and interactive games related to internet security, etc.	Watch videos and interactive games	And animation, game related to internet security resources	2 Hours
			amount to	8 Hours

After-school arrangements and references:

1. Students are required to review the classroom content and requirements according to their own actual situation to improve the effectiveness of the training.

2. Pay attention to the new media platforms related to internet security, read the relevant news and materials related to internet security knowledge, and maintain the normalization of internet security education.

Topic 3: Improve the ability to prevent and respond to internet security risks

Training objectives:

1. Improve your firewall configuration and use skills

2. Improve the configuration and use skills of anti-virus software

3. Improve the skills of preventing online telecom fraud

4. Improve the standard use of public networks

5. Improve the software rights management and privacy protection setting skills

6. Improve your skills on how to ensure the security of the electronic payment environment

Training preparation:

1. Preparation of teaching resources, including multimedia classrooms, the Internet, books, videos, etc

2. Understand the basic information of the training students

Training process:

The whole training process is divided into 8 hours and divided into six parts for training. The training methods include theoretical teaching, case presentation, group discussion, practical teaching, interactive questions and answers. The training materials and tools mainly include PPT, related cases, operation manuals, and videos, etc. The specific contents are as follows:

Table 4.13 Improve the ability to prevent and respond to internet security risks

Problems that need to be addressed	**Training content**	**Training method**	**Training materials and tools**	**time-share**
Improve your firewall configuration and usage skills	1. Learn the basic principles of the firewall; 2. How to configure the practical operation of the firewall.	practical teaching	PPT, and firewall related information, related to the firewall software products	1 Hour
Improve the configuration and use skills of antivirus software skills	1. Understand the principle and functions of anti-virus software, scan, isolate, delete viruses, etc. 2. Learn the guide for using antivirus software. 3. Learn how to install and configure anti-virus software on your own electronic devices.	practical teaching	PPT, and antivirus software related information, related products	1 Hour

Table 4.13 (Continued)

Problems that need to be addressed	**Training content**	**Training method**	**Training materials and tools**	**time-share**
Improve the skills of preventing network telecom fraud	1. Identify fraud information. Identify fake websites and phishing emails, and check the authenticity of the web address and the source of the email. 2. Handle unfamiliar incoming calls and messages. SMS, social software messages, etc., to carefully screen, to confirm the source and authenticity of the information. 3. Timely consultation and help. Ask relatives, friends or professionals to avoid blind decisions.	playing	Prevent network telecom fraud cases	2 Hours

Table 4.13 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	time-share
Improve your skills to regulate the use of public networks	1. Understand the risks of public networks. Including unencrypted communications, malicious phishing, and data theft. 2. Be careful to connect to public networks. Try to avoid using open networks that do not require passwords or authentication, which are often less secure. 3. Don't do anything when connecting to a public network. Use sensitive information for online banking transactions, log in to personal accounts, share important files, or send confidential information.	Theory teaching group discussion	PPT: Information showing the skills of regulating the use of public networks	1 Hour
Improve software rights management and privacy protection setting skills	1. Learn what the permission settings and privacy settings are. 2. Learn the permission setting of the operating system and the application program. 3. Learn the privacy protection Settings.	practical teaching	PPT: permission setting and, privacy protection setting	1 Hour

Table 4.13 (Continued)

Problems that need to be addressed	**Training content**	**Training method**	**Training materials and tools**	**time-share**
How to ensure the security of the electronic payment environment skills	1. Learn the working principle of electronic payment, including the parties involved (such as consumers, merchants, payment gateways, banks, etc.) and transaction processes; 2. Practice, implement a strong password strategy for payment accounts, and encourage the use of multi-factor authentication (MFA) to enhance account security 3. Update the electronic payment system and related software to fix known security vulnerabilities.	practical teaching	Students' electronic payment-related software	2 Hours
			amount to	8 Hours

After-school arrangements and references:

1. Students are required to review the classroom content and requirements according to their own actual situation to improve the effectiveness of the training.

2. Join relevant communities or forums to exchange experiences and skills with other security experts.

Topic 4: Improve the ability to maintain internet security ethics

Training objectives:

1. Enhance the sense of responsibility for maintaining cyber security

2. Master the ability to distinguish between the network information

3. Master the relevant content of network intellectual property rights protection

4. Strengthen the civilized norms of behavior when using the Internet

Training preparation:

1. Preparation of teaching resources, including multimedia classrooms, the Internet, books, videos, etc.

2. Understand the basic information of the training students

Training process:

The whole training process is divided into 8 hours and four parts. The training methods include theoretical teaching, case presentation, group discussion, role playing, interactive games. The training materials and tools mainly include PPT, related cases, news materials, video animation, etc. The specific contents are as follows:

Table 4.14 Improve the ability to maintain internet security ethics

Problems that need to be addressed	Training content	Training method	Training materials and tools	time-share
Enhance the sense of responsibility for maintaining cyber security	1. The concept and responsibilities of digital citizenship 2. Learn from some of the main responsibilities that college students should assume in maintaining internet security. Consciously abide by laws and regulations, advocate network civilization, report network illegal behavior, etc.	group activity	Publicity poster making tools, the theme of "how to maintain the responsibility of internet security" was designed in groups	2 Hours

Table 4.14 (Continued)

Problems that need to be addressed	Training content	Training method	Training materials and tools	time-share
Master the ability to distinguish between the network information	1. Learn to verify the sources of online information. Choose authoritative media, conduct cross-validation, etc. 2. Speak out correctly on the Internet. Unverified information is not forwarded to avoid misleading by false information, resulting in the spread of rumors. 3. Cultivate dialectical thinking and learn to distinguish between facts and opinions.	Case explains	Videos and cases related to the spread of Internet rumors	2 Hours
Master the relevant content of network intellectual property rights protection	1. Learn the meaning and characteristics of network intellectual property rights 2. Online infringement cases and legal protection of copyright and other intellectual property rights	Case explains	Video and cases related to network intellectual property rights	2 Hours
Strengthen the civilized norms of the behavior when using the network	1. Types of online uncivilized Internet behavior. Online gambling, browsing unhealthy websites, online violence, etc. 2. Learn the content of the National Convention on Youth Network Civilization	Theory teaching	PPT: Display the "National Youth Network Civilization Convention" and other contents	2 Hours
			amount to	8 Hours

After-school arrangements and references:

1. Students are required to review the classroom content and requirements according to their own actual situation to improve the effectiveness of the training.

2. The internet security publicity posters made during the training process will be posted on the campus to form the training results.

