A Survey of Cybersecurity Awareness among Undergraduate Students at Yunnan University of Finance and Economics in China

Miss Xiaoyu Du

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Arts in Information Studies
Department of Library Science
Faculty Of Arts
Chulalongkorn University
Academic Year 2023

การสำรวจความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ของนักศึกษาระดับปริญญาตรีแห่ง มหาวิทยาลัยยูนนานด้านการเงินและเศรษฐศาสตร์ในสาธารณรัฐประชาชนจีน

น.ส.เซียวหยุ ตู

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาอักษรศาสตรมหาบัณฑิต

สาขาวิชาสารสนเทศศึกษา ภาควิชาบรรณารักษศาสตร์

คณะอักษรศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2566

Thesis Title	A Survey of Cybersecurity Awareness among Undergraduate Students at Yunnan University of Finance and Economics in China
By	Miss Xiaoyu Du
Field of Study	Information Studies
Thesis Advisor	Assistant Professor THIPPAYA CHINTAKOVID, Ph.D.

Accepted by the FACULTY OF ARTS, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master of Arts

.... Dean of the FACULTY OF ARTS
(Associate Professor SURADECH CHOTIUDOMPANT, Ph.D.)

THESIS COMMITTEE

.... Chairman
(Associate Professor SONGPHAN CHOEMPRAYONG, Ph.D.)

.... Thesis Advisor
(Assistant Professor THIPPAYA CHINTAKOVID, Ph.D.)

.... External Examiner
(Suporn Pongnumkul, Ph.D.)

เซียวหยุตู : การสำรวจความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ของนักศึกษาระดับปริญญาตรีแห่งมหาวิทยาลัยยูนนานด้านการเงินและเศรษฐศาสตร์ในสาธารณรัฐประชาชนจีน. (A Survey of Cybersecurity Awareness among Undergraduate Students at Yunnan University of Finance and Economics in China) อ.ที่ปรึกษาหลัก : ทิพยา จินตโกวิท

การฉ้อโกงทางไซเบอร์และการสื่อสารโทรคมนาคมเป็นความเสี่ยงออนไลน์ที่พบได้อย่างแพร่หลายและสร้างปัญหาให้กับนักศึกษามหาวิทยาลัย นักศึกษาระดับปริญญาตรีมีความเสี่ยงต่อการถูกฉ้อโกงเนื่องจากขาดประสบการณ์และความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ การจะยกระดับความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ของนักศึกษานั้นครูหรืออาจารย์จำเป็นต้องจัดการอบรมด้านความมั่นคงทางไซเบอร์ให้นักศึกษา วัตถุประสงค์หลักของงานวิจัยชิ้นนี้เพื่อศึกษาว่านักศึกษาจีนระดับปริญญาตรีเรียนรู้เรื่องความมั่นคงทางไซเบอร์อย่างไร และศึกษาความสัมพันธ์ระหว่างการฝึกอบรมกับความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ แบบสอบถามถูกจัดทำขึ้นเพื่อสำรวจแนวทางการเรียนรู้และระดับของความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ของนักศึกษาระดับปริญญาตรีแห่งมหาวิทยาลัยยูนนานด้านการเงินและเศรษฐศาสตร์ในสาธารณรัฐประชาชนจีน การประเมินความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ในสี่ประเด็น ได้แก่ ความรู้ด้านความมั่นคงทางไซเบอร์ ความเป็นส่วนตัว การจัดการรหัสผ่าน และความไว้วางใจ นักศึกษาระดับปริญญาตรีจำนวน 384 คนเข้าร่วมตอบแบบสำรวจ การวิเคราะห์ผลใช้วิธีการวิเคราะห์สหสัมพันธ์สเปียร์แมนเพื่อทดสอบสมมติฐานของงานวิจัย ผลการศึกษาพบว่าการฝึกอบรมมีความสัมพันธ์กับความตระหนักรู้ด้านความมั่นคงทางไซเบอร์อย่างมีนัยสำคัญ นักศึกษาผู้ตอบแบบสอบถามที่เคยเรียนรู้เกี่ยวกับความมั่นคงทางไซเบอร์ด้วยวิธีการแบบเป็นทางการหรือไม่เป็นทางการ มีความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ในระดับที่สูงกว่าผู้ที่ไม่เคยเรียนรู้ งานวิจัยวิเคราะห์ผลเพิ่มเติมเพื่อตรวจสอบความสัมพันธ์ระหว่างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์กับประเภทของวิธีการเรียนรู้ วิชาเอก และเพศ พบว่าวิชาเอกไม่มีความสัมพันธ์อย่างมีนัยสำคัญกับความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ ในทางกลับกัน แนวทางการเรียนรู้และเพศแสดงความสัมพันธ์ที่มีนัยสำคัญทางสถิติกับความตระหนักรู้ด้านมั่นคงทางไซเบอร์

สาขาวิชา	สารสนเทศศึกษา	ลายมือชื่อนิสิต	....
ปีการศึกษา	2566	ลายมือชื่อ อ.ที่ปรึกษาหลัก	....

6388501422 : MAJOR INFORMATION STUDIES
KEYWOR
D: Cybersecurity, College students, China

Xiaoyu Du : A Survey of Cybersecurity Awareness among Undergraduate Students at Yunnan University of Finance and Economics in China. Advisor: Asst. Prof. THIPPAYA CHINTAKOVID, Ph.D.

Telecommunications and cyber fraud are prevalent online risks that have caused trouble for college students. Undergraduate students are particularly vulnerable to fraud due to a lack of experience and cybersecurity awareness. It is essential for educators to provide cybersecurity-related training to raise the students’ level of cybersecurity awareness. The aim of this study was to see how Chinese undergraduate students learned about cybersecurity and examine a relationship between training and cybersecurity awareness. A questionnaire was administered to survey cybersecurity learning approaches and a degree of cybersecurity awareness of undergraduates at Yunnan University of Finance and Economics in China. Four aspects of cybersecurity awareness were assessed, namely, cybersecurity knowledge, privacy, password management and trust. A total of 384 undergraduate students participated in the survey. Spearman correlation analysis was used to test the research hypothesis. The study’s findings revealed that training had a significant relationship with cybersecurity awareness. Respondents who learned about cybersecurity via either formal or informal approaches showed higher level of cybersecurity awareness. The analysis further investigated relationships between cybersecurity awareness and types of learning methods, major, and gender. The analysis found that major had no significant relationship with cybersecurity awareness. Learning approaches and gender, however, showed statistically significant relationships with cybersecurity awareness.

Field of Study:	Information Studies	Student's Signature ....
Academic Year:	2023	Advisor's Signature ....

ACKNOWLEDGEMENTS

Words cannot express my gratitude to my professor and chair of my committee for their invaluable patience and feedback. I also could not have undertaken this journey without my defense committee, who generously provided knowledge and expertise.

I am also grateful to the undergraduate students at Yunnan University of Finance and Economics for their information in this survey.

Lastly, I would be remiss in not mentioning my family, especially my parents. Their belief in me has kept my spirits and motivation high during this process. I would like to thank my advisor again who has always encouraged me and helped me academically.

Xiaoyu Du

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

Chapter1 Introduction

1.1 Background

In China, there were 70.4% Internet users as of December 2020, and those between the ages of 20 and 29 made up 17.8% of all Internet users (China Internet Network Information Center & Commission, 2021). Due to the ease and speed of the Internet, it has become a common channel for college students to learn and share information. College students have been open to trying new things and do so rapidly, but they have been also susceptible to being duped and misled (Wang, 2020).

In 2022, more than 55% of Internet users in China have encountered cybersecurity problems (China Internet Network Information Center & Commission, 2022). The rapid growth and expansion of telecommunications and cyber fraud endangers not only the economic interests of citizens but also the long-term health of the economy and society, raising the stakes and complicating societal control. The governance of telecommunications and cyber fraud, a pressing issue of people's livelihood, has been gradually deemed important and urgent in the field of social management (Li & Wen, 2022). Five types of online fraud—rebate, "Pig-Butchering scam," loan, agency credit card, and impersonation of e-commerce logistics customer service—rank among the top five in 2021, accounting for 73.9% of all cases (China, 2022a). Regarding the age composition of victims, the young group under 40 years old accounted for 79% of victims' ages, making up the majority of those who fell victim to telecommunications and cyber fraud (China, 2022a). Because of their low financial resources and lack of security awareness, the group under the age of 20, who are primarily students in school or young adults just entering society, has been particularly vulnerable to fraud, including fake shopping service transactions and rebates (China, 2022b).

The Research Report on the Governance of Telecommunications and Cyber Fraud (Tencent, 2019), which was produced under the guidance of the Supreme People's Procuratorate and the Ministry of Public Security and released by Tencent, shows that 54% of the victims of telecommunications and cyber fraud are between the ages of 18 and 28, which is the age range overlapping with the age of college students. Jin (2022)found that college student victims had fluke psychology, profit seeking psychology, sympathy psychology, curiosity seeking psychology and beauty seeking psychology before being deceived. They usually did not think that they will become victims of online fraud. Owing to their psychology, the students' pursuit of money would lead them to wrong decisions under the guidance of swindlers.

Moreover, most of the students transitioning from high school to college are not yet fully mature in mind. They are weakly aware of self-prevention and protection, making it convenient for fraudsters to commit fraud. Generally, freshmen at college lack social skills, think in a simple way, are not on a lookout for danger, and are easy to trust (Xiang & Kang, 2022). According to a report on network security propaganda from the Shandong Provincial Public Security Department, a university student made an online purchase with a suspect who identified himself as "customer service." The suspect failed to take the order and instead sent a phishing link to steal the student bank card number, identity card, and other information. Five thousand yuan was withdrawn from the bank card after the "verification code" used for money transfer was revealed (Province, 2018).

College students' low self-esteem and guilt after being defrauded may lead them to do catastrophic things since they lack social and life experience (Jin, 2022),. The telecommunications and cyber fraud committed against college students resulted in major losses for their personal belongings as well as potential long-term effects on their physical and mental well-being. For instance, in Huilai, Guangdong, a prospective college student who lost 9,800 yuan due to telecommunications and cyber fraud in August 2016 left a note for his family, then left his house, and plunged into the sea to end his life (Zheng, 2022).

Fraud may be avoided if the college students are aware of online risks they may face and know how to use the Internet safely. In this regard, this study examined how well the Chinese college students knew about potential cyber threats and ways to protect themselves as well as how they learned about cybersecurity. The study's findings contributed to the current understanding of how well the students were aware of cybersecurity issues and the learning approaches to cybersecurity among Chinese undergraduate students at Yunnan University of Finance and Economics.

1.2 Motivation

In recent years, prior research has shown that Chinese college students' cybersecurity awareness has decreased. Some of the students' awareness has been inconsistent with their behavior. They have taken steps that trap themselves even though they foresee cybersecurity danger (Song, 2020; Wang, 2020; Wu, 2018; Yu, 2019; Zhou, 2021). Although some Chinese college students have had a basic level of cybersecurity awareness, the lack of experience has made it difficult for them to protect their own interests when facing cybersecurity risks. Constantly updating the knowledge to keep up with the development of science and technology is necessary, but still lacking among the college students (Zhou, 2021). According to Chinese academics (Song, 2020; Wu, 2018; Yu, 2019), students should have interests in learning as well as external support for cybersecurity education from their families, the community, and government regulations.

