World Journal of Educational Research
ISSN 2375-9771 (Print) ISSN 2333-5998 (Online)
Vol. 11, No. 4, 2024
www.scholink.org/ojs/index.php/wjer

Original Paper

Educating University Students on Information Security Awareness: A Smartphone Perspective

Hongbo Guo[1*], Jijian Wang[1], Fei Yang[1] & Zhidong Feng[1]

[1] School of Information Engineering, Yulin University, Yulin, Shaanxi Province, China

Received: May 24, 2024 Accepted: July 06, 2024 Online Published: July 26, 2024

doi:10.22158/wjer.v11n4p66 URL: http://dx.doi.org/10.22158/wjer.v11n4p66

Abstract

This study examines the information security awareness of university students, focusing on their knowledge, awareness, and practices related to smartphone usage. Using a 35-question survey, data were collected from 1364 students across six universities in China. Descriptive statistics, cross-analysis, and exploratory factor analysis were employed to assess students' security awareness levels. Results indicated that most students preferred Android, expressed concerns about personal finance and privacy risks, and primarily acquired security knowledge through internet media. Despite a satisfactory overall awareness, gaps were found in password setting and Wi-Fi connection practices. Male students performed better in knowledge and practice, while no significant differences were observed across grades. These insights are crucial for enhancing information security education programs.

Keywords

smartphone security awareness, information security awareness, cybersecurity knowledge, smartphone security behavior, information security education

1. Introduction

With the wide application of information and communication technology in various industries, the Net has brought innumerable conveniences and enormous wealth to people and effectively promoted the progress and prosperity of human society, and its influence has penetrated into all sectors of society. However, the Net not only provides convenient and fast services to citizens, but also has many negative impacts on people’s lives. Security issues and cyber-attacks are becoming increasingly apparent. As technology proliferates, cyber threats and vulnerabilities are also on the rise and require urgent attention (Chandarman & Niekerk, 2017). Hong and Furnell (2021) found that most people do not think about the security of their sensitive data when shopping, checking email or using social media online, and that the risks to the security of personal data are high when using the internet. Human error and insufficient knowledge are often the cause of cybersecurity problems (Hong & Furnell, 2021). According to Verizon's annual data breach report in 2021, 85% of data breaches are due to human factors (“2021 DBIR Results & Analysis”, 2021). Therefore, reducing human error or vulnerability is an important way to improve the security of personal or organizational information (Giannakas et al., 2019), and improving people’s information security awareness (ISA) is a topic of concern for many people around the world.

As the most essential and direct access terminal of mobile Internet, the smartphone has grown from a device that could only make phone calls and transmit text messages to a portable personal computer that incorporates search, social networking, gaming, payment, location services, and other capabilities (Qiu et al., 2020). As a result, smart phones are currently the most common Internet-capable gadgets in the world. According to the 49th China Statistical Report on Internet Development (CNNIC, 2022), there were 1.02 billion Chinese smartphone users by the end of 2021, representing 99.7 percent of all Internet users in China. However, while individuals appreciate these convenient smartphone services, personal information security issues are simultaneously occurring. The amount of information involved in smart phones is not only more comprehensive and richer than that of personal computers, but also more valuable due to its dynamic, real-time, and holographic nature (Yang et al., 2022). Therefore, the information security issues associated with smart phones are significantly more severe than those associated with traditional personal computers. Unfortunately, several research have indicated that the information security vulnerabilities encountered by intelligent mobile terminals are rising (Moletsane & Tsibolane, 2020). Smartphones are no longer used just for traditional communication due to the sophisticated PC-like features and the ease they provide. Smartphones are being utilized for work, school, and personal errands, allowing users to access more important personal information (Taha & Dahabiyeh, 2020). In turn, this makes cellphones desirable targets for security assaults. Consequently, it is more important to examine the security threat awareness and security processes of cellphones than it is to investigate general information security awareness.

As the workforce of tomorrow, university students must grasp fundamental information security skills so they can not only secure their own information, but also the information of their future employers (Jones et al., 2014). Since frequent Internet users among university students lack social experience and cybersecurity understanding, they confront greater network security issues (Alharbi & Tawfiq, 2021). Cybersecurity awareness-related themes are becoming more important than ever to discuss in higher education settings (Hunt, 2016). In addition, several studies have discovered that university students' cybersecurity understanding, particularly their cybersecurity practices, are still quite limited (Ma & Fan, 2022; Moallem, 2018). Similar to this result, Chen (2021) discovered that cyber security incidents involving Chinese university students have occurred often in recent years. Consequently, it is necessary to investigate university students' ISA in smartphone use and to examine the relationship between the knowledge, awareness, and behavior of smartphone security, which will help to identify existing problems and propose appropriate countermeasures for the education of university students' information security.

This study aims to examine the ISA level among university students, emphasizing especially on the knowledge, awareness, and practice components of smartphone usage (Zwilling et al., 2020; Moletsane & Tsibolane, 2020). The specific goals are to develop a questionnaire for ISA assessment and to examine student performance in these three areas. Furthermore, the study intends to investigate any possible discrepancies between students of various genders and grade levels. The following research questions guide this study:

Q1: What are the key hazards that university students are most concerned about, their preferred routes for learning knowledge, and their degrees of proficiency with respect to various areas of smartphone information security?

