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

Xiaoyu Du(✉) and Thippaya Chintakovid

Department of Library Science, Faculty of Arts, Chulalongkorn University, Bangkok, Thailand
thippaya.c@chula.ac.th

Abstract. In 2022, more than 55% of internet users have encountered cybersecurity problems, which makes it have negative impact on public security. The group under the age of 20 is mainly students at school or young people just entering society. Because of their low financial resources and lack of security awareness, they are particularly vulnerable to fraud. We want to know what the current cybersecurity awareness of college students is. This study conducted a questionnaire survey on undergraduates of Yunnan University of Finance and Economics. According to the four aspects of cybersecurity awareness, their awareness was evaluated, namely, cybersecurity knowledge, privacy, password management and trust. We use quantitative research to verify the hypothesis through Spearman correlation. Finally, according to the collected data, we describe and analyze it, and provide some suggestions for cybersecurity education.

Keywords: Cybersecurity · Cybersecurity awareness · Survey · College students

1 Introduction

In June 2022, the number of Internet users had reached 74.4 percent of the total population in China, with Internet users aged 20–29 years old accounting for 17.2 percent [1]. For college students, the Internet's speed and convenience makes it a common channel for obtaining and exchanging knowledge and information. Although college students are quick to accept new experiences, they are easily deceived and misled [2]. Scams appear one after the other nowadays. Telecommunications, online loans, phishing links, and other forms of online fraud are currently the most common among college students [3]. University students aged 18 to 22 are the main group of victims of part-time fraud, accounting for 36.1% [4]. A university student helped increase the popularity of an online store as a part-time job by pretending to be a buyer and making multiple purchases. The suspect stated that the student needed to pay for the goods first and he would return the money and transfer profits to the student's account. However, the student made a purchase eight times, but the suspect did not return his money.

The ultimate source of cybersecurity vulnerabilities is frequently not cybersecurity technology, but ordinary users [5]. In the preceding cases, the victim trusted the identity of

X. Yuan et al. (Eds.): ICEKIM 2023, AHCS 13, pp. 740–753, 2023.
https://doi.org/10.2991/978-94-6463-172-2_78

the other party and did not confirm his identity, resulting in the loss of money. They lacked the skills and knowledge to verify the identity of the information sender and were not rigorous in protecting their information. College students rarely consider how to protect their information in a cyber environment and lack understanding of cybersecurity. It is essential that the college students should be aware of prevalent cybercrimes and know how to protect their data and actions online. The ability to perceive and anticipate cyber hazards and dangers is also important [6].

Fraud can be avoided if the college students are aware of online risks they may face and know how to use the Internet safely. Most prior research only focused on describing the college students' cybersecurity awareness. They did not explore students' educational approaches, gender, and field of study [2, 7–9]. In this regard, this study examined how well Chinese college students knew about potential cyber threats and ways to protect themselves as well as how they learned about cybersecurity. It also discussed the relationship between cybersecurity awareness and other attributes related to the students, i.e., educational methods, majors, and gender. The study's findings would contribute 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. They would offer informed recommendations to cybersecurity awareness education among Chinese college students.

2 Literature Review

2.1 Cybersecurity Awareness Among College Students

Previous research revealed mixed results regarding Chinese students' knowledge and skills in dealing with cybersecurity risks. A research work 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 [10]. In the 2019 cybersecurity awareness survey, Yu Miao [9] 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. The results of these two surveys are contradictory, so it is necessary to further investigate the cybersecurity awareness of Chinese college students.

Studies showed that cybersecurity awareness should be cultivated not only by lectures or courses offered at schools, but also by families and society [2, 7, 8]. After all, there is still a gap between knowledge understanding and practical use. Alharbi and Tassaddiq [11] conducted a survey on the cybersecurity awareness and found that most respondents knew firewall and anti-virus software. However, only 14.2% of the respondents knew about the cybersecurity problems encountered through social networking. Regarding the browser security and cybersecurity knowledge, the respondents were not fully aware of the security problems related to web browsers. The overall findings explained that even though the level of awareness was good, people's behavior was the main obstacle to deal with cybersecurity threats and challenges.

