Modern Management Based on Big Data IV
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA230168

Undergraduates' Knowledge Attitude and Behavior (KAB) Towards the Disclosure of Personal Data Online in China

Xiaoyu Li[a], Qin An[b], Wilson Cheong Hin Hong[c], Yunfeng Zhang[d], Kimberly Kolletar-Zhu[e], Xiaoshu Xu[e1]

[a]*Law School, Wenzhou University, Wenzhou City, 325035, China*
[b]*International Business School, Chengdu Institute Sichuan International Studies University, Chengdu, 610000, China*
[c]*Centre for Teaching and Learning Enhancement, Macao Institute for Tourism Studies, China*
[d]*Centre for Portuguese Studies, Macao Polytechnic University, Macao 999078, China*
[e]*School of Foreign Studies, Wenzhou University, Wenzhou City, 325035, China*

Abstract. In the midst of the COVID-19 pandemic, the employment and education sectors have shifted significantly toward online platforms. However, the increased reliance on these digital spaces has raised concerns about personal security information. Scholars have taken note of this issue and have explored its implications, with some employing the extended knowledge, attitude, and behavior (KAB) model to investigate the moderating effects of societal education level on the relationship between knowledge and attitude. Hong et al. [1] conducted a study to examine undergraduates' KAB regarding personal data sharing in Chinese higher education institutions during the pandemic. Using a questionnaire, the study recruited 156 participants from three universities in West and East China. Using SPSS 23.0, data analysis revealed a widespread lack of awareness, a positive attitude, and proper behavior among college students regarding online personal information leakage during the pandemic. Notably, disparities were observed in KAB among students of different grades, majors, and genders. Students in their sophomore, junior, and senior years were found to be more concerned than freshmen about the availability of their personal information online; what's more, science majors were more concerned than students of other majors. There appear to be significant gender differences in personal information sharing, ie., males are more concerned about the security of personal information online than females. Through this study, we aim to emphasize that college students' awareness of personal information protection needs to be improved and suggest that university administrators and policymakers increase information security training. The findings of this study contribute to the theoretical and practical efforts to improve information security in higher education. Future studies should broaden the survey sample and examine the primary factors that influence college students' KAB of personal information security to ensure the generalization of findings.

[1]Corresponding Author: Xiaoshu Xu, Wenzhou University, China; Email: lisaxu@wzu.edu.cn.
Xiaoshu Xu received China National Social Science Late-stage Funding Project (21FJKB013). The questionnaire data used to support the findings of this study have been deposited in the figshare repository (10.6084/m9.figshare.21994346). The authors declare that they have no conflicts of interest to report regarding the present study.

Keywords. KBA model, disclosure of personal data, survey, higher education, online security

1. Introduction

The novel corona-virus pneumonia has a huge impact on all sectors of medicine, health, the economy, and society. In the field of education, the United Nations' Education Policy Brief for the Period and Beyond of COVID-19, released on August 4, 2020, states that the spread of COVID-19 has affected nearly 1.6 billion students in more than 190 countries and territories worldwide, with 94% of students worldwide affected by the closure of schools and educational institutions. In low- and lower-middle-income countries, the proportion is as high as 99 percent. Online education and online working were quite popular throughout the pandemic period, as were numerous apps, online streaming, telemarketing, and so on. As a result, the issue of personal data security arises. The popularity of online learning and data analysis has made learning analytics an essential component of educational technology [2]. In education, the use of students' personal information is increasing, and students' behavior can even be captured and evaluated.

According to the 2021 College Students' Financial Anti-Fraud Research Report, 46% of undergraduate students have been victims of fraud. College and university information security is inadequate.

There is insufficient daily administration and maintenance, network security work is not prioritized, knowledge of information security protection is low, and weaknesses are not addressed or updated on time, among other reasons, because colleges and universities prioritize building but overlook management. All of these qualities put the institution's information system at risk of security breaches. The information security knowledge, abilities, and attitudes of Chinese undergraduates have not received much research. Large-scale empirical studies and updated research data were lacking in the earlier studies.

This study used the “Star” questionnaire to investigate Chinese college students. The questionnaire consists of three parts. The first part focuses on college students' understanding of online personal information security. The second part examines their attitude towards network personal information security, and the third part examines their behavior in network personal information security. The purpose of this study is to understand the current situation of college students' attitudes, knowledge, and ability in personal information security and to make suggestions on the protection of college students' personal information.

2. Materials and Methods

2.1. KAB Model

The Knowledge Attitude Behavior (KAB) model is based on three interrelated parts of the social psychology model: cognition (knowledge), influence (attitude), and behavior, [3] [4].The knowledge-attitude-behaviour (KAB) model was first proposed by Kruger and Kearney to measure information security awareness. The main proposition of KAB is that users have sufficient information security knowledge and a more positive attitude towards information security, which leads to more positive information security behavior. The theoretical framework underpinning KAB entails a comprehension of the interrelationships among its three constituents. Specifically, KAB posits that the progressive accumulation of knowledge in a relevant domain, such as online security, health, or education, will gradually influence an individual's attitude, subsequently instigating a change in their behavior. Knowledge refers to what is known (declarative), how it is known (procedural), when it is known, and why it is known (conditional) [5], whereas attitude and behavior are defined as belief and perception, respectively [6]. The KAB is a dynamic, interactive model that was originally used in the fields of health and environmental psychology, criminology, climate change, and education and is now applied in network security research.

Specifically, Parsons et al. examined the information security loopholes caused by individuals based on (KAB) [7]. The Personal-perspective-based Information Security Questionnaire (HAIS-Q) was developed in 2014, and it outlined the development of its concept as well as the validity and reliability tests [8]. Knowledge of the policies and procedures was also studied, as was the relationship between attitudes towards policies and procedures and the use of work computers (KAB); further knowledge of policies and procedures in 2015 [9]; attitudes towards policies and procedures; and self-reported behavior, combined with organizational factors. Subsequent empirical studies further demonstrated the effectiveness of HAIS-Q as an effective tool for measuring information security factors [10].

