Journal for the Education of Gifted Young Scientists, 11(3), 351-367, Sept 2023
e-ISSN: 2149- 360X
jegys.org
dergipark.org.tr/jegys

youngwisepub.com
gencbilgeyayincilik.com

Research Article

A survey on college students' cybersecurity awareness and education from the perspective of China

Hongbo Guo [1] and Hasan Tinmaz[2*]

General graduate school, Woosong University, Daejeon, South Korea

Article Info

Received: 6 July 2023
Accepted: 30 August 2023
Available online: 30 Sept 2023

Keywords
College students
CSA
Cybersecurity
Higher education
Information security
Information security education

Abstract

As people increasingly rely on information and communication technology (ICT), a variety of cyber security issues are emerging, making improving cyber security awareness (CSA) an important topic. This quantitative study focuses on a group of college students from eight local public universities in China (n=1710) and aims to investigate their CSA and education levels using a 32-question questionnaire. Descriptive statistics and cross analysis were used to analyze the current situation related to cybersecurity in college. The results showed that nearly 50% of students spend more than four hours online, with female students spending more online time than males. Smartphones are currently the most popular devices, and spam is the most common issue they encounter. Descriptive statistics, independent samples t-test, and One-way ANOVA test were used to analyze the levels of CSA and education. For CSA, all students are still weak in their password practices. Male students have higher CSA levels in usage habit related to device and HTTP use, but female students perform better in social media. Majors do not make a significant difference in CSA, and freshmen perform better than juniors in device and HTTP application. Regarding cybersecurity education, almost all students believe that colleges need to strengthen information security education. Male students are more familiar with cybersecurity laws, and there are differences in the education methods chosen by students in different majors. Students majoring in computer-related fields prefer more specialized knowledge. This study not only provides valuable insights into the prevailing state of CSA among college students but also offers effective recommendations for enhancing cybersecurity education practices in colleges. The findings underscore the importance of addressing weaknesses in password practices and emphasize the need for comprehensive educational approaches that encompass various facets of cybersecurity. Institutions should consider tailoring their instructional strategies to meet the unique needs of students from diverse academic disciplines. Moreover, fostering awareness of cybersecurity laws and regulations is crucial for all students, regardless of their major.

To cite this article:

Guo, H., & Tinmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. *Journal for the Education of Gifted Young Scientists*, *11*(3), 351-367. DOI: http://dx.doi.org/10.17478/jegys.1323423

Introduction

With the rapid advancement of information technology and the widespread adoption of network systems, individuals have become increasingly dependent on the Internet, which has permeated various aspects of daily life, including education, public services, payments, social interactions, and entertainment. According to the 49th Statistical Report on

[1] PhD Candidate, General graduate school, Woosong University, Daejeon, South Korea. School of Information Engineering, Yulin University, Yulin, China E-mail: forestway@163.com ORCID: 0000-0001-9048-3656
[2] Corresponding Author: Assist. Prof., Endicott College of International Studies, AI & Big Data Department, Daejeon, South Korea. E-mail: htinmaz@endicott.ac.kr ORCID: 0000-0003-4310-0848

Internet Development in China, published by the China Internet Network Information Center (CNNIC) in February 2022, the number of Internet users in China had surpassed 1.032 billion by the end of 2021, with a penetration rate of 73.3%, and 35% of these users were under the age of 29 (CNNIC, 2022). While the Internet has brought immense convenience and revolutionized global lifestyles, it also carries potential negative consequences if misused (Annansingh & Veli, 2016). The instability and insecurity prevalent in cyberspace pose significant threats to both individuals and organizations (Li, Tsigkanos, Jin, Hu & Ghezzi, 2020).

The widespread adoption of the Internet has introduced numerous cyber-related risks, including cyber addiction, personal information exposure, and online fraud (Ratten & Vanessa, 2015). The CNNIC reported that many Chinese Internet users experienced network security problems in 2021, with 22.1% of all netizens experiencing personal information leakage, 16.6% encountering online fraud, 9.1% suffering from viruses or Trojan horses on their devices, and 6.6% having their account numbers or passwords stolen in the past six months (CNNIC, 2022).

It is observed that as the age of the youth group increases, the proportion of cyber security incidents also increases. College students are more prone to cyber events compared to primary and secondary school students as they use the internet more widely, and hence face more security problems. Combatting silent privacy invasion through CSA and basic information security skills is found to be an effective strategy for most internet users. For college students, this not only helps in personal data protection on campus but also prepares them to cope with cyber threats in their future workplace. Al-Ghamdi (2021) states that having a good understanding of cyber security can help detect all kinds of malicious incidents and make accurate decisions on the internet. Al-Janabi and Al-Shourbaji (2016) emphasize that good CSA plays an essential role in protecting sensitive information from cyber-attacks.

The emphasis on CSA by Rahim et al (2015) is to equip internet users with the basic ability to detect and deal with cyber threats rather than scare or create apprehension. Although college students' awareness of cyber security may be higher than the average level, previous studies show that they lack adequate information security education to identify potential risks in practical applications (Sarathchandra, Haltinner & Lichtenberg, 2016). The cybersecurity level is considered as a touchstone to measure a country's cyber strength, which reflects a country's strategic political status among other countries (Gamreklidze, 2015).

The Chinese government has made cyber security a part of its national strategy, and various industries spend a considerable amount on network security construction annually. Most colleges are also gradually improving their network security infrastructure and offer information security courses for computer-related majors. However, universities in China have not given much attention to their students' cybersecurity training and education. Therefore, improving the cyber security level of every student is an important and meaningful question for higher education.

To address the issues mentioned above, it is necessary to explore the current level of CSA and the existing problems faced by college students. This paper focuses on the CSA and the basic defense ability of university undergraduates. By issuing a questionnaire to students in a local university and analyzing the data, the study aims to understand the actual situation of CSA and the protection ability of local university students in China. Additionally, the study intends to provide reasonable suggestions for improving students' CSA and protection skills in local universities.