2.2 Assessment of Cybersecurity Awareness

Survey is a common approach used to assess college students' cybersecurity awareness. In the survey by Chandarman and Niekerk [12], the students from a private tertiary education institution in South Africa's KwaZulu-Natal Province had a positive self-awareness of various cybersecurity issues. Nevertheless, it was still necessary to promote the training of cybersecurity awareness and ensure that students' knowledge, cybersecurity behavior and attitude were correct.

Students from the Computer Science Department of Yobe State University participated in a survey of cybersecurity knowledge and their Internet behavior. These students showed a high awareness of privacy and trust, but they lacked the basic knowledge of password management, phishing and two-factor authentication [13]. Moallem [14] also examined cybersecurity awareness of university students in the San Francisco Bay area in California, USA. The study found that most respondents evaluated themselves as having average or higher cybersecurity awareness. However, the survey data could not point out whether the students' knowledge translates to secure behavior.

The previous research investigated the cybersecurity issues including password security, cyberbullying, phishing, malware, downloading, sharing and use of paid content [12]; password management, desire, and awareness of learning cybersecurity [13]; two-factor authentication (2FA), password setting [14]; cybersecurity knowledge, trust, privacy [13, 14]; and identity theft [12].

Other issues related to cybersecurity awareness were users' understanding of the importance of information security and of the responsibilities for their actions; 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 are basic digital and technical literacy [15].

In this study, 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. Issues concerning the cybersecurity awareness include cybersecurity knowledge, privacy, password management, and trust. The cybersecurity knowledge deals with the extent that the students can recognize different types of internet fraud. Privacy is concerned with whether the 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. Controlling access to personal information, i.e., configuring who can access what information and at which times [16], is an example of appropriate measure to protect personal information. Password is considered as one of the tools for information protection. It provides access to authenticated systems. Most users tend to reuse usernames and passwords with different online accounts. It is important to examine whether the students are aware of proper ways to set and manage their passwords. Lastly, trust exists between software platforms and their users. Many platforms gather and analyze users' information for the benefits of the business. This study will investigate whether the students are conscious of suitable practices to evaluate whether they can trust the software platforms or not, for example, the reliability and trustworthiness of the platforms.

2.3 Approaches to Cybersecurity Education

Based on the survey reported in [7], only 8.1% of college students stated that their school set up relevant courses for cybersecurity, and 9.7% mentioned that their school carried out activities to improve cyber literacy. Wu [8] conducted a survey by randomly sampling college students from all over China. She found that the students had weak awareness of cybersecurity. They did not carefully read the privacy terms and did not understand relevant laws and regulations, and so on. Since 2018, cybersecurity has been added to the major or courses in China [17]. As an elective course, students are free to choose whether to attend or not. Most students think that cybersecurity is not related to their major or is not beneficial to their academic performance, so they do not choose this type of course [7].

3 Research Objectives

This study has two research objectives as follows

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.

4 Research Hypothesis

This research posed the following research hypothesis.

H1: Receiving formal and informal training about cybersecurity is positively related to the extent of cybersecurity awareness among Chinese undergraduate students.

In the hypothesis, cybersecurity awareness is defined as students' understanding of cybersecurity risks and proper ways to deal with them. The study hypothesized that either the formal or informal learning approaches would relate to the extent of cybersecurity awareness. If the students have learned about cybersecurity, they would know about cybersecurity threats and practices for handling them.

5 Methodology

5.1 Scope of Study

The study's population is defined as undergraduate students who studied at Yunnan University of Finance and Economics in China.

5.2 Data Collection

5.2.1 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 is selected as the study's setting due to its multidisciplinary nature. Economics and management are offered as the university's main disciplines. Other fields include law, philosophy, literature, art, science, and engineering. The total number of students is considered as a total number of the population in this study.