McCormac et al. examined the connection between individual information security awareness and individual differences in characteristics using the HAIS-Q (age, gender, personality, and risk-taking). The HAIS-test-retest Q's reliability and internal consistency were both investigated in 2017 [11]. Individual resiliency, workplace stress, and their ISA (KAB) were all studied in 2018 [12].

Sawaya et al. surveyed 3,500 online users from seven countries using the Security Behavior Intention Scale (SeBIS), testing the effectiveness of common security defenses with a special focus on cultural implications. People from Asian countries, particularly Japan, for example, exhibited less safe behavior [13].

Wahyudiwan et al. investigated the ISA level of MERTHE personnel in 2017 using the (KAB) model's three components and the seven key areas of information security. They concluded that knowledge has a positive impact on attitudes and behavior when it comes to information security [14].

Cain et al. conducted 10 cybersecurity-related questions to perform a knowledge and behavior questionnaire survey on corporate employees in 2018, evaluating the impact of age, gender, criminal background, professional expertise, and cybersecurity training [15].

Wiley et al. conducted a 2019 survey of employees in Australian organizations to examine the connection between cybersecurity awareness, organizational culture, and safety culture [16].

Abanoub Riad et al. investigated Estonian dental students' oral health-related (KAB) to promote oral health and disease prevention [17].

2.2. Online Information Security

The student-centered education model does a lot of student data research to understand and help students' efficiency, assist teachers and improve teaching procedures. While the number of research publications on cybersecurity is rising in general, empirical research on security practices in higher education is critically insufficient [18]. For example, Chandarman and Van Niekerk employed the Theory of Planned Behavior Model (TPB) to measure the CSA level of students in South African private higher education institutions [19].

Lean-Ping and Chien-Fatt used the TPB model to investigate the individual information security self-awareness of students at 11 Malaysian universities. This is based on the 2003 National Institute of Standards and Technology Special Report (NIST SP 800-50) [20].

Kim surveyed undergraduates at a business school in the United States about their understanding and attitudes toward information security [21]. Berki et al. assessed prospective IT workers on their knowledge, concepts, and awareness of cybersecurity while utilizing cloud-based services by looking at current IT students' higher education degree programs and cybersecurity courses in five countries: China, Finland, Greece, Nepal, and the United Kingdom [22].

In the studies conducted by Parsons et al., 1112 undergraduates completed the HAIS-Q and participated in lab-based phishing trials [9] [10]. Higher HAIS-Q scores performed better in phishing studies, indicating that HAIS-Q can predict certain aspects of information security behavior.

Vidakis uses the xAPI library to capture data in a serious game environment, which is compatible with the experience API (xAPI) and implemented in the Unity 3D game engine. Use learning analytics in serious games to simplify data generation and record educationally valuable events [2].

2.3. Disclosure of personal data

The concepts of "personal data," "personal information," and "personal data" are used in the legislation of different countries and regions. The Personal Data Ordinance in Hong Kong, China, defines personal data. Personal data is governed by the 2010 "Law on Personal Data Protection" and the 1995 "Law on Computer Processing of Personal Data Protection." The term "personal data" is directly used in legislation in the United Kingdom and the European Union. The concept of "personal data" is used in China's Civil Code and Personal Information Protection Law.

Personal information refers to any sort of information stored electronically or in other ways that, alone or in conjunction with other information, can identify the identity of a specific natural person or reflect the actions of a specific natural person.

Name, date of birth, ID card number, personal biometric information, address, communication contact information, communication records and contents, account passwords, property information, credit information, whereabouts and traces, accommodation information, health and physiological information, transaction information, and other similar information. Information security technology and personal information security standards specify the method and type of personal information to be determined. Personal information should aid in the identification of a specific natural person in two ways: one, through identification, that is, from information to individual; and two, by the information itself, a special identification of a specific natural person. The second is the association, that is, from the individual to the information, such as the known specific natural person, generated by the specific natural person in his or her activities. Information that conforms to one of the above two circumstances shall be judged to be personal information.

According to the 2016 China Personal Information Security and Privacy Protection Report, more than 70% of individuals consider personal information leakage to be a serious problem.

People who know personal information about them, such as their name or place of employment, have called up to 81% of those surveyed. 53 percent have experienced harassment as a result of exposing personal information when searching or browsing the web.

Furthermore, 36% were harassed or defrauded by marketing after their personal information was compromised, such as when renting, purchasing a home, buying a car, taking an exam, or enrolling in college. According to the 2021 National Internet Users' Satisfaction Survey Report on Internet Security, "nearly 80% of Internet users received sales calls from various agents; more than 60% of Internet users received junk mail; and nearly 60% of Internet users received relevant promotional messages."

In addition to harassment, public Internet users can estimate the risk of personal information leakage in other ways, such as: more than forty percent of netizens think of a great data kill because personal information has been leaked; nearly forty percent of netizens check the default agreement to the service agreement; this allows the application to collect user information, which can lead to personal information leakage; and so on.

The "Research Report on OTT Terminal Data Security and Personal Information Protection," published by the China Citic Institute in 2022, highlighted the issues of data security and personal information leakage caused by terminal applications, as well as the serious phenomenon of SDK collection and processing data. According to the report's objective conclusion, personal information security has remained a difficult issue in China in recent years.

During the COVID-19 pandemic in recent years, hundreds of millions of users collected mobile data on a large scale, especially call data logs and social media reports. In previous pandemic studies, researchers have used CDRs provided by mobile network operators to map people's movements. Back in 2014, the GSM Association issued guidelines on privacy when using mobile phone data in response to the Ebola outbreak. However, the long and widespread nature of the current outbreak has led to the use of big data, which has raised privacy and data protection issues.