Q2: Are there statistically significant differences between male and female students in their concerns about smartphone security risks, as well as between students of different grade levels in the learning sources of smartphone security knowledge?

Q3: What are the statistically significant differences between male and female students, as well as between students of varying grade levels, on each aspect of smartphone security?

2. Literature Review

2.1 Research on Information Security Awareness

ISA can assist Internet users in identifying a variety of information security issues and enhancing their understanding of cyber hazards, so that they are aware of cyber risks when using the Internet (Rahim et al., 2015). In recent years, an increasing number of scholars have begun to focus on cybersecurity awareness, which is distinct from previous cybersecurity research that always centered on information security technology, because humans are the manager and user of the system and have a significant impact on the security of the information system (Zhang et al., 2016). Existing literature on cybersecurity awareness focuses primarily on two directions: first, the research on the influence factors of cybersecurity awareness and behavior in various research environments, and second, the assessment of the cybersecurity level of specific groups, such as adolescents, organization employees, or students.

Regarding the current ISA research, there are few educational context-based studies. Matyokurehwa et al. (2020) examined the ISA of university students from the standpoint of three dimensions of social engineering assaults, malware attacks, and internet of things attacks, and found that the students' ISA is positively connected with all three aspects. Alharbi and Tassaddiq (2021) used a quantitative method to examine the students' level of network security awareness in a Saudi Arabian university and discovered that despite the fact that 92% of the students have received formal network security training, they do not understand the concept of network security. In accordance with this result, Al-Janabi and Al-Shourbaji (2016) assessed the cybersecurity awareness of the students, faculty, and staff in a Middle Eastern university and discovered that the majority of university students lack the necessary knowledge and a sufficient understanding of the critical role of information security. In addition, Senthilkumar and

Easwaramoorthy (2017) discovered that university students in Tamil Nadu had an above-average level of cybersecurity knowledge, but that it still has to be bolstered further.

Some studies found that information security events are frequently not caused by a lack of necessary information security expertise, but rather by an inconsistency between knowledge and practice (Slusky & Partow-Navid, 2012). Similar to this result, Moallem (2018) researched students in Silicon Valley and discovered that even in the most technologically advanced environment in the world, university students' cybersecurity practices are still inadequate. The Silicon Valley university students believe that their data is not secure while using the Internet, but they are unclear on how to protect their data. In addition, Moallem (2018) found that diverse training techniques are required to improve students' abilities to identify cyber threats and respond to a variety of potential cyberattacks.

2.2 Research on Smartphone Security Awareness

Regarding research on ISA or information security risk in smartphone use, only a small number of studies have been conducted. Koyuncu and Pusatli (2019) used a survey to investigate the smartphone security level in Turkey; the result is comparable to the research discussed in the previous section in that the overall level is not encouraging (Al-Janabi & Al-Shourbaji, 2016; Senthilkumar & Easwaramoorthy, 2017; Slusky & Partow-Navid, 2012; Moallem, 2018). In addition, they discovered that the oldest group (age > 50) and the youngest group (age < 21) have the lowest smartphone security awareness, while those with a high level of education and those who have received network security training have the highest levels.

Shah and Agarwal (2020) examined smartphone security awareness in India through quantitative research. In spite of a great desire to secure information on personal devices, the participants' performance was deemed inadequate, according to their report. In addition, the study discovered statistically significant variations between smartphone security behavior and independent variables such as gender, age, mobile operating system (OS), and native language (Shah & Agarwal, 2020).

Jones and Chin (2015) utilized the same survey instrument to determine whether the smartphone security behavior of undergraduates at a university in the United States altered between 2011 and 2014. Surprisingly, the results revealed that the level of students' information security practices has not increased, and in some cases has decreased, despite the fact that more and more students are using smartphones with increasingly robust functions, particularly in the financial realm. This indicates that the overall level of university students' ISA has not increased over time. In contrast to study undertaken on a single information technology, the ISA must be regularly examined and investigated in order to keep up with changes and continuously raise people's information security level.

Harris et al. (2014) evaluated the smartphone security levels of college students majoring in IT but not in information security, majoring in information security, and not majoring in IT and found no significant differences. The results of Taha and Dahabiyeh's (2020) investigation and comparison of university students' smartphone and computer cybersecurity awareness revealed that students are familiar with general security dangers and prevention techniques. Intriguingly, however, their cybersecurity efforts and behavior vary between utilizing PCs and mobile phones, suggesting that people may have distinct protection motivations for various intelligent gadgets.

There are also a number of studies on cybersecurity awareness in China's higher education context. The majority of these studies used qualitative methods to describe the significance and current situation of university students' cybersecurity awareness, while others employed quantitative methods for analysis. Xu et al. (2019) evaluated the postgraduates' awareness and concluded that the outcome is unsatisfactory and that the university should take action to rectify the situation. Zhou et al. (2017) conducted an anonymous questionnaire survey of 800 university students in Nanjing in 2016, and discovered that 79.9 percent of respondents did not generally read the membership information protection and responsibility clauses of unfamiliar websites, while 27.4 percent of respondents frequently backed up and secured their most important personal documents. In conclusion, the vast majority of relevant research concludes that the cybersecurity proficiency of Chinese university students is inadequate and needs improvement.