Since the exact number of the population cannot be obtained, the sample size for the survey is calculated based on the following equation where n is the number of sample size. Z is defined as a statistic value, e as an error value, and p as a proportion. q is defined as 1-p. The confidence level is set at 95%.

$$\mathrm{Z} = 1.96,\ \mathrm{e} = 5\%,\ \mathrm{p} = 0.5$$

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

Thus, the sample size for this survey is 384.

5.2.2 Data Collection Instrument

The questionnaire was developed by adapting questions based on prior research works [11, 13, 14, 18, 19]. The questions were translated from English into Chinese. Language specialists reviewed the accuracy of the English - Chinese translation. A panel of experts related to cybersecurity and cybersecurity awareness evaluated the validity of the questionnaire. An item-objective congruence (IOC) index was calculated to determine the questionnaire's content validity. Three experts 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 align with the purpose. Questions that obtained an IOC index less than 0.5 were either revised or removed from the final questionnaire. A pilot study was run with eighteen Chinese students, who were not later included in the study's sample, to test the language, clarity, and reliability of the questionnaire. The reliability obtained was 0.820. The questionnaire was sent to all kinds of student groups at Yunnan University of Finance and Economics to ensure that the respondents were students studying at the university.

The questionnaire was separated into two parts. The first section asked about approaches to cybersecurity learning based on students' experiences. The second section gathered students' understanding about cybersecurity awareness, including basic knowledge about cybersecurity, privacy, password management, and trust.

Students could freely choose whether to take part in the survey or not. The questionnaire was distributed via a QR code created by the generator program called Wenjuanxing, which is recognized by WeChat, one of China's most popular chat software. The Wenjuanxing marked each response by number. Students' names and other identifying 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. Each participant was required to express the level of agreement and disagreement with the statement using the five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). Examples of questionnaire items are demonstrated below.

Cybersecurity Knowledge

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

Privacy

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.

6 Results

The following presents the study's results as well as the demographic data of the respondents.

6.1 Age, Gender and Year of Study

Out of 384 respondents, 109 male participants (28.4%) and 275 female participants (71.6%) took part in the survey. Twenty-six percent of them were 17–19 years old, 72% were 20–22 years old, and 2% were 23–25 years old. Most of the survey respondents were second-year and third-year students, 25.6% and 50.3% respectively. There were only 4 freshmen (1%) and 12 seniors (3.1%).

6.2 Faculty and Cybersecurity Learning Approach

Table 1 shows that practically all college students from all institutions responded to the questionnaire.

The Business School and School of Tourism and Hotel Management had the highest participation rates, 36.7% and 28.6% respectively. Next is 12.2% from Accounting School and 7.8% from others. 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.

As shown in Table 2, 180 respondents (46.9%) learnt about cybersecurity through university courses, 124 (32.3%) learned about it online, and 54 (14.1%) learned about it from social cybering communities. The remaining 16 students (4.2%) relied on public lectures to get cybersecurity knowledge, and 10 students (2.6%) had not learned about cybersecurity. It shows that most students have already had the learning foundation of cybersecurity. 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.

Table 1. Number of research participants by faculty

Faculty	Number	Percent
Business School	141	36.7
School of Economics	9	2.3
Accounting School	47	12.2
International Institute of Language and Culture	1	0.3
School of Logistics	2	0.5
School of Tourism and Hotel Management	110	28.6
School of City and Environment	6	1.6
Institute of Finance	4	1.0
School of Finance and Public Administration	1	0.3
Law School	4	1.0
School of Media and Design Art	2	0.5
School of Information	7	1.8
School of Statistics and Mathematics	8	2.1
Ministry of Sports	9	2.3
International Business School	3	0.8
Others	30	7.8
Total	384	100.0

Table 2. Results of "Have you ever learned cybersecurity?"