Literature Review

Related Studies

With the widespread application of information technology and the frequent occurrence of cyber threats, a lot of research literature on network security has emerged. In the last few decades, most academic research in this field has focused on cybersecurity technology, which has been summarized into different research communities such as cryptography, identity authentication, and so on (Katsikeas, Johnson, Ekstedt & Lagerström, 2021). However, there has been a gradual increase in research interest on CSA, which is also known as ISA in recent years (Corallo, Lazoi, Lezzi & Luperto, 2022). This phenomenon shows that information security is no longer just the business of professionals, but also closely related to users' ISA. As approximately every world citizen is an internet user nowadays, only hardware or software technology cannot guarantee information security. Therefore, we can say that improving users' ISA and training their basic network security skills is essential in every industry today.

Most of the existing literature related to ISA has focused on assessing and promoting ISA among individuals, organizations, and countries. Others were mainly interested in exploring interconnections between behavior habits, psychological activities, and people's ISA. This paper divides all the relevant literature into three categories based on their research objectives and scope.

The first literature category focuses on CSA among individuals in society and employees in organizations. Okesola et al (2016) used quantitative methods to assess an individual's level of awareness of cybersecurity risks in southwest Nigeria and found that most users of social networks, especially female users, have low CSA. Grassegger and Nedbal (2021) stated that focusing only on technical measures is not enough to ensure the information security for the organizations, and improving ISA for all employees is also essential. From the perspective of activity theory, Ho and Gross (2021) proposed a conceptualization of cyber defense as an activity system, offering a transformative approach to enhancing organizational cyber awareness. Some scholars also suggest that organizations should provide specially designed electronic or board games to train and improve their employees' ISA (Hart, Margheri, Paci & Sassone, 2020).

The second literature category focuses on the investigation and education of teenagers' ISA. Maennel et al (2019) believe that it is far from enough to put ISA education at the college level. Both the awareness and ability of cybersecurity should be taught and developed as an essential skill among children. Kritzinger et al. (2017) analyzed the current level of ISA and existing measures of school learners in the South Africa and United Kingdom, compared the differences between developing and developed countries in the construction of ISA, and finally gave suggestions for the two countries respectively. Annansingh and Veli (2016) discussed the Internet risks awareness and e-safety needs of children and gave some suggestions to parents and relevant government departments. Elbedour et al (2020) discussed the negative impact of cyberbullying on society and then, from the perspective of prevention and intervention, believe that school psychologists and counselors play an important role in this aspect and provide the corresponding practical methods to solve the problem. Quayyum et al. (2021) reviewed all the literature from 2011 to 2021 focusing on the analysis of the sources of network risks for children and found a lot of cyber risk exits everywhere on the Internet.

The third literature category focuses on the intersection of 'college or university' and 'CSA or ISA', which has a similar scope to this paper. However, some of these studies have different objectives and directions. Alqahtani (2022) assessed ISA among university students using a quantitative research method, finding that knowledge of password security, browser security, and social media activity had a significant impact on students' ISA. Senthilkumar and Easwaramoorthy (2017) surveyed college students to investigate their level of network security awareness and believed that perfect ISA could help students better protect themselves from hacker attacks. Al-Janabi and Al-Shourbaji (2016) investigated the ISA level of students and staff in educational environments in the Middle East and found that comprehensive ISA training programs could remedy the lack of necessary knowledge and understanding of information security. Garba et al (2020) surveyed students about their basic knowledge of ISA in Yobe State University (Nigeria) and suggested that corresponding ISA programs should be established gradually. The study also found that female students are more likely to be victims of cyber-attacks, and college students are enthusiastic about learning more about cybersecurity.

Limited research exists on college students' ISA or CSA in China. Xu et al (2019) analyzed the ISA level and protection skills of postgraduates in nine universities in Beijing and found that their education in this field needs to be strengthened. Liu and Chen (2021) identified weak awareness of personal information security and insufficient education subjects' publicity as the main problems in information security protection of college students from the perspective of telecom fraud.

Significance of the Study

Numerous scholars have conducted research on cyber security risks, primarily focusing on cyber security technologies. However, in today's digital age, where nearly everyone is an internet user, relying solely on technology for protection against cyber threats is insufficient (Al-Janabi & Al-Shourbaji, 2016). Therefore, enhancing users' awareness and skills is crucial to effectively address cyber security threats, which are as important as information technology for individuals and organizations. Specially, as future professionals, university students need to possess fundamental cyber security skills to meet the demands of the network age.

Regrettably, there is a significant dearth of quantitative research in this field in China. Therefore, this study aims to bridge this gap by conducting a quantitative investigation on CSA among college students. The findings of this study can offer valuable insights for local universities in China (or similar cases outside of China) to develop and enhance students' CSA and information security practices. Furthermore, this study holds reference value for examining CSA in other organizations or industries.

Conceptual Framework

This research intends to analyze the cyber security levels of college students from the perspectives of awareness and education. Regarding the cybersecurity awareness assessment, this study used the three aspects of password management, usage habit, and social media since these topics are most relevant to college students' daily network operation and are widely employed in similar studies (Alharbi & Tassaddiq, 2021). Since the password is one of the most important components in data and information security (Alqahtani, 2022), it is also risky because it is susceptible to attack.

This study investigates the cybersecurity awareness of usage habits from the perspectives of http and device usage, as they are typical Internet user activities. According to Okesola et al (2016), even though the good function of social media for many activities has continued to develop in recent years, malicious users and hackers have also continued to utilize them as a covert means of assaulting and abusing unwary and ignorant individuals. In terms of cybersecurity education, the purpose of this study is to evaluate college students' perspectives and evaluations of the cyber security education provided by their colleges and institutions. In conclusion, this study creates four dimensions to assess the level of cybersecurity awareness and education possessed by college students.

Research Questions

This study specifically focuses on college students in the Chinese higher education context. Its main objectives are to investigate the current state of cybersecurity, assess the level of awareness and education regarding cybersecurity, and examine the differences in various dimensions of cybersecurity among students based on their gender, grade levels, and majors. The specific research questions addressed in this study are as follows:

Q1: How much time do students usually spend online? What devices do they use daily? What cyber threats do they often encounter?