Topic 5: Improve the psychological ability of internet security

Training objectives:

1. Master the ability to identify common psychological problems of internet security

2. It can improve students' psychological quality in internet security incidents

3. Make students master the way to seek help when they encounter internet security psychological problems

Training preparation:

1. Preparation of teaching resources, including multimedia classrooms, the Internet, books, videos, etc.

2. Understand the basic information of the training students

Training process:

The whole training process is divided into 8 hours and divided into three parts. The training methods include theoretical teaching, case presentation, and psychological group counseling. The training materials and tools mainly include PPT, related cases, group counselor tools, etc. The specific contents are as follows:

Table 4.15 Improve the psychological ability of internet security

Problems that need to be addressed	**Training content**	**Training method**	**Training materials and tools**	**time-share**
Improve the ability to identify common psychological problems in internet security	Types and impact of internet security psychological problems. Such as a long time addicted to online games, by the network language violence Potential symptoms of anxiety or depression.	Case study	Cases about the psychological problems of internet security	3 Hours
Improve the psychological quality in the internet security incidents	1. Methods to deal with psychological problems caused by internet security; cognitive therapy, naturopathy, motivation analysis, etc. 2. How to relieve the psychological pressure caused by network problems. Learn ways to relieve stress	Psychological group tutoring	A tool used for psychological group counseling	3 Hours

Table 4.15 (Continued)

Problems that need to be addressed	**Training content**	**Training method**	**Training materials and tools**	**time-share**
Grasp the way to seek help when encountering internet security psychological problems	1. School: I can communicate with teachers and the psychological education department of the school 2. Society: psychological counseling institutions and hospitals, call the psychological counseling hotline. 3. Family and friends. Talk to people you trust.	panel discussion	Mind mapping tool: Discuss what to do in case of cyber violence and turn it into a mind mapping	2 Hours
				8 Hours

After-school arrangements and references:

1. After the training, interviews were conducted to understand whether students' understanding of internet security psychological problems and their coping ability have been improved

2. Conduct a simulation test of internet security psychological problems to evaluate students' coping ability and response speed.

Training materials presentation – PPT

Picture of the implementation process of model application

	Explanation of Internet Security Literacy Enhancement Courseware 2024-3-18
	Watch video materials 2024-3-18
	Organize group discussions 2024-4-28
	Display of online exam questions 2024-4-28
	Students use the "Chaoxing" app on their mobile phones for online testing 2024-4-28

Training evaluation presentation -test questions

Internet Security Awareness

1. (Multiple choice question) Which of the following options can easily cause our personal information to be illegally stolen?

A. Randomly discard delivery notes or packages

B. Share your location, address, birthday, and other information freely on social networks

C. Computers and phones do not have lock screen passwords set

D. Regularly update passwords for various platforms

Answer: ABC

2. (Multiple choice question) What are the main aspects of the importance of cybersecurity awareness for individuals and society?

A. Prevent personal information leakage

B. Maintaining National Information Security

C. Ensure the normal operation of the network

D. Improve network efficiency

Answer: ABCD

3. (Multiple choice question) Which of the following behaviors may increase internet security risks?

A. Using weak passwords

B. Click on unknown links at will

C. Regularly update software and operating systems

D. Not using antivirus software

Answer: ABD

4. (Multiple choice question) What are the possible forms of harm that may be caused during online activities

A. Infringement of personal privacy and online pornography

B. Internet addiction

C. Harmful information dissemination

D. Online job seeking and online dating traps

Correct answer: ABCD

5. (Single choice question) A friend's WeChat suddenly sent a link asking you to help him vote. The most reasonable way is to.

A. Open directly

B. Not participating in any online voting

C. Copy to computer and open again

D. Confirm the authenticity with friends and then decide whether to vote at your discretion

Answer: D

6. (Single choice question) Closing the automatic connection function of WIFI can prevent _____.

A. All malicious attacks

B. Counterfeit hotspot attacks

C. Malicious code

D. Virus attack

Answer: B

7. (Multiple choice question) Nowadays, smart devices can directly collect corresponding body information, such as the smart wristbands we wear to collect personal health data. Which of the following behaviors may cause personal information leakage?

A. Lending the wristband to others

B. Accessing unfamiliar networks

C. The battery level of the wristband is low

D. Share path information during running

Answer: ABD

8. What is the importance of regularly backing up network information and data?

A. Save storage space

B. Facilitate data sharing

C. Prevent data loss

D. Improve network speed

Answer: C **(Other questions can be found in the appendix)**

Corresponding to Research Objective3:

Implementation and validation of the model. Divided into two steps, the first step is to apply the internet security literacy improvement model, implement the improvement model on a group of student samples, and verify the implementation effect of the model by comparing and analyzing the scores of student tests before and after. The second step is to invite experts to evaluate the model.

Step 1: Select 28 students from one class of Big Data Enterprise Management at Guangxi Agricultural Vocational and Technical University for training. Conduct a pre-test before the start of five training topics and a post -test after each training session. After the entire training session, conduct a comprehensive test. The specific score data is as follows:

Table 4.16 Record of Student Pre - and Post Test Scores

(n=28)

Student ID	Topic 1		Topic2		Topic3		Topic 4		Topic5		Comprehensive test scores
	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	
1	85	90	60	75	65	75	85	90	80	90	75
2	60	80	90	95	65	75	60	75	65	75	85
3	60	75	80	90	70	90	80	95	60	75	85
4	70	80	75	80	50	85	80	95	90	95	80
5	90	95	80	85	65	75	60	80	70	90	90
6	80	90	80	95	75	80	75	80	80	85	90
7	65	75	65	75	85	90	80	85	50	85	75
8	70	90	80	90	80	95	90	95	85	90	85
9	80	95	90	90	75	80	70	80	80	90	95
10	75	80	60	80	50	70	65	70	75	80	85
11	80	85	90	95	65	70	80	90	80	85	75
12	85	90	60	75	65	70	70	80	65	75	85
13	90	95	80	90	75	80	70	80	85	90	90
14	50	80	65	70	80	95	55	70	65	70	85
15	75	80	75	80	65	70	65	65	65	75	80

Table 4.16 (Continued)

(n=28)

Student ID	Topic 1		Topic2		Topic3		Topic 4		Topic5		Comprehensive test scores
	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	Pre test scores	Post test scores	
16	50	85	70	80	90	95	80	90	80	95	70
17	60	65	75	80	85	90	80	85	75	80	95
18	80	95	60	65	85	90	80	90	80	95	75
19	65	75	80	85	50	80	90	90	65	75	70
20	80	90	60	80	85	90	90	95	60	65	90
21	90	95	85	90	60	80	65	75	90	95	95
22	65	75	65	75	70	80	80	95	85	90	85
23	85	90	80	95	85	90	70	90	55	70	85
24	80	90	80	90	85	90	80	95	80	95	90
25	65	65	75	80	50	85	75	80	65	75	90
26	80	90	90	95	85	90	90	95	70	80	80
27	60	75	80	85	80	95	80	95	85	90	90
28	80	95	70	90	90	90	60	75	60	80	95

As can be seen from the analysis of Table 4.17, the highest score in the pre-test is 90 and the highest score in the post-test is 95, The highest score in the post-test was higher than that in the pre-test, indicating that students' performance had improved significantly in the post-test. In the lowest score section: the lowest score in the pre-test 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 pre-test, indicating that the performance of all students has improved, and at least no students have scored below 70. In the average score: the average score of the pre-test is 73, and the average score of the post-test is 84. The average score of the post-test is higher than that of the pre-test, indicating that the overall performance of the students has been significantly improved. In terms of standard deviation: the standard deviation of the pre-test is 10.8, and the standard deviation of the post-test is 8.4, which measures the degree of dispersion of the data.

The standard deviation of the post-test is smaller than that of the pre-test, indicating that the score distribution of students in the post-test is more concentrated, that is, students' performance is more consistent. In terms of the number of qualified students (more than 70 points): the number of qualified students in the pre-test is 17, and the number of qualified students in the post-test is 28. The number of qualified students in the post-test is more than that in the pre-test, indicating that more students have reached the qualification standard in the post-test. In terms of the number of outstanding students (above 90 points): the number of outstanding students in the pre-test is 1, and the number of outstanding students in the post-test is 12. The number of outstanding students in the post-test is significantly increased than that in the pre-test, indicating that more students have achieved excellent results in the post-test.