Approaches for cybersecurity learning can be provided via university courses or other channels outside universities. Based on a review of previous research on cybersecurity education (Alotaibi et al., 2016; Crick et al., 2019; Pal, 2022; Rahman et al., 2020; Slusky & Partow-Navid, 2012; Wolf et al., 2020), this study classifies learning methods into formal and informal training. Teaching in classrooms is considered a formal method of learning because it requires teachers to facilitate learning process and lay the foundation for students' cybersecurity awareness. Informal training, on the other hand, depends on students' own exploration and summarization of cybersecurity knowledge. They can obtain cybersecurity knowledge from websites or other channels without any guidance. The method of informal training also enables students to gain cybersecurity awareness.

At the Yunnan University of Finance and Economics, as found on the university's website, School of Information offers university courses related to cybersecurity for undergraduates majoring in information security, for instance, software security technology and information security management and guarantee. It is not certain whether students from other majors can take these classes. Nevertheless, other faculties, e.g., School of Tourism and Hotel Management, School of Logistics, Institute of Finance, International Institute of Language and Culture, Business School, School of City and Environment, Zhonghua Vocational College, Accounting School, and even School of

Information, annually organize extracurricular activities such as cybersecurity training and a knowledge contest as a part of cybersecurity education.

Based on the cybersecurity education currently adopted at the university, this study posed a question whether the formal and informal approaches had a relationship with the cybersecurity awareness of the undergraduate students at Yunnan University of Finance and Economics. The study's research objectives and research hypothesis are described in section 1.3 and 1.4, respectively.

1.3 Research Objectives

1.Examine how Chinese undergraduate students have learned about cybersecurity.

2. Investigate the relationship between learning approaches to cybersecurity and the extent of cybersecurity awareness.

1.4 Research Hypothesis

The research formed a hypothesis as follows.

Receiving formal and informal training about cybersecurity is positively related to the extent of cybersecurity awareness among Chinese undergraduate students.

In this hypothesis, formal training was defined as a method of learning that teachers assist in a learning process, e.g., learning via university courses. Informal training referred to students' self-learning without any guidance, e.g., learning about cybersecurity through websites, social networking communities, and other public lectures. Cybersecurity awareness is defined as students' understanding of cybersecurity risks and proper ways to deal with them.

Chapter 2 Literature review

2.1 Cybersecurity, cybersecurity fraud and cybersecurity awareness

This section discusses definitions of cybersecurity, cyber fraud, and cybersecurity awareness. According to the International Telecommunication Union (2019), cybersecurity is concerned with tools (e.g., security safeguards, guidelines, technologies), methods (e.g., risk management methods), processes (e.g., assurances), activities (e.g., actions, training), mechanisms (e.g., policies), and concepts (e.g., security concents) used to protect cyber environment, and assets of organizations and users. Its goal is to ensure that the availability, integrity, and confidentiality of organization and user's assets is achieved and maintained against security threats in the cyber environment. Similarly, in the perspective of corporates, cybersecurity is the protection of computer systems, networks, and services from information leakage, theft, and damage. This definition is mainly aimed at the cybersecurity threats that enterprises may face (Stieglitz et al., 2022). Basically, the protection of tangible and intangible resources and assets owned by organizations and users from online threats is the main purpose of cybersecurity. In this study, only the protection of user's assets in cyberspace, particularly personal information, was the focus of the research.

Regarding cyber fraud, according to the 48th statistical report on the development of Internet in China (China Internet Network Information Center & Commission, 2021), cyber fraud placed second in the list of the most significant four forms of cybersecurity problems in 2021 as follows: personal information disclosure (22.8%), cyber fraud (17.2%), viruses or Trojans in devices (9.4%), and account or privacy theft (8.6%). Except viruses or Trojans in devices, the probability of occurrence has increased, and each type of the cybersecurity threats has affected teenagers, especially college students. In China, cyber fraud means against college students have been cancellation of student online loan account fraud, online part-time fraud, and etc. (China, 2022a).

Cyber fraud is a commonly found economic crime on the Internet. It may involve concealing information or providing misleading information for the purpose of defrauding the victim of money, property, or any other benefits (Warf, 2018). According to Hao (2022), the goal of cyber fraud is to illegally take victims' personal information and money by exploiting the preys' false understanding to voluntarily hand over their valuable possessions. Song (2020) referred cyber fraud to the illegal activities that criminals use telecommunications, Internet and other technologies and tools to steal the victim's funds to deposit into the bank account under their control by sending text messages, making calls, planting Trojans and other means.

Many tactics have been used in cyber fraud. Phishing is one of the methods designed to steal personal information, and in turn, money from Internet users. Their goal is to convince cyber users that they are using a trusted entity and willingly provide sensitive information such as bank accounts or credit card information. Criminals utilize phony e-mails, phony websites, or both to attempt to steal these sensitive data (Gupta et al., 2017). It is challenging to avoid phishing as phishers can easily create convincing and false websites with HTTPS protocol and SSL certificates (Alwanain, 2019).

With the continuous upgrading of the fraud commercial producer such as reselling phone cards and network accounts, stealing and selling personal information, and making and selling network hacker tools, fraudsters can know basic personal information of victims in advance through various channels. At present, they illegally obtain citizens' personal information via the following ways: using rogue software or phishing websites; exploiting system vulnerabilities or information databases; purchasing through illegal channels such as secret networks; and obtaining from public channels such as enterprises' official websites and government organizations' websites (China, 2022b).

Cyberspace may not be unfamiliar to undergraduate students, but it is not uncommon that some students have not paid much attention to potential threats. Undergraduate students must enhance their awareness to protect the personal information security against the prevalent online risks. Cybersecurity awareness refers to understanding the importance of information security and taking necessary actions (Mathisen, 2004). Nurse (2021) defined cybersecurity awareness as the level of understanding or knowledge of cybersecurity or information security. Cyber hazard awareness as well as appropriate protective measures are also considered as cybersecurity awareness. Zhang (2017) believed cybersecurity awareness refers to the degree of sensitivity to recognize possible cybersecurity risks, the degree of compliance to enforce cybersecurity behavioral norms, and the degree of responsiveness to cybersecurity incidents.

For college students, cybersecurity awareness means that undergraduate students can actively and reasonably deal with cyber threats such as phishing email, information leakage, and etc. that may endanger personal assets, life safety, and psychological health. Also, they should be able to solve the problems that threaten their own security (Yan, 2020). College students should also have a clear understanding and correct judgment of the previous information security incidents occurred on the Internet (Zhou, 2021). In this study, the cybersecurity awareness is defined as students' understanding of cybersecurity risks and proper ways to deal with them.

2.2 Cybersecurity education in China

In China, although cybersecurity education has been recognized of its importance, prior research has shown that Chinese college students have not sufficiently learned about cybersecurity. According to the survey by Song (2020), only 8.1% of college students said that the school offered courses specifically about cybersecurity while 44.6% responded that cybersecurity was a topic discussed in other courses. Almost ten percent of the survey respondents (9.7%) stated that the school frequently carried out activities to improve cyber literacy whereas 76.5% answered that the activities were occasionally organized. Wu (2018) conducted a random sampling survey of college students across China. She found that students' awareness of cybersecurity was weak. They were unfamiliar with the pertinent rules and laws. Most students did not take cybersecurity-related courses because they believed cybersecurity was not relevant to their degree or would negatively affect their grades. In addition, Zhou (2021) believed that guiding documents, laws, and regulations related to cybersecurity education in colleges and universities were relatively lacking. The computer courses offered also did not touch on cybersecurity as much as it should be.

However, a traditional method of lecturing led to poor results (Hao, 2022). Researchers who conducted field surveys in China found that theoretical teaching was not suitable for undergraduates. Only providing online courses and elective courses could not make students accept the knowledge and practice of cybersecurity (Wang, 2020; Yan, 2020; Yu, 2019). Chinese researchers said that they needed to innovate cybersecurity educational methods to improve students' awareness and anti-fraud ability (Wang, 2020; Yan, 2020; Yu, 2019; Zhou, 2021).

As knowledge about cybersecurity has not been included as required courses in formal learning settings, students have obtained relevant information from other sources on their own. In Yan (2020)'s cybersecurity education survey, 83.54% of questionnaire respondents obtained their cybersecurity knowledge through Internet and other media, and 54.7% learned about it through classes.

At Yunnan University of Finance and Economics, according to the information available on its official website, the university has arranged courses and extracurricular activities to impart cybersecurity-related knowledge to students. Examples of cybersecurity-related courses are software security technology, virus principle and prevention technology, information security management and guarantee, e-commerce and e-government security, information hiding technology, etc. However, these courses are certainly available for students majoring in information security. It is uncertain whether other majors can take these courses.

The university has also organized various academic activities related to cybersecurity. The university's official website shows that each college has held cybersecurity-themed activities since 2016 until now. Relevant activities include cybersecurity knowledge contests, cybersecurity training and other types. In 2021, the Cyber Security Publicity Week was held, calling on students to learn cybersecurity topics on the national resource platform and urging students to install security protection software.

In sum, cybersecurity learning approaches can be divided into formal and informal training. Formal training is based on professional knowledge of teachers or instructors who guide students on their learning process. Classroom teaching is the method of learning to ensure that students can effectively receive knowledge in a short time (Manson & Pike, 2014). Informal training refers to the way that students independently learn and explore the subject. Learners rely on other sources on the Internet, and probably, groups of people who are interested in similar topics such as social networking communities. Both formal and informal approaches are likely to impact students' knowledge and understanding about cybersecurity.

2.3 Cybersecurity awareness among Chinese college students

Several studies have been conducted to understand the overall picture of cybersecurity awareness among Chinese college students. The following presents a list of recent research on cybersecurity awareness of Chinese students.

Based on 498 valid responses, Wu (2018) found that most college students did not have adequate knowledge about cybersecurity and law, however, they were aware of the need to stop cyber fraud. In general, there was some awareness of cybersecurity. She thought that society, families, and schools would all help raise the knowledge of cybersecurity.

Yu (2019) found that more than 50% of college students knew little about cybersecurity, and 2.65% of them said they would never know about cybersecurity. Only 23.3% of the students often learned about cybersecurity. Based on the survey's results, merely a small part of the students would take the initiative to learn about cybersecurity.

Liu et al. (2020) conducted scenario tests to see whether Chinese college students could make correct judgments for different cybersecurity risks. An example of scenarios used in the test was whether a personal computer with private content can be lent to others. The survey results showed that 62.54% of students answered correctly between 56% and 90% of all correct answers. However, more than a quarter (32.28%) of the students answered correctly less than 50% of the total number of the correct answers.

Song (2020) also performed a study on the cyber literacy of students in five universities in the northern China. The research primarily concentrated on students' self-control, information screening and security literacy, law and morality, network ecological construction, and learning of cyber literacy. College students were found to have basic cyber literacy. They were able to control their behavior to avoid cyber risks. The universities also had basic support and training though the researcher proposed that the environment for cyber literacy training needed to be improved.

Yan (2020) conducted a survey to examine cybersecurity-related knowledge and skills of college students in Hunan Province. Results showed that the cybersecurity awareness of college students in Hunan Province was weak. The students needed more training because their knowledge and abilities were insufficient. Cybersecurity education, thus, had to be improved

Zhou (2021) administered a survey and interviewed college students from institutions in the northern part of China to investigate their knowledge of and attitudes towards cybersecurity. Results showed that the students had low awareness of cybersecurity, which must be raised. A lack of cybersecurity training provided at the universities, the complexity of social network environment, and a lack of knowledge about personal cybersecurity all contributed to the students' lack of awareness for maintaining cybersecurity.

In conclusion, most prior research revealed that Chinese college students had inadequate knowledge about cybersecurity as well as a low degree of cybersecurity awareness, except the study by Liu et al. (2020). In addition, these studies recognized that cybersecurity learning was essential for raising the level of cybersecurity awareness. Nevertheless, the relationship between learning and cybersecurity awareness had not been investigated. This study, therefore, examined the correlation between cybersecurity awareness and learning approaches. It also conducted another survey of cybersecurity awareness among Chinese college students at Yunnan University of Finance and Economics.