The vast majority of studies on smartphone awareness in China simply provide qualitative overviews of potential problems and simple remedies. Existing literature has only two quantitative studies on smartphone security awareness, to the best of our knowledge. Zhang et al. (2017) examined the factors influencing the security awareness of smart phones and discovered that there were numerous serious issues with the use of smart phones in China, such as ignorance of information security when downloading or utilizing applications, inadequate mobile phone settings, and the absence of appropriate disaster recovery procedures. Zhou and Wang (2017) investigated the smartphone security awareness and behavior of university students in a university in Tianjin, China, and discovered that the overall smartphone security level of university students is relatively low, they have a better grasp of common-sense information security knowledge than professional knowledge in using smartphones, and there are significant hidden dangers in university students' use of applications.

In China, research on smartphone information security has mostly neglected empirical investigations in favor of technological studies. Existing qualitative research on ISA in smartphone usage is limited, but empirical research in this field is severely lacking. In addition, few studies have particularly targeted university students within the context of smartphone security research. In addition, additional research is required to assess the relevance of previous conclusions in light of the continuously changing application environment caused by the evolution of ICT. This research explores university students in China as the survey context to resolve these shortcomings. Through an examination of the current level of information security knowledge, awareness, and behavior among smartphone-using university students, the study intends to provide countermeasures to address existing problems. The findings will serve as a great resource for the development of university-student-specific information security education.

3. Method

3.1 Data Collection and Study Sample

An online questionnaire was utilized to collect data, employing a random sampling method (McCombes, 2021). The data collection took place at six local universities in the northwest region of China, specifically targeting undergraduate institutions. The questionnaire was generated using the professional platform "WJX" which is well-known in China for collecting survey data. The survey link was shared through popular platforms such as WeChat and QQ in October 2022, which took almost two months to collect the data. To enhance participation, the snowball sampling method was employed, encouraging respondents to invite others to complete the survey (Zhang et al., 2017). Additionally, to maximize the survey response rate, one or two teachers from each selected university were involved in collecting the questionnaires. They actively motivated students within their respective institutions to participate and provide careful responses.

At the end of data collection process, the final sample size is 1364. As the Table 1 shows that, there are 1364 participants involved in this study. In the sample, the number of male participants is 485, and the number of females is 879. The proportion of female (64.4%) is higher than male respondents (35.6%), which indicates that female students are more active in participation or interested in the topic of smartphone security. As regard to the school level, 505 participants are freshman (37%), 364 participants are sophomore (26.7%), 264 participants are junior (19.4%), and 231 participants are senior students (16.9%).

Table 1. Demographic Information of Research Respondents

Levels	Variable	n	%
Gender	Male	485	35.60
	Female	879	64.40
Grade level	Freshman	505	37.00
	Sophomore	364	26.70
	Junior	264	19.40
	Senior	231	16.90

3.2 Study Instrument

This study's survey consists of two parts and thirty-five questions. The first section focuses on collecting the respondents' demographic and basic information, while the second section employs scale items to measure the respondents' ISA level from the three viewpoints of knowledge, awareness, and practice. In addition to the cited literature, two experts in the disciplines of social sciences and information security were consulted to guarantee the questionnaire's validity.

In the first section, there are five questions: two demographic questions on the gender and educational level of university students, and three questions regarding the smartphone operating system, the information security risk of smartphones, and the source of respondents' smartphone security knowledge. In the second section, thirty Likert scale questions ranging from 1 (strongly disagree) to 5 (strongly agree) are used to assess the level of smartphone security among university students. Among the thirty scale questions, ten are aimed to assess the level of smartphone security knowledge, ten are about smartphone security awareness, and the other ten are about smartphone security practice. The measuring components of these thirty scale questions were developed based on previous studies pertaining to smartphone security settings, risk perception, data protection, and other usage patterns Specifically, it featured passwords, verification, Bluetooth, camera, GPS, screen lock, Apps, etc. (Koyuncu & Pusatli, 2019; Mai & Tick, 2021; Moletsane & Tsibolane, 2020; Shah & Agarwal, 2020; Zhang et al., 2017; Zwilling et al., 2020), which cover the vast majority of smartphone security concerns. Given that the survey was conducted at local institutions in China, the questionnaire's content was also translated into Chinese to facilitate comprehension.

3.3 Data Analysis

To evaluate the fundamental data and compare the mean of each scale question, descriptive statistics and cross analysis were used. To ensure and enhance the construct validity of the survey, exploratory factor analysis (EFA) was employed. EFA is a statistical approach used to determine the relationships between measured variables (Norris & Lecavalier, 2010). Its objective was to verify the structure and dependability of the measurement model (Middleton, 2022).

In addition, the Independent-samples t-test and the One-way ANOVA test were utilized in order to carry out comparison analyses. These tests were carried out to investigate the similarities and differences between the various situations and groups. For the purpose of this investigation, the primary analytic tool that was utilized was the SPSS 22.0 software, which made both the processing of data and the statistical analysis much simpler.

4. Results

4.1 Descriptive Statistics of Participants' Perception Related to Smartphone Security

As presented in Table 2, 82.6% of university students are Android users, whereas only 17.4% are iOS users. With regard to the cybersecurity risks that smartphone users were most concerned about, privacy information leaking accounted for 16% and financial theft for 14%. Smartphone users pay close attention to virus attacks (13.3 %), data loss (13.4 %), account theft (12.8 %), and online fraud (12.9 %). Other risks with lower concern are spam (9.5%) and cyberbullying (7.7%).