Table 4.17 Student Pre - and Post Test Score Analysis Table

(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 Persons	1 Persons
Post Test	95	70	84	8.4	28 Persons	12 Persons

To sum up, it can be seen from the statistical data of students' internet security literacy test results that the overall performance of middle school students in the post-test has been significantly improved, not only the average score and the number of qualified students has increased, but also the number of excellent students has also increased significantly, and the score distribution of students has become more concentrated. This means that the introduction of the training model in this study has a positive impact on the improvement of students' cybersecurity literacy.

Step 2, invite experts to evaluate the model. Invite experts to evaluate the model. 5 experts with more than 15 years of work experience were invited to conduct CIPP evaluation of the model using the expert evaluation method.

Table 4.18 Results of Expert Assessment

(n=5)

	1	2	3	4	5
C—Context Evaluation	✔	✔	✔	✔	✔
I—Input Evaluation	✔	✔	✔	✔	✔
P—Process Evaluation	✔	✔	✔	✔	✔
P—Product Evaluation	✔	✔	✔	✔	✔

Basic information of experts: Among the 5 experts, there are 4 males and 1 female. The highest level of work experience is 25 years, while the lowest level is 15 years. And each expert gave positive feedback in four aspects: Context, Input, Process, and Product (using“ ✔ ” Represents.

The first point is that Context Evaluation focuses on the background, objectives, resources, and environment of the project, and all five experts agree with the model used in this study.

The second point is that Input Evaluation involves the resources, personnel, time, and other inputs used in the project, and all five experts agree with the model used in this study.

The third point is that Process Evaluation evaluates the implementation process, methods, management, and communication of the project, and all five experts agree with the model used in this study.

The fourth point is that Product Evaluation evaluates the results, output, impact, and value of the project, and all five experts agree with the model used in this study.

Since the five experts have given positive evaluations in all aspects of CIPP evaluation, it indicates 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.

In summary, it is important to note that while expert assessment provides valuable insights, it is still subjective and can be influenced by the expert's personal experience and biases. Therefore, in addition to expert evaluation, it is also necessary to evaluate the effectiveness and practicability of the model application more comprehensively based on the problems encountered in the application of the model and the feedback of students in the process of pre- and post-test experiments, so as to continuously adjust and improve the content of the internet security literacy improvement model.

Chapter 5

Conclusion Discussion and Recommendations

This study aims to enhance the internet security literacy of college students. The objectives of this study include: 1) to investigate the current situation of internet security literacy among college students in Guangxi, China; 2) to construct a model for enhancing the internet security literacy of college students; and 3) to evaluate the model for enhancing the internet security literacy of college students. The internet security literacy of college students includes five aspects, namely: 1) possessing awareness of internet security; 2) The ability to master internet security knowledge; 3) The ability to prevent and respond to internet security risks; 4) Standardize the ethical behavior ability of internet security; 5) Establish the ability to ensure online psychological security. The sample for this study is college students from Guangxi universities and experts in the field of internet security in Guangxi universities. The tools used in this study include the Survey Questionnaire on the Current Situation of College Students' internet security Literacy and the Evaluation Form for the Improvement Model of College Students' internet security Literacy. The methods used in this study include expert investigation, Delphi method, pre - and post test experiments, and expert evaluation. The conclusions, discussions, and recommendations of this study are as follows:

Conclusion

The researchers divided the conclusions into three parts based on the research objectives:

Objective 1: Conclusion on the Current Situation of internet Security Literacy among College Students in Guangxi

Using expert survey method to analyze the current situation of internet security literacy among college students in Guangxi, the following conclusions are drawn: there are still some problems in the overall internet security literacy of college students in Guangxi. 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 in maintaining internet security, and insufficient psychological adjustment ability in dealing with internet security are generally at a lower than average level and require further improvement.

Objective 2: Conclusion on the Model of Improving the internet security Literacy of Guangxi University Students

1. There is insufficient training on enhancing the internet security literacy of college students, and there is no specialized model established to adapt to the group of college students in enhancing internet security literacy. The training content coverage is insufficient, the training methods lack flexibility, and there is a lack of experiential training that deviates from the needs and laws of college students. It is necessary to establish a systematic and scientific training model that is suitable for college students to enhance their internet security literacy.

2. The above suggestions have established a foundation for the next step of building a model to enhance the internet security literacy of college students. Building a training model that revolves around five dimensions of internet security literacy, combines online and offline, and has been validated by experts in this field, can better enhance the internet security literacy of college students.

Objective 3: Conclusion on the Implementation and Evaluation of the internet Security Literacy Enhancement Model for College Students.

The results of the pre - and post test experiments indicate that the training mode of this study has a good effect on improving the internet security literacy of college students. The overall performance of middle school students in the post test showed a significant improvement, 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 became 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.

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

Discussion

In research objective 1 process of the current status of internet security literacy among college students, the following results were found and discussed:

1. Regarding internet security literacy, this study believes that internet security literacy includes five aspects: 1) having awareness of internet security; 2) The ability to master internet security knowledge; 3) The ability to prevent and respond to internet security risks; 4) Standardize the ethical behavior ability of internet security; 5) The ability to establish internet psychological security is consistent with Luo Li's (2012) research, which proposed that national information security literacy refers to the understanding of information security and various comprehensive abilities exhibited by citizens in an informationized and internet environment, including information security awareness, information security knowledge, information ethics and ethics, and information security capabilities. A national information security literacy evaluation index system has been established. This indicator system takes four elements of information security awareness, information security knowledge, information legal ethics, and information security capabilities as the consistent criteria layer. The difference is that this study has added a section on internet security psychological ability. Internet security psychology mainly focuses on the impact of internet security on individual psychological states, including but not limited to personal privacy leakage, online violence, and internet addiction.

2. The internet security literacy of college students in Guangxi needs to be improved. There are still 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 in maintaining internet security, and insufficient psychological adjustment ability in dealing with

internet security. Overall, the level is below average and needs further improvement. This is consistent with the research proposed by Que Fengyi (2022), which found that the internet security literacy of college students is at a moderate level through investigation. 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 network violations.

3. From the perspective of research methods on the current status of internet security literacy among college students, most scholars adopt the form of questionnaire surveys to study the current status of internet security literacy among college students, using college students as samples, internet security literacy among college students as independent variables, and combining relevant factors as independent variables. The inconsistency with this study lies in the use of literature review and expert survey methods. By using experts in the field of internet security as survey subjects, it can more scientifically reveal the characteristics and shortcomings of college students' internet security literacy, which helps to formulate targeted improvement strategies

In the construction process of the internet security literacy model for college students in research objective 2, the following results were found and discussed:

1. There is insufficient training on enhancing the internet security literacy of college students, and there is no specialized model established to adapt to the group of college students in enhancing internet security literacy. The training content coverage is insufficient, the training methods lack flexibility, and there is a lack of experiential training that deviates from the needs and laws of college students. It is necessary to establish a systematic and scientific training model that is suitable for college students to enhance their internet security literacy. This is in line with Wang Guangli's (2020) proposal that the cultivation of internet security awareness among contemporary college students has achieved fruitful results. However, at present, there are also problems such as insufficient effectiveness in university cultivation, weak awareness of internet security among college students, limited homework for family education and cultivation, and low utilization of social resources. The reasons

for these problems are analyzed to be incomplete cultivation and management of universities, lack of self-awareness among college students, lack of family education and peer assistance, and incomplete management of the network environment. The main reasons proposed by Yao Ying (2021) are consistent with the views that the education subject does not attach enough importance to it, the education object lacks strong awareness of internet security, the education content lacks specificity, the education form is single, and the education technology support is insufficient.