2.4 Cybersecurity awareness, major, and gender

In terms of a relationship between major and cybersecurity awareness, previous research results were indicative of differences in level of cybersecurity awareness among majors. A. A. Garba et al. (2020) found that computer science students at Yobe State University in Nigeria had a high awareness of cybersecurity. On the contrary, Tibi et al. (2019) described that computer science students had lower awareness of cybercrime than science students. The study collected the data from Arab students majoring in computer science, language, and science at a teacher training college in Israel. Results found that science students had the highest level of awareness, compared with the other two. Another survey conducted by Moallem (2019) revealed that students from public universities in California, USA, who were in the field of human-computer interaction, human factors/ergonomics and cybersecurity had low awareness of cybersecurity. These surveys indicated that computer science students may not have higher awareness of cybersecurity than other majors. In the context of China, a review of research on cybersecurity awareness in China (Li, 2018; Song, 2020; Wang, 2020; Wu, 2018; Yu, 2019; Zhou, 2021) showed that none of the studies analyzed the data from the perspective of major.

In the aspect of finance and economics, Garrison and Posey (2006) studied a level of cybersecurity awareness of students in accounting and stated that the students needed to improve their cybersecurity awareness. Likewise, Subramaniam (2017)'s survey on the level of cybersecurity awareness of college students in the northern part of the Malay Peninsula found that there were differences in the level of cybersecurity awareness among students from different majors, and accounting students had the lowest level of awareness.

Regarding a relationship between gender and cybersecurity awareness, Liu et al. (2020) discovered that Chinese male undergraduate students were more inclined to adopt cybersecurity behaviors than female undergraduate students. A. A. Garba et al. (2020) also found that female students were more likely to be victims of cyberattacks than male students. However, these results contradicted the findings by Subramaniam (2017), which found no difference in the level of cybersecurity awareness between male and female students in the northern part of the Malay Peninsula. The results of the study by Aljohani and Elfadil (2020) also showed no gender difference in the awareness of cybersecurity.

The results of prior studies on the relationship between major and cybersecurity awareness, and gender and cybersecurity awareness are not uniform. In addition, no research works on cybersecurity in China have discussed cybersecurity awareness from the perspective of major and gender. This survey, therefore, has explored the relationship between major and cybersecurity awareness, and gender and cybersecurity awareness.

2.5 Assessment of cybersecurity awareness

Survey is a common approach used to evaluate college students' cybersecurity awareness as discussed in other sections. This section focuses on issues used for an assessment of cybersecurity awareness. Cybersecurity related issues that have been investigated in prior research included password security, cyberbullying, phishing, malware, downloading, sharing and use of paid content (Chandarman & Van Niekerk, 2017); password management, desire, and acceptance awareness of learning cybersecurity (A. Garba et al., 2020); two-factor authentication (2FA), password setting (Moallem, 2019); cybersecurity knowledge, trust, privacy (A. A. Garba et al., 2020; Moallem, 2019); and identity theft (Chandarman & Van Niekerk, 2017).

Other issues related to cybersecurity awareness were users' understanding of the importance of information security and of the responsibilities for their actions (Shaw et al., 2009); the ability to recognize spam, phishing, malware, and other attacks, the capability to guard personal information and online privacy and to judge the credibility and usefulness of online information, and use of secure passwords (Frydenberg & Lorenz, 2020).

This study focuses on internet fraud as a cybersecurity risk because it poses a major threat for college students' online safety. The cybersecurity awareness of college students, thus, refers to the degree that the students are aware of potential cyber frauds, and how to protect themselves. In this study, issues concerning the cybersecurity awareness include cybersecurity knowledge, privacy, password management, and trust. These four components have been investigated in other works as follows: cybersecurity knowledge (Alharbi & Tassaddiq, 2021; A. A. Garba et al., 2020; Moallem, 2019; Tibi et al., 2019); privacy (Alharbi & Tassaddiq, 2021; Garba, 2021; A. A. Garba et al., 2020; Moallem, 2019; Slusky & Partow-Navid, 2012); password management (Alharbi & Tassaddiq, 2021; Aljohani & Elfadil, 2020; Alqahtani, 2022b; A. A. Garba et al., 2020; Garrison & Posey, 2006; Kader, 2020; Moallem, 2019; Slusky & Partow-Navid, 2012); and trust (Aljohani & Elfadil, 2020; A. A. Garba et al., 2020; Moallem, 2019). The following subsections describe each element accordingly.

2.5.1 Cybersecurity Knowledge

Cybersecurity knowledge helps protect students from potential risks on the Internet. It is concerned with not only understanding the concepts of cybersecurity, i.e., web security, and cybersecurity threats, but also knowing how to detect and properly deal with cyber harms.

In terms of knowledge about the concepts, most surveys (Elmi, 2019; A. A. Garba et al., 2020; Moallem, 2019; Stanciu & Tinca, 2016; Tibi et al., 2019) asked participants to identify and recognize various terms related to cyber crisis to judge whether participants had basic knowledge of cybersecurity. Some surveys (A. A. Garba et al., 2020; Moallem, 2019) found that few participants knew the meaning and principle of each term, indicating that cybersecurity knowledge was weak, making it easy for them to be threatened in real life.

A study by McPhee and Bailetti (2014) emphasized that a lack of knowledge essentially led to unsafe online behavior of Internet users. Internet users could detect and avoided any evident threats if they were educated and aware of their surroundings (Alzahrani, 2021). Stanciu and Tinca (2016) proved that students who knew about phishing attacks were less likely to being deceived; training helped to reduce information security risks; and appropriate cybersecurity practices should be considered in cybersecurity awareness. To this sense, understanding cybersecurity is essential for Internet users since it covers how to handle threats to the network so that threats have a minimal impact on people's lives (Hart et al., 2020).

Therefore, in this study, cybersecurity knowledge includes fundamental concepts related to web security, knowledge about identification and risks of Internet fraud, and suitable cybersecurity practices.

2.5.2 Privacy

Privacy is concerned with whether students know how to safeguard their personal information such as names, contact information, and personal images so that it will not get into the hands of cybercriminals. It is the right to choose who has access to what information at what time (Westin, 1967). It can also be referred to as "selective control over the acquisition of self" (Altman, 1975).

Nowadays, the more mature the technology is and the more diversified the software is, the more personal information Internet users expose in software platforms. Computer networks often collect a large amount of user information. If this information is not reasonably used, it can lead to great violations of the privacy of relevant network users (Zou, 2022). While using the Internet for different activities, users usually ignore unsafe factors in the network, such as the inability of various login systems to protect account information, the vulnerability of system firewalls, the inadvertent disclosure of personal information such as personal phone numbers and home addresses, and the failure to update anti-virus software in time (Zhang, 2020). Users are also accustomed to network risks and new things on the network, such as online social networking, online job hunting and online shopping. They are not vigilant and easy to disclose personal information, which has become the target of telecommunications and cyber fraud.

College students have insufficient social experience and weak discrimination ability. When they suffer from telecommunications and cyber fraud, they are easy to be deceived, intimidated, and coerced (Zheng, 2022). According to Rifon et al. (2005), as long as students paid attention to privacy issues during Internet use, they would be worried about their privacy leading to the protection of their privacy. So, the protection of personal information is necessary in cybersecurity awareness.

Thus, privacy, in this study, is defined as the protection of personal identifiable information (PII), either direct information such as profiles and photos, or indirect ones, e.g., geographical locations and contacts.

2.5.3 Password Management

Password is considered as one of the tools for information protection. It provides access to authenticated systems. Authentication by user ID or username and password is the most common way to register and log into a system. It is also the approach that gives hackers a chance to steal users' personal information. One of the easiest ways for hackers to access user credentials is to obtain login information from the user himself (Moallem, 2021). To access user accounts, hackers use many methods, for example, phishing. By sending fraudulent e-mails disguised as legitimate e-mails, cybercriminals claim that they are trustworthy and try to get their hands on information needed for authentication.

Most users also tend to reuse usernames and passwords with different online accounts. Another commonly found phenomenon is to merge private information into the password selected by the user. This is not a good practice. One of the most serious security problems that happened in the context of data theft was caused by password duplication (Alqahtani, 2022a).

Another concern is that most passwords are easy to crack. Hackers only need to use technologies such as a password dictionary to easily crack passwords. So, long passwords are necessary, making them more difficult to break. Professionals' advice is to choose a familiar way to remember complex passwords, such as the abbreviations of favorite songs.

It is important to examine whether students are aware of proper ways to set and manage their passwords. This research, then, refers password management to the practice of setting strong passwords and not repeatedly using them.

2.5.4 Trust

Trust is the belief that another person or organization that a person depends on will act in a socially acceptable way - honest, caring, and capable (Gefen et al., 2005; Giffin, 1967; McKnight & Chervany, 2002). It is crucial in many economic and social interactions, especially in an Internet environment where visual and other social cues are clearly missing (Reichheld & Schefter, 2000). It allows people to assume the possibility of opportunistic behavior of the individuals or organizations they trust. In doing so, it reduces the overwhelming social complexity involved in evaluating the motives and behaviors of others (Lewis & Weigert, 1985; Luhmann, 1979).

If users always trust the Internet without any caution, they are likely to become victims of telecommunications and cyber fraud. Vigilance against cyber environment is, therefore, a behavior that users should have. According to a study of cyber fraud, most survey respondents had almost no prevention in the whole process of being cheated. The respondents believed that they were in a completely "safe" cyber environment. They highly trusted the fraudster, and then encountered the whole fraud link in a short time. The use of the Internet in daily life for several activities, e.g., for school, makes college students unable to effectively identify diverse and fragmented information. Part of the successful implementation of online fraud stems from the victim's trust in the fraudster (Cai & Li, 2022).

Thus, trust in this research is concerned with being vigilant within the cyber environment. This study investigated whether students were conscious of suitable practices to evaluate whether they could trust the software platforms or not.

Chapter 3 Methodology

3.1 Study's settings, population, and sample size

This study focused on investigating the cybersecurity awareness of the college students at Yunnan University of Finance and Economics which was selected as the study's setting due to its multidisciplinary nature. Yunnan University of Finance and Economics, a provincial key university, was founded in 1951. It is a teaching and research university. Economics and management are offered as the university's main disciplines. Other fields include law, philosophy, literature, art, science, and engineering.

The exact number of the population could not be obtained because the official website of the university only provided an approximate number of students in school. Therefore, the sample size for the survey was calculated based on the following equation, which is an approach for determining a sample size when the size of the population is unknown. n is the number of sample size. *Z* was defined as a statistic value that was dependent on a confidence level, which was set at 95%. *e* was a term for an acceptable error, *p* as an estimated proportion of a characteristic that is present in the population, and *q* as 1-*p*.

Z = 1.96, e = 5%, p = 0.5

$$n_0 = \frac{Z^2pq}{e^2} = \frac{(1.96)^2(.5)(.5)}{(.05)^2} = 384.16$$

Thus, the sample size for this survey was 384.

3.2 Inclusion and exclusion criteria

The following were inclusion criteria for survey respondents. Each participant must meet both criteria.

1) Be an undergraduate student.

2) Study in any major at Yunnan University of Finance and Economics.

The exclusion criteria were as follows.

1) Be a graduate student at Yunnan University of Finance and Economics..

2) Be a teacher, lecturer, or professor at Yunnan University of Finance and Economics.