In this study, a special multiple-choice question was devised to determine where university students learned their smartphone security expertise. According to Table 2, websites and social media are the most common route for university students to acquire information security expertise, accounting for 25.3% of the total. The second most preferred source of smartphone security knowledge, accounting for 22%, is current affairs. The participants believe that experience from colleagues or classmates (17.2%)

is also an essential approach to acquire security knowledge, along with personal experience of risk events (10.4%), information security lectures and courses (11.3%), and only 0.6% of respondents reported that they never pay attention to cyber threats.

Table 2. Users' Basic Information Related to Smartphone Security

Variables	Level	n	%
Smartphone operating system	android	1126	82.60
	iOS	238	17.40
Users' most cared smartphone risks	Virus attacks	992	13.30
	Privacy information leakage	1189	16.00
	Spam	705	9.50
	Financial theft	1044	14.00
	Online fraud	964	12.90
	Data loss	995	13.40
	Cyberbullying	573	7.70
	Account stolen	950	12.80
	Others	33	0.40
Source of the users' knowledge of smartphone information security	Current affairs news report	1062	22.00
	Internet media (websites, blogs, WeChat)	1219	25.30
	Experience from friends or classmates	830	17.20
	Lectures on Information Security	546	11.30
	Information security related courses	543	11.30
	Personal experience of risk events	503	10.40
	Never pay attention	93	1.90
	Others	29	0.60

4.2 Cross Analysis between Demographic and Basic Perception of Smartphone Security

A specific multiple-choice question about cared cyber threats in smartphone use was included in the first portion of the survey in order to determine whether students of different genders were concerned about varied security concerns associated with smartphone use. This study analyzed the sample size of each gender group and the frequency of each risk category, as well as performed a cross-analysis, in order to assess whether this difference existed. According to Table 3, the significance value of the Chi-Square test is 0.03 (2 = 17.36, df = 8), indicating that both male and female students have significantly different risk preferences. Table 3 demonstrates the level of concern about various smartphone security risks among college students of different genders.

Table 3. Cross Tabulation of Gender and Smartphone Security Risk

gender		Cared smartphone security risk								
		Virus attacks	Privacy leakage	Spam	Financial theft	Online fraud	Data loss	Cyber bullying	Account stolen	Others
male	n	290	394	227	330	291	314	151	294	17
	%	12.6%	17.1%	9.8%	14.3%	12.6%	13.6%	6.5%	12.7%	0.7%
female	n	702	795	478	714	673	681	422	656	16
	%	13.7%	15.5%	9.3%	13.9%	13.1%	13.3%	8.2%	12.8%	0.3%

To determine whether students in different grade levels preferred distinct sources of smartphone security knowledge, the cross-analysis technique was applied again, with the sample size and frequency of each learning source additionally taken into account. The significance value of the Chi-Square test is 0.04 (χ2 = 33.49, df = 21), which is less than 0.05, indicating that students of different grade levels obtain smartphone security knowledge from significantly varied sources. The results were shown in Table 4.

Table 4. Cross Tabulation of Grade and Learning Source

Grade level		Learning source of the knowledge of smartphone security							
		Current affairs	Internet media	Friends	Lectures	Courses	Risk event	Never pay attention	Others
Freshman	n	408	475	323	231	252	199	36	7
	%	21.1%	24.6%	16.7%	12.0%	13.1%	10.3%	1.9%	0.4%
Sophomore	n	282	327	232	141	142	151	21	7
	%	21.6%	25.1%	17.8%	10.8%	10.9%	11.6%	1.6%	0.5%
Junior	n	201	221	151	104	94	87	24	7
	%	22.6%	24.9%	17.0%	11.7%	10.6%	9.8%	2.7%	0.8%
Senior	n	171	196	124	70	55	66	12	8
	%	24.4%	27.9%	17.7%	10.0%	7.8%	9.4%	1.7%	1.1%

4.3 Descriptive Statistics of the Original Survey

Table 5 presents the results of an analysis conducted using the descriptive statistical approach on the sample size, mean value, and standard deviation of each of the thirty scale questions contained in the survey. In this section, the three highest- and three lowest-scoring questions were reviewed in detail.

Regarding the three questions with the highest mean score among the thirty scale questions, question 8 has the highest mean score with a value of 4.31, indicating that the vast majority of participants recognize that losing a smartphone is not only a physical loss, but would also result in substantial property losses and other risks. The question 16 with the second-highest mean score, 4.18, demonstrates that the majority of students are able to consider personal privacy security when sharing material online. The question 17 with the third-highest mean score, 4.15, suggests that the majority of students are vigilant while clicking links.

Regarding the three survey items with the lowest mean scores, question 11 has the lowest mean score with a value of 2.05. Question 21 has the second lowest mean score among the thirty scale questions, with a mean score of 2.37. Considering the content of the questions, the preceding two questions are all about using the same password for several applications, indicating that the majority of university students do not comprehend the significance of passwords. The question 29 has the third lowest mean score of 2.77, indicating that the majority of smartphone users lack sufficient security awareness when using public Wi-Fi.