2. The model for improving the internet security literacy of college students constructed in this study is divided into two parts. The first part is based on literature review and the existing problems in the research status, focusing on five themes: awareness, knowledge, skills, ethics, and psychology. The second part designs the entire training from five aspects: training content, training methods, training materials and tools, training time, and training evaluation. By using the Delphi method to collect expert opinions in three rounds, suggestions can be collected more scientifically, making the training model more accurate and reasonable. This is in line with Yang Lu's (2021) proposal to study strategies to strengthen internet security education for college students from three aspects: environment, individuals, and universities. The first is to improve the education and teaching environment. In the network, some internet security events can be displayed to students by means of online education public service videos, official account and other mobile devices; The second is that college students should have the ability to identify all kinds of false and negative content in the network. At the same time, they should also be able to surf the Internet in moderation and be good at using Internet technology to obtain useful learning information. In terms of internet security education content in universities, practical teaching can be promoted through classroom teaching, college competitions, themed class meetings, and special lectures, guided by real-life scenarios. When designing the teaching of internet security awareness education, we should fully consider the diversity and personalized differences of the educational objects, as stated by Yu Kun (2023). One is the combination of online and offline, with virtual simulation projects being logged in through the web in a one-stop manner, allowing for flexible and autonomous implementation of a teaching mode

that combines online and offline. The second is to combine in class and extracurricular activities, utilizing the internet security awareness education modules in the virtual simulation experiment project to enable students to engage in independent learning outside of class based on their own differences. The third is to combine teaching and assessment, combining process assessment with outcome assessment. The fourth is to combine promotion and competition, utilizing virtual simulation experiment project resources to organize training, peer communication, online and offline competitions, award promotion and other activities, and combining various methods to improve students' professional abilities and professional qualities. The entire process is reported through campus network news. Many scholars have conducted research on improving safety awareness and strengthening safety thinking, and some have emphasized the importance of combining theory and practice in the education process. However, research on practical methods, content, and effects is not sufficient. Therefore, unlike this, this study tends to focus on improving education and teaching methods to enhance internet security literacy. By establishing a scientifically effective training program that emphasizes experiential training, it constitutes a model for enhancing the internet security literacy of college students.

In the process of evaluating the internet security literacy model of college students in research objective 3, the following results were found and discussed:

Regarding how to evaluate the improvement model of college students' literacy, different scholars have selected different methods based on research practice. The most commonly used methods include the Kirkpatrick four level training evaluation model, Delphi method, expert evaluation method, and pre - and post test experimental method. For example, Zhang Wen (2022) took the compatibility between the CIPP model and the ideological and political education evaluation system as the starting point, embedded the CIPP model in the ideological and political education evaluation system, and constructed an ideological and political education evaluation system with "background input process results" as the indicator. Liu Xiaoping (2023) selected two classes of the same grade and major from a public security college as the experimental group and control group. Positive psychological

intervention was integrated into the teaching design of the experimental group, while no intervention was observed in the control group. The measurement results of the experimental group and the control group using the PERMA Happiness Index Scale and the Depression Anxiety Stress Self Rating Scale indicate that incorporating positive psychological concepts, theories, and application technologies into the mental health education of college students in public security colleges can improve their positive character and happiness index.

Based on the actual situation of this study, this article adopts the CIPP principle and selects the expert evaluation method and pre - and post test experiments to evaluate the improvement model of internet security literacy of Guangxi university students. These two methods have stronger applicability in the field of internet security literacy of Guangxi university students. Experts have given positive evaluations in all aspects of CIPP evaluation, indicating that the model is considered effective and appropriate in terms of background, input, process, and product. The design and implementation of the model have been recognized by experts. It should be noted that although expert evaluations provide valuable insights, they are still subjective and may be influenced by the expert's personal experience and biases. Therefore, in addition to expert evaluation, it is also necessary to combine the problems encountered during the model application process and the feedback from students during the pre - and post test experiments. From the statistical data provided on the scores of student internet security literacy tests, it can be seen that the overall performance of students in the post test has significantly improved. Not only has the average score and the number of qualified students increased, but the number of outstanding students has also increased significantly. At the same time, the distribution of student scores is 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.

Recommendations

1. Promote and apply the internet security literacy improvement model among college students.

At present, there is a lack of training model to improve internet security literacy among college students. The model verified and evaluated in this study is scientific and practical, which can be widely promoted and applied among college students, and has reference significance for colleges and universities to enhance students' internet security awareness, knowledge, skills and ability to deal with internet threats.

2. The training content and methods on internet security should keep up with the times.

Nowadays, society is undergoing rapid changes, and testing needs to be constantly adjusted. The teaching content should be continuously adjusted according to the updates of internet security knowledge. The teaching methods will be constantly adjusted over time. In the teaching process, in order to achieve better teaching results, training methods will be continuously adjusted according to the teaching time.

3. Strengthen the construction of internet security teaching staff and improve the quality of training.

Choose experts with rich internet security practices and teaching experience as trainers to ensure the accuracy and practicality of training content. Strengthening the construction of the education team can increase training for teachers, parents, and relevant social organizations or institutions, increase the introduction of professional and technical education talents in internet security, improve the overall level of internet security knowledge of the education team, and provide a high-level and strong professional education team for the smooth implementation of youth internet security education.

4. Strengthen cooperation between schools and relevant government departments and enterprises.

Actively seeking internet construction partners, such as telecommunications and mobile companies, to utilize the technological advantages of enterprises to assist the operation of campus internet security universities. Internet telecommunications companies and internet security companies have more advantages in technology and prevention experience, but lack a platform for communication and joint cultivation with universities. Internet security technology experts and legal experts can be invited to schools for training, introducing cutting-edge internet security protection knowledge and technology, enriching teaching resources, or organizing students to visit relevant departments of enterprises to enhance their practical abilities in internet security.

Future Researches

Through the research work of this project, I have gained a deep understanding of the current situation of internet security literacy among college students in Guangxi. I have proposed an improvement model for internet security literacy among college students in Guangxi from five aspects: awareness, knowledge, skills, ethics, and psychology. The model has been applied for evaluation.

The benefits of this research application are: 1) improving personal internet security prevention capabilities. It helps to enhance the awareness of internet security among college students. Through learning and practice, college students can master methods and skills to protect personal information and property security, effectively avoiding becoming victims of cybercrime. 2) Promote the development of a healthy online environment. The improvement of internet security literacy helps college students establish correct values and moral values in the cyberspace, reducing the occurrence of negative behaviors such as online violence and rumors. 3) Provide important reference basis for the government and relevant institutions to formulate internet security policies and regulations.

The limitation of this study is that: 1) Research on internet security literacy often uses methods such as questionnaire surveys and interviews to collect data. Although these methods can obtain certain information, they may have issues such as strong subjectivity and insufficient sample representativeness. 2) The complexity and variability of network environment and the internet security issues faced by college students in actual learning and life may also make it difficult for research results to fully reflect the actual situation. 3) Due to limitations in time, resources, and other aspects, some research may be difficult to effectively apply and promote in practice in the short term, requiring long-term education and practice, constantly updating and improving response strategies and methods.

In summary, we will continue to conduct in-depth research on the updates and applications of internet security technology in the future. With the continuous development of network technology, future research will need to focus on the updates and responses of emerging internet security technologies, such as the impact of AI application in education on college students' internet security literacy, and the application of artificial intelligence in network attack and defense. We will build a scientific and systematic innovative internet security course training system to enhance the interactivity and effectiveness of college students' internet security education. To provide support for the development of internet security in the field of national education, and to provide reference for the improvement of internet security literacy in universities in Guangxi.