Q2: Is there any statistically significant difference(s) between male and female students about the online time?

Q3: What kind of cybersecurity education methods do the students like, and is there any difference(s) in the choice of cyber security education methods among students of different majors?

Q4: What is the overall level of cyber security of college students and the performance of various dimensions of password, device and http use, social media, and cyber security education?

Q5: Is there any statistically significant difference(s) between male and female students in each dimension of cyber security and if any, what gender makes the difference?

Q6: Is there any statistically significant difference(s) among students of different majors in each dimension of network security and if any, which major(s) make the difference?

Q7: Is there any statistically significant difference(s) among students of different grades in each dimension of cyber security and if any, which grade(s) make the difference?

Method

Research Model

The researchers utilized cross-sectional research model where the study data collected from participants at a single point in time to analyze further differences and relationships. To serve that purpose, an online quantitative survey was administered to students via WeChat groups, email, and the teaching software platform with the help of university teachers. It is worth mentioning that students were not compelled to complete the questionnaire and participated voluntarily. Data collection was conducted from June to August 2022, which lasted for nearly two months.

Participants

This study initiated by collecting data from undergraduate students at eight public universities in China, which are primarily comprehensive universities with a diverse array of majors and comparatively lower rankings in the country. Convenience sampling was utilized as a non-probability sampling method to collect data from participants who were easily accessible to the researchers, either physically or through the internet. This approach is commonly used and allows for greater practicality in obtaining data (Edgar & Manz, 2017).

Table 1. Demographic information of respondents

Variable	Items	n	%
Gender	Male	774	45.30
	Female	936	54.70
Grade	Freshman	571	33.40
	Sophomore	610	35.70
	Junior	292	17.10
	Senior	237	13.90
Major category	Liberal arts	675	39.50
	Science & Engineering	819	47.90
	Computer related	216	12.60

Finally, a total of 2116 questionnaires were collected, after excluding 406 questionnaires with too short response time and invalid answers, the final sample size has become 1710. According to the data presented in Table 1, there was a relatively equal distribution of male and female respondents, among which 774 were female (45.3%) and 936 were male (54.7%), the participants were mainly freshmen (33.4%) and sophomores (35.7%), which indicates that lower grade students are more active in participation or interested in the topic of cyber security. Regarding the major, 675 participants (39.5%) were from liberal arts, physical and art majors, 819 participants (47.9%) were from science and engineering (non-IT related) majors, and 216 participants were from computer related majors, which is acceptable and consistent with the population of the college students where the questionnaire was issued.

Data Collection Tools

The college students' cybersecurity awareness questionnaire was used in this study comprised 32 items, including 25 scale items are used for measuring the four factors of password, usage habit, social media, and education, as established in previous studies (Alqahtani, 2022; Alharbi & Tassaddiq, 2021), they were assessed using a 5-point Likert scale, ranging from 1 (strongly agree) to 5 (strongly disagree). The remaining 7 items pertained to demographic information, such as gender, grade, major, online time, web device, cyber threats, and education status (Sun, 2018). To facilitate a more comprehensive analysis of cybersecurity education, students were classified into three major categories, namely liberal arts (including art and physical education), science and engineering (excluding IT-related majors), and computer science (Xu, Zeng, Wang, & Zhang, 2019).

The measurement items were originally created in English and later translated into Chinese. Prior to distribution, the initial version of the questionnaire underwent a review by experts in the English language, minor adjustments and modifications was conducted based on expert feedback. This step also functioned as a measure of content validity.

Cronbach's alpha reliability was used to examine the internal consistency of the questionnaire. The Cronbach's alpha coefficient of the twenty-five items was 0.85 (n=1710), which indicates that the reliability of the data is at a good level.

Table 2. The Cronbach's alpha of four dimensions

Dimension	*M*	*SD*	Cronbach's alpha
Password	3.01	0.60	0.73
Device and http use	3.39	0.81	0.83
Social media	3.46	0.82	0.80
Education	3.53	0.71	0.86

Table 2 displays the Cronbach's alpha values for each dimension. These values range from 0.73 to 0.86 and are all greater than 0.70, indicating that the Cronbach's alpha values for each dimension satisfied the requirements for the research. (Morrison 2019).

Results

Descriptive statistics of the online time, devices daily used and cyber threats experienced

In this study, descriptive statistics were used to investigate how much time college students usually spend online, the devices they use on a daily basis, and the types of cyber threats they usually face. All of these factors are frequently connected to the users' level of cybersecurity awareness. In addition, the methods of education in cybersecurity that were found to be most popular among students were investigated in this section.

As shown in Table 3, almost 50% of college students spend more than 4 hours online, with only 8.1% spending less than 2 hours online. The remaining 2-3 hours and 3-4 hours account for 20% and 22%, respectively. In terms of internet devices, smartphones are the most widely used, accounting for 62%, while desktops account for only 1.9%. Based on the analysis, it can be deduced that there is a growing trend of students dedicating more time to online activities. Smartphones have emerged as the favored device, while desktop computers are gradually losing popularity among young individuals in their everyday routines.

To explore numerous cybersecurity issues that most students have encountered, the questionnaire included the special question "What network security threats have you encountered so far?". As presented in Table 3, spam was the most common issue encountered, accounting for 27.3%. Information leakage was also prevalent, accounting for 16.4%. Other network security incidents with high incidence were false rumors (12.4%), online fraud (11.1%), and pornographic information (10.2%). Financial theft, consumer disputes, and cyberbullying were rare among college students. Some students reported not encountering any incidents in this field.

To investigate the education methods that most college students preferred in cybersecurity education, a special question “Which types of education methods that you like to improve your cybersecurity awareness” was proposed in the study. According to Table 3, network media publicity is the most popular education technique selected by students, accounting for 32.4%. Display board or window advertising is another effective method for promoting cybersecurity education in higher education, which accounts for 20.5%. Classroom teaching (16.3%), community activities (14.5%), and special lectures are also popular among students (13.7%). Furthermore, other approaches account for 2.6 percent of the total.