3.3 Data collection instrument

The questionnaire was developed by adapting questions based on prior research works (Alharbi & Tassaddiq, 2021; A. Garba et al., 2020; Khalid et al., 2018; Moallem, 2019; Senthilkumar & Easwaramoorthy, 2017). The questions were translated from English into Chinese. A language specialist who graduated from English major reviewed the accuracy of the English - Chinese translation. Three experts in cybersecurity and cybersecurity awareness evaluated the validity of the questionnaire. Each expert evaluated each question by giving either -1 if they thought that the question did not align with the purpose of the study, 0 if they were not sure whether the question matched with the study's objectives, or 1 if the question aligned with the purpose. An item-objective congruence (IOC) index was calculated to determine the questionnaire's content validity. Questions that obtained an IOC index less than 0.5 were either revised or removed from the final questionnaire. Appendix A shows a table reporting IOC scores. In addition, a pilot study was run with at least eighteen Chinese students, who were not included in the study's sample, to test the language and clarity of the questionnaire items, and reliability of the Likert items. The reliability score was 0.820. Appendix B shows the revised questionnaire used for the data collection.

The questionnaire is separated into two parts. The first section asks about educational approaches on cybersecurity based on students' experiences. The second section gathers students' feedback about cybersecurity awareness, including basic knowledge about cybersecurity, privacy, password management, and trust.

Students' basic cybersecurity knowledge refers to the fundamental concepts related to web security, the knowledge about identification and risks of internet fraud, and suitable cybersecurity practices. Examples of the concepts concerning the web security are HTTPS protocol and cookies. Phishing or scam emails are examples of internet fraud. Privacy refers to the protection of personal identifiable information (PII), either direct information such as profiles and photos, or indirect ones, e.g., geographical locations and contacts. It is concerned with how the PII is shared and accessed. Management of passwords investigates the strength of passwords usually set by the students and whether they are used repeatedly or not.

Trust deals with vigilance against their own cyber environment, for instance, reading the software's information collection terms to understand what kind of information will be gathered and how it will be acquired, before using the software.

A conceptual framework of this study is shown in Figure 3-1.

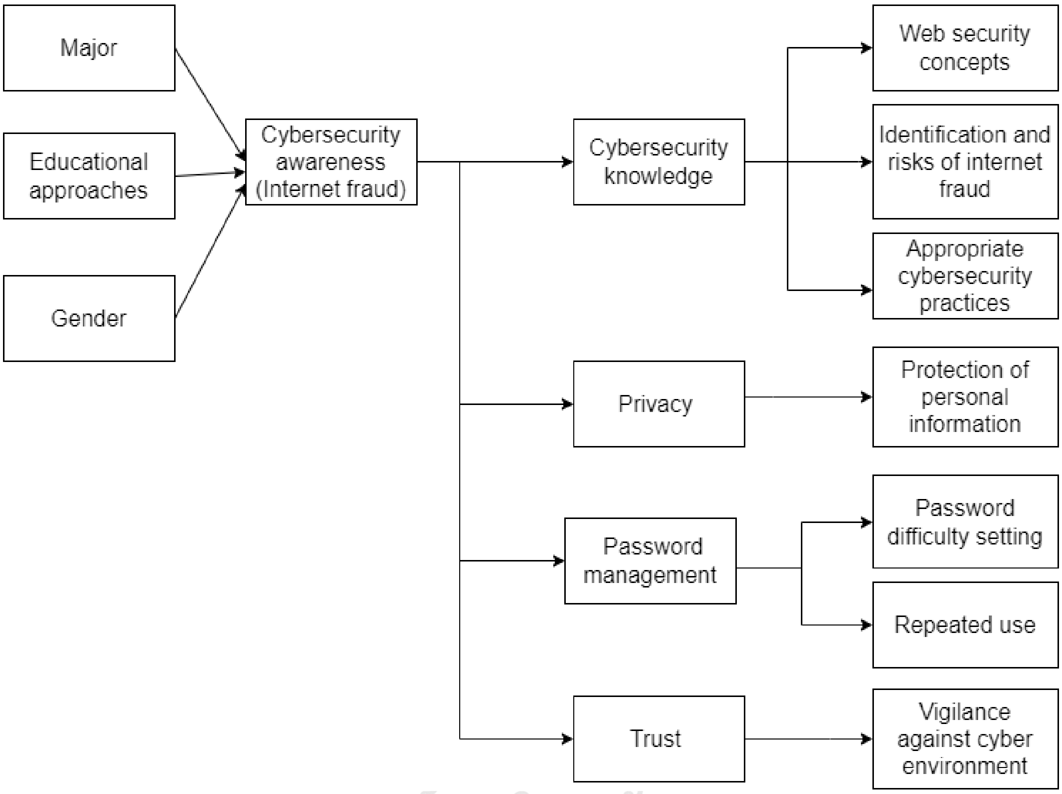
Major
Educational approaches
Gender
Cybersecurity awareness (Internet fraud)
Cybersecurity knowledge
Privacy
Password management
Trust
Web security concepts
Identification and risks of internet fraud
Appropriate cybersecurity practices
Protection of personal information
Password difficulty setting
Repeated use
Vigilance against cyber environment

Figure 3-1. The study’s conceptual framework

For the second part of the questionnaire, each participant expressed the level of agreement or disagreement with the statement on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). Examples of questionnaire items are demonstrated below.

<u>Cybersecurity Knowledge</u>

1. I know what two-factor authentication (2FA) is.
2. I know the difference between using HTTP and HTTPS.
3. When you receive an email requiring your credential information such as name, date of birth, age, your credit card number, you should reply to this email.

<u>Privacy</u>

4. I only provide my personal information when I was asked by an organization that I know well.
5. When I receive links for any promotional content, e.g., job advertisement, sales promotion, etc., I click them without checking whether they come from official or trusted sources.

Password Management

6. I use passwords that are difficult to guess as account passwords, such as excluding initials and birthdays.
7. My social media account, email account, and online bank account use the same password.

Trust

8. I believe that the online infrastructures of organizations such as schools, banks, and online services providers are secure and not easy to break into.
9. I believe that social media applications will not disclose my shared photos or address if I do not give a permission.

3.4 Data collection

Before the study could start collecting responses, it was necessary to apply for an approval from the Institutional Review Board (IRB) of Chulalongkorn University to ensure that the research procedure was in accordance with the ethics of human research accepted at an international level. Once the research obtained a Certificate of Research Approval, the questionnaire was publicized via free online chat groups established by students in the university. Students could choose whether to take part in the survey or not. There were no obligations. The questionnaire was distributed via a QR code created by the generator program called Wenjuanxing, which was recognized by WeChat, one of China's most popular chat software. The Wenjuanxing marked each response by number. Students' names and other identification information were not collected. The questionnaire was set to accept only one time of response from each account to avoid repeated data from the same respondent.

The data were collected between August and October 2022. The study received a total number of 393 responses. After screening the data, there were 9 incomplete questionnaires. Therefore, only 384 responses were valid and used for the data analysis in Chapter 4.

Chapter 4 Results

4.1 Reliability of the questionnaire

To test the reliability of the twenty-six Likert-scale items of the questionnaire after administering the survey, Cronbach's alpha value was computed as shown in Table 4-1. According to Taber (2018), the acceptable standard value of Cronbach's alpha for social science is 0.70. The study's questionnaire obtained a Cronbach's alpha value of 0.75, passing the acceptable standard value.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
0.750	0.758	26

Table 4-1. Cronbach's alpha reliability score of the survey's Likert-scale items.

4.2 Demographic information

Three hundred and ninety-three students took part in the survey. However, nine respondents were excluded from the data analysis as their responses were incomplete, yielding 384 complete questionnaires. The following is the data presentation and analysis based on the valid data, including the proportion of responses to each questionnaire item.

4.2.1 Gender, age, and year of study

Out of 384 respondents, 109 male participants (28.4%) and 275 female participants (71.6%) took part in the survey, as shown in Table 4-2. The age ranges were 17-19 years old (100 students, 26%), 20-22 years old (277 students, 72%), and 23-25 years old (7 students, 2%), as illustrated in Table 4-3. Participants' ages were different from what was anticipated. Although the common belief was that undergraduate students were between 18 and 22 years old, some students between 23 and 25 years old also responded to the questionnaire. Table 4-4 shows that most of the survey respondents were second-year and third-year students, 175 (45.6%) and 193 (50.3%) students, respectively. There were only 4 freshmen (1%) and 12 seniors (3.1%).

Gender	Frequency	Percent
Male	109	28.4
Female	275	71.6
Total	384	100.0

Table 4-2. Gender of survey respondents.

Age (years old)	Frequency	Percent
17-19	100	26.0
20-22	277	72.0
23-25	7	2.0
Total	384	100.0

Table 4-3. Age of survey respondents.

Year of study	Frequency	Percent
1st year	4	1.0
2nd year	175	45.6
3rd year	193	50.3
4th year	12	3.1
Total	384	100.0

Table 4-4. Year of study of survey respondents.

4.2.2 Faculty and cybersecurity learning approaches

Table 4-5 shows that college students from all institutions responded to the questionnaire. The top three faculties with high number of survey respondents are Business School (141 students, 36.7%), School of Tourism and Hotel Management (110 students, 28.6%), and Accounting School (47 students, 12.2%). Next is the participation from others (30 students, 7.8%) which refers to the respondents from Zhonghua Vocational College, another institution within the university. The rest of the students were from other colleges of Yunnan University of Finance and Economics. For the International Institute of Language and Culture and School of Finance and Public Administration, only one person each took the survey.

Faculty	Number	Percent
Business School	141	36.7

School of Tourism and Hotel Management	110	28.6
Accounting School	47	12.2
Others	30	7.8
Ministry of sports	9	2.3
School of Economics	9	2.3
School of Statistics and Mathematics	8	2.1
School of Information	7	1.8
School of City and Environment	6	1.6
Institute of Finance	4	1.0
Law School	4	1.0
International Business School	3	0.8
School of Logistics	2	0.5
School of Media and Design Art	2	0.5
International Institute of Language and Culture	1	0.3
School of Finance and Public Administration	1	0.3
Total	384	100.0

Table 4-5. Faculty information of survey respondents.

“Have you ever learned cybersecurity?” was the question used to learn about the students’ learning approaches for cybersecurity. The respondents could choose only an answer for this question. As shown in Table 4-6, 180 respondents (46.9%) took university courses related to cybersecurity, 124 (32.3%) learned about it from websites, and 54 (14.1%) gained knowledge from social cybering communities. The remaining 16 students (4.2%) relied on public lectures, and 10 students (2.6%) had not learned about cybersecurity. The responses showed that most students had knowledge about cybersecurity to some degree. They engaged with both formal and informal ways of learning. This study considered the university courses to be formal training, and the rest, including websites, social networking communities, and public lectures, were informal training. Half of the students (50.6%) acquired cybersecurity knowledge from informal training.

Cybersecurity Education	Number	Percent
Yes, I have. I learned from university course.	180	46.9
Yes, I have. I learned from websites.	124	32.3

Cybersecurity Education	Number	Percent
Yes, I have. I learned from social cybering communities.	54	14.1
Yes, I have. I learned from public lecture.	16	4.2
No, I have not.	10	2.6
Total	384	100.0

Table 4-6. Number of responses to the question "Have you ever learned cybersecurity?"