The Internet of Things is an emerging technology that generates big data. The Internet of Things has been used in a variety of industries, such as health care, home automation, smart cars, and industrial automation. While the characteristics of the Internet of Things provide us with convenience, they also pose risks [23].

The extensive collection and use of data is the main reason for personal information disclosure. For example, in the retail industry, marketing uses decision-making and business planning to assess customer needs. The customer database is processed, and a comparison of age prediction techniques for "Blessed Friday" shoppers based on machine learning is proposed to determine which age group is more interested in "Blessed Friday" [24].

With the advancement of online social networking, undergraduates are active on variety of social networking platforms. As offline communication becomes more difficult, social media platforms such as Twitter and Weibo have evolved into convergence points for online social mindsets. Highly personal, sensitive, and potentially stigmatizing data is disclosed on social networking sites such as Facebook and Weibo [25].

Weinberger et al. [26] investigated and simulated the differences in attitudes toward online privacy and anonymity among male and female Israeli students in order to better understand their security awareness and behavior toward personal information leakage in an epidemic situation [26]. This study looked at undergraduates' personal privacy literacy from three perspectives: knowledge, attitude, and behavior (KAB). Based on Weinberger et al.'s [26] questionnaire, this study created a questionnaire on undergraduates' knowledge, attitudes, and actions regarding personal information security.

3. Research Design

3.1. Research Questions

- Q1: Are undergraduates knowledgeable about the disclosure of personal data online?
- Q2: What are the undergraduates' attitudes toward the disclosure of personal data online?
- Q3: What is the undergraduates' behavior towards the disclosure of personal data online?

In order to find the answers to these questions, we conducted a questionnaire survey of certain undergraduate students in China on their knowledge, attitude, and behavior regarding online personal information security[2]. We attempt to lay out a thorough framework of beliefs, values, and actions. Three components make up the questionnaire. The first component focuses on undergraduates' understanding of online personal information security; the second component examines their attitudes toward network personal information security; and the third component examines their conduct with regard to network personal information security.

The rest of this article is as follows:

- First, we'll go over our research methodology.
- Second, we will present the findings and analysis.
- Third, we present our findings and conclusions.
- Finally, we summarize the study's limitations.

3.2. Research Instruments

First, scales from previous research were consulted during the questionnaire design process of this article, and the scale that was consistent with this study was selected. The researchers inquire with information technology experts about their opinions, update and modify the maturity scale to reflect the specific research situation of this paper, and create a preliminary questionnaire. Second, discuss any suggestions made to the initial questionnaire item set, linguistic expression, etc. In response to feedback, the questionnaire has been modified to make it easier for respondents to accurately define the meaning of the term, to reduce the number of items, and to adjust the measuring items in the words. This alters the final form of the questionnaire. The Likert scale was used to assess students, and the Likert 5 subscales ranged from strongly disagreeing (1) to strongly agreeing (5) as the possibility of answers for all items, with only one answer allowed for each item. The setting of the online questionnaire does not allow blank

[2] Appendix A(1).docx

answers. The advantage of this setting is that it does not lose data and is convenient for accurate data analysis. If respondents do not want to answer, they can directly give up. It only takes about ten minutes to complete the entire questionnaire, and most respondents are willing to complete it all. Third, this research conducts an empirical investigation based on a questionnaire of knowledge, attitude, and behavior related to online personal information security. The data were analyzed using SPSS 23.0.

4. Results and Discussion

In the 2021-2022 academic year, this study is based on a survey of undergraduates from five universities in China. A total of 288 questionnaires were collected in this survey, excluding those that took less than three minutes. A total of 156 valid responses were collected in China. There were 22 students in year one, 114 in year two, 17 in year three, and 3 in year four. 110 were in liberal arts, 10 in engineering, and 36 in natural science. There were 41 males and 114 females. The descriptive information of the participants is shown in Table 1.

First, all undergraduates were screened to inform respondents about the background of the research project. And respondents have a background in higher education , often use the network, and have experienced online learning. Work participants contacted alumni in person, and two English educators invited undergraduates to fill out questionnaires by email and on-site. Senior students, because of the curriculum, busy internships and learning, it is difficult to find senior students. However, the grade and subject distribution of invited students in the sample is uneven.

Table 1. Data description

Data Description	Value Label	N
Year	Freshman Year 1	22
	Sophomore Year 2	114
	Junior Year 3	17
	Senior Year 4	3
Major	Liberal Arts	110
	Engineering	10
	Science	36
Gender	Male	41
	Female	114

4.1. Scale validity

Using Exploratory Factor Analysis (EFA) with Principle Component Analysis and Promax rotation provided by SPSS 23.0, Bartlett's Test of Sphericity was found to be significant (p<.001), meeting the assumption of correlations among question items [27]. Kaiser-Meyer-Olkin was at .81, suggesting the sample size is adequate and there are latent variables within the scale [28]. Hence, both criteria for EFA were met.

With Eigenvalue set at 1, EFA indicates that there are 12 variables. The first variable explained 23.71% of total variance, and the second explained 9.85% (see Table 2 for variables and variance percentage).