Table 3. Online habits and cyber security issues encountered

Variable	Items	n	%
Online duration	1-2 hours	139	8.10
	2-3 hours	342	20.00
	3-4 hours	377	22.00
	Above 4 hours	852	49.80
Popular device	Smart phone	1674	61.30
	Tablet	271	9.90
	Desktop	53	1.90
	Laptop	735	26.90
Cyber security issues	Virus attacks	524	11.70
	Information leakage	738	16.40
	Spam	1228	27.30
	Financial theft	93	2.10
	Online fraud	499	11.10
	Consumer disputes	153	3.40
	Pornographic	459	10.20
	Cyberbullying	126	2.80
	False rumors	556	12.40
	Others	115	2.60
Education method	Classroom teaching	544	16.30
	Special lecture	458	13.70
	Display board or window publicity	685	20.50
	Community activities	484	14.50
	Network media publicity	1081	32.40
	Others	85	2.60

Cross analysis between gender and online time

To examine the relationship between gender and online time, this study conducted a cross-analysis of the corresponding data. As shown in Table 4, there were gender differences in the time spent on the internet by college students. The significance value of the Chi-Square test was 0.00<0.05 ($\chi 2 = 81.53$, $df = 3$), indicating that the effect of gender on time spent online was significant, with female college students spending more time online than male students.

Table 4. Cross analysis of gender and online time

Gender		Time spent online each day			
		1-2 hours	2-3 hours	3-4 hours	More than 4 hours
Male	n	100	196	137	341
	%	12.90	25.30	17.70	44.10
Female	n	39	146	240	511
	%	4.20	15.60	25.60	54.60

Cross analysis between Major category and education method

For the cybersecurity education, an important objective of this study is to investigate whether students from different majors have varying preferences for educational methods. A specific question about this topic was included in the demographic section of the questionnaire, asking participants to select their preferred method of receiving CSA education from a list of options including classroom teaching, special lectures, and others. Table 5 indicates that there are differences in the choices made by students from different major groups. To further investigate the existence of these differences, the sample size of each major category and the frequency of each education method were considered. The results of the Chi-Square test show a significance value of 0.02 ($\chi 2 = 28.43$, $df = 10$), which is below the threshold of 0.05, indicating that students from different majors indeed have different preferences when it comes to cybersecurity learning methods.

Table 5. Cross tabulation of major category and education method

Major category		Education method					
		Classroom teaching	Special lecture	Display board or window publicity	Community activities	Network media publicity	Other
Liberal arts	n	214	162	291	174	427	38
	%	16.4%	12.4%	22.3%	13.3%	32.7%	2.9%
Science and Engineering	n	248	211	328	244	525	40
	%	15.5%	13.2%	20.6%	15.3%	32.9%	2.5%
Computer related	n	82	85	66	66	129	7
	%	18.9%	19.5%	15.2%	15.2%	29.7%	1.6%

Analysis of the Survey

Table 6 displays the mean scores and standard deviations for each scale item, the results show that the item with the highest mean score is 3.97, suggesting that most students believe that their university should enhance the cultivation of their cybersecurity skills. The second highest mean score is 3.80, indicating that most students do not prefer sharing or sending passwords with their classmates. The third highest mean score is 3.79, which implies that most students think it is essential to set a complex password. On the other hand, the lowest mean scores are all related to passwords. The three questions with the lowest mean scores are 2.24, 2.32, and 2.47, which reveal that more than half of the students use a strong or previous password for different websites and accounts, and almost half of them feel frustrated to have a long and complex password for each website and account. For the four dimensions, the education obtained the highest mean score, while the password was the lowest.

Table 6. The basic statistics of survey questions (n=1710)

Dimension	Survey questions	*M*	*SD*
Password Management	P1. I believe that all passwords should include upper and lower characters, numbers, and symbols.	3.79	1.10
	P2. I change my password periodically.	2.55	1.24
	P3. I use previously used passwords.	2.32	1.15
	P4. I use one strong password for across different websites and accounts.	2.24	1.16
	P5. I feel annoyed to have a long and strong password for each website and account.	2.47	1.18
	P6. I do not mind sharing or sending passwords with my friends.	3.61	1.23
	P7. I do not mind sharing or sending passwords with my family.	3.30	1.27
	P8. I do not mind sharing or sending passwords with my classmates.	3.80	1.18
Usage Habit	U1. The web browser should be updated regularly.	3.52	1.06
	U2. I update my computer regularly.	3.33	1.12
	U3. I install the updates of my phone regularly.	3.55	1.12
	U4. I avoid installing extensions from third-party websites.	3.64	1.06
	U5. I check the security settings and configurations of the web browser periodically.	3.24	1.11
	U6. I check the browser history and find suspicious activities.	3.06	1.15
Social Media	S1. It is ok to accept friend requests from unknown people.	3.56	1.09
	S2. It is acceptable to post personal pictures on social media.	3.30	1.16
	S3. There is no problem with sharing my current location publicly on social media.	3.54	1.1
	S4. There is no problem to add all personal information to social media platforms.	3.77	1.09
	S5. I know how to report any threat or suspicious activity on social media.	2.89	1.07
Education in College	E1. I am familiar with various cyber security laws and regulations issued by the state.	3.23	0.91
	E2. I have developed the ability to deal with common network security threats.	3.33	0.92
	E3. It is necessary for colleges to strengthen the cultivation of college students' cyber security ability.	3.97	0.9
	E4. My college attaches importance to cyber security education.	3.63	0.95
	E5. My college often carries out cyber security education activities.	3.51	0.94
	E6. The effect of network security education in our school is very good.	3.53	0.94

Comparative tests

To analyze the difference in the four dimensions of the survey questions between male and female students, independent samples t-test was conducted. Firstly, the significance of Levene's test was checked for the equality of variances, and then the significance value of independent samples t-test was checked. Table 7 shows that the significance of the password dimension is 0.43, which is higher than 0.05, indicating that there is no significant difference in password behavior between genders of university students. However, the p-values of the other three dimensions are all much less than 0.05, which means that there are significant differences in usage habit, social media, and cybersecurity education between different genders.