4.3 Survey results

4.3.1 Cybersecurity knowledge

The first three questions of the cybersecurity knowledge part of the questionnaire asked the students whether they knew about two-factor authentication (2FA), HTTP and HTTPS protocol and cookies. 2FA is mainly used to ensure the security of the user's account. It is usually not enabled by default and needs to be manually enabled by the user. In addition to a username and password required for account login, an SMS verification code is also required. The difference between HTTP and HTTPS is whether the web page has an encrypted transmission protocol, which can protect users' information and other contents. Users can observe whether the websites use HTTPS to ensure that the information they enter on the web pages will be protected. Otherwise, there may be a risk of information disclosure. Cookies can track users' browsing behavior and record it as text files that will be exchanged between users' computers and network servers. They are useful for information personalization. However, they present a risk to users' privacy. Regarding the two-factor authentication, 141 students (29.3%) knew about 2FA whereas 83 respondents (21.6%) did not know what it was. Only 65 students (16.9%) stated that they could tell the difference between HTTP and HTTPS while 150 students (39.1%) could not. For cookies, 110 respondents (28.7%) knew what cookies were, but 114 survey respondents (29.7%) did not know them. The proportion of responses to each questionnaire statement is shown in Table 4-7.

Regarding the knowledge about cybersecurity risks, 279 respondents (72.7%), as shown in Table 4-7, would not strongly believe that the strange callers who claimed to know their personal information were well-intended people. Strange emails and messages may also carry risks. Phishing links are usually used to lure students. In the survey results, 306 students (79.7%) avoided clicking unfamiliar links whereas 61 respondents (15.9%) clicked the links sent in emails or messages from unknown senders. When it came to whether to reply to an email with personal information, almost all students (346 students, 90.1%) stated that they would not provide their information.

As illustrated in Table 4-7, the questions 12 to 16 were concerned with students' knowledge about proper cybersecurity practices. 218 students (56.8%) firmly said that they would log out after using the public computer, and 102 students (26.6%) also agreed that they would log out after completing the task. Although most students (160 students, 41.7%) did not clearly indicate whether they understand the concept of cookies, 257 respondents (67%) stated that they read the policy before clicking "Accept Cookies." Regarding the situation when their personal information was illegally occupied or used, 310 students (80.8%) stated that they would seek help from authorities or trusted people. Two hundred and fifty-five respondents (66.4%) indicated that they would not install software that was not verified by the standard App store. In terms of ensuring the security of their personal computers, 238 students (62%) knew that turning off the security settings and tools might cause their own system to be at risk; however, 80 students (20.8%) chose to disable them. The answers about cybersecurity knowledge revealed that most respondents did not clearly state whether they understood 2FA (160 students, 41.7%), HTTP and HTTPS protocol (169 students, 44%), and cookies (160 students, 41.7%). Nevertheless, most students were aware of cybersecurity risks and avoided harmful behaviors.

Cybersecurity knowledge survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
6. I know what two-factor authentication (2FA) is.	31 (8.1%)	52 (13.5%)	160 (41.7%)	112 (29.2%)	29 (0.1%)
7. I know the difference between using HTTP and HTTPS.	43 (11.2%)	107 (27.9%)	169 (44.0%)	53 (13.8%)	12 (3.1%)
8. I know what cookies are.	25 (6.5%)	89 (23.2%)	160 (41.7%)	81 (21.1%)	29 (7.6%)

9. When I receive a strange call and the other person say he/she knows my name, ID number, phone number, address and so on, I believe that the other side is a good person.	279 (72.7%)	75 (19.5%)	18 (4.7%)	9 (2.3%)	3 (0.8%)
10. I avoid clicking links in emails or messages sent by an unknown person.	41 (10.7%)	20 (5.2%)	17 (4.4%)	102 (26.6%)	204 (53.1%)
11. When I receive an email requiring my credential information such as name, date of birth, age, credit card number, I should reply to this email.	283 (73.7%)	63 (16.4%)	21 (5.5%)	12 (3.1%)	5 (1.3%)
12. When I use a computer in public spaces, such as Internet cafes, or libraries, to log into my online accounts, I always log out before I leave the computer.	23 (6.0%)	14 (3.6%)	27 (7.0%)	102 (26.6%)	218 (56.8%)
13. When websites ask me to accept their cookies policy, I do not read the information and click "Accept Cookies" immediately.	170 (44.3%)	87 (22.7%)	79 (20.6%)	29 (7.6%)	19 (4.9%)
14. I know what I should do (call the police, seek help from school or parents) when I know that my personal information has been compromised.	18 (4.7%)	16 (4.2%)	40 (10.4%)	94 (24.5%)	216 (56.3%)
15. I do not install software that is not verified by the standard App store.	34 (8.9%)	30 (7.8%)	65 (16.9%)	100 (26.0%)	155 (40.4%)
16. The security settings and tools slow me down and are pesky. I turn them off or disable them.	150 (39.1%)	88 (22.9%)	66 (17.2%)	37 (9.6%)	43 (11.2%)

Table 4-7. Responses regarding cybersecurity knowledge.

4.3.2 Privacy

Table 4-8 shows that 284 students (74%) worried about the security of their personal information on the Internet whereas 53 students (13.8%) did not have any concern. Two hundred and seventy-two respondents (70.8%) stated that they would provide personal information to the organizations they knew well. On the contrary, 55 students (14.3%) refused to provide their personal data. Most of the students (310 students, 80.7%) did not click to view the promotional ads from unknown sources while merely 48 students (12.5%) thought they should check them out.

The students expressed a high degree of consistency on their willingness to provide personal data. Three hundred and forty-two respondents (89%) stated that they would not easily give the information to anyone; however, 25 students (6.5%) indicated otherwise. As for their personal profile on social media, 296 respondents (77.1%) said they would not provide a complete profile online, but 40 students (10.4%) thought they would give full profile information to let others know them better. When questioned about sharing their information in daily lives with the public on social media platforms, almost a quarter of the students (85 students, 22.1%) often shared their activities while more than half (201 students, 52.4%) did not.

Nowadays, many students choose online shopping for convenience and affordable prices. Two hundred and thirty-seven students (61.7%) were concerned that the amount of their personal information was unnecessarily requested when shopping online. On the other hand, 83 students (21.6%) did not think they were asked for too much personal data. Sixty-four respondents (16.7%) did not reveal their perception towards the amount of personal information inquired by online purchases. When the mobile phone requested access to the user's contact information and location, 107 (27.9%) and 116 (30.2%) students strongly agreed and agreed, respectively, that they would reject the request. However, 86 respondents (22.4%) would comply with the requirements.

Privacy survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
17. I am worried if my personal information was	17 (4.4%)	36 (9.4%)	47 (12.2%)	135 (35.2%)	149 (38.8%)

Privacy survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
not securely kept online.					
18. I only provide my personal information when I was asked by an organization that I know well.	17 (4.4%)	38 (9.9%)	57 (14.8%)	144 (37.5%)	128 (33.3%)
19. When I receive links for any promotional content, e.g., job advertisement, sales promotion, etc., I click them without checking whether they come from official or trusted sources.	237 (61.7%)	73 (19.0%)	26 (6.8%)	26 (6.8%)	22 (5.7%)
20. I am willing to give my personal information to anyone asking for it, even if they are strangers.	302 (78.6%)	40 (10.4%)	17 (4.4%)	13 (3.4%)	12 (3.1%)
21. I add a complete personal profile on my social media account because I want other people to know details about me.	187 (48.7%)	109 (28.4%)	48 (12.5%)	23 (6.0%)	17 (4.4%)
22. I often share activities in my daily life with the public on social media applications.	87 (22.7%)	114 (29.7%)	98 (25.5%)	65 (16.9%)	20 (5.2%)
23. I am concerned that I am asked for too much personal information when I register or make online purchases.	51 (13.3%)	32 (8.3%)	64 (16.7%)	143 (37.2%)	94 (24.5%)
24. I usually reject requests of mobile applications for accessing my contacts or locations.	35 (9.1%)	51 (13.3%)	75 (19.5%)	116 (30.2%)	107 (27.9%)

Table 4-8. Responses regarding privacy

4.3.3 Password management

The college students' responses to the questions about password management are illustrated in Table 4-9. Two hundred and thirty-four respondents (60.9%) chose to use the password that was not easy to crack as their account passwords. However, when they rated their responses for password strength, 245 students (63.8%) thought their passwords were not strong enough. Less than a quarter (74 students,19.2%) believed their passwords were sufficiently strong. Only 40 students (10.4%) set the same password for the social media account, email account, and online bank account. The majority (296 students, 77.1%) indicated that they used different passwords for different accounts. Two hundred and ninety-six respondents (77%) did not share with others the username and password of different types of their accounts, but 39 students (10.2%) shared their login information. More than half of them (199 students, 51.9%) used 2FA if possible while 68 students (17.7%) felt that they did not use it. However, some students (117 students, 30.5%) did not mention that they used or did not use the more secure type of authentication.

Password management survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
25. I use passwords that are difficult to guess as account passwords, such as excluding initials and birthdays.	26 (6.8%)	51 (13.3%)	73 (19.0%)	110 (28.6%)	124 (32.3%)
26. I am worried that my password is not strong enough.	32 (8.3%)	42 (10.9%)	65 (16.9%)	133 (34.6%)	112 (29.2%)
27. My social media account, email account, and online bank account use the same password.	187 (48.7%)	109 (28.4%)	48 (12.5%)	23 (6.0%)	17 (4.4%)
28. I do not share the username and password of my social media account, email account, or online bank account with others.	16 (4.2%)	23 (6.0%)	49 (12.8%)	105 (27.3%)	191 (49.7%)

Password management survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
29. I use two-factor authentication (2FA) for my online accounts whenever it is possible.	30 (7.8%)	38 (9.9%)	117 (30.5%)	102 (26.6%)	97 (25.3%)

Table 4-9. Responses regarding password management.

4.3.4 Trust

Regarding trust in the information technology infrastructure of organizations, 136 students (35.4%) believed that the online infrastructure of organizations, e.g., schools, banks, and online services providers, that they interacted with were secure and not easy to be hacked. On the contrary, 193 respondents (36.2%) thought in an opposite direction. One hundred and nine students (28.4%) neither agreed or disagreed that the organizations' online infrastructure were secure. Two hundred and thirty respondents (59.9%) did not believe that social media applications would not disclose their data if they did not permit them to do so. Only a handful of students (63 students, 16.4%) trusted that the social networking platforms would safely keep their data if no permission was granted for disclosure. The responses to the trust-related questionnaire statements are illustrated in Table 4-10.

Trust survey items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
30. I believe that the online infrastructures of organizations such as schools, banks, and online services providers are secure and not easy to break into.	59 (15.4%)	80 (20.8%)	109 (28.4%)	88 (22.9%)	48 (12.5%)
31. I believe that social media applications will not disclose my shared photos or address if I do not give a permission.	141 (36.7%)	89 (23.2%)	91 (23.7%)	44 (11.5%)	19 (4.9%)

Table 4-10. Responses regarding trust.

4.4 Spearman correlation analysis

The study's research hypothesis was that receiving formal and informal training about cybersecurity is positively related to the extent of cybersecurity awareness among Chinese undergraduate students. To test the hypothesis, Spearman correlation analysis, a nonparametric statistical method, was used to examine the relationship between training and cybersecurity awareness. It was chosen for the analysis due to the nature of the study's data. Training was considered a dichotomous categorical variable consisting of a training group and a no training group. Cybersecurity awareness was treated as an interval variable because its mean was computed and used in the data analysis.

For the 'training' variable, the respondents were grouped into training and no training based on their responses to the question "Have you ever learned cybersecurity?" The training group included both answers related to formal and informal training. Formal training referred to acquiring cybersecurity knowledge in school courses. Informal training was concerned with learning about cybersecurity through websites, social networking communities and public lectures. In total, 374 students responded that they had learned about cybersecurity. While 184 respondents indicated learning via university courses, 194 students obtained knowledge through other informal methods. Ten students answered having no training about cybersecurity. In addition, it was interesting to learn whether there was a relationship between cybersecurity awareness and types of training. Another correlation analysis was then performed to investigate the relationship between cybersecurity awareness and types of training (formal vs. informal ones).

