International Journal of Information Security (2023) 22:305–317
https://doi.org/10.1007/s10207-022-00637-z

REGULAR CONTRIBUTION

How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates

Qin An[1] · Wilson Cheong Hin Hong[2] · XiaoShu Xu[3,4] · Yunfeng Zhang[5] · Kimberly Kolletar-Zhu[3]

Accepted: 11 November 2022 / Published online: 24 November 2022

Abstract
During the pandemic, the prevailing online learning has brought tremendous benefits to the education field. However, it has also become a target for cybercriminals. Cybersecurity awareness (CSA) or Internet security awareness in the education sector turns out to be critical to mitigating cybersecurity risks. However, previous research indicated that using education level alone to judge CSA level received inconsistent results. This study postulated Social Educational Level (SEL) as a moderator with an extended Knowledge-Attitude-Behaviour model, used students' year level as a proxy for the impact of education level, and used work exposure for the influence of social education level, to compare CSA among undergraduates, postgraduates and working graduates. The participants in the study were divided into six groups, namely year 1 university students, year 2-3university students, final-year students, postgraduate students, young working graduates, and experienced working graduates. The Human Aspects of Information Security Questionnaire was used to conduct a large-scale survey. The multivariate regression model analysis showed significant differences among the *knowledge, attitude* and *behaviour* dimensions across groups with different conditions of year-level and work exposure. However, it was found that SEL played a more significant role than an individual's education level. The study suggested that a greater endeavour be committed to educating the public at large together with individuals, institutes, corporate and governments to improve the national CSA level.

Keywords Cybersecurity awareness · CSA · Internet security awareness · ISA · Social educational level · KAB model · HAIS-Q · Online learning

1 Introduction

The coronavirus' global spread was causing ripples in all domains. The Internet has become a target for cybersecurity threats because it has become a place and platform for students to learn and employees to get to work. However, students and employees who did not major in information technology (IT) were forced to switch from offline to online in a short period of time with relatively less ISA, posing significant security risks. For example, since the spread of COVID-19, cyber-attacks have grown in sophistication and quantity. Since such rapid digital transformations in education, for example, online learning has become a new target for cybercriminals. The investigation of cybersecurity awareness and the impact of social educational level on Chinese netizens was beneficial.

Previous research mostly used behavioural models to assess ISA, such as the Theory of Planned Behaviour (TPB) [1, 2], Protection Motivation Theory (PMT) [3], and the Knowledge-Attitude-Behaviour (KAB) model [4]. Based on KAB, the HAIS-Q was a comprehensive scale with high internal consistency and external reliability that was used to investigate internet security knowledge, attitude, and behaviour [5]. Parsons et al. acknowledged that social influence should be considered when using the HAIS-Q [6]. Hence, an extended KAB model, proposed by Hong et al.,

✉ XiaoShu Xu
lisaxu@wzu.edu.cn

[1] International Business School, Chengdu Institute Sichuan International Studies University, Chengdu, China

[2] Centre for Teaching and Learning Enhancement, Macao Institute for Tourism Studies, Macau, Macao

[3] School of Foreign Studies, Wenzhou University, Wenzhou, China

[4] Stamford International University, Bangkok, Thailand

[5] Centre for Portuguese Studies, Macau Polytechnic University, Macau, Macao

was applied [7], which suggested that more social contact at work implied a decrease in SEL.

There were numerous studies on ISA; however, few of them were in the Chinese context, and even fewer focused on empirical research on cybersecurity risks in higher education [8], not to mention that the influence of education level on ISA might be contradictory in previous research. Some studies found that education level has a positive effect [9], while others found that it has no effect [10, 11]. This was due to the fact that in addition to the individual's internal factors (e.g. education level), external factors of social influence were rarely the focus of research. Social influence is known as the effect of social interactions and communications with others on one's beliefs and actions [12]. Family, friends and colleagues are the common sources of social influence. To this end, Hong et al. investigated the impact of the average education level of a society on one's ISA [7], which was referred to as *social education level* (SEL). SEL was found to be a better predictor of social influence on ISA than nationalities and gross domestic product (GDP), which refers to the total market values of goods and services produced by workers and capital within a country during a given period (usually 1 year).

To assess the positive effects of education level and the negative influence of SEL, we recruited respondents with various education levels, including undergraduates and postgraduate students, and took into account three levels of work exposure, ranging from no exposure to the work environment (non-final-year undergraduates) to new exposure (young working graduates) and long-term exposure (experienced working graduates). This study assumed that a higher year level of university students means a higher (personal) education level and that a lower SEL could be observed in increased social contact at work. Students'/graduates' educational level and SEL exposure were expected to mediate cybersecurity knowledge, attitude, and behaviour.