Table 2. Independent sample t-tests on gender vs four dimensions

Dimension	Levene's Test		Independent samples t-test		
	F	***p***	***t***	***df***	***p***
Password	0.86	0.35	0.78	1708.00	0.43
Usage habit	19.93	0.00	4.65	1546.22	0.00
Social media	18.34	0.00	5.97	1483.44	0.00
Education	29.30	0.00	2.52	1525.21	0.01

Combining the results of Tables 8, it is obvious that male students' CSA level are higher than female students in the use habit and education. On the other hand, female students scored higher than male students in the social media.

Table 3. The basic statistics of genders in four dimensions of cyber security

Dimension	Gender	n	M	SD
Password (*not significant*)	Male	774	3.00	0.62
	Female	936	3.02	0.58
Usage habit	Male	774	3.49	0.86
	Female	936	3.31	0.75
Social media	Male	774	3.33	0.90
	Female	936	3.57	0.73
Education	Male	774	3.58	0.77
	Female	936	3.49	0.66

To further examine the source of the difference in cybersecurity education between male and female students, additional independent samples t-tests were conducted on each question of the education dimension. As shown in Table 9, the p-values for the first and second questions are both below 0.05, indicating that there are statistically significant differences between genders on these questions.

Table 4. Independent samples t-tests on the items of education dimension

Education item	Levene's Test		Independent samples t-test		
	F	***p***	***t***	***df***	***p***
E1	34.37	0.00	6.13	1590.25	0.00
E2	28.11	0.00	5.43	1583.52	0.00
E3	14.00	0.00	-0.86	1581.06	0.39
E4	19.24	0.00	-0.13	1546.79	0.90
E5	17.56	0.00	0.50	1551.14	0.62
E6	12.68	0.00	0.84	1572.13	0.40

Regarding to the two significant questions, Table 10 demonstrates that male students have more familiarity with legal aspects of cybersecurity and feel more skilled in finding solutions to cyber security problems.

Table 5. The basic statistics of genders in education dimension

Education item	Gender	n	M	SD
E1	Male	774	3.37	0.94
	Female	936	3.10	0.87
E2	Male	774	3.46	0.95
	Female	936	3.22	0.87
E3	Male	774	3.95	0.95
	Female	936	3.99	0.86
E4	Male	774	3.63	1.01
	Female	936	3.63	0.88
E5	Male	774	3.52	1.00
	Female	936	3.50	0.88
E6	Male	774	3.56	0.99
	Female	936	3.52	0.89

The one-way ANOVA test was utilized by the researchers to determine whether there were differences in each measurement dimension of the study for different majors. Equality of variances was indicated by Levene's test of homogeneity of variances, and Tukey post-hoc tests were then conducted. As presented in Table 11, no significant differences were found among majors in the dimensions of password, usage habit, and social media. However, in the education dimension, the first major group was found to be significantly different from the other two groups, while the difference between the other two groups was found to be insignificant. Interestingly, the mean scores of liberal arts students in cybersecurity education were found to be higher than those of students from the other two majors.

Table 11. One-way ANOVA tests on major groups vs four dimensions

Dimensions	Levels*	*n*	*M*	*SD*	*F* (df=1709)	*p*	*Tukey post-hoc test results***
Password	Group 1	675	3.03	0.58	1.125	0.325	NS
	Group 2	819	2.99	0.61			
	Group 3	216	2.98	0.59			
Usage habit	Group 1	675	3.44	0.79	2.687	0.068	NS
	Group 2	819	3.35	0.81			
	Group 3	216	3.34	0.81			
Social media	Group 1	675	3.43	0.82	0.865	0.421	NS
	Group 2	819	3.46	0.82			
	Group 3	216	3.51	0.79			
Education	Group 1	675	3.59	0.72	4.799	0.008	Group 1> Group 2 Group 1 > Group 3
	Group 2	819	3.50	0.70			
	Group 3	216	3.44	0.70			

* Group 1: Liberal arts, physical education and art - Group 2: Science and Engineering (non-IT related) - Group 3: Computer related

**NS: Non-significant

Furtherly, in order to identify the sources of differences in the education of cybersecurity among students from various majors, the study conducted additional One-Way ANOVA tests on each question of the education dimension. Levene's test of homogeneity of variances indicated equal variances, and Tukey post-hoc tests were then conducted. As shown in Table 12, there were no significant differences among majors in E 1, E3, E4, and E5 of the education dimension, while significant differences were observed in E 2 and E6.

Regarding the two questions that exhibited notable distinctions, it was observed that the first main group demonstrated a significant difference from the other two groups, whereas the disparity between the remaining two

groups was not deemed significant. It is noteworthy that the mean scores for the liberal arts category surpassed those of the other two major categories in relation to these two questions.

Table 12. One-way ANOVA tests on different majors vs six items of education dimension

Education item	Levels*	*n*	*M*	*SD*	*F* (df=1709)	*p*	*Tukey post-hoc test results***
E1	Group 1	675	3.27	0.92	2.456	0.086	NS
	Group 2	819	3.22	0.88			
	Group 3	216	3.11	1.00			
E2	Group 1	675	3.43	0.91	6.712	0.001	Group 1> Group 2 Group 1 > Group 3
	Group 2	819	3.29	0.88			
	Group 3	216	3.20	1.02			
E3	Group 1	675	4.01	0.88	2.962	0.052	NS
	Group 2	819	3.91	0.92			
	Group 3	216	4.05	0.90			
E4	Group 1	675	3.68	0.94	2.326	0.098	NS
	Group 2	819	3.62	0.94			
	Group 3	216	3.52	0.95			
E5	Group 1	675	3.57	0.94	3.251	0.039	NS
	Group 2	819	3.48	0.93			
	Group 3	216	3.40	0.94			
E6	Group 1	675	3.62	0.94	5.844	0.003	Group 1> Group 2 Group 1 > Group 3
	Group 2	819	3.49	0.93			
	Group 3	216	3.41	0.94			

* Group 1: Liberal arts, physical education and art - Group 2: Science and Engineering (non-IT related) - Group 3: Computer related

**NS: Non-significant

To investigate whether there were statistically significant differences for each dimension across different schooling levels, a one-way ANOVA test was performed. Since Levene's test of homogeneity of variances indicated equal variances, Tukey post-hoc tests were used to determine which group(s) differed among the four levels. As presented in Table 13, there were no significant differences in password, social media, and education dimensions among different school levels. Regarding usage habit that is represented by device and HTTP use, freshmen were found to be significantly different from juniors, but not from the other two levels, and there were no significant differences between the other school levels. Surprisingly, the mean score of freshmen in the usage habit was higher than those of juniors.