Regarding the 'cybersecurity awareness' variable, it was measured by asking the respondents to rate their opinion on 26 statements. These questionnaire items were divided into four parts: cybersecurity knowledge (11 items), privacy (8 items), password management (5 items), and trust (2 items). Means were calculated for each component of the variable and for the four parts altogether as cybersecurity awareness. The means were used for Spearman correlation analysis.

Besides the hypothesis testing, the analysis was conducted to investigate relationships between cybersecurity awareness and other factors, namely, major and gender. This section presents descriptive statistics and results of the correlation analysis for the hypothesis testing, i.e., the relationship between training (with training vs. without training) and cybersecurity awareness, and other relationships between cybersecurity awareness and types of training (formal vs. informal learning approaches), major, and, lastly, gender.

4.4.1 Learning approach and cybersecurity awareness

4.4.1.1 Test of research hypothesis on learning approach

Below show descriptive statistics of overall cybersecurity awareness, cybersecurity knowledge, privacy, password management and trust for the students with training (N = 374 students) in Table 4-11 and without training (N = 10) in Table 4-12.

As shown in Table 4-11, the highest means of cybersecurity knowledge, privacy, password management and trust were 5.00, indicating that there were students in the training group indicating 5 for all items of each component. However, there was no one rated 5 for all 26 statements, which is why the maximum mean of cybersecurity awareness was 4.65.

In Table 4-12, the maximum average scores of cybersecurity awareness was 3.69 for the no training group. The maximum values of cybersecurity knowledge, privacy, password management, and trust were 4.18, 4.00, 4.60, and 3.50, respectively.

With training	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	374	2.35	4.65	3.70	0.42
Cybersecurity knowledge	374	2.18	5.00	3.84	0.52
Privacy	374	1.38	5.00	3.80	0.54
Password management	374	1.60	5.00	3.64	0.68
Trust	374	1.00	5.00	2.62	1.02

Table 4-11. Descriptive statistics of students who had learned about cybersecurity.

Without training	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	10	2.65	3.69	3.20	0.38
Cybersecurity knowledge	10	2.82	4.18	3.33	0.42
Privacy	10	2.50	4.00	3.33	0.50
Password	10	1.60	4.60	3.10	1.03

Without training	N	Minimum	Maximum	Mean	Std. Deviation
management					
Trust	10	1.00	3.50	2.20	0.98

Table 4-12. Descriptive statistics of students who had not learned about cybersecurity.

In the analysis, the group with training was coded 1 while the group without training was coded 2. The results of Spearman correlation analysis showed that training was significantly related to cybersecurity awareness r_s (382) = - .175, p < 0.005. The mean of cybersecurity awareness for the training group was 3.70 higher than the no training group with the mean of 3.20. Since it was the analysis of correlation between a dichotomous variable and interval variables, if the group with training were coded 2 and the group without training coded 1, the results would reveal a positive correlation coefficient. Table 4-13 also shows a significant relationship between training and cybersecurity knowledge r_s (382) = -.157, p < 0.005, and training and privacy r_s (382) = - .138, p < 0.005. However, whether students have been trained did not have a significant correlation with password management r_s (382) = - .079, p = 0.121 and trust r_s (382) = - .059, p = 0.249.

The results support the research hypothesis that students who have learned about cybersecurity would demonstrate different degree of cybersecurity awareness compared with those who have no training. In other words, training did help college students to gain cybersecurity awareness. Another question was asked whether types of training, i.e., formal or informal learning approaches, were significantly related to cybersecurity awareness or not. The next section describes a correlation analysis between training approaches and cybersecurity awareness.

	Correlation Coefficient	Sig. (2-tailed)	N
Training	1.000		384
Cybersecurity awareness	-.175**	0.001	
Cybersecurity knowledge	-.157**	0.002	
Privacy	-.138**	0.007	
Password management	-0.079	0.121	
Trust	-0.059	0.249	

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4-13. Correlation coefficients of training, cybersecurity awareness, and components of cybersecurity awareness.

4.4.1.2 Analysis of correlation between formal and informal learning approaches

Further analysis was conducted to investigate a relationship between types of learning methods (formal vs. informal training) and cybersecurity awareness. Thus, the responses to the question about learning methods were grouped into formal (184 students) and informal (194 students) training. Ten students who answered that they had not learned cybersecurity were excluded from both categories.

Table 4-14 and Table 4-15 show descriptive statistics of overall cybersecurity awareness, cybersecurity knowledge, privacy, password management and trust for formal and informal training.

Formal training	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	180	2.46	4.65	3.80	0.39
Cybersecurity knowledge	180	2.45	5.00	3.94	0.50
Privacy	180	2.50	4.88	3.89	0.49
Password management	180	1.60	5.00	3.76	0.64
Trust	180	1.00	5.00	2.76	0.97

Table 4-14. Descriptive statistics of the students in formal training group.

Informal training	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	194	2.35	4.62	3.60	0.42
Cybersecurity knowledge	194	2.18	4.82	3.74	0.52
Privacy	194	1.38	5.00	3.72	0.58
Password management	194	1.80	5.00	3.53	0.69

Informal training	N	Minimum	Maximum	Mean	Std. Deviation
Trust	194	1.00	5.00	2.48	1.05

Table 4-15. Descriptive statistics of the students in informal training group.

Table 4-16 shows the degrees of correlation between learning methods, cybersecurity awareness, and each component of cybersecurity awareness. In the data analysis, the formal training was coded 1 and informal training coded 2. The correlation results revealed a statistically significant relationship between the learning methods and cybersecurity awareness r_s (372) = -.241, p < .0005. The negative sign means that the average value of cybersecurity awareness for informal training (3.60) was lower than the formal training (3.80). Similar to the analysis described in 4.4.1.1, if the groups of learning methods were coded 1 for informal training and 2 for formal training, the correlation coefficients would be positive. The statistically significant results with either a positive or a negative sign could be interpreted that students who formally learned about cybersecurity showed higher degree of cybersecurity awareness than those who relied on informal learning approaches.

The study also investigated relationships between learning methods and cybersecurity knowledge, privacy, password management, and trust. For each part of the cybersecurity awareness, the analysis also showed statistically significant correlation results. All negative correlation values mean that students in the informal training group had lower average scores than those in the formal training group.

	Correlation Coefficient	Sig. (2-tailed)	N
Learning approach	1.000		374
Cybersecurity awareness	-.241**	0.000	
Cybersecurity knowledge	-.179**	0.000	
Privacy	-.148**	0.004	
Password management	-.181**	0.000	
Trust	-.148**	0.004	

Table 4-16. Correlation coefficients of learning approach, cybersecurity awareness, and components of cybersecurity awareness.

**. Correlation is significant at the 0.01 level (2-tailed).

4.4.2 Major and cybersecurity awareness

Major was identified based on the college selected by the students. Since the main fields of study offered in the university are related to finance and economics, the majors were divided into two categories: finance (213 students) and non-finance (171 students) for the data analysis. Non-finance related majors included the International Institute of Language and Culture, School of Tourism and Hotel Management, School of City and Environment, Law School, School of Media and Design Art, School of Information, School of Statistics and Mathematics, Ministry of Sports, and others. Spearman correlation analysis was conducted to examine the relationship between major and cybersecurity awareness. The study also investigated relationships between majors and cybersecurity knowledge, privacy, password management, and trust.

Table 4-17 and Table 4-18 show descriptive statistics of overall cybersecurity awareness, cybersecurity knowledge, privacy, password management and trust for finance and non-finance related majors. In Table 4-17, some students with the finance-related majors rated 5 for all items of cybersecurity knowledge, privacy, password management and trust, resulting in the maximum value of means at 5.00. However, none of them rated 5 for all 26 statements. That’s why, the maximum mean of cybersecurity awareness was 4.65.

As shown in Table 4-19, none of the correlation results were statistically significant. The results could be interpreted that the field of study had nothing to do with the degree of cybersecurity awareness. Cybersecurity awareness was similar among finance-related and non-finance related majors.

Finance-related major	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	213	2.35	4.65	3.66	0.45
Cybersecurity knowledge	213	2.18	5.00	3.78	0.54
Privacy	213	1.38	5.00	3.81	0.60

Finance-related major	N	Minimum	Maximum	Mean	Std. Deviation
Password management	213	1.60	5.00	3.61	0.72
Trust	213	1.00	5.00	2.54	1.00

Table 4-17. Descriptive statistics of students with finance–related majors.

Non – finance related major	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	171	2.42	4.50	3.71	0.39
Cybersecurity knowledge	171	2.27	4.91	3.88	0.49
Privacy	171	2.00	4.88	3.77	0.47
Password management	171	1.80	5.00	3.64	0.65
Trust	171	1.00	5.00	2.69	1.04

Table 4-18. Descriptive statistics of students with non-finance related majors.

	Correlation Coefficient	Sig. (2-tailed)	N
Major	1.000		384
Cybersecurity awareness	0.069	0.179	
Cybersecurity knowledge	0.099	0.054	
Privacy	-0.065	0.202	
Password management	0.028	0.580	
Trust	0.078	0.125	

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4-19. Correlation coefficients of major, cybersecurity awareness, and components of cybersecurity awareness.

4.4.3 Gender and cybersecurity awareness

In this survey, 109 male and 275 female respondents completed the questionnaire. Average scores of the overall cybersecurity awareness, cybersecurity knowledge, privacy, password management, and trust are shown in Table 4-20 and Table 4-21. Table 4-20 shows the maximum mean values of 5.00 for all four components of cybersecurity awareness as some male students rated 5 for all items of cybersecurity knowledge, privacy, password management and trust. However, the maximum mean of cybersecurity awareness was 4.65 because no male students rated 5 for all 26 statements.

Male	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	109	2.42	4.65	3.53	0.49
Cybersecurity knowledge	109	2.27	5.00	3.66	0.58
Privacy	109	1.38	5.00	3.60	0.61
Password management	109	1.60	5.00	3.49	0.77
Trust	109	1.00	5.00	2.68	1.11

Table 4-20. Descriptive statistics of male respondents.

Female	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity awareness	275	2.35	4.62	3.74	0.38
Cybersecurity knowledge	275	2.18	4.91	3.89	0.48
Privacy	275	2.50	4.88	3.87	0.50
Password management	275	1.60	5.00	3.68	0.65
Trust	275	1.00	5.00	2.58	0.98

Table 4-21. Descriptive statistics of female respondents.

The male group was coded as 1 and female group coded 2. In Table 4-22, there were statistically significant relationships between gender and cybersecurity awareness r_s (382) = .232, $p < .0005$; gender and cybersecurity knowledge r_s (382) = .199, $p < .0005$; gender and privacy r_s (382) = .220, $p < .0005$; and gender and password management r_s (382) = .129, $p = .012$. The positive signs meant that the average scores of each variable for the female group were higher than the male group. Again, this was a correlation analysis between a dichotomous variable (male vs. female) and interval variables. Either positive or negative statistically significant results could be interpreted that female students showed higher degree of cybersecurity awareness than male students. Female students had higher average values of cybersecurity knowledge, privacy, and password management.

	Correlation Coefficient	Sig. (2-tailed)	N
Gender	1.000		384
Cybersecurity awareness	.232**	0.000	
Cybersecurity knowledge	.199**	0.000	
Privacy	.220**	0.000	
Password management	.129*	0.012	
Trust	-0.039	0.442	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4-22. Correlation Coefficients of gender, cybersecurity awareness and components of cybersecurity awareness.