Given that relatively few large-scale ISA studies have been conducted in higher education and few attempts have been made to compare undergraduate students, postgraduate students, and working graduates, this study aimed to examine the influence of education level and SEL on students' and graduates' ISA, which may contribute in a theoretical and practical way by quantifying education influence and social impact on ISA.

2 Literature review

2.1 HAIS-Q and extended KAB model

A review of previous ISA studies revealed that some pre-existing, well-established behavioural models were used to investigate the issue of ISA. The Theory of Planned Behaviour (TPB) [2], which evolved from the Theory of Reasoned Action [13], the Protection Motivation Theory (PMT) [14], the Health Belief Model [15], the General Deterrence Theory [16], the Technology Acceptance Model (TAM) [17], and the Knowledge-Attitude-Behaviour (KAB) model [4], have all attracted the interest of many ISA scholars [18].

Take the Theory of Planned Behaviour, whose key points include intention (attitude, subjective norms) and perceived behavioural control [13], which have been applied to adolescents' acceptance of friendship requests sent by online strangers on social networking sites [19]. This theory has also been used to assess students' levels of Cybersecurity awareness (CSA) at a private tertiary education institution [20], as well as to investigate Information Systems Security Policy (ISSP) compliance using two relevant theories, TPB and PMT [21].

The Theory of Planned Behaviour was composed of two items: perceived vulnerability and perceived severity [3], which have been found to be very useful in predicting behaviours related to an individual's computer security behaviours both at home and in organisations [22]; an individual's internet security perceptions and behaviours in a poly context [23] or an individual's continued engagement in protective security [24] and Information Systems Security Policy compliance [25, 26].

These models, however, have been criticised for failing to capture the complexities and specific phenomena of cybersecurity [27]. The KAB, a dynamic and sometimes reciprocal model, on the other hand, was originally used in the health and environmental psychology area [28] as well as in the criminology and education fields [29] and has also been applied to the ISA context [30, 31]. KAB has received much attention among scholars and has been applied to various fields of research because previous research found that knowledge alone was not sufficient to cause behavioural changes [32].

Simultaneously, based on the KAB model, the conceptualised Human Aspects of Information Security Questionnaire (HAIS-Q) has been developed [33]. HAIS-Q research has shown that age, gender, resilience, job stress, education level, and some other personal characteristics can predict ISA to some extent [34]. In particular, education in information and communication technology (ICT) could positively benefit one's IS behaviour [35, 36]. In addition, it was also found that ISA would be higher as age increased, or among the female group, which was not consistent with findings from previous research results that no ISA difference could be seen between men and women [37], if individuals possess higher education [9], if one is more conscientious and agreeable [38]; and if one owned a propensity to take fewer risks [5]. Furthermore, if one was more resilient but underwent less job stress, they would have a higher ISA [34]. Moreover, an inverse relationship between Internet addiction, cyber-loafing tendencies, and ISA has been discovered [39]. A significant positive relationship between organizational culture, security culture, and ISA [9] has also been tested from the social influence or work environment perspective. Furthermore, the bank's employees have higher ISA than the general workforce participants in all focus areas and overall [37].

Although Parson et al. [6] acknowledged in their initial HAIS-Q proposal that other social factors should be considered when using the KAB model or HAIS-Q in future research, there was no easy way to quantify social influence. To adapt the framework, Hong et al. [7] proposed an extended model of KAB (see Fig. 1), which suggested that more social contact at work implied a decrease in SEL. SEL was about how the general education level of an internet user's immediate circle, such as family, friends, and colleagues, influenced the user's cybersecurity behaviours [7].

@@@An extended KAB model, *Source*: Hong, W. C. H., et al. [7].