Table 13. One-way ANOVA tests on different school levels vs four dimensions

Dimensions	Levels	*n*	*M*	*SD*	*F* (df=1709)	*p*	*Tukey post-hoc test results**
Password	Freshman	571	3.06	0.61	2.449	0.062	NS
	Sophomore	610	2.99	0.57			
	Junior	292	2.95	0.59			
	Senior	237	3.01	0.65			
Usage habit	Freshman	571	3.46	0.78	3.900	0.009	Freshman>Junior
	Sophomore	610	3.39	0.82			
	Junior	292	3.27	0.78			
	Senior	237	3.36	0.87			
Social media	Freshman	571	3.41	0.86	1.485	0.217	NS
	Sophomore	610	3.46	0.80			
	Junior	292	3.50	0.76			
	Senior	237	3.53	0.85			
Education	Freshman	571	3.55	0.72	2.404	0.066	NS
	Sophomore	610	3.51	0.75			
	Junior	292	3.48	0.58			
	Senior	237	3.63	0.75			

*NS: Non-significant

Discussion

To answer the first research question, it needs to investigate the college students' online duration, device daily use and cyber threats encountered. The results of demographic information showed that nearly half (49.8%) of college students spend more than 4 hours, with spam being the most common cyber threat. False rumors, online fraud, and pornographic content also had high incidence rates among undergraduates in China. Smartphones were the most popular device for online activities, with 61.3% of participants using them. These findings are consistent with a previous study conducted by Sun (2018), in which he found that 42% of college students spend more than four hours online per day, and identified spam as the number one online threat students face. Comparing the online duration between this study and the research of Sun (2018), we can infer that the Internet is more widely used than before with the rapid development of ICT. Regarding Internet access devices, Ahmed et al. (2017) also found that most of the participants (69%) preferred smartphones, which is also similar to the result of this study.

To answer the second research question, the difference between male and female students' online duration was examined. The results of the cross-analysis demonstrated that female college students spend more time online than male students. However, no similar analyses have been conducted in previous studies. This result can potentially be attributed to female students' inclination towards engaging in online activities such as online shopping, social media, and video consumption.

To answer the third research question, it needs to explore the preferred methods of cybersecurity education among students, as well as the variations observed among students from different majors. The study applied cross-analysis again, and the results demonstrated that students of different majors have different preferences in the learning methods of cybersecurity. Students of computer-related majors are more willing to accept professional education methods such as classroom teaching and special lectures, but non-computer majors prefer general education methods such as display boards and window publicity. Interestingly, most students majoring in liberal arts, physical education, or art do not like such a practical educational method as community activities. This result may be caused by the different knowledge backgrounds of different majors. Therefore, considering the knowledge background of students of different majors in the implementation of cybersecurity education is crucial for higher education institutes.

To answer the fourth question, the cybersecurity level of college students and their performance of each cybersecurity dimension including education were assessed. The study found that the overall cybersecurity level of college students is relatively high, which is in line with the findings of the study conducted by Alharbi and Tassaddiq (2021). However, the mean of the password dimension is relatively low compared with the other three dimensions. Specifically, most students can update applications regularly, pay attention to the safe use of devices and browsers, and protect personal privacy on social media. In addition, it is noteworthy that almost half of the participants expressed unfamiliarity with the process of reporting threats or suspicious activities on social media. This finding contrasts with the results of Alharbi and Tassaddiq's (2021) study, where over 70% of respondents claimed knowledge of reporting threats they encountered. This disparity could be attributed to the differences in the sample's countries or cybersecurity education levels. Regarding cybersecurity education, most students believe that colleges should strengthen their cybersecurity education. This finding aligns with previous literature. Garba et al. (2020) found that over 95% of respondents had the desire to learn more about cybersecurity, and it is necessary to teach students how to secure their internet connection. Password protection remains a significant problem and needs to be improved, which is consistent with previous literature. Moallem (2018) discovered that while most students recognize the importance of CSA, but they still do not pay much attention to security practices such as using strong passwords for different websites or avoiding weak passwords. Alharbi and Tassaddiq (2021) found that 60.7% of students found strong and long passwords annoying and used the same password for all their accounts and websites. The researchers believe that students lack sufficient cybersecurity knowledge, particularly in regards to passwords, or may not have experienced password incidents that directly caused trouble, causing them to undervalue the importance of passwords in their daily online activities. This finding underscores the potential for a gap between practicing good security measures and possessing adequate knowledge and understanding (Rajesh Chandarman & Brett Van Niekerk, 2017).

To answer the fifth question, it needs to examine the differences between male and female students in each measurement dimension of cyber security. The results of the independent samples t-test demonstrated that students of different genders exhibit significant differences in usage habits, social media, and education, but not in password. Male students' CSA is higher than female students' in usage habits and education, but female students perform better in social media, indicating that female students pay more attention to personal privacy protection, while male students attach more importance to practice. Regarding the differences in cybersecurity education, male students are familiar with legal issues of cybersecurity and feel more skillful in the solutions of network security issues. This is similar to the conclusion that males have better knowledge of cybersecurity than females found by Garba et al. (2020).