Table 2. The percentage variance explained by the variables

Variables	Eigenvalues	% of Variance	Cumulative %	Rotation Sums of Squared Loadings
1	12.09	23.7	23.7	7.53
2	5.02	9.85	33.55	6.99
3	3.89	7.63	41.18	5.99
4	2.76	5.42	46.60	5.61
5	2.44	4.78	51.39	4.69
6	1.66	3.25	54.64	5.38
7	1.56	3.05	57.69	2.58
8	1.51	2.97	60.65	3.52
9	1.44	2.81	63.47	5.30
10	1.22	2.40	65.87	3.12
11	1.11	2.18	68.05	2.55
12	1.03	2.02	70.07	4.17

As suggested in the literature, items that did not obtain a loading of 0.3 were suppressed [29] (p. 692). Then, items that did not have any components above 0.3 loading were removed. Questions that that were found to be valid included *knowledge*: k1, k3, k4, k5, k7, k10, k12, k14, k18, k21, k22, k27; *attitude*: a1, a2, a3, a4, a5, a7, a18, a10, a11, a12, a14, a15, a16, a22, a23, a24, a25, a26, a27; and *behaviour*: b1, b2, b3, b4, b5, b7, b8, b9, b10, b11, b12, b13, b14, b18, b19, b21, b22, b23, b24, and b27 (see table 3 for the factor loading of individual items). As can be seen, there are no satisfying items in component 12, which is normal considering its eigenvalue is only marginally above 1 [30].

Table 3. The factor loading of individual items

Loading	1	2	3	4	5	6	7	8	9	10	11	12
k1	0.698											
k3	0.723											
k4	0.478										0.702	
k5											0.722	
k7	0.702											
k10	0.854											
k12	0.736						0.301					
k14	0.557											
k18	0.694											
k21	0.775											
k22	0.508											0.368
k27	0.420											
a1									0.392			

a2								0.638			
a3								0.649	0.351		
a4								0.797			
a5								0.397			
a7							0.821				
a18							0.708			0.321	
a10		0.816									
a11		0.421		0.372							0.294
a12		0.597									
a14		0.837									
a15		0.886									
a16		0.846									
a22	0.672										0.331
a23	0.534				0.564						
a24	0.890										
a25	0.897										
a26	0.951										
a27	0.825										
b1									0.465		
b2									0.826		
b3			0.899								
b4			0.661								
b5			0.767								
b7			0.614								
b8						0.675					
b9						0.752					
b10				0.708							
b11				0.946							
b12				0.602							
b13				0.500		0.321					
b14				0.431		0.305					
b18				0.787							
b19				0.385							
b21					0.809						
b22					0.837						

b23		0.698
b24	0.353	0.558
b27		0.303

4.2. Validity of the data

Reliability describes the consistency of the measured items within a scale. Cronbach's alpha was employed, and the knowledge dimension was found to be at .905 (see Table 4 for the alpha values and descriptive statistics of the knowledge dimension).

Table 4. Reliability Test Scale: Knowledge

Cronbach's Alpha	Cronbach's Alpha coefficients based on standardized entries		Number of items
.905	.905		12
	Item Statistics		
	Mean	**Std. Deviation**	**N**
k1	3.23	1.15	156
k3	3.13	1.11	156
k4	2.32	1.03	156
k5	2.16	1.07	156
k7	2.94	1.08	156
k10	2.72	1.14	156
k12	2.79	1.16	156
k14	2.38	1.06	156
k18	2.85	1.09	156
k21	2.74	1.19	156
k22	2.14	1.03	156
k27	1.74	0.90	156

We then analyzed the internal reliability of attitudes toward online personal information leakage. Cronbach's alpha was found to be at .896 (see Table 5 for the Alpha values and descriptive statistics of the attitude dimension).

Table 5. Reliability Test Scale: Attitude

Cronbach's Alpha	Cronbach's Alpha coefficients based on standardized entries		Number of items
.896	.896		19
	Item Statistics		
	Mean	**Std. Deviation**	**N**
a1	3.13	1.11	156
a2	2.90	1.24	156
a3	2.78	1.12	156
a4	2.86	1.10	156
a5	2.60	1.03	156
a7	2.18	1.02	156
a10	3.54	1.10	156
a11	3.12	1.05	156
a12	3.33	1.09	156
a14	3.53	1.14	156
a15	3.45	1.09	156
a16	3.37	1.05	156
a18	2.76	1.13	156
a22	2.79	1.12	156
a23	3.10	1.20	156

a24	2.56	1.07	156
a25	2.63	1.11	156
a26	2.58	1.08	156
a27	2.42	1.11	156

Finally, Cronbach's alpha of behaviour was at .857 (see Table 6).

Table 6. Reliability Test Scale: Behavior

Cronbach's Alpha	Cronbach's Alpha coefficients based on standardized entries		Number of items
.857	.857		20
	Item Statistics		
	Mean	Std. Deviation	N
b1	2.94	1.11	156
b2	2.58	1.23	156
b3	2.03	.89	156
b4	2.34	.98	156
b5	2.08	.96	156
b7	1.67	.92	156
b8	3.11	1.21	156
b9	3.24	1.22	156
b10	3.64	1.13	156
b11	3.12	1.17	156
b12	3.32	1.10	156
b13	3.53	1.28	156
b14	3.68	1.27	156
b18	2.39	1.13	156
b19	3.29	1.10	156
b21	3.13	1.16	156
b22	2.70	1.12	156
b23	2.90	1.21	156
b24	2.26	1.08	156
b27	1.94	.97	156

Hence, it can be concluded that both the validity and reliability of the proposed scale was satisfactory.

4.3. Assumption testing for regression analysis

The variables' normality was examined. Because there were more than 50 participants, predetermined tests like Kolmogorov-Smirnov and Shapiro-Wilk were inappropriate. A manual evaluation was used to determine the skewness and kurtosis values. The term "normal distribution" was used to describe samples with skewness between -2 and +2 and kurtosis between -7 and 7. Average knowledge (skewness = -.240, kurtosis = 1.31), attitude (skewness = -.40, kurtosis =-.66), and behavior (skewness = -.17, kurtosis =.36) were all within the acceptable threshold range and were normally distributed.