References

Chen Qi, Xiong Huixiang, Dai Qinquan & Gu Jiay. (2022). Research on the evaluation and promotion strategy of college students' internet information security literacy ability under the platform society. **Library and Information work** (07), 75-87.

GLi & Liu Zeyuan. (2014). Research on the evaluation index system of college entrepreneurship education ability based on CIPP. **Journal of Northeastern University** (Social Science Edition) (04), 377-382.

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

Gao Donghuai, CAI Hua, Dong Lipeng, Shen Xiajuan & Xu Weizhong. (2013). Design of students' internet information security literacy evaluation scale. **Chinese Medical Education Technology** (02), 173-177.

Huang Hang & Wei Mingyao. (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.

Jin-bo wang. (2012). The enlightenment of ke's four-level training evaluation mode to the evaluation of dry teaching training in China. **Journal of Beijing Petroleum Management Cadre Institute** (01), 78-80.

Liu Feng. (2010). Analysis and formation of college students' information security literacy. *Computer Education* (21), 77-80.

Li Rui, Pan Limin, Hao Jingwei, Zhang Hanqing, Luo Lin Lin & Wu Qian. (2020). High accuracy of internet security awareness of individual assessment and group index construction method. **Journal of Beijing Institute of Technology** (09), 1002-1008.

Luo Yi.(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 Enjin. (2014). Application of Ke's four-level training evaluation model in enterprise training. **Metallurgical Education in China** (02), 63-67.

Li jiang. (2022). Exploring the education path of the overall national security concept based on the platform of "easy class". **Modern vocational Education** *(*28), 19-21.

Qi Bin, Zou Hongxia, Wang Yu & Li Jixing. (2019). Adaptive testing technology of internet security awareness based on IRT. **Journal of Beijing University of Technology** (05), 436-443.

Que feng yi.(2022). **Evaluation Index System and Applied Research of College Students in the Era of Big Data** (Master's dissertation, Wuhan University of Engineering).

Wang Jianhui & Zhang Bei. (2016). Investigation report on college students' awareness of internet information security. **Technology wind** (12), 64-65.

Wang Guangli. (2020). **Research on the cultivation path of internet security awareness among contemporary college students** (master's dissertation, Changsha University of Science and Technology).

Wang Rui. (2020). **Research on influencing factors and promotion strategies of youth groups in Linfen City** (master's thesis, Shanxi Normal University).

Wear sweet. (2020). **Research on the influencing factors of youth internet security subjectivity from the perspective of internet Literacy Education** (Master's dissertation, Jinan University).

Wu Lizhi & Wu Tiantian. (2014). **Based on Delphi method.** Open Education Research (05), 91-101.

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

Wang Ke, Wang Jian & Xiang Biao. (2022). Research on the construction of information literacy evaluation index system of PE graduate students in the New Era. **Journal of Wuhan Institute of Physical Education** (03), 93-100.

Xu Xiangyun & Wang Jiajia. (2022). A theoretical framework based on the CIPP evaluation model. **College Education Management** (01), 47-60.

Xu Fu yong, Shen Jian, Li Jianying. (2005). **Research on the comprehensive evaluation method of internet security based on Delphi and ANN**. Microcomputer development (10), 11-13 + 15.

Yao Ying. (2021). **Research on Youth internet Security Education in the New Era** (Master's dissertation, Southwestern University of Finance and Economics)

Yang Lu. (2021). **Research on internet Security Education for College Students in the Era of Mobile Internet** (Master's dissertation, Xi' an University of Technology)

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

Zhang Wen. (2022). Research on innovative evaluation system of ideological and political Teaching based on CIPP mode. **Journal of Hubei Normal University** (Philosophy and Social Sciences Edition) (01), 117-122.

Zhang Qing. (2022). **Research on the current situation of digital civic literacy and educational Countermeasures** (Master's dissertation, Jiangsu University).

Appendix

Appendix A

List of Specialists and Letters of specialists Invitation for IOC Verification

Expert information on participating in IOC Test					
No.	**Expert Name**	**Experience (years)**	**Positional titles**	**School**	**education**
1	Luo Yunfang	17	professor	Guangxi Vocational and Technical College	doctor
2	E Erjiang	11	associate professor	Guangxi Minzu University	doctor
3	Li Yuanli	15	associate professor	Guangxi Vocational University of Agriculture	master
4	Xie Gang	11	senior eng	Guangxi Polytechnic of Construction	master
5	Wu Dingwei	20	professor	Guangxi University of Finance and Economics	master

Ref.No. MHESI 0643.14/๑๗๑

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Invitation to validate research instrument

Dear Associate Professor Li Yuanli, Guangxi Vocational University of Agriculture

Mrs.Long Yifei is a graduate student in Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is undertaking research entitled " Internet Security Literacy Enhancements Model for College Student in Guangxi "

The thesis advisory committee has considered that you are an expert in this topic. Your recommendations would be useful for further improvement of this research instrument.

With your expertise, we would like to ask your permission to validate the attached research instrument. In this regard, we would like to avail ourselves of this opportunity to express our sincere thanks and appreciation for your help.

Yours faithfully,

Assistant Professor Akaranun Asvarutpokin
(Vice Dean of Graduate School for Dean of Graduate School)

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Appendix B

Official Letter

Ref.No. MHESI 0643.14/ ๑๙๒

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Request for Cooperation in Data Collection

Dear Guangxi Vocational University of Agriculture

This is to certify that Mrs.Long Yifei is a Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is conducting research entitled "Internet Security Literacy Enhancements Model for College Student in Guangxi" under the supervision of Associate Professor Dr. Sombat Teekasap as major advisor and Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama as co-advisor her contact information is as follows: telephone number 13877151316, email longyifei12345@qq.com

In this regard, the student researcher has to collect data from Teachers and College Students in Guangxi Universities using questionnaire and interview . The students will subsequently coordinate with you and provide more detail on this matter.

Accordingly, I would like to kindly request for your permission to allow this student researcher to collect data for academic purposes. Your cooperation will be highly appreciated.

Yours sincerely,

(Assistant Professor Akaranun Asavarutpokin)
Vice Dean of Graduate School

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Ref.No. MHESI 0643.14/ ๙๕๖

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Request for Cooperation in Data Collection

Dear Guangxi Minzu University

This is to certify that Mrs.Long Yifei is a Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is conducting research entitled "Internet Security Literacy Enhancements Model for College Student in Guangxi" under the supervision of Associate Professor Dr. Sombat Teekasap as major advisor and Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama as co-advisor her contact information is as follows: telephone number 13877151316, email longyifei12345@qq.com

In this regard, the student researcher has to collect data from Teachers and College Students in Guangxi Universities using questionnaire and interview . The students will subsequently coordinate with you and provide more detail on this matter.

Accordingly, I would like to kindly request for your permission to allow this student researcher to collect data for academic purposes. Your cooperation will be highly appreciated.

Yours sincerely,

(Assistant Professor Akaranun Asavarutpokin)
Vice Dean of Graduate School

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Ref.No. MHESI 0643.14/ 994

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Request for Cooperation in Data Collection

Dear Guangxi Polytechnic of Construction

This is to certify that Mrs.Long Yifei is a Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is conducting research entitled "Internet Security Literacy Enhancements Model for College Student in Guangxi" under the supervision of Associate Professor Dr. Sombat Teekasap as major advisor and Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama as co-advisor her contact information is as follows: telephone number 13877151316, email longyifei12345@qq.com

In this regard, the student researcher has to collect data from Teachers and College Students in Guangxi Universities using questionnaire and interview . The students will subsequently coordinate with you and provide more detail on this matter.