To answer the sixth research question, the differences among students of different majors in each measurement dimension were examined. The results of the One-way ANOVA test showed that the major category has no significant difference in password, usage habits, and social media. Surprisingly, computer major students' level is equal to other majors, although they have learned more IT knowledge from their professional courses. This finding is in line with the view that participants who show good IT knowledge in the survey are still weak in practice (Alotaibi et al., 2016). However, the first major group (liberal arts) is significantly different from the other two groups in education. Interestingly, the average mean of students in liberal arts is higher than that of students in the other two major categories in cybersecurity education, which is very consistent with the research of Sun (2018). To further explore where the differences exist, each question of education was tested. Interestingly, the results showed that students in liberal arts have great confidence in their cybersecurity ability and satisfaction with college education in cybersecurity. The study believes that the result may be due to differences in knowledge structure. Students majoring in liberal arts lack sufficient computer knowledge and understanding, so they think the knowledge is simple, and the skill is easy to master in the cybersecurity field.

To answer the last research question, the differences among students of different grades were examined by the One-way ANOVA test. The study found that school levels do not make a significant difference in CSA except for education. Similarly, the research of Matyokurehwa et al. (2020) reported that there is no statistically significant association between age and CSA. Surprisingly, the study found that freshmen perform better in usage habits of HTTP and devices, which

indicates that students' CSA levels do not improve or may even decrease during college in certain cybersecurity practices. The reason can be attributed to the fact that the university did not provide continuous cybersecurity education, so the education must be strengthened in higher education. On the other hand, students in higher grades think they are already proficient in using network applications, so they may think it is no longer necessary to attach importance to cyber risks.

Conclusion and Implications

In the context of limited literature on cybersecurity awareness and education for college students, this study utilized a quantitative approach and collected data through a survey instrument from ten local universities in China. Firstly, the study investigated students' online habits and the cybersecurity incidents they encountered, revealing that nearly half of the students spend more than 4 hours online daily, and female students tend to spend more time online than male students. Secondly, by analyzing data from the perspective of three cybersecurity dimensions: password, usage, and social media, the study found that most students have good awareness but weak practical skills, and gender, grade, and major also influence CSA. Lastly, through analyzing the participants' responses to education data, most students considered cybersecurity education necessary for colleges, and students of different majors had certain differences in the choice of cybersecurity education methods and self-evaluation of cybersecurity. Overall, despite having a certain level of awareness and knowledge of cybersecurity, college students still need to improve their practice skills, and colleges and universities should strengthen cybersecurity education.

Implications for Practice

The study is useful for researchers engaged in college students' cybersecurity education, especially in the design of questionnaires, analysis methods, and comparison of results. The analysis method of this paper can also serve as a reference for university network security investigators to obtain accurate evaluations of people's CSA. Moreover, this study has practical significance for cybersecurity education in universities, and three recommendations are outlined below.

First, it is crucial to strengthen the basic cybersecurity knowledge of all students, especially female students. The content should include daily applications such as passwords and responses to common cyber security threats. Although most participants have good knowledge of cybersecurity, such as passwords, they do not pay much attention to practice and continue to use the same passwords for different websites, indicating that they lack the knowledge to protect themselves and do not fully understand the importance of passwords in practice. In particular, liberal arts majors lack the necessary knowledge of network security, which results in their blind confidence.

Second, continuous cybersecurity education during college is necessary. This study found that students' cybersecurity levels did not increase but decreased in college due to the lack of readily available education (Hunt, 2016). In addition, colleges and universities should not solely rely on classroom teaching to improve students' CSA; instead, diversified education methods need to be explored.

Third, adopting appropriate cybersecurity education methods based on the knowledge structure of students of different majors is crucial. This study found that computer-related majors should offer more specialized courses and lectures, while non-computer majors need to adopt a universal approach. Additionally, network media publicity is a useful education method that cannot be ignored in cybersecurity education today.

Study Limitations and Further Work

Future research on cyber security awareness (CSA) among college students should consider including students from a wider range of higher education institutions to improve sample representativeness. While the survey questions used in this study were designed based on previous research and professional experiences, they may not be sufficient to comprehensively assess the level of CSA among college students. Future studies should also consider including additional variables such as physical security, Internet of Things security, mobile terminal security, and more, to gain a more comprehensive understanding of the current CSA level of college students. This information can then be used to develop more effective cybersecurity education programs tailored to the needs of different groups of students based on their grade

level and majors. In addition, future research could benefit from combining qualitative research methods, such as interviews, with the quantitative methods used in this study to generate more practical results.

Declarations

Conflict of interest the authors declare that they have no conflict of interest.

Acknowledgements

The authors gained ethical approval from the Research Ethical Board at Woosong University with the approval dated 24.03.2022, and the study complied with ethical standards of Social and Human Sciences.

This work was partially supported by the Shaanxi education science "13th Five-Year Plan" 2020 annual program in Shaanxi Province of China (Grant No. SGH20Y1338), Yulin Science and Technology Project Plan in Yulin of China (Grant No. CXY202000706), and Yulin High-tech Zone Science and Technology Plan Project (Grant No. CXY202166).

Biodata of Authors

Hongbo Guo completed his undergraduate studies at Xi'an University of Science and Technology (Xi'an, China) in the School of Communication and Information Engineering in 2007; he received M.S degree from the same university majoring communication and information system in 2010. He is currently a Ph.D. candidate in General graduate school, Woosong University (Daejeon, South Korea) majoring IT management. Likewise, he is also an associate professor in School of Information Engineering, Yulin University (Yulin, China). His research areas are management information system, supply chain informatization, business data analysis, information security and Industry 4.0.

Hasan Tinmaz completed his undergraduate studies at Middle East Technical University (Ankara, Turkiye) in the Faculty of Education, Computer Education Department in 2001; he graduated from the same university's Graduate Program in Curriculum and Instruction in 2004. Having completed his doctoral studies with his thesis on the uses, gratification and integration of social media in Middle East Technical University, Computer Education and Instructional Technologies program, he still works as an Assist. Professor in AI & Big Data department of Endicott College of International Studies, Woosong University (Daejeon, South Korea). His research areas are social media, educational technology, curriculum and instruction design, technology management, psychological and sociological issues in technology, technology planning, Industry 4.0, Artificial Intelligence and Metaverse.