Table 7. Skewness and Kurtosis

		Statistic	Std. Error
knowledge_mean	The average	2.60	0.06
	Partial degrees	0.24	0.19
	kurtosis	0.42	0.39
attitude_mean	The average	2.93	0.05
	Partial degrees	0.39	0.19
	kurtosis	0.66	0.39
behavior_mean	The average	2.79	0.05

	Partial degrees	0.17	0.19
	kurtosis	1.31	0.39

Figures 1-Figure 3 show that the data are roughly normally distributed.

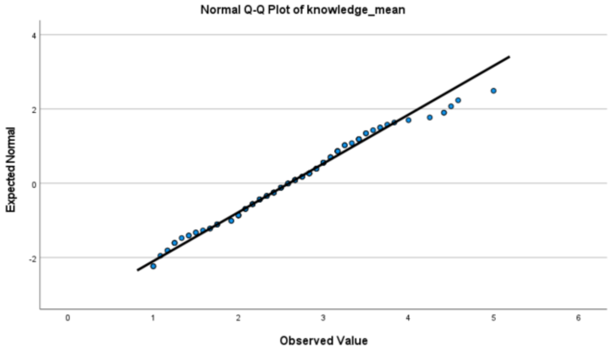

Figure 1. Plot of knowledge mean

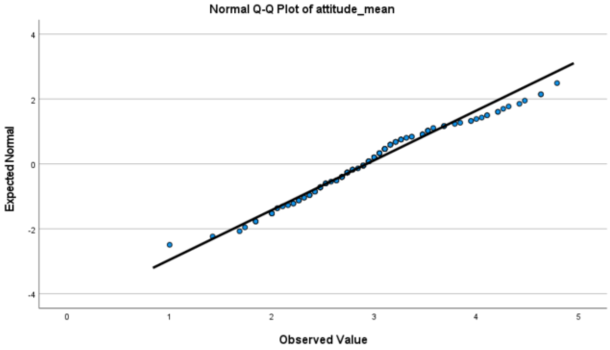

Figure 2. Plot of attitude mean

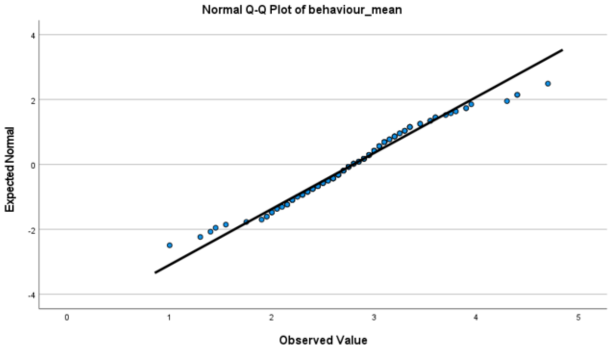

Figure 3. Plot of behavior mean

Figures 1-3 show that the data develops roughly along the normal distribution line in the quantile plot, with some deviations in the tail.

Based on these figures, we can safely assume that this set of data is normally distributed.

Because equal variance is not achieved, Pillai's Trace can only be used for analysis, where the significance test shows that the significance value of gender is 017 [31].

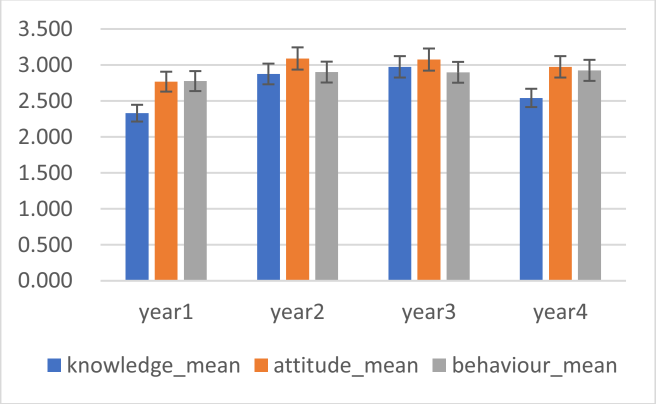

Figure 4. Average values and differences in knowledge, attitude, and behavior of different years.

Figure 4 depicts the average values and differences in knowledge, attitude, and behavior of different grades regarding the disclosure of personal information online. The mean values of the freshman's knowledge, attitude, and behavior are 2.330, 2.768, and 2.776, respectively. Sophomores' mean values for knowledge, attitude, and behavior were 2.875, 3.090, and 2.901, respectively. Juniors' mean knowledge, attitude, and behavior scores were 2.974, 3.075, and 2.898, respectively. Seniors' mean values for knowledge, attitude, and behavior were 2.542, 2.974, and 2.925, respectively. In terms of knowledge, the difference between freshmen and juniors was the largest. In terms of attitude, the difference was greatest between freshmen and sophomores. In terms of behavioral averages, the freshman and senior years differed the most. Less understanding to understanding, less agreement to mostly agreement, and less agreement to mostly agreement are the mean values for knowledge, attitude, and behavior, respectively.

Further investigation reveals that senior students are more concerned about online personal information disclosure than junior students (freshmen). Senior students have a relatively low level of knowledge on this subject, which should be noted. Seniors clearly have more experience with and understanding of online social networking and shopping than juniors.

Furthermore, seniors are about to enter society and will be more concerned with social issues as well as personal rights and interests. More than half of all undergraduates who have been victimized are freshmen, according to law enforcement statistics. Freshmen appear to be less concerned about online personal information disclosure.