Table 5. The Basic Descriptive Statistics of Survey Questions (n=1364)

Survey questions	*M*	*SD*
1. Setting long and complex passwords can protect my information security.	3.90	0.96
2. I clearly know why I need to enter the verification code when I log in to my account.	4.13	0.93
3. I know that websites that I am visiting can obtain mobile phone models, phone numbers and other information.	3.81	1.05
4. I know that APP installed on my phone can easily collect my information, even if it is not actively opened.	3.81	1.05
5. I know the function of mobile phone PIN (Personal Identification Number).	3.48	1.15
6. I am familiar with the security settings of my phone.	3.71	0.96
7. I know that the cloud client will automatically back up personal information such as address book, photos and SMS on the mobile phone.	3.94	0.93
8. I clearly know that losing a mobile phone will not only lead to data loss, but also may bring huge property losses and other risks.	4.31	0.85
9. I believe that the APP has the ability to remotely turn on my mobile camera.	3.89	1.05
10. I am familiar with the personal information security laws and regulations issued by the state.	3.66	1.01
11. I think it is risky to set the same password in different application systems.	2.05	0.94
12. I pay more attention to the information security of my phone than using a personal computer.	3.75	0.99
13. For security reasons, I will delete the apps, which are not used or are not useful.	4.01	0.92

14. I never tell others the content of my SMS verification code.	4.14	0.89
15. I believe that installing anti-virus software is not enough to ensure the safety of my phone.	3.98	0.89
16. I will consider security risks when publishing content containing personal information on the Internet.	4.18	0.86
17. I avoid clicking on links from unknown sources or strange emails on mobile phones.	4.15	0.87
18. When registering an account, I was dissatisfied with the requirements for filling in information such as mobile phone number or ID card number.	3.64	1.08
19. I pay attention to what the installed application can access, run and activate on my phone.	3.98	0.89
20. I read the user license agreement of the application carefully when I install a new APP.	3.58	1.12
21. I set the same password for different APPs.	2.37	1.05
22. My phone has a complex lock screen password.	3.50	1.05
23. I often consciously turn off the GPS of my mobile phone.	3.49	1.14
24. I often consciously turn off the Bluetooth of my mobile phone.	3.73	1.08
25. The applications installed on my phone are downloaded from safe and reliable sources (such as official application stores).	4.05	0.91
26. Antivirus software is installed and used on my mobile phone.	3.56	1.15
27. I am used to apply security patches to my phone as soon as possible.	3.49	1.11
28. The PIN verification of my phone was enabled.	3.52	1.10
29. I use an open Wi-Fi connection in public places when I perform key operations such as payment.	2.77	1.20
30. I often back up important data in my mobile phone on a regular basis.	3.52	1.10

4.4 Exploratory Factor Analysis of the Survey

The thirty questions in the second section of the survey assessed the knowledge, awareness, and practice of smartphone security among university students. EFA and Cronbach alpha reliability analysis were utilized to assess collected data for precise measurement (Tinmaz & Lee, 2020).

Through the initial factor analysis, the Kaiser-Meyer-Olkin (KMO) coefficient (KMO measure of sampling adequacy test) is 0.965 and the approximate $\chi2$ (435, n = 1364) is equal to 25,991.904 and $p < 0.00$ (Bartlett's test of sphericity), indicating that the sample size of this study is adequate for conducting the analysis. The data were then subjected to factor analysis.

Principal component exploratory factor analysis was used to examine the dimensionality of the thirty items, and three factors were then rotated using the varimax rotation process. Using factor loadings and eigenvalues, twelve items were omitted from analysis during the analysis. The numbers of the removed questions are 1, 2, 5, 6, 7, 10, 11, 12, 18, 21, 24, and 29. The mean and standard deviation for each question can be found in Table 5.

The final step involved fitting three components to the varimax rotation model. According to Table 6, the rotating solution was concluded with three interpretable factors: awareness (M = 4.10, SD = 0.72), practice (M = 3.52, SD = 0.86), and knowledge (M = 3.84, SD = 0.86). At the conclusion of the factor analysis, the reliability of overall questions and the inner-reliability of each factor were determined. The Cronbach of all factor questions is 0.94, while the Cronbach of factor1 is 0.93, factor2 is 0.89, and factor3 is 0.81. According to Moletsane and Tsibolane (2020), a reliability value of 0.6 or above is deemed acceptable in exploratory studies, hence these results demonstrated an exceptionally high level of reliability.

Table 6. Principal-components Analysis with Varimax Rotation, Coefficient Alphas and Basic Statistics for Smartphone Security

Factor loading (α = .94, 18 items, n = 1364)					
Item Number	Factor 1 – General smartphone security awareness (α = .93), eight items, n = 1364	Factor 2 –General smartphone security practice (α = .89), seven items, n = 1364	Factor 3 –Application security knowledge (α = .81), three items, n = 1364	*M*	*SD*
16	.849			4.10	0.72
17	.840				
14	.781				
8	.759				
13	.721				
25	.687				
15	.671				
19	.669				
27		.862		3.52	0.86
28		.785			
26		.765			
30		.756			
20		.676			
22		.642			
23		.631			
4			.806	3.84	0.89
3			.781		
9			.662		

4.5 Comparative Tests Based on Genders and Grades

The independent samples t-test was used to analyze the difference between male and female students on the three factors of awareness, practice, and knowledge. The significance of Levene's test for the equality of variances was checked first, followed by the significance value of the independent samples t-test. According to Table 7, the significant values of the Levene's test for factors 1 and 2 are 0.00<0.05, however the significance value for factor 3 is 0.53>0.05. Regarding the independent samples t-test, the p-value of factor 1 is 0.17, which is greater than 0.05, showing that there is no significant difference between male and female university students in smartphone security awareness. However, the p-values of factors 2 and 3 are both 0.00, which is less than 0.05, indicating that there is substantial gender-based difference in smartphone security practices and application security awareness among university students.