Chapter 5 Discussions & Conclusion

5.1 Discussions

A review of literature related to cybersecurity awareness showed that most studies have realized the significance of cybersecurity education in raising students' awareness of cybersecurity. Nonetheless, no research works examining the relationship between learning and cybersecurity awareness were found. This study hypothesized that receiving formal and informal training about cybersecurity was positively related to the extent of cybersecurity awareness among Chinese undergraduate students. The research hypothesis was supported by the results of Spearman correlation analysis. Students learning about cybersecurity via formal approaches, i.e., university courses, and through informal methods, i.e., websites, social networking groups, and public lectures, rated higher average scores of cybersecurity awareness than those having no training about cybersecurity. Likewise, the training group had higher means of cybersecurity knowledge and privacy than the no training group. However, the mean of password management and trust were not significantly related to cybersecurity awareness.

The data analysis also revealed that formal and informal training had significant relationships with undergraduates' cybersecurity awareness and its four aspects. Even though both formal and informal training could improve the students' overall cybersecurity awareness, cybersecurity knowledge, privacy, password management, and trust, the results showed that the informal learning group had lower means of all variables than the formal education group. For the undergraduates at Yunnan University of Finance and Economics, cybersecurity courses offered at the college seemed to help students in learning about cybersecurity. However, further investigation can be conducted to learn which courses the students from different majors had taken. In sum, the research hypothesis was accepted, confirming that cybersecurity education is essential to the awareness of cybersecurity irrespective of types of learning approaches.

Regarding how the students learned about cybersecurity, nearly half of the respondents obtained knowledge of cybersecurity through university courses (46.9%). The rest of them acquired knowledge through websites (32.3%), social networking communities (14.1%), and public lectures (4.2%). Ten students, accounted for 2.6%, had not obtained knowledge related to cybersecurity. The survey results revealed that the undergraduates depended on informal ways of learning than learning in a university setting. Nevertheless, the limitation of this study was that the questionnaire allowed the students to choose only one answer for their learning methods. More comprehensive surveys on approaches and sources for learning cybersecurity could be performed as future works.

The data analysis was also performed on major and gender. The relationship between major and cybersecurity awareness was not observed in this study. The study’s results were inconsistent with previous research indicating differences in cybersecurity awareness among majors. Surprisingly, in terms of gender, a prior study showed that men had higher awareness of cybersecurity than women (Liu et.al., 2019), but this survey found that women's awareness of cybersecurity was a bit higher than men’s. The results, in addition, revealed that gender was related to cybersecurity knowledge, privacy and password management. However, no correlation between gender and trust was observed. Future research needs to further explore which topics or issues women know better than men so that universities can better design gender specific courses.

In summary, the research have proved through quantitative analysis that students' cybersecurity awareness was related to training and kinds of learning methods. Universities should constantly research and innovate on cybersecurity education, provide undergraduates with better cybersecurity learning approaches, and enhance cybersecurity awareness.

5.2 Conclusion

This research was a descriptive survey research on the cybersecurity awareness among Chinese undergraduate students at Yunnan University of Finance and Economics. Its objectives were to examine how Chinese college students learned about cybersecurity and whether the learning methods had a relationship with the extent of cybersecurity awareness. Cybersecurity awareness was defined in terms of cybersecurity knowledge, privacy, password management, and trust.

Regarding the training and types of learning approaches, the research findings revealed that half of the questionnaire respondents relied on informal learning methods whereas a bit less than half learned from university courses. The results of Spearman correlation analysis supported the research hypothesis. There was a statistically significant relationship between training and cybersecurity awareness. The students in the training group showed higher degree of cybersecurity awareness than those in the no training group. Training also had significant relationships with cybersecurity knowledge and privacy. Again, the undergraduates who either learned about cybersecurity in formal or informal settings rated higher scores on cybersecurity knowledge and privacy than those without any training.

Moreover, statistically significant relationships were found between learning methods and cybersecurity awareness and all of its four components, namely, cybersecurity knowledge, privacy, password management, and trust. Students in the informal training group had lower average scores for all variables related to cybersecurity awareness than those in the formal training group. Based on the findings, universities should consider offering more courses about cybersecurity because students can gain essential information that will make them understand cybersecurity threats and know how to cope with these risks.

The study further explored whether relationships existed between major and cybersecurity awareness, and between gender and cybersecurity awareness. No statistically significant relationships were found for major. However, there were statistically significant relationships between gender and cybersecurity awareness, cybersecurity knowledge, privacy, and password management. Surprisingly, females showed higher scores than males for cybersecurity awareness and three of the components of the cybersecurity awareness. Future research needs to further investigate which topic or issues females know better than males so that universities have a better idea to design courses tailored for each gender.

In conclusion, although the population of this research was college students at a particular university in China, the study contributed to understanding the current situation of cybersecurity awareness among Chinese students. In the future, more surveys can be conducted with undergraduates in other universities to paint a more comprehensive picture of Chinese students’ degree of cybersecurity awareness.

REFERENCES

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing. *5*(2), 23.

Aljohani, W., & Elfadil, N. (2020). Measuring Cybersecurity Awareness of Students: A Case Study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing*, *9*(6), 141-155.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)*, *6*(2), 660-666.

Alqahtani, M. A. (2022a). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Computational Intelligence and Neuroscience*.

Alqahtani, M. A. (2022b). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5), 2589.

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, and crowding*.

Alwanain, M. I. (2019). An Evaluation of User Awareness for the Detection of Phishing Emails. *International Journal of Advanced Computer Science and Applications*, *10*(10).

Alzahrani, L. (2021). Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. *International Journal of Advanced Computer Science and Applications*, *12*(11).

Cai, Z., & Li, D. (2022). 网络诈骗防范中大学生观念安全的培育(The cultivation of college students' concept security in the prevention of cyber fraud). *Education Observe*(08), 39-41+47.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*, 133-155.

China Internet Network Information Center, C. A. o. C., & Commission, O. o. t. C. C. A. (2021). *The 47th China Statistical Report on Internet Development*.

China Internet Network Information Center, C. A. o. C., & Commission, O. o. t. C. C. A. (2022). *The 50th China Statistical Report on Internet Development*.

China, M. o. P. S. o. t. P. s. R. o. (2022a). *2021 年电信网络诈骗热点案例盘点(An inventory of hot cases of telecom cyber fraud in 2021)*. C. A.-C. Report.

China, M. o. P. S. o. t. P. s. R. o. (2022b). *2021 年电信网络诈骗状况分析(Analysis of telecom cyber fraud in 2021)*. C. A.-C. Report.

Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK case study on cybersecurity education and accreditation. *2019 IEEE Frontiers in Education Conference (FIE)*, 1-9.

Elmi, A. H. (2019). A Survey on Cyber Security awareness among university students in Mogadishu. .

Frydenberg, M., & Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, *18*(4), 33-45.

Garba, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series*, *2*(1), 82-86.

Garba, A. A. (2021). Cybersecurity Awareness of University Students in Nigeria: Analysis Approach. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(12), 3739-3752.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *Int. J. Emerg. Technol*, *11*(5), 41-49.

Garrison, C. P., & Posey, O. G. (2006). Computer security awareness of accounting students. *Southwest Decision Sciences Thirty-Sixth Annual Meeting*.

Gefen, D., Rose, G. M., Warkentin, M., & Pavlou, P. A. (2005). Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa. *Journal of Global Information Management (JGIM)*, *13*(1), 54-78.

Giffin, K. (1967). The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychological Bulletin*, *68*(2), 104-120.

Gupta, B., Arachchilage, N., & Psannis, K. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.

Hao, L. (2022). 辅导员视域下大学生网络诈骗防范研究(Research on college students' cyber fraud prevention from the perspective of counselors). *公关世界*(08), 31-32.

Hart, S., Andrea, M., Federica, P., & Vladimiro, S. (2020). Risk: A Serious Game for Cyber Security Awareness And Education. *Computers & Security*, 95.

Jin, Y. (2022). 坚守心理防线，让骗局无处遁形——大学生受害者心理分析及防范策略(Stick to the Psychological Defense Line, Let the Deception No Place to Escape -- Psychological Analysis of College Students' Victims and Preventive Strategies). *心理与健康*.

Kader, N. A. (2020). CYBER SECURITY AWARENESS-A NECESSITY FOR MORE PRODUCTIVE DIGITAL EXPERIENCE. *IJRAR- International Journal of Research and Analytical Reviews* *7*(2), 174-177.

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(421), 11-14.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, *63*, 967-985.

Li, B. (2018). *Research on College Students' Internet Literacy in the Context of Ideological and Political Education* [Master, Hebei Economy and trade University].

Li, G., & Wen, Y. (2022). Research on the Detection Countermeasures of Telecommunication Network Fraud Based on Big Data for Killing Pigs and Plates. *Journal of Robotics*, 1-11.

Liu, C., Wang, Z., Wang, C., Liu, Y., & Wang, H. (2020). The Status Quo and Effects of Undergraduate Students' Cybersecurity Judgment: A study in China. *Journal of Physics: Conference Series 148*. (IOP)

Luhmann, N. (1979). *Trust and power*. London: John Wiley and Sons.

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *Acm Inroads*, *5*(1), 47-52.

Mathisen, J. (2004). *Measuring Information Security Awareness. A survey showing the Norwegian way to do it*

McKnight, D. H., & Chervany, N. L. (2002). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, *6*(2), 35-53.

McPhee, C., & Bailetti, T. (2014). Cybersecurity. *Technology Innovation Management Review*, *4*(10), 3.

Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty*. CRC Press.

Moallem, A. (2021). CYBERSECURITY, PRIVACY, AND TRUST. *HANDBOOK OF HUMAN FACTORS AND ERGONOMICS*, 1107–1120.

Nurse, J. R. (2021). Cybersecurity awareness. *arXiv preprint arXiv:2103.00474*.

Pal, S. S. (2022). *MCDM for Selection of Cybersecurity Technologies Used in Cybersecurity Education* [Doctoral dissertation, The George Washington University].

Province, P. S. D. o. S. (2018). *Shandong public security issued a warning: These are common telecom network fraud techniques*.

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

Reichheld, F. F., & Schefter, P. (2000). Eloyalty: Your secret weapon on the Web. *Harvard Business Review*, *78*(4), 105-113.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer affairs*, *39*(2), 339-362.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineerin*, *263*(4). (IOP)

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26.

Song, C. (2020). *Research on the Cultivation of College Students' Network Literacy in the New Era*. [Master, Jilin Agriculture University].

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality–an empirical study. *Accounting and Management Information Systems, 15*(1), 112-130.

Stieglitz, S., Zerfaß, A., Ziegele, D., Clausen, S., & Berger, K. (2022). Cybersecurity. *Communications Trend Radar 2022. Language awareness, closed communication, gigification, synthetic media & cybersecurity*, 29.

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Proceeding of the 6th Global Summit on Education*, 1-14.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education*, *48*(6), 1273-1296.

Tencent. (2019). *2019 年上半年电信网络诈骗治理研究报告(The Research Report on the Governance of Telecommunications and Cyber Fraud)*.

Tibi, M. H., Hadeje, K., & Watted, B. (2019). CybercrimeAwareness among Students at a Teacher Training College. *Int. J. Comput. Trends Technol*, *67*(6), 11-17.

Wang, G. (2020). *Study on the Cultivation Path of Network Security Consciousness of Contemporary College Students* [Master, Changsha University of Science & Techonology].

Warf, B. (2018). *The SAGE Encyclopedia of the Internet*. Sage.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, *10*(9), 533-537.

Wolf, S., Burrows, A. C , Borowczak, M., Johnson, M., Cooley, R, & Mogenson, K. (2020). Integrated outreach: Increasing engagement in computer science and cybersecurity. *Education Sciences*, *10*(12), 353.