Figure 5 depicts the average values and professional differences in the three aspects of knowledge, attitude, and behavior for various majors. In general, the mean values of knowledge, attitude, and behavior in the liberal arts are 2.599, 2.926, and 2.806, respectively. The mean values of knowledge, attitude, and behavior in engineering are 2.442, 2.800, and 2.895, respectively. The mean values of knowledge, attitude, and behavior in science were 3.000, 3.204, and 2.904, respectively. In terms of knowledge, the difference between engineering and science was the largest. In terms of attitude, the difference was greatest between engineering and science. In terms of behavior, the difference was greatest between science and engineering. Less understanding of understanding, less agreement to mostly agreement, and less agreement to mostly agreement are the mean values of knowledge, attitude, and behavior, respectively.

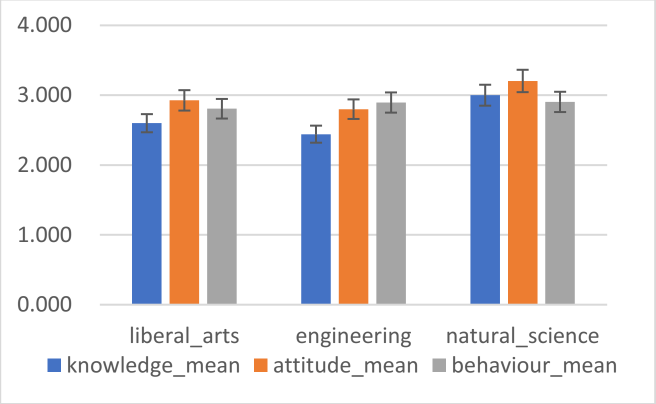

Figure 5. Average values and professional differences of the three aspects of knowledge, attitude, and behavior of different majors

Further investigation revealed that the values of knowledge, attitude, and behavior of undergraduates from all majors regarding personal information disclosure were greater than 2.4. Students majoring in science are more concerned about online personal information disclosure than students majoring in other fields. Engineering students are less concerned about the problem. The gap between genders, the average knowledge, the average attitude, and the average behavior of different genders are shown in Figure 6.

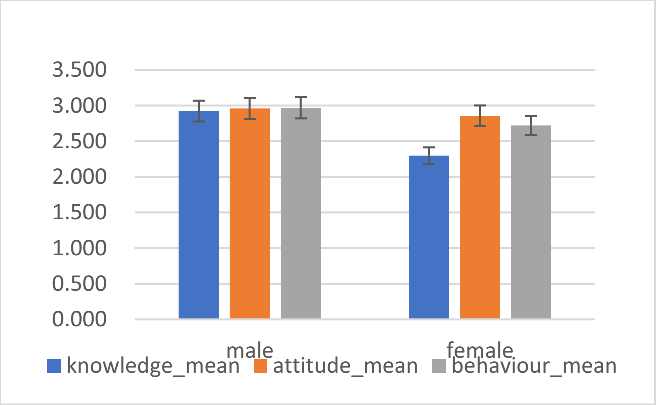

Figure 6. Average values and gender differences of knowledge, attitude, and behavior of different genders

Figure 6 depicts the average values and gender differences in knowledge, attitudes, and behaviors. In general, the mean values of boys' knowledge, attitude, and behavior were 2.922, 2.958, and 2.968, respectively. Girls' mean knowledge, attitude, and behavior scores were 2.298, 2.858, and 2.719, respectively. Less understanding of understanding, less agreement to basic agreement, and less agreement to basic agreement were associated with lower mean values of knowledge, attitude, and behavior, respectively.

Then, a multiple regression analysis was run, which suggests that there are significant differences among the tested variables of grade level, discipline, and gender. However, multivariate analysis reveals that only gender had significant differences (<.001).

On the one hand, for the knowledge, attitude, and behavior of the surveyed personal information network, the average value for a male is higher than that of a female. The difference in knowledge about the disclosure of personal information online was the largest. The conclusion is that undergraduates do not place a high value on the disclosure of personal information online, and male students place a higher value on the security of personal information online than female students.

5. Conclusions

This paper examines the knowledge, attitude, and behavior of Chinese undergraduates' online information disclosure from three aspects. Using quantitative analysis, this paper conducts a comprehensive investigation into the disclosure of Chinese undergraduates' online personal information through the questionnaire research method and uses SPSS 23.0 to conduct correlation analysis and regression analysis on the collected sample data.

The results of the questionnaire survey revealed that undergraduates' knowledge, attitude, and behavior regarding the disclosure of personal information online during the epidemic were not optimistic, with the majority scoring far below the satisfactory score of 4. Schools need to increase courses on personal information protection. Although there is a certain awareness of information security, the overall level of attention is low. Essentially, it was in the stage of "less understanding to understanding, less agreement to basic agreement, and less agreement to basic agreement." Furthermore, gender, grade, and other major factors influence undergraduates' attention to this issue. We investigated the differences in undergraduates' knowledge, attitudes, and behaviors regarding the disclosure of personal information online by grade, major, and gender.

According to the findings, senior students were more concerned about the disclosure of personal information online than junior students (freshmen). Students majoring in science are more concerned than students majoring in other fields about the disclosure of online personal information. Engineering students are less concerned about the issue. Although there are only 10 engineering students in this survey, this conclusion verifies a social survey in 2017. According to a survey conducted by the organizing committee of the 2017 China Media Leaders Conference and the Social Survey Center of Shanghai Jiao Tong University, QQ is the most popular social media platform used by undergraduates, followed by WeChat and Weibo. Engineering students are the most likely to use QQ media. Because engineering students rely too heavily on social networking platforms and have too much faith in information technology, they fail to consider the issue of online personal information disclosure. There is a significant gender difference in the disclosure of personal information on the Internet, with male students paying more attention to the safety of personal information online than female students. Students know about general security threats and protection procedures. However, they did not take sufficient measures to protect their devices or information and did not follow good information security practices.