References

Ahmed, N., Kulsum, U., Bin Azad, I., Momtaz, A. S., Haque, M. E., & Rahman, M. S. (2017). Cybersecurity Awareness Survey: An analysis from bangladesh perspective. *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*. https://doi.org/10.1109/r10-htc.2017.8289074

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), 1650007. https://doi.org/10.1142/s0219649216500076

Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*, https://doi.org/10.1016/j.matpr.2021.04.098.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.1109/icitst.2016.7856687

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, 12(5), 2589. doi:10.3390/app12052589.

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK. *Interactive Technology and Smart Education*, 13(2), 147–165.https://doi.org/10.1108/ITSE-09-2015-0029.

CNNIC (2022). *The 49th Statistical Report on Internet Development in China*. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/ .

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A Systematic Literature Review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.com*pind.2022.103614*

Edgar, Thomas W., & Manz David O.. (2017). *Research Methods for Cyber Security - 1st Edition*, [eBook edition]. Elsevier. https://www.elsevier.com/books/research-methods-for-cyber-security/edgar/978-0-12-805349-2.

Elbedour, S., Alqahtani, S., El Sheikh Rihan, I., Bawalsah, J. A., Booker-Ammah, B., & Turner, J. F. (2020). Cyberbullying: Roles of school psychologists and school counselors in addressing a pervasive social justice issue. *Children and Youth Services Review*, *109*, 104720. https://doi.org/10.1016/j.childyouth.2019.104720

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue. *Journal of International Communication*, *20*(2), 200–217. https://doi.org/10.1080/13216597.2014.954593

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. https://www.academia.edu/download/64160387/ A Study on Cybersecurity Awareness.pdf

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing Organizational Cyber Awareness. *Computers & Security*, *108*, 102357. https://doi.org/10.1016/j.cose.2021.102357

Hunt, T. (n.d.). *Cyber Security Awareness in Higher Education.* ScholarWorks@CWU, https://digitalcommons.cwu.edu/source/2016/cob/1/

Katsikeas, S., Johnson, P., Ekstedt, M., & Lagerström, R. (2021). Research communities in cyber security: A comprehensive literature review. *Computer Science Review*, *42*, 100431. https://doi.org/10.1016/j.cosrev.2021.100431

Klein, G., Zwilling, M., & Lesjak, D. (2022). A comparative study in Israel and Slovenia regarding the awareness, knowledge, and behavior regarding cyber security. R*esearch Anthology on Business Aspects of Cybersecurity*, 424-439. https://doi.org/10.4018/978-1-6684-3698-1.ch020

Kritzinger, E., Bada, M., & Nurse, J. R. (2017). A study into the Cybersecurity Awareness Initiatives for school learners in South Africa and the UK. *Information Security Education for a Global Digital Society*, 110–120. https://doi.org/10.1007/978-3-319-58553-6_10

Li, N., Tsigkanos, C., Jin, Z., Hu, Z., & Ghezzi, C. (2020). Early validation of Cyber–Physical Space Systems via multi-concerns integration. *Journal of Systems and Software*, *170*, 110742. https://doi.org/10.1016/j.jss.2020.110742

Liu, S. H., & Chen, J. (2021). Research on countermeasures of college Students' personal information security protection -- taking telecom network fraud as an example. *University: Research and Management*, (6), 73-74.
https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7iJTKGjg9uTdeTsOI_ra5_XVaXU2rLKrXTEU207jWtzbBARioEJ3Wr0mJV9M5ade9a&uniplatform=NZKPT

Liu, X. H., & Chao, C. X. (2011). A survey of college students' awareness of cyber security and the current situation of education. *Vocational Education Forum*, 14, 94-96. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKgchrJ08w1e7tvjWANqNvp-BLuadic5ChiGVwneXb4f8CKUJYzs-wqeQYvSnPiIF8eG9lpdsI4_W&uniplatform=NZKPT

Maennel, K., Mäses, S., Sütterlin, S., Ernits, M., & Maennel, O. (2019). Using technical cybersecurity exercises in university admissions and skill evaluation. *IFAC-PapersOnLine*, *52*(19), 169-174. https://doi.org/10.1016/j.ifacol.2019.12.169

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2020). Cybersecurity awareness in Zimbabwean Universities: Perspectives from the students. *Security and Privacy, 4*(2). https://doi.org/10.1002/spy2.141

Moallem, A. (2018). Cyber security awareness among college students. *Advances in Intelligent Systems and Computing,* 79-87. https://doi.org/10.1007/978-3-319-94782-2_8

Morrison, J. (2019, September 20). Assessing questionnaire reliability. Retrieved May 7, 2022, from https://select-statistics.co.uk/blog/assessing-questionnaire-reliability/.

Okesola, J. O., Onashoga, A., & Ogunbanwo, A. (2016). An investigation into users' information security awareness on social networks in south western Nigeria. *South African Journal of Information Management, 18*(1), 1-7. https://doi.org/10.4102/sajim.v18i1.721

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rahim, N. H., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/k-12-2014-0283

Rajesh Chandarman, & Brett Van Niekerk. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, (20). https://doi.org/10.23962/10539/23572

Ratten, V. (2015). A cross-cultural comparison of online behavioural advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory. *Journal of Science & Technology Policy Management*, *6*(1), 25–36. https://doi.org/10.1108/jstpm-06-2014-0029

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College students' cybersecurity risk perceptions, awareness, and practices. *2016 Cybersecurity Symposium (CYBERSEC)*. https://doi.org/10.1109/cybersec.2016.018

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil nadu. *IOP Conference Series: Materials Science and Engineering*, *263*, 042043. https://doi.org/10.1088/1757-899x/263/4/042043

Sun, W. (2018). *Investigation and Research on Network Security Consciousness of University students in Dalian* (Master's thesis, Dalian University of Technology, Dalian, China). https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201901&filename=1018718387.nh.

Xu, D. H., Zeng, L., Wang, R. J., & Zhang, Z. (2019). Investigation on network security awareness and protection skills of postgraduates. *China University of science & Technology* (z1), 125-128. https://doi.org/10.16209/j.cnki.cust.2019.z1.033