Wu, Y. (2018). *Research on the Cultivation of Network Security Consciousness of College Students in the Media Age* [Master, China West Normal University].

Xiang, Y., & Kang, R. (2022). 高校电信网络诈骗现状分析及防范策略研究 Analysis of the current situation of university telecommunication and cyber fraud and research on preventive strategies. *Legality Vision*(08), 148-150.

Yan, X. (2020). *The research of problems and countermeasures for college students' network security education* [Master, Hunan Normal University].

Yu, M. (2019). *The Research on Network Security Awareness Cultivation of College Students* [Master, Northeast Forestry University].

Zhang, H. (2020). Research on the Cultivation of College Students' Network Security Awareness in the New Situation. *Journal of Hubei Open Vocational College*, 49-50+57.

Zhang, J. (2017). *网络安全意识提升(Cybersecurity awareness promotion)*.

Zheng, W. (2022). 人民安全视角下大学生电信网络诈骗防范路径研究(Research on the prevention path of college students' telecom network fraud from the perspective of people's security). *Journal of Taiyuan Urban Vocational College*.

Zhou, P. (2021). *Research on the problems and countermeasures of college students network information security consciousness* [Master, Changchun University of Science and Technology].

Zou, H. (2022). 着眼全民全社会数字素养提升 推动网络安全意识教育创新发展(Focusing on the improvement of digital literacy of the whole people and society, promoting the innovative development of network security awareness education). *China Information Security*(01), 28-31.

Appendix A IOC score table

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
Q1	What is your gender?	1	1	1	3	1.00	Accept	Q1: What is your gender?
Q2	What is your age?	1	1	1	3	1.00	Accept	Q2: What is your age?
Q3	What is your year of study?	1	0	1	2	0.67	Accept	Q3: What is your year of study?
Q4	Which school/institute are you studying at?	1	1	1	3	1.00	Accept	Q4: Which school/institute are you studying at?
Q5	Have you ever learned cybersecurity?	1	1	1	3	1.00	Accept	Q5: Have you ever learned cybersecurity?
Q6	I know what two-factor authentication (2FA) is.	1	1	1	3	1.00	Accept	Q6: I know what two-factor authentication (2FA) is.
Q7	I know the difference between using HTTP and HTTPS.	1	1	1	3	1.00	Accept	Q7: I know the difference between using HTTP and HTTPS.
Q8	I know what cookies are.	1	1	1	3	1.00	Accept	Q8: I know what cookies are.
Q9	When I receive a strange call and the other person say he/she know my name, ID number, phone number, address and so on, I believe that the other side is a	1	-1	1	1	0.33	Revise/ Remove	Q9*: When I receive a strange call and the other person say he/she know my name, ID number, phone number,

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
	good person.							address and so on, I believe that the other side is a good person.
Q10	I avoid clicking links in emails or messages sent by an unknown person.	1	1	1	3	1.00	Accept	Q10: I avoid clicking links in emails or messages sent by an unknown person.
Q11	When I receive an email requiring my credential information such as name, date of birth, age, credit card number, I should reply to this email.	1	0	1	2	0.67	Accept	Q11: When I receive an email requiring my credential information such as name, date of birth, age, credit card number, I should reply to this email.
Q12	When I use a computer in public spaces, such as Internet cafes, or libraries, to log into my online accounts, I always log out before I leave the computer.	1	1	1	3	1.00	Accept	Q12: When I use a computer in public spaces, such as Internet cafes, or libraries, to log into my online accounts, I always log out before I leave the computer.
Q13	When websites ask me to accept their cookies policy, I do not read the information and click "Accept Cookies" immediately.	1	1	0	2	0.67	Accept	Q13: When websites ask me to accept their cookies policy, I do not read the information and click "Accept Cookies" immediately.

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
Q14	I know what I should do (call the police, seek help from school or parents) when I know that my personal information has been compromised.	1	1	-1	1	0.33	Revise/ Remove	Q14*: I know what I should do (call the police, seek help from school or parents) when I know that my personal information has been compromised.
Q15	I do not install software that is not verified by the standard App store.	1	0	1	2	0.67	Accept	Q15: I do not install software that is not verified by the standard App store.
Q16	The security settings and tools slow me down and are pesky. I turn them off or disable them.	1	1	1	3	1.00	Accept	Q16: The security settings and tools slow me down and are pesky. I turn them off or disable them.
Q17	I am worried if my personal information was not securely kept online.	1	1	1	3	1.00	Accept	Q17: I am worried if my personal information was not securely kept online.
Q18	I only provide my personal information when I was asked by an organization that I know well.	1	1	1	3	1.00	Accept	Q18: I only provide my personal information when I was asked by an organization that I know well.
Q19	I am worried when I received any suspicious online advertisement.	-1	0	1	0	0.00	Revise/ Remove	Q19: When I receive links for **any promotional content, e.g., job advertisement, sales promotion, etc.,** I click them without checking whether they come from official or trusted

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
								sources.
Q20	I provide my personal information whenever I received calls from strangers.	1	-1	1	1	0.33	Revise/ Remove	Q20: **I am willing to give my personal information to anyone asking for it, even if they are strangers.**
Q21	I add a complete personal profile on my social media account because I want other people to know details about me.	1	0	1	2	0.67	Accept	Q21: I add a complete personal profile on my social media account because I want other people to know details about me.
Q22	I often share activities in my daily life with the public on social media applications.	1	1	1	3	1.00	Accept	Q22: I often share activities in my daily life with the public on social media applications.
Q23	I am concerned that I am asked for too much personal information when I register or make online purchases.	1	1	1	3	1.00	Accept	Q23: I am concerned that I am asked for too much personal information when I register or make online purchases.
Q24	I usually reject requests of mobile applications for accessing my contacts or locations.	1	1	1	3	1.00	Accept	Q24: I usually reject requests of mobile applications for accessing my contacts or locations.
Q25	I use passwords that are difficult to guess as account passwords, such as	1	1	1	3	1.00	Accept	Q25: I use passwords that are difficult to guess as account

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
	excluding initials and birthdays.							passwords, such as excluding initials and birthdays.
Q26	I am worried that my password is not strong enough.	1	1	1	3	1.00	Accept	Q26: I am worried that my password is not strong enough.
Q27	My social media account, email account, and online bank account use the same password.	1	1	1	3	1.00	Accept	Q27: My social media account, email account, and online bank account use the same password.
Q28	I do not share the username and password of my social media account, email account, or online bank account with others.	1	1	1	3	1.00	Accept	Q28: I do not share the username and password of my social media account, email account, or online bank account with others.
Q29	I use two-factor authentication (2FA) for my online accounts whenever it is possible.	1	0	1	2	0.67	Accept	Q29: I use two-factor authentication (2FA) for my online accounts whenever it is possible.
Q30	I believe that the online infrastructures of organizations such as schools, banks, and online services providers are secure and not easy to break into.	1	1	1	3	1.00	Accept	Q30: I believe that the online infrastructures of organizations such as schools, banks, and online services providers are secure and not easy to break into.

Items	Questions	Item-Objective Congruence (IOC) score					Results	Developed questions
		Expert1	Expert2	Expert3	Total score	Average score		
Q31	I believe that social media applications will not disclose my shared photos or address if I do not give a permission.	1	1	1	3	1.00	Accept	Q31: I believe that social media applications will not disclose my shared photos or address if I do not give a permission.
Q32	I read an application user agreement before clicking the "I accept" button.	1	-1	-1	-1	-0.33	Revise/ Remove	

*Though the experts suggested that Q9 and Q14 should be placed in the section of privacy, the researcher did not follow this recommendation as the focus of Q9 and Q14 was on students' ability to detect and handle potential cybersecurity risks. In other words, Q9 and Q14 were appropriate for the section of cybersecurity knowledge because they were in accordance with identification of internet fraud and appropriate practices.

Appendix B Questionnaire

Appendix B: Questionnaire

At present, cybersecurity has become an inevitable and rigorous problem in cyberspace. While using the cyber, you do not lack the trouble of cyber fraud, phishing SMS and other problems. In order to better understand the current cybersecurity awareness of undergraduates and the education methods of cybersecurity, we will investigate the cybersecurity awareness of undergraduates. Please fill in according to the actual situation. Thank you for your cooperation and participation!

Note: This questionnaire is only for undergraduate students. If you are a student with a master’s degree or above, please do not answer this questionnaire.

Part 1 Basic Information

The following questions will involve your basic information. Please answer truthfully.

1. What is your gender?

   A. Male

   B. Female

2. What is your age?

   ____

3. What is your year of study?

   A. Freshman

   B. Sophomore

   C. Junior

   D. Senior

4. Which school/institute are you studying at?

   A. Business School

   B. School of Economics

   C. Accounting School

   D. International Institute of Language and Culture

E. School of Logistics

F. School of Tourism and Hotel Management

G. School of City and Environment

H. Institute of Finance

I. School of Finance and Public Administration

J. Law School

K. School of Media and Design Art

L. School of Information

M. School of Statistics and Mathematics

N. International Business School

O. Ministry of sports

5. Have you ever learned cybersecurity?

A. Yes, I have. I learned from university course.

B. Yes, I have. I learned from websites.

C. Yes, I have. I learned from social cybering communities.

D. Yes, I have. I learned from public lecture.

E. No, I have not.

Part 2 Cybersecurity Awareness

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Cybersecurity Knowledge					
6. I know what two-factor authentication (2FA) is.					
7. I know the difference between using HTTP and HTTPS.					
8. I know what cookies are.					
9. When I receive a strange call and the other person say he/she knows my name, ID number, phone number, address and so on, I believe that the other side is a good person.					
10. I avoid clicking links in emails or messages sent by an unknown person.					
11. When I receive an email requiring my credential information such as name, date of birth, age, credit card number, I should reply to this email.					
12. When I use a computer in public spaces, such as Internet cafes, or libraries, to log					

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
into my online accounts, I always log out before I leave the computer.					
13. When websites ask me to accept their cookies policy, I do not read the information and click "Accept Cookies" immediately.					
14. I know what I should do (call the police, seek help from school or parents) when I know that my personal information has been compromised.					
15. I do not install software that is not verified by the standard App store.					
16. The security settings and tools slow me down and are pesky. I turn them off or disable them.					
Privacy					
17. I am worried if my personal information was not securely kept online.					
18. I only provide my personal information when I was asked by an organization that I know well.					
19. When I receive links for any promotional content, e.g. job advertisement, sales promotion, etc., I click them without checking whether they come from official or trusted sources.					
20. I am willing to give my personal information to anyone asking for it, even if they are strangers.					
21. I add a complete personal profile on my social media account because I want other people to know details about me.					
22. I often share activities in my daily life with the public on social media applications.	`				
23. I am concerned that I am asked for too much personal information when I register or make online purchases.					
24. I usually reject requests of mobile applications for accessing my contacts or locations.					
Password Management					
25. I use passwords that are difficult to guess as account passwords, such as excluding initials and birthdays.					
26. I am worried that my password is not strong enough.					
27. My social media account, email account, and online bank account use the same password.					
28. I do not share the username and password of my social media account, email account, or online bank account with others.					
29. I use two-factor authentication (2FA) for my online accounts whenever it is possible.					
Trust					

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
30. I believe that the online infrastructures of organizations such as schools, banks, and online services providers are secure and not easy to break into.					
31. I believe that social media applications will not disclose my shared photos or address if I do not give a permission.					

VITA

NAME	Xiaoyu Du
DATE OF BIRTH	27 July 1998
PLACE OF BIRTH	China
INSTITUTIONS ATTENDED	Faculty of Arts
HOME ADDRESS	Yunnan Province, Kunming City, Dianchibowu Building7, 1703