This finding is consistent with previous research. According to Weinberger et al. [26] women's relatively high level of online privacy self-efficacy (which may be based on their lower level of technological threat awareness) is not matched by their relatively low level of technological online privacy literacy. As a result, they are less capable than men of safeguarding their identity and personal information. On the other hand, men are more aware of technological threats than they are of their online privacy self-efficacy, which, when combined with their relatively high online privacy literacy, enables them to better protect their identity and personal data.

There are few provisions in Chinese law that specifically protect students' personal information, which is one reason for the frequent incidents of students' personal information leakage. Schools also have shortcomings in protecting students' personal information, which include: a lack of awareness of personal information protection, a lack of corresponding protection mechanisms, a low level of network security technology, and insufficient education for students. In light of this issue, the author believes that education and publicity should be prioritized. Schools should offer relevant courses, lectures, forums, and other events to publicize and explain personal information protection issues. Students can spontaneously form relevant associations, create relevant public homepages on Weibo, WeChat, and other social networking sites, and use the network platform to make undergraduates more conveniently and frequently access knowledge about personal information protection, thereby improving their cognition and understanding of the issue. Undergraduates should also focus on increasing their awareness of personal information protection and protecting their rights and interests in personal information. They should, for example, refuse to provide personal information to an information collection organization they do not trust. Avoid using your own real data in general business processing. If you must use real information, you should carefully read the terms of personal information protection and write down the terms of service. Providers should be held accountable for their own violations of the provisions and the method of obtaining compensation. When you discover that your personal information has been compromised, you should immediately contact the appropriate institutions to stop the infringement and negotiate a resolution. Simultaneously, through administrative supervision procedures, you should request that the special regulatory agencies implement the necessary administrative supervision of the infringement agencies and infringements. When administrative actions are ineffective, they should seek legal recourse.

Among them, Article 66 of the People's Republic of China's Personal Information Protection Law specifies administrative liability rules for improper handling of personal information. In conjunction with other provisions, the entire process of handling personal information, such as collection, storage, processing, sharing, transfer, disclosure, and destruction, shall be included in the scope of the regulation. The authority to punish departments responsible for personal data protection in various circumstances has been clarified. Illegal acts are classified into two types: general acts and serious acts. For serious illegal enterprises, the maximum fine limit is less than 50 million renminbi, or less than 5% of the previous year's turnover. While regulating illegal enterprises, relevant responsible personnel are also punished, and senior management of enterprises may be barred from working for an extended period of time. In order to regulate and govern the security of personal information collected from apps and protect consumers' legitimate rights and interests, the China Consumers Association proposed the following in 2018: First, expedite the Personal Information Protection Law legislative process. Second, research the scope and means of putting the real-name system in place. Third, we will increase the level of supervision and inspection. Fourth, we will step up the crackdown even more. Fifth, increase consumer awareness.

6. Limitations and future directions

This paper investigates undergraduates' personal information security literacy in three dimensions: knowledge, attitude, and behavior (KAB). Based on Weinberger et al.'s [26] questionnaire, the study constructed a modified questionnaire regarding undergraduates' knowledge, attitudes, and behaviors toward personal information security. Some limitations need to be addressed in future research: first, a limited number of participants; this study only involved three universities in the East and West regions of China regarding 156 undergraduates' online information disclosure. In future research, more participants from different regions and levels of universities in China could take part in the investigation, which could expand the display and generalization of data. Second, research on other factors that influence undergraduates' knowledge, attitudes, and behavior toward personal information security could be investigated to further research on personal data and Information Security in higher education. Finally, although the survey object of this study is college students, future research can be extended to junior high school students, graduate students, teachers, and so on.

References

[1] Hong WCH, Chi C, Liu J, Zhang YF, Lei VN-L, and Xu XS, "The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates," Education and Information Technologies, Jun. 2022, doi: https://doi.org/10.1007/s10639-022-11121-5.

[2] Vidakis N, Barianos AK, Trampas AM, Papadakis Kalogiannakis, SM and Vassilakis K, "In-Game Raw Data Collection and Visualization in the Context of the 'ThimelEdu' Educational game. In: International Conference on Computer Supported Education," in CCIS Series Book, Heraklion Crete-Greece, May 2019, pp. 629–646.

[3] Eifert G and Craill L, "The Relationship between affect, behaviour, and cognition in behavioural and cognitive treatments of depression and phobic anxiety," Behaviour Change, vol. 6, no. 2, pp. 96–103, 1989, doi: https://doi.org/10.1017/S0813483900007634.

[4] MacKinnon NJ and Hoey J, "Operationalizing the relation between affect and cognition with the somatic transform,"EmotionReview,vol.13,no.3,pp.245–256,Jun.2021,doi: https://doi.org/10.1177/17540739211014946

[5] Schrader PG and Lawless KA, "The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments," Performance Improvement, vol. 43, no. 9, pp. 8–15, Sep. 2004, doi: https://doi.org/10.1002/pfi.4140430905.

[6] An Q, Hong WCH, Xu XS, Zhang YF, and Kolletar-Zhu K, "How Education Level Influences Internet Security Knowledge, Behaviour, and Attitude: A Comparison among Undergraduates, Postgraduates and Working Graduates," International Journal of Information Security, pp. 1–13, 2022,doi: https://doi.org/10.1007/s10207-022-00637-z

[7] Parsons K, McCormac A, Pattinson MR, Butavicius M, and Jerram C, "An analysis of information security vulnerabilities at three Australian government organisations," in EISMC, 2013, pp. 34–44.

[8] Parsons K, McCormac A, Butavicius M, Pattinson M, and Jerram C, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Computers & Security, vol. 42, no. 1, pp. 165–176, May 2014, doi: https://doi.org/10.1016/j.cose.2013.12.003.