Table 7. Independent Sample t-tests on Gender vs Three Factors

Factor		Levene's Test		Independent samples t-test		
		F	*p*	*t*	*df*	*p*
Factor 1	awareness	19.25	0.00	1.36	888.50	0.17
Factor 2	practice	32.92	0.00	6.20	871.10	0.00
Factor 3	knowledge	0.53	0.47	4.05	1362	0.00

To determine where male and female students vary in factor 2 and factor 3, the mean and standard deviation of each group's components were compared. According to Table 8, the results showed that male students perform better than females in factor 2 and factor 3.

Table 8. The Basic Statistics of Genders in Three Factors

Factor		*Gender*	*n*	*M*	*SD*
Factor 1	awareness	Male	485	4.14	0.786
		Female	879	4.10	0.685
Factor 2	practice	Male	485	3.72	0.938
		Female	879	3.41	0.798
Factor 3	knowledge	Male	485	3.97	0.917
		Female	879	3.76	0.874

Table 9 displays the results of a one-way ANOVA test conducted to examine whether differences exist in each component for university students of different grade levels. First, the significance values of the One-way ANOVA test for factor 1, factor 2, and factor 3 are separately 0.03, 0.50, and 0.04, indicating that there is a significant difference in factor 1 and factor 3 between students of different school levels, but there is no significant difference found in factor 2. Levene's test of homogeneity of variances revealed that the variance of factor 2 (p=0.11) is equal for university students of different grade levels, however the variances of factors 1 (p=0.00) and factor 3 (p=0.04) are not equal. Subsequently, Tukey post-hoc tests and Dunnett's C post-hoc tests were performed to determine where the differences exist in factor 1 and factor 3. Incorporating the significance level of the post-hoc tests and the descriptive statistics of each factor, the study determined that freshmen have a higher level of factor 1 than juniors. In addition, there are no significant differences between university students of different grade levels with regard to the remaining two factors.

Table 9. One-way ANOVA Tests on Different Grades vs Three Factors

factors		*Levels*	*n*	*M*	*SD*	*F* *(df=1364)*	*p*	*post-hoc test* *results**
Factor 1	awareness	Freshman	505	4.19	0.65	4.642	0.00	Freshman>Junior
		Sophomore	364	4.07	0.75			
		Junior	264	4.01	0.76			
		Senior	231	4.06	0.77			
Factor 2	practice	Freshman	505	3.53	0.86	0.791	0.50	NS
		Sophomore	364	3.47	0.82			
		Junior	264	3.57	0.86			
		Senior	231	3.52	0.93			
Factor 3	knowledge	Freshman	505	3.77	0.91	2.707	0.04	NS
		Sophomore	364	3.80	0.95			
		Junior	264	3.90	0.83			
		Senior	231	3.95	0.84			

*NS: Non-significant.

5. Discussion

The findings of this study shed light on several important aspects related to smartphone security among university students. Firstly, the study revealed that Android operating system is highly prevalent among university students in China, with 82.6% of participants using Android phones. This indicates the popularity of Android smartphones among this demographic. In terms of cybersecurity risks, the study identified privacy information leakage as the primary concern among participants. This highlights the increasing reliance on smartphones for personal daily activities, where the handling of sensitive information raises concerns. Additionally, financial theft in smartphone use emerged as a distinctive concern that differs from the use of computers. The study also found that college students pay significant attention to risks such as virus attacks, data loss, account theft, and online fraud, indicating their overall awareness of major smartphone security risks. However, students comparatively pay less attention to spam and cyberbullying, as they perceive these threats as having minimal impact on their financial and privacy security.

Regarding the acquisition of smartphone security knowledge, Internet media and current affairs news reports were identified as the most popular sources among university students. Surprisingly, the study found that experiences shared by friends or classmates and personal encounters with risk events were also considered important sources of security knowledge. This suggests that an increasing number of individuals have faced cyber threats in smartphone usage, leading to the exchange of experiences and knowledge among peers. On the other hand, the study revealed that lectures and courses on information security offered by colleges had a limited contribution compared to other sources. This indicates a need to strengthen information security education at the university level. Nevertheless, the study noted that only a small number of students claimed to never pay attention to smartphone security, indicating a general awareness of its importance among the majority of participants. This finding aligns with previous research by Garba et al. (2020), which highlighted the high level of enthusiasm and desire among over 95% of respondents to learn more about cybersecurity.

In terms of performance in various aspects of smartphone security, the study found that college students generally had a good understanding of security aspects related to smartphone loss, personal information release, and link clicking during smartphone use. However, the study identified weaknesses in managing passwords and Wi-Fi connections, suggesting a lack of in-depth cybersecurity knowledge and security practices in these areas. This finding corresponds to the conclusion drawn by Alharbi and Tassaddiq (2021), who reported that a significant percentage of students found it annoying to set strong or long passwords and tended to use the same password for multiple websites and accounts. In addition, the study found that most university students have a satisfactory level of smartphone security awareness, but it is much lower in security practice, which proves the viewpoint that there is a possibility of disconnection between good security practice and having sufficient knowledge and understanding (Chandarman & Niekerk, 2017).