Accordingly, I would like to kindly request for your permission to allow this student researcher to collect data for academic purposes. Your cooperation will be highly appreciated.

Yours sincerely,

(Assistant Professor Akaranun Asavarutpokin)
Vice Dean of Graduate School

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Ref.No. MHESI 0643.14/๑๙๕

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Request for Cooperation in Data Collection

Dear Guangxi University of Science and Technology

This is to certify that Mrs.Long Yifei is a Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is conducting research entitled "Internet Security Literacy Enhancements Model for College Student in Guangxi" under the supervision of Associate Professor Dr. Sombat Teekasap as major advisor and Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama as co-advisor her contact information is as follows: telephone number 13877151316, email longyifei12345@qq.com

In this regard, the student researcher has to collect data from Teachers and College Students in Guangxi Universities using questionnaire and interview . The students will subsequently coordinate with you and provide more detail on this matter.

Accordingly, I would like to kindly request for your permission to allow this student researcher to collect data for academic purposes. Your cooperation will be highly appreciated.

Yours sincerely,

(Assistant Professor Akaranun Asavarutpokin)
Vice Dean of Graduate School

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Ref.No. MHESI 0643.14/ ๙๔

Bansomdejchaopraya Rajabhat University
1061 Itsaraparb Hirunrujee
Thonburi Bangkok 10600

29 March 2024

Subject: Request for Cooperation in Data Collection

Dear Guilin University of Technology

This is to certify that Mrs.Long Yifei is a Doctor of Philosophy Program in Digital Technology Management for Education of Bansomdejchaopraya Rajabhat University. She is conducting research entitled "Internet Security Literacy Enhancements Model for College Student in Guangxi" under the supervision of Associate Professor Dr. Sombat Teekasap as major advisor and Dr.Nainapas Injoungjirakit and Assistant Professor Dr.Prapai Sridama as co-advisor her contact information is as follows: telephone number 13877151316, email longyifei12345@qq.com

In this regard, the student researcher has to collect data from Teachers and College Students in Guangxi Universities using questionnaire and interview . The students will subsequently coordinate with you and provide more detail on this matter.

Accordingly, I would like to kindly request for your permission to allow this student researcher to collect data for academic purposes. Your cooperation will be highly appreciated.

Yours sincerely,

(Assistant Professor Akaranun Asavarutpokin)
Vice Dean of Graduate School

Bansomdejchaopraya Rajabhat University
Tel.+662-473-7000
www.bsru.ac.th
E-mail: grad@bsru.ac.th

Appendix C

Research Instruments

The current status of college students' internet security literacy expert questionnaire

shalom! In order to comprehensively investigate the current situation of college students' internet security literacy, we carried out this expert survey, the data obtained data is only used for statistical analysis, absolutely confidential, please answer according to your actual situation. Sincerely thank you for your strong support and cooperation! The survey of the Current Situation of College Students' Internet Security Literacy is divided into three parts:

Part 1: Basic information of the interviewees

1. Your name:_____.
2. Your working years:_____year.
3. Your highest academic level:_____.
4. Your professional title or position:_____.
5. Your work unit:_____.

Part 2: the current situation investigation of college students' internet security literacy

College students' internet security literacy status survey is divided into consciousness, knowledge, skills, morality, psychological five aspects, please combine you judge "yes", "no" or "not sure" and choose the corresponding options, if the answer "not" or "uncertain", please according to the previous work experience simple reason or advice.

question	Yes	No	Not sure	Suggestions and reasons (answer No or Not sure)
1. Awareness: Have and enhance internet security awareness				
1.1 College students do not pay attention to the protection of personal network identity information				
1.2 College students do not pay attention to the protection of personal network activity information				
1.3 College students lack the awareness of regular backup of information and materials				
1.4 College students lack the awareness of preventing online fraud				
1.5 College students lack the awareness of preventing non-performing online loans				
Add to the problems in this part:				

question	Yes	No	Not sure	Suggestions and reasons (answer No or Not sure)
2. Knowledge: the ability to learn and master internet security knowledge				
2.1 College students lack of understanding of internet security laws and regulations such as the internet security Law and the Personal Information Protection Law				
2.2 College students lack of understanding of basic knowledge such as the concept of internet security				
2.3 College students do not understand how to protect their rights after encountering internet security problems				
2.4 College students' initiative to learn and understand internet security knowledge is not strong				
2.5 College students have a single way to learn and master internet security knowledge, and the learning effect is poor				
Add to the problems in this part:				

question	Yes	No	Not sure	Suggestions and reasons (answer No or Not sure)
3. Skills: the ability to prevent and respond to cybersecurity risks				
3.1 College students need to improve their firewall configuration and use skills				
3.2 College students need to improve the configuration and use skills of anti-virus software				
3.3 College students need to improve their skills to prevent network telecom fraud				
3.4 College students have the problem of random links to public networks				
3.5 College students do not pay attention to software permission management and privacy protection				
3.6 College students do not pay attention to the security of the electronic payment environment				
Add to the problems in this part:				
4. Morality: the ability to regulate and maintain internet security ethics				
4.1 College students' sense of responsibility for maintaining internet security needs to be improved				

question	Yes	No	Not sure	Suggestions and reasons (answer No or Not sure)
4.2 College students who publish or forward false information without confirmation				
4.3 College students lack the awareness of online intellectual property protection, such as using pirated software and not identifying copyright				
4.4 College students participate in online gambling, part-time brushing orders, browsing bad websites and other network anomie behaviors				
Add to the problems in this part:				
5. Psychology: cultivate and develop the ability of network psychological security				
5.1 College students are addicted to Internet addiction such as online games and mobile phone separation anxiety				
5.2 College students will cause psychological problems due to internet security incidents such as network violence and network fraud				
5.3 College students lack the ability to self, regulate and intervene when				

question	Yes	No	Not sure	Suggestions and reasons (answer No or Not sure)
they encounter psychological problems of internet security				
5.4 College students lack the ability to seek professional counseling and help when encountering psychological problems of internet security				
Add to the problems in this part:				

Part 3: the survey on improving college students' internet security literacy

1. What are the ways for schools to conduct internet security education? (multiple choice)

A. Classroom learning B. expert talks C. Online and offline publicity

D. Simulation drills and practical activities E. other

2. What do you think are the deficiencies in internet security education in schools? (multiple choice)

A. Overall lack of attention to

B. The teaching content is not comprehensive and thorough

C. The teaching form is relatively simple D. Teaching resources are not rich enough

E. other

3. What kind of training methods do you think can better improve the internet security literacy of college students?

College students' internet security literacy test questions

The following is a set of internet security literacy, test questions, from the awareness, knowledge, skills, moral, psychological test:

Internet security awareness article

1. (Multiple choice) Which of the following options are likely to cause our personal information illegally stolen?

A. Discard express orders or packages at will

B . Share your location, address, birthday, and other information on social internets

C . Computer and mobile phone do not set the lock screen password

D . Update the passwords of the various platforms regularly

answer: ABC

2. (Multiple choice) What is the importance of internet security awareness for individuals and society?

A. Prevent personal information leakage

B. Safeguarding national information security

C. Ensure the normal operation of the network

D. Improve the efficiency of network use

answer: ABCD

3. (Multiple choice) Which of the following behaviors may increase the internet security risks?