2.2 ISA influencing factors

When attempting to understand what shapes human behaviour, looking at an individual in isolation could be problematic. It has been found that individuals of different nationality backgrounds but similar levels of ISA exhibited highly varied cybersecurity behaviours and safety responses [31]. Past studies have found personal education level [35], gender [40], age [41], stress level [34] self-efficacy [42], and cultural beliefs [9] to be salient predictors of cybersecurity awareness and behaviours. An individual's knowledge of information and communication technology (ICT), especially, has been widely suggested to positively correlate with ISA and safe behaviours [35, 43, 44]. However, no internet users live or work in isolation from other internet users, but they are under the constant influence of one another to adjust and readjust thoughts and actions. Hence, personal factors must be viewed in conjunction with social factors. Existing studies have found that social influence is a key motivator to safe or unsafe cybersecurity behaviours [12, 19, 45–47]. Some found that the online experience of friends and family impacted our own beliefs and behaviours [46, 48], and that imitation of others is a primary reason for safe practices [45]. Similarly, the working environment where one is immersed has a tremendous impact on individuals' ISA and practice [7, 47]. Hong et al. [7] found that workplace influence in China, especially from colleagues of lower education levels, severely deteriorated university graduates' attitudes towards safe internet practices. The deterioration emerged as early as in the (full-time) internship period, resulting in poor cybersecurity behaviours. Worse still, respondents' cybersecurity knowledge appeared to be reshaped by the working environment. This echoes the findings of Elkhannoubi & Belaissaoui [12], who contended that social influence plays a more significant role in developing countries, as the individuals high in ISA are only the minority of the society. SEL as a relatively objective factor that is quantifiable by published indices such as the Education Index [49] and literacy rate [50] can serve to measure how much an individual is under social influence.

2.3 The influences of education level and SEL on ISA in China

Previous research found that ISA scores increased with age [34, 37, 41] and that individuals with a higher education had higher ISA scores [9, 51]. However, some ISA education research discovered that final-year students, who were more educated and older, consistently scored the lowest in ISA when compared to other year-levels of students. To name a few, Li et al. [10] discovered that the senior group had significantly less awareness than the junior groups. Huang et al. [11] discovered that senior students were the most vulnerable to safety incidents. These findings in the Chinese context differed significantly from previous international research, in which an individual's education level was known to positively correlate with ISA [51].

At the same time, the impact of a country's GDP and development level on its population's ISA was volatile. As a result, SEL could be used as a factor to quantify external influence, including social influence and national context. SEL is concerned with how the general education level of an internet user's immediate circle, such as family, friends, and

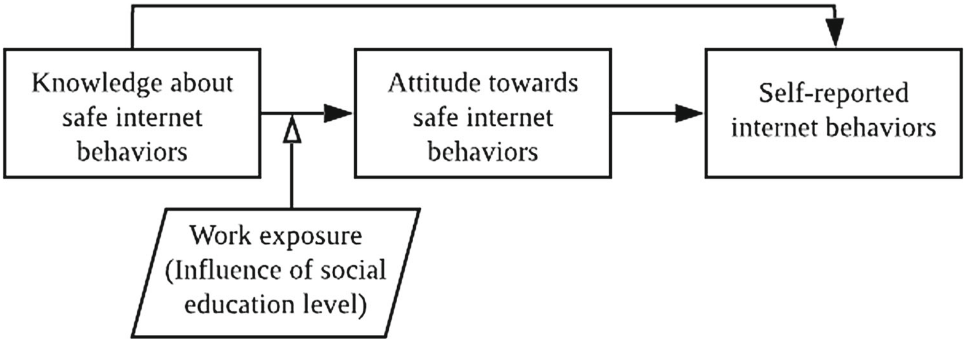
Knowledge about safe internet behaviors
Attitude towards safe internet behaviors
Self-reported internet behaviors
Work exposure (Influence of social education level)

Fig. 1 An extended KAB model, *Source*: Hong, W. C. H., et al. [7]. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Education and Information Technologies

colleagues, influences the user's cybersecurity behaviours [7].

Previous research revealed some additional limitations. For example, to determine whether increased exposure to society affects ISA or whether academic growth influences it, it was necessary to compare the ISA of non-final-year students, final-year students, postgraduate students, as well as interns (final-year students), young working graduates, and experienced working graduates. A thorough literature review, however, revealed that there had been little comparative ISA research among these three groups, namely, different year levels of university students, postgraduate students, and working graduates. Furthermore, the majority of previous research on ISA in higher education had relatively small sample sizes. A sample size of 333 to 400 for each group of respondents has been recommended for better generalizability [52]. Despite the abundance of ISA research, a recent systematic review of ISA in higher education revealed that the majority of existing ISA surveys did not meet such criteria [8].

According to the findings of the preceding study, learners' attitudes towards cybersecurity would be influenced by their internal education level and external environment, which would eventually change their internet behaviours. Furthermore, education level had a positive effect and work exposure time had a negative effect on a person's ISA [7, 9].

Hence, the following hypotheses were proposed:

H1 University students of different years of study, postgraduate students, and working graduates will display differing cybersecurity knowledge.

H1a Postgraduate students will score significantly higher in knowledge than final-year students.

H1b Postgraduate students will score significantly higher in knowledge than working graduates.

H1c Postgraduate students will score significantly higher in knowledge than non-final-year students.