The study used cross analysis to investigate any potential variations between male and female students' concerns about risks linked to smartphone security. The findings showed that students of different genders choose smartphone security threats that are considerably different from one another. Although the most concerning issue for both genders is privacy leaking, female students are more aware of smartphone security concerns such as virus attacks, online fraud, and cyberbullying, while male students are more alert to privacy leakage, financial theft, and data loss. Female students pay the same attention to spam and accounts that have been stolen as do male students. In addition, students from both genders pay equal attention to spam and accounts safety.

The cross analysis was once more employed to look at the variations in students' preferred learning strategies for security knowledge across grade levels. The findings demonstrated that, especially for seniors, Internet media and current affairs news broadcasts are the students' favorite learning resources for understanding smartphone security. Learning security knowledge through the experiences of friends or classmates is also found to be an important technique, with no variation seen among students across different grades. In order to learn about smartphone security, it's also critical to explore educational options like information security lectures and courses. Freshmen exhibit a larger inclination to use these channels than students in other grades. In addition, there is minimal difference between university students in different grade levels when it comes to how valuable it is to learn about security through personal experiences with risky events.

Regarding the students' performance in terms of smartphone security awareness, practice, and knowledge, the results showed that while university students generally have a good level of smartphone security awareness, it is significantly lower in security practice, which supports the idea that there may be a disconnect between having sufficient knowledge and understanding and good security practice (Chandarman & Niekerk, 2017). Independent sample t-test results revealed that there is no difference between gender groups in terms of general smartphone security awareness, supporting Sun's finding that there is no statistically significant relationship between gender and ISA. In contrast, male students outperform female students in terms of smartphone security awareness and general security practices. One-way ANOVA analysis was employed to look at how university students in different grades differed in each area of smartphone security. The findings showed that neither the security practice nor security knowledge is significantly impacted by the educational level. This is consistent with the study by Matyokurehwa et al. (2020), while they found a similar lack of statistically significant correlation between age and cyber security. Unexpectedly, it is discovered that freshmen outperform juniors in smartphone security awareness, indicating that ISA for university students does not rise with grade level. On the other hand, there is still a paucity of cyber security education at the university level.

6. Conclusion

This study highlighted the importance of the information security awareness related to smartphone use and aimed to examine university students' performance in this field in China context. It started by looking at the operating systems of the students, concerned about potential risks, and learning approaches linked to smartphone security. It was discovered that the majority of university students in China used the Android system and Internet media was recognized as the best resource for learning about the smartphone security knowledge. Both male and female students give personal privacy and financial security the most care, while female students are more worried about online threats including virus attacks, fraud, and cyberbullying. Although students across various grades performed broadly similarly in their favourite learning approaches to obtain about security knowledge, freshmen demonstrated a larger preference for educational techniques like lectures and courses. The majority of the students are well-aware of security in general, but they still struggle with passwords and Wi-Fi connections. To gain further insights, a comprehensive questionnaire was developed to assess users' smartphone security levels. Based on the factor analysis, three key factors of awareness, knowledge, and practice are constructed. Furthermore, this study specifically investigated the influence of gender and grade level on these three dimensions of smartphone security. The findings revealed that gender did not significantly impact awareness, whereas male students demonstrated higher levels of practice and knowledge compared to their female counterparts. Additionally, no substantial disparities in practice or knowledge were observed among students of different grade levels. However, freshmen exhibited greater awareness compared to juniors.

6.1 Implications for Practice

Researchers in this field will benefit from this study because it has a wealth of information that can be consulted, particularly with regard to questionnaire design and analysis techniques. The conclusions of this study can also be used by researchers to compare and analyze university students from various areas, universities, and academic levels. The information security status of the students can be learned from this study by the university administrator, who can use it to help the university demonstrate information education. In order to increase students' cybersecurity knowledge for university education, it's crucial to understand current security levels, worries about cyber threats, preferred learning styles, and variances in each dimension.

To enhance university students' comprehension of information security, it is imperative to provide lectures and courses specifically focused on this subject. Although most students have basic smartphone security concepts, The study demonstrated their incapacity to handle complex issues like passwords and Wi-Fi connections. This shows that further professional information security knowledge cannot be learned in a conventional manner; instead, professional education is required. This indicates that it is difficult to gain more professional information security knowledge through informal learning channels and that universities must invest in professional education to some extent. Additionally, there is almost no difference in smartphone security awareness, practice or knowledge among students from different grade levels, which suggests that colleges and universities have not provided adequate information security education.

6.2 Limitations and Further Research

While this paper makes a significant contribution to the understanding of university students' smartphone security awareness, it still has certain limitations. First of all, this study's sample was restricted to regional general universities in Northwest China. The sample of future studies might be widened to include universities from multiple levels, regions, and cultural backgrounds. As a result, researchers will be able to compare the differences in smartphone security knowledge among university students from various educational backgrounds. Second, while the primary goals of this study were to measure and survey, future research might add relevant theories to offer a more thorough knowledge of the variables impacting students' cybersecurity behavior in the context of higher education. Combing with relevant theories like the general deterrence theory (GDT), Protection Motivation Theory (PMT), or Theory of Planned Behavior (TPB) may offer valuable insights into the motivations and decision-making processes underlying students' cybersecurity practices. Lastly, the research method employed in this study is only quantitative. Qualitative research techniques like focus groups, interviews, and case studies may be useful in the future. The experiences, views, and difficulties faced by university students in the area of information security can be thoroughly found and analyzed using qualitative methodologies. By combining quantitative and qualitative approaches, researchers can find more potential problems and explore effective solutions in enhancing students' ISA level in the higher education context.