A. Use weak passwords

B. Click on the unknown link at will

C. Regularly update the software and the operating system

D. Do not use antivirus software

answer: ABD

4. (Multiple choice) The form of damage caused in internet activities is ()

A. Violation of personal privacy and Internet pornography

B. internet addiction

C. Dissemination of harmful information

D. internet job hunting, online love trap

answer: ABCD

5. (Multiple choice) A friend's we chat suddenly sent a link to help him vote, the most reasonable way to do is.

A. Open directly

B. Do not participate in any online voting

C. Copy it to the computer and then open it on

D. Confirm the authenticity with your friends, and then decide whether to vote

answer: D

6. (Multiple choice) Turn off the automatic connection function of WIFI can prevent .

A. All malicious attacks

B. Fake hot spot attack

C. Malicious code

D. The virus attack

answer: B

7.(Multiple choice) Now, smart devices can directly collect the corresponding information about the body, such as the smart bracelet we wear to collect personal health data. Which of the following behaviors may cause personal information disclosure?

A . Lend the bracelet to others

B . Access to unfamiliar internets

C . The power of the bracelet is low

D . Share the path information during a run

answer: ABD

8.What is the importance of regular backup of internet information?

A. Save storage space

B. Easy data sharing

C. Prevent data loss

D. Improve internet speed

answer: C

Internet security knowledge article

1. (Multiple choice) What is the main function of the firewall?

A. Filter internet traffic

B. Store internet data

C. Accelerated internet access

D. Backup system files

answer: A

2.(Multiple choice) Which internet security technology can be used to verify user identity?

A. firewall

B. intrusion detection system

C. Biometrics

D. data encryption

answer: C

3. (Multiple choice) () refers to the defects existing in the specific implementation of hardware, software, protocol or system security strategy, with which the attacker can access or destroy the system without authorization.

A. patch

B. upgrade

C. leak

D. hacker

answers: C

4. (Multiple choice) Remote and local administrator permissions should correspond to ( )

A. elementary

B. middle rank

C. senior

D. middle and high ranking

answers: C

5. (Multiple choice) Online shopping fraud case has the following several expression forms ( )

A. Multiple remittances

B. fake links and fake web pages

C. Refuse to pay for the safe payment method

D. collect the deposit to cheat money, shoddy

answer: ABCD

6. (Multiple choice) internet security vulnerabilities can be roughly divided into the following categories of ( )

A. Classification according to the discovery time of vulnerabilities

B. Classification according to the cause of the vulnerability

C. Classification according to the severity of the vulnerability

D. According to the threat caused by the vulnerability

answer: ABCD

7. (Single choice) When encountering internet security problems, which of the following rights protection methods is correct?

A. Immediately remove the relevant evidence and stop using the affected equipment

B. Talk privately to the hackers and pay a ransom to recover the data

C. Immediately report to the local public security organ and provide relevant evidence

D. Search for the solution on the Internet and try to fix it

answer: C

Internet security skills section

1. (Multiple choice) How to identify whether an email is a phishing email?

A. Check if the sender's address is true

B. Click on the link in the email right now

C. Ignore all emails from strangers

D. Delete all messages directly

answer: A

2. (Multiple choice) Which of the following measures is not recommended when setting up internet security policies?(single selection)

A. Limits unnecessary internet ports

B. Allow all external access

C. Regularly update the security patches

D. Use a strong password policy

answer: B

3. (Multiple choice) The way to do the data backup well does not include ( )

A. Copy the important data on the u disk

B. Record the important data on the CD

C. Upload important data to cyberspace for backup through FTP

D. Put the important data on the computer desktop

answers: D

4. (Single choice) Which one does not belong to the way to avoid the internet trap and prevent the internet fraud?

A. do not easily meet with netizens

B. When browsing the web, choose a legal large portal and not easily believe the winning information on the Internet

C. easily believe the Internet unknown test of personal emotional intelligence, IQ, friends and other software

answers: C

5. (Multiple choice) The following methods to prevent computer viruses and hackers are ( )

A. Install the antivirus software and upgrade it in time

B. Do not access unknown links, download and install software of unknown sources

C. Install the operating system patches in time

D. Protect important data and make good data backup

answer: ABCD

6. (Multiple choice) Which of the following specifications is required when using a public internet?

A. Share personal sensitive information on a public internet

B. Enable the file-sharing functionality for public networks

C. Protect data transfers using a VPN or encrypted connection

D. Ignore the security warnings for the public network

answer: C

Internet security ethics chapter

1. (Multiple choice) Which of the following behaviors is unethical in the network environment?

A. Respect for the privacy of others

B. Don't spread rumors

C. Malicious attack on other people's websites

D. Follow the rules of the Internet

answer: C

2. (Multiple choice) As an Internet user, how should we treat the information on the Internet?(single selection)

A. Forward unverified information at will

B. Not participating in cyberviolence

C. Maliciously tamper with the information released by others

D. Disaway the privacy of others

answer: B

3. (Multiple choice) What should we do if we browse bad information or bad comments in BBS, E-Mail and QQ when going online?

A.do not harm their own interests, do not care

B. Introduce it to other students to browse and read it

C. Read the information and participate in the comments

D. Delete, close, and report immediately

answers: D

4. (Single choice) is it not an infringement of intellectual property rights?

A. Copying away from others' papers

B. Illegal download

C. Illegal use of musical works copyright by others

D. Purchase music works of copyright enjoyed by others

answers: D

5. (Single choice) Related content of internet intellectual property protection, which of the following is correct?

A. All the information on the internet is available at will

B. As long as the source, you can copy and paste other people's articles

C. Without the permission of the copyright owner, he shall not use, copy or disseminate his works

D. Publish someone else's work on your own website without telling the original author

answer: C

6.(Single choice) To strengthen the civilized norms of behavior when using the Internet, which of the following behaviors is inappropriate?

A. Respect for the views and privacy of others

B. Do not spread unconfirmed information

C. Personal attacks and abuse on the Internet

D. Do not use insulting language or words

answer :C

Internet security psychology article

1. (single choice) When encountered internet fraud, which of the following mentality is not recommended?

A. Keep calm and call the police immediately

B. Panic, transfer money at will

C. Collect evidence and seek help

D. Remind people around you to be on guard

answer: B

2. (Single choice) How to adjust my mentality in the face of negative information on the Internet?

A. Neglect and avoid participation in the discussion

B. Immediately believe it and forward it

C. Be rational and be authentic

D. Emotional response, vent dissatisfaction

answer: C

3. (Multiple choice) Correct online mentality, make internet learning become a positive factor to help personal growth, what are the main practices?

A. Set up the internet learning goals

B. Make a study plan

C. Choose the best learning tool or select the best learning materials

D.do not indulge in the internet world

Correct answer: ABCD

4 .(Single choice) In the internet security incident, which of the following practices reflects a good psychological quality?

A. After encountering internet fraud, immediately blame yourself and fall into remorse

B. Stay calm and seek help when facing cyber threats

C. After receiving a malicious email, click the link in the email

D. When you find out your account is stolen, try to fix it yourself without reporting it

answer: B

5 .(Single choice) Students in the internet security psychological problems for help, which of the following is correct?