H2 University students of different years of study, postgraduate students and working graduates will display differing cybersecurity attitudes.

H2a Postgraduate students will score significantly higher in attitudes than final-year students.

H2b Postgraduate students will score significantly higher in attitudes than working graduates.

H2c Postgraduate students will score significantly higher in attitudes than non-final-year students.

H3 University students of different years of study, postgraduate students, and working graduates will display differing cybersecurity behaviours.

H2a Postgraduate students will score significantly higher in behaviours than final-year students.

H2b Postgraduate students will score significantly higher in behaviours than working graduates.

H2c Postgraduate students will score significantly higher in behaviours than non-final-year students.

3 Methodology

3.1 Sample and sampling method

Snowball and criterion sampling methods were used to recruit participants. Students were invited to complete the questionnaire via email or personal contact, and then they contacted their peers to participate in the survey. Furthermore, as a criterion for participation, all students were first screened as having received cybersecurity training during their higher education and as having completed a mandatory full-time internship for half a year or a full year in their final year of study, allowing comparisons to be made between different levels of work exposure (i.e. prior, short-term and long-term work exposure).

In total, 1882 valid responses were obtained from more than ten higher education institutions and 110 Chinese businesses. There were 480 year 1 students, 372 year 2–3 students, 325 final-year students, 230 postgraduate students (age range = 18–25), and 343 young working graduates, 132 experienced working graduates (age range = 18–46); 938 majored in liberal arts and social sciences, 499 natural sciences, and 445 technology and engineering; 691 males and 1191 females. Table 1 contains descriptive information about the participants.

The participants were divided into two groups based on our hypothesis, which stated that work exposure time had a negative effect on a person's ISA and education level had a positive effect. Internships, young graduates, and experienced graduates were thus regarded as the first short-term and long-term work exposure to a work environment. Furthermore, non-final-year students, final-year students, and postgraduates were viewed as three distinct educational levels.

3.2 Instrument design

Hong et al.'s [7] survey questions were adopted. They translated, verified, and adjusted the questionnaire based on the Questionnaire on Human Aspects of Information Security (HAIS-Q). It was then distributed online via one of the largest local survey platforms, Wenjuanxing, also known as Sojump

Table 1 A table of participants' demographic information

Education/working status			
Variable	Categories	Number	Percentage
Grades	Year 1 students	480	25.5%
	Year 2-3students	372	19.8%
	Final-year students	325	17.3%
	Postgraduate students	230	12.2%
	Young working graduates	343	18.2%
	Experienced working graduates	132	7.0%
Age	18–25	1550	82.4%
	26–35	200	10.6%
	36–45	90	4.9%
	46 or above	42	2.2%
Discipline	Liberal arts and social sciences	938	49.8%
	Natural sciences	499	26.5%
	Technology and engineering	445	23.6%
Gender	Male	691	36.7%
	Female	1191	63.3%

[53]. Meanwhile, each question was scored using a five-point Likert scale (5 = strongly agree, 1 = strongly disagree).

The study proposal submission form was submitted to and approved by the academic committee of the first author's university in December 2021. All survey responses were kept anonymous, and their participation in this study was entirely voluntary. When participants clicked on the survey, they would be prompted to a page containing brief information about the survey and their rights to privacy and anonymity. They then provided their consent by clicking "agree to continue".

3.3 Data analyses

Data results ($N = 1882$) were analysed by using IBM Statistic Package for Social Science (SPSS). Cronbach's alpha was used to check internal reliability. Normality testing, correlations and multivariate regressions were adopted to analyse the variables.

4 Findings

4.1 Internal reliability

Each of the three dimensions was checked for internal reliability. The knowledge dimension reported a Cronbach's alpha of 0.84, while attitude and behaviour had an alpha value of 0.91 and 0.77, respectively, which indicated good to excellent levels of internal consistency in the subscales.

4.2 Data normality

The moderating effects of education level and work exposure on Internet security knowledge, attitude, and behaviour variables were investigated in this study.

The education level was divided into four levels: freshmen (low education level), sophomores and juniors (medium education level), seniors (higher-medium education level), and postgraduates (advanced education level). Meanwhile, work exposure was classified as follows: non-graduation years (low exposure), graduation years (medium exposure), and working graduates (high exposure).

The ISA variables were then examined for normality. Direct hypothesis testing was not recommended because both Kolmogorov–Smirnov and Shapiro–Wilk were designed for smaller sample sizes ($n \leq 50$) [54]. Skewness and kurtosis values, on the other hand, were determined manually. A larger sample with skewness between