Responses	Number	Percent
Yes, I have. I learned from university course.	180	46.9
Yes, I have. I learned from websites.	124	32.3
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 3. Reliability Statistics

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

7 Study Findings

7.1 Reliability

To test the reliability of the survey data, Cronbach's alpha value was used as shown in Table 3. According to Taber [20], 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.

7.2 Spearman Correlation Analysis

7.2.1 Learning Approach

As mentioned earlier, 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 learn cybersecurity were excluded from both categories.

The responses to all 26 questions in the questionnaire were averaged to form scores for cybersecurity awareness. For the components of the cybersecurity awareness, which are cybersecurity knowledge, privacy, password management, and trust, all responses were also averaged separately for each part. Spearman correlation analysis was conducted to examine the relationship between learning methods (two nominal groups) and cybersecurity awareness (average scores). The study also investigated relationships between learning methods and cybersecurity knowledge, privacy, password management, and trust. The analysis also used average scores of each part of the cybersecurity awareness.

Table 4 and Table 5 show descriptive statistics of overall cybersecurity awareness, cybersecurity knowledge, privacy, password management and trust for formal and informal training.

Table 4. Descriptive Statistics for Formal training

Formal	N	Mean	Std. Deviation
Cybersecurity Awareness	180.00	3.80	0.39
Cybersecurity knowledge	180.00	3.94	0.50
Privacy	180.00	3.89	0.49
Password management	180.00	3.76	0.64
Trust	180.00	2.76	0.97

Table 5. Descriptive Statistics for informal training

Informal	N	Mean	Std. Deviation
Cybersecurity Awareness	194.00	3.60	0.42
Cybersecurity knowledge	194.00	3.74	0.52
Privacy	194.00	3.72	0.58
Password management	194.00	3.53	0.69
Trust	194.00	2.48	1.05

Table 6 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 was lower than the formal training. Since it is a correlation analysis between a dichotomous variable and interval variables, if the groups of learning methods were coded 1 for informal training and 2 for formal training, the results would reveal a positive correlation value. The statistically significant results with either a positive or a negative sign can be interpreted that students who formally learned about cybersecurity showed higher degree of cybersecurity awareness than those who relied on informal learning approaches. Therefore, the result supports the study's research hypothesis that formal and informal training have relationships with cybersecurity awareness.

For each part of the cybersecurity awareness, the analysis also shows 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.

7.2.2 Major

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, we divided the majors into two categories: finance (213 students) and non-finance (171 students) for the data

Table 6. Correlation Coefficients of learning methods, cybersecurity awareness and components of cybersecurity awareness

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

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

Table 7. Descriptive Statistics for Finance-related majors

Finance	**N**	**Mean**	**Std. Deviation**
Cybersecurity Awareness	213.00	3.66	0.45
Cybersecurity knowledge	213.00	3.78	0.54
Privacy	213.00	3.81	0.60
Password management	213.00	3.61	0.72
Trust	213.00	2.54	1.00

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 7 and Table 8 show descriptive statistics of overall cybersecurity awareness, cybersecurity knowledge, privacy, password management and trust for finance and non-finance related majors. As shown in Table 9, none of the correlation results are statistically significant. The results can be interpreted that the field of study has nothing to do with the degree of cybersecurity awareness. Cybersecurity awareness is similar among finance-related and non-finance related majors.

7.2.3 Gender

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 10 and Table 11.

Table 8. Descriptive statistics for Non-Finance-related majors

Non-finance	**N**	**Mean**	**Std. Deviation**
Cybersecurity Awareness	171.00	3.71	0.39
Cybersecurity knowledge	171.00	3.88	0.49
Privacy	171.00	3.77	0.47
Password management	171.00	3.64	0.65
Trust	171.00	2.69	1.04

Table 9. Correlation Coefficients of major, cybersecurity awareness and components of cybersecurity awareness

	Correlation Coefficient	**Sig. (2-tailed)**
Major	1.000	
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

The male group was coded as 1 and female group coded 2. In Table 12, 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 mean that the average scores of each variable for the female group were higher than the male group. Again, this is a correlation analysis between a dichotomous variable (male vs. female) and interval variables. If the groups were reversely coded, i.e., female as 1 and male as 2, the results would reveal negative correlation values. Either positive or negative statistically significant results can 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.