A. Bear it alone and try to solve problems on their own

B. Discuss it openly and seek advice on social media

C. Go to the school's cybersecurity department or psychological counseling center for help

D. Ask strangers or unreliable websites for help

answer: C

Appendix D

The Results of the Quality Analysis of Research Instruments

Evaluation Results of IOC for the current status of college students' internet security literacy expert questionnaire

Item	Experts' rating					Total	Mean	Results
	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5			
1. Awareness: Have and enhance internet security awareness								
1.1 College students do not pay attention to the protection of personal network identity information	+1	+1	+1	+1	+1	5	1.00	Valid
1.2 College students do not pay attention to the protection of personal network activity information	0	+1	+1	+1	+1	4	0.80	Valid
1.3 College students lack the awareness of regular backup of information and materials	+1	+1	+1	+1	+1	5	1.00	Valid
1.4 College students lack the awareness of preventing online fraud	+1	+1	+1	+1	+1	5	1.00	Valid
1.5 College students lack the awareness of preventing non-performing online loans	-1	+1	+1	+1	+1	3	0.60	Valid
2. Knowledge: the ability to learn and master internet security knowledge								
2.1 College students lack of understanding of internet security laws and regulations such as the internet security Law and the Personal Information Protection Law	+1	+1	+1	+1	-1	3	0.60	Valid

Item	Experts' rating					Total	Mean	Results
	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5			
2.2 College students lack of understanding of basic knowledge such as the concept of internet security	+1	+1	+1	+1	+1	5	1.00	Valid
2.3 College students do not understand how to protect their rights after encountering internet security problems	+1	+1	+1	+1	+1	5	1.00	Valid
2.4 College students' initiative to learn and understand internet security knowledge is not strong	+1	+1	+1	+1	+1	5	1.00	Valid
2.5 College students have a single way to learn and master internet security knowledge, and the learning effect is poor	+1	+1	+1	+1	+1	5	1.00	Valid
3. Skills: the ability to prevent and respond to cybersecurity risks								
3.1 College students need to improve their firewall configuration and use skills	+1	+1	+1	+1	+1	5	1.00	Valid
3.2 College students need to improve the configuration and use skills of anti-virus software	+1	+1	-1	+1	+1	3	0.60	Valid
3.3 College students need to improve their skills to prevent network telecom fraud	+1	+1	+1	+1	+1	5	1.00	Valid
3.4 College students have the problem of random links to public networks	+1	+1	+1	0	+1	4	0.80	Valid

Item	Experts' rating					Total	Mean	Results
	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5			
3.5 College students do not pay attention to software permission management and privacy protection	-1	+1	+1	+1	+1	3	0.60	Valid
3.6 College students do not pay attention to the security of the electronic payment environment	+1	0	+1	+1	+1	4	0.80	Valid
4. Morality: the ability to regulate and maintain internet security ethics								
4.1 College students' sense of responsibility for maintaining internet security needs to be improved	+1	+1	+1	+1	+1	5	1.00	Valid
4.2 College students who publish or forward false information without confirmation	-1	+1	+1	+1	+1	3	0.60	Valid
4.3 College students lack the awareness of online intellectual property protection, such as using pirated software and not identifying copyright	+1	+1	+1	+1	+1	5	1.00	Valid
4.4 College students participate in online gambling, part-time brushing orders, browsing bad websites and other network anomie behaviors	+1	+1	+1	+1	0	4	0.80	Valid

Item	Experts' rating					Total	Mean	Results
	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5			
5. Psychology: cultivate and develop the ability of network psychological security								
5.1 College students are addicted to Internet addiction such as online games and mobile phone separation anxiety	+1	+1	0	+1	+1	4	0.80	Valid
5.2 College students will cause psychological problems due to internet security incidents such as network violence and network fraud	+1	+1	+1	+1	-1	3	0.60	Valid
5.3 College students lack the ability to self, regulate and intervene when they encounter psychological problems of internet security	+1	+1	+1	+1	+1	5	1.00	Valid
5.4 College students lack the ability to seek professional counseling and help when encountering psychological problems of internet security	+1	+1	+1	+1	+1	5	1.00	Valid
The survey on improving college students' internet security literacy								
1. What are the ways for schools to conduct internet security education? (multiple choice) A. Classroom learning: B. expert talks C. Online and offline publicity	+1	+1	+1	+1	+1	5	1.00	Valid

Item	Experts' rating					Total	Mean	Results
	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5			
D. Simulation drills and practical activities E. other								
2. What do you think are the deficiencies in internet security education in schools? (multiple choice) A. Overall lack of attention to B. The teaching content is not comprehensive and thorough C. The teaching form is relatively simple D. Teaching resources are not rich enough. E. other	+1	+1	+1	+1	+1	5	1.00	Valid
3. What kind of training methods do you think can better improve the internet security literacy of college students?	0	+1	+1	+1	+1	4	0.80	Valid

Appendix F

Certificate of English

BANSOMDEJCHAOPRAYA
RAJABHAT UNIVERSITY

This is to certify that

Mrs. Long Yifei

Achieved BSRU English Proficiency Test (BSRU-TEP) level

C1

Given on 22nd August 2021

(Assistant Professor Dr Kulsirin Aphiratvoradej)
Director

Appendix F

The Document for Acceptance Research

Employment of Think Tank Times

Long Yifei comrade

Your title is **"Research on the Path of Internet Security Literacy Into College Students"** Manuscript, initially approved and arranged in 2024__Year 7_Monthly periodical issue is hereby notified. Supervisor: Shanxi Academy of Social Sciences, sponsor: Shanxi Social Science Press (domestic serial number: CN 14-1391 / D, international serial number: ISSN 20964609, postal code: 22-570).

Think tank Time Theory Department May 17,2024

Manuscript number: XP2024051647 Tel: 0351-6077457 Submission must abide by the following copyright statement:

1. The journal does not accept works that violate relevant national laws and regulations and pseudoscientific content; violate copyright or other rights due to plagiarism or confidentiality, the publication and the journal shall not bear joint liability; in order to improve the quality of the publication and maintain the serious publication of the journal

The magazine refuses plagiarism and false articles; if the article provides false materials and false content, the original author reserves the right to hold the person responsible responsible. Please do not send other journals to this manuscript, if already sent other periods

Journal, please quickly submit the name of the publication and the date of the delivery of the journal, to avoid repeated publication.

2. The views of the articles published by the journal are the views of the author and do not represent the views or positions of the journal; the journal has the right to delete or adjust the articles according to the purpose and requirements of the journal. If the author disagrees, please make a statement when submitting the articles (if not, it shall be deemed to agree to modify the articles according to the content of the article).

3. In order to meet the needs of China's information construction, realize the network of journal editing and publishing, and expand the channels of knowledge and information exchange between the journal and the author, the articles and works published in the journal shall be regarded as the authors agree to disseminate their works through the journal. If the author does not agree with the inclusion of the work, please declare to this magazine at the time of contribution.

Research Profile

Name-Surname: Long Yifei

Birthday: March 09, 1989

Place of Birth: Liuzhou , Guangxi, China

Educational Background:

- Doctor of Educational Digital Technology Management, Bansomdejchaopraya Rajabhat University, 2021-2024
- Master of Educational Economics and Management, Guangxi University, 2012-2015
- Bachelor of Economics, Guangxi University of Finance and Economics, 2008-2012

Work Experience:

- Lecturer, Guangxi Vocational University of Agriculture, from 2021 to the present
- Assistant, Xingjian College of Arts and Sciences, Guangxi University, from 2012 to 2020

Office Location:

- Guangxi Vocational University of Agriculture

Current Contact Location:

- 176 Daxue East Road, Nanning City, Guangxi, China