Acknowledgement

This paper is founded by Shaanxi Provincial Education Science 13th Five Year Plan Project (Grant No. SGH18H416).

References

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

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information and Knowledge Management*, *15*(1), 1650007. https://doi.org/10.1142/S0219649216500076

Chandarman, R., & Niekerk, B. V. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *205*(20), 133-155. https://doi.org/10.23962/10539/23572

Chen, Z. (2021). An empirical analysis of contemporary college students' awareness of network security. *Network Security Technology and Application*, *12*, 91-92.

CNNIC (2022). *The 49th Statistical Report on Internet Development in China*. Retrieved December 12, 2022, from http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/

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. *International Journal on Emerging Technologies*, *11*(5), 41-49.

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, *28*(3), 81-106. https://doi.org/10.1080/19393555.2019.1657527

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, *10*(4), 186-202. https://doi.org/10.1080/15536548.2014.974429

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Hunt, T. (2016). *Cyber Security Awareness in Higher Education*. Retrieved November 26, 2023, from https://digitalcommons.cwu.edu/source/2016/cob/1/

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management*, *35*(5), 561-571. https://doi.org/10.1016/j.ijinfomgt.2015.06.003

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6), 73-83. https://doi.org/10.1007/s11528-014-0806-x

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, *2019*(1), 2786913. https://doi.org/10.1155/2019/2786913

Ma, Y. P., & Fan, J. Y. (2022). Research on personal information security consciousness of university students in the big data era. *Science & Technology Information*, *05*, 238-241.

Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, *18*(8), 67-89. https://doi.org/10.12700/APH.18.8.2021.8.4

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2020). Cybersecurity awareness in Zimbabwean Universities: Perspectives from the students. *Security and Privacy*, *4*(2), e141. https://doi.org/10.1002/spy2.141

McCombes, S. (2021). *What Is a Research Design | Types, Guide & Examples*. Retrieved December 11, 2022, from https://www.scribbr.com/methodology/research-design/

Middleton, F. (2022). *Reliability vs. validity in research: Difference, types and examples*. Retrieved December 28, 2022, from https://www.scribbr.com/methodology/reliability-vs-validity/

Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9* (pp. 79-87). Springer International Publishing. https://doi.org/10.1201/9780429031908

Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In *2020 conference on information communications technology and society (ICTAS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICTAS47918.2020.233978

Norris, M., & Lecavalier, L. (2010). Evaluating the use of exploratory factor analysis in developmental disability psychological research. *Journal of autism and developmental disorders*, *40*, 8-20. https://doi.org/10.1007/s10803-009-0816-2

Qiu, D., Wang, H., & Li, Z. (2020). Discussion on mobile phone information safety in the mobile internet era. *Telecom Engineering Technics and Standardization*, *08*, 21-26. https://doi.org/10.13992/j.cnki.tetas.2020.08.005

Rahim, N., Hamid, S., Mat Kiah, M., 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

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. In *IOP Conference Series: Materials Science and Engineering* (Vol. 263, No. 4, p. 042043). IOP Publishing. https://doi.org/10.1088/1757-899X/263/4/042043

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: An empirical analysis. *Information & Computer Security*, *28*(2), 293-318. https://doi.org/10.1108/ICS-04-2019-0041

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26. https://doi.org/10.1080/15536548.2012.10845664

Sun, W. (2018). *Investigation and Research on Network Security Consciousness of University students in Dalian* (Master's thesis). Dalian University of Technology, Dalian, China.

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721-1736. https://doi.org/10.1007/s10639-020-10330-0

Tian, L., Liu, N., & Peng, B. (2019). Overview of network security awareness research. *Information Security and Communication Confidentiality*, *6*, 36-45.

Tinmaz, H., & Lee, J. (2020). General and instructional perceptions of South Korean messenger: 'KakaoTalk'. *International Journal of Learning and Change*, *12*(2), 143-168. https://doi.org/10.1504/IJLC.2020.106715

Verizon Business. (2021). 2021 DBIR Results & Analysis. Retrieved December 15, 2022, from https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

Yang, G., Ye, J., Yang, L., & Feng, K. (2022). Current situation and prospect of information security risks of intelligent devices. *Information Security and Communications Privac*y, *2*, 17-22.

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., and Li, J. (2016). Review on cyberspace security. *Scientia Sinica Informationis*, *2*, 125-164.

Zhang, X., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: An empirical analysis. *The Electronic Library*, *35*(6), 1177-1190. https://doi.org/10.1108/EL-09-2016-0183

Zhou, F. F., and Wang, J. J. (2018). Investigation and analysis of information security consciousness and behavior of smartphone users in university students. *Library and Information Work*, *10*, 47-53.

Zhou, J., Zhang, Y., & Zhang, C. (2017). Research on the network security behavior of college students—A case study of Nanjing University. *Education Modernization*, *19*, 165-166.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269