Table 10. Descriptive Statistics for male respondents

Male	N	Mean	Std. Deviation
Cybersecurity Awareness	109.00	3.53	0.49
Cybersecurity knowledge	109.00	3.66	0.58
Privacy	109.00	3.60	0.61
Password management	109.00	3.49	0.77
Trust	109.00	2.68	1.11

Table 11. Descriptive Statistics for female respondents

Female	N	Mean	Std. Deviation
Cybersecurity Awareness	275.00	3.74	0.38
Cybersecurity knowledge	275.00	3.89	0.48
Privacy	275.00	3.87	0.50
Password management	275.00	3.68	0.65
Trust	275.00	2.58	0.98

Table 12. Correlation Coefficients of gender, cybersecurity awareness and components of cybersecurity awareness

	Correlation Coefficient	Sig. (2-tailed)
Gender	1.000	
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)

8 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 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 were statistically significant relationships between learning methods and cybersecurity awareness, learning methods and cybersecurity knowledge, learning methods and privacy, learning methods and password management, and learning methods 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 about how to cope with these risks.

The study, in addition, 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, gender and cybersecurity knowledge, gender and privacy, and gender 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 explore 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 contributes to understanding the current situation of cybersecurity awareness among Chinese students. Future works can conduct several surveys with college students in other universities to paint a more comprehensive picture of Chinese students' degree of cybersecurity awareness.

References

1. China Internet Network Information Center. (2022). The 50th Statistical Report on China's Internet Development
2. Wang Guangli. (2020). Study on the Cultivation Path of Network Security Consciousness of Contemporary College Students. Master's thesis
3. China Internet Network Information Center, Cyberspace Administration of China, Office of the Central Cyberspace Affairs Commission. (2021). *The 47th China Statistical Report on Internet Development_* Department Government Affairs_ China government network.
4. Government & Enterprise Security Group, 360 Security Center & Network Security Corps of Beijing Municipal Public Security Bureau. (2019). Research Report on the Trend of Online Fraud in 2019.
5. Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375–382.
6. Nurse J.R.C. (2021) Cybersecurity Awareness. In: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg.
7. Song Chenwei. (2020). Research on the Cultivation of College Students' Network Literacy in the New Era. Master's thesis

8. Wu Yuehua. (2018). Research on the Cultivation of Network Security Consciousness of College Students in the Media Age. Master's thesis
9. Yu Miao. (2019). The Research on Network Security Awareness Cultivation of College Students. Master's thesis
10. Liu, Z., Hong, Y., & Pi, D. (2014). A large-scale study of web password habits of Chinese network users. *Journal of Software, 9*(2).
11. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23.
12. Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, 20, 133–155. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
13. Garba, A., Maheyzah Binti Sirat, Siti Hajar, & Ibrahim Bukar Dauda. (2020). Cyber security awareness among university students: A case study. Science Proceedings Series, 2(1), 82–86.
14. Moallem, A. (2019). Cybersecurity awareness among students and faculty. CRC Press.
15. 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.
16. Westin, A.F., 1967. Privacy and freedom. Atheneum Books, New York.
17. Austin, G. and Lu, W., 2021. Five years of cyber security education reform in China. In: G. Austin, ed., *CYBER SECURITY EDUCATION Principles and Policies.*
18. 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.
19. Fariza Khalid, Md Yusoff Daud, Mohd Jasmy Abdul Rahman, Md Khalid Mohamad Nasir. (2018) An Investigation of University Students' Awareness on Cyber Security. *International Journal of Engineering & Technology*, 7 (4.21) (2018) 11–14.
20. 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.