[9] Parsons K, Young E, Butavicius M, McCormac A, Pattinson MR, and Jerram C, "The Influence of Organizational Information Security Culture on Information Security Decision Making," Journal of Cognitive Engineering and Decision Making, vol. 9, no. 2, pp. 117–129, May 2015, doi: https://doi.org/10.1177/1555343415575152.

[10] Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, and Zwaans T, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," Computers & Security, vol. 66, no. 1, pp. 40–51, May 2017, doi: https://doi.org/10.1016/j.cose.2017.01.004.

[11] McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, and Pattinson M, "Individual differences and information security awareness," Computers in Human Behavior, vol. 69, no. 1, pp. 151–156, Apr. 2017, doi: https://doi.org/10.1016/j.chb.2016.11.065.

[12] McCormac A, Calic D, Parsons K, Butavicius M, Pattinson M, and Lillie M, "The effect of resilience and job stress on information security awareness," Information & Computer Security, vol. 26, no. 3, pp. 277–289, Jul. 2018, doi: https://doi.org/10.1108/ics-03-2018-0032.

[13] Sawaya Y, Sharif M, Christin N, Kubota A, Nakarai A, and Yamada A, "Self-confidence trumps knowledge: A cross-cultural study of security behavior," in ACM SIGCHI Conference on human factors in computing systems, 2017, pp. 2202–2214.

[14] Wahyudiwan DDH, Suchyo YG, and Gandhi A, "Information security awareness level measurement for employee: Case study at Ministry of Research, Technology, and Higher Education," in 3rd International Conference on Science in Information Technology: Theory and Application of IT for Education, 2017, pp. 654–658.

[15] Cain AA, Edwards ME, and Still JD, "An exploratory study of cyber hygiene behaviors and knowledge," Journal of Information Security and Applications, vol. 42, no. 1, pp. 36–45, Oct. 2018, doi: https://doi.org/10.1016/j.jisa.2018.08.002.

[16] Wiley A, McCormac A, and Calic D, "More than the individual: Examining the relationship between culture and Information security awareness," Computers & Security, vol. 88, no. 1, p. 101640, Jan. 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.

[17] Riad A et al., "Estonian Dental Students' Oral Health-Related Knowledge, Attitudes and Behaviours (KAB): National Survey-Based Study," International Journal of Environmental Research and Public Health, vol. 19, no. 3, p. 1908, Feb. 2022, doi: https://doi.org/10.3390/IJERPH19031908.

[18] Ulven JB and Wangen G, "A systematic review of cybersecurity risks in higher education," Future Internet, vol. 13, no. 2, p. 39, Feb. 2021, doi: https://doi.org/10.3390/fi13020039.

[19] Chandarman R and Van Niekerk B, "Students' cybersecurity awareness at a private tertiary educational institution," The African Journal of Information and Communication, vol. 20, no. 1, pp. 133–155, Dec. 2017, doi: https://doi.org/10.23962/10539/23572.

[20] Lean-Ping O and Chien-Fatt C, "Information security awareness: An application of psychological factors - A study in Malaysia," in CCIT, International Conference on Computer, 2014, pp. 98–101.

[21] Kim EB, "Information security awareness status of business college: Undergraduate students," Information Security Journal: A Global Perspective, vol. 22, no. 4, pp. 171–179, Jul. 2013, doi: https://doi.org/10.1080/19393555.2013.828803.

[22] Berki E, Kandel CS, Zhao Y, and Chaudhary SA, "Comparative study of cyber-security knowledge in higher education institutes of five countries," in EDULEARN17 Conference 3rd-5th, 2017.

[23] Shaukat K, Alam TM, Hameed IA, Khan WA, Abbas N, and Luo S, "A Review on Security Challenges in Internet of Things (IoT)," IEEE Xplore, pp. 1–6, Sep. 2021,doi: https://doi.org/10.23919/ICAC50006.2021.9594183.

[24] Shaukat K, Luo S, Abbas N, Mahboob Alam T, Ehtesham Tahir M, and Hameed IA, "An Analysis of Blessed Friday Sale at a Retail Store Using Classification Models," in 2021 The 4th International Conference on Software Engineering and Information Management, Jan. 2021, pp. 193–198. doi: https://doi.org/10.1145/3451471.3451502.

[25] Nosko A, Wood E, and Molema S, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," Computers in Human Behavior, vol. 26, no. 3, pp. 406–418, 2010.

[26] Weinberger M, Zhitomirsky-Geffet M, and Bouhnik D, "Sex differences in attitudes towards online privacy and anonymity among Israeli students with different technical backgrounds," Information Research, vol. 22, no. 4, pp. 1–23, 2017.

[27] Bartlett MS, "Properties of sufficiency and statistical tests," in Proceedings of the Royal Society of London. Series A - Mathematical and Physical Sciences, May 1937, vol. A-160, no. 901, pp. 268–282. doi: https://royalsocietypublishing.org/doi/10.1098/rspa.1937.0109.

[28] Kaiser HF and Rice J, "Little Jiffy, Mark Iv," Educational and Psychological Measurement, vol. 34, no. 1, pp. 111–117, Apr. 1974, doi: https://doi.org/10.1177/001316447403400115.

[29] Field A, Discovering Statistics Using IBM SPSS Statistics, 5th ed. Los Angeles: Sage Publications, 2018.

[30] Cliff N, "The eigenvalues-greater-than-one rule and the reliability of components.," Psychological Bulletin, vol. 103, no. 2, pp. 276–279, 1988, doi: https://doi.org/10.1037/0033-2909.103.2.276.

[31] Anderson MJ and Walsh DCI, "PERMANOVA, ANOSIM, and the Mantel test in the face of heterogeneous dispersions: What null hypothesis are you testing?," Ecological Monographs, vol. 83, no. 4, pp. 557–574, Nov. 013, doi: https://doi.org/10.1890/12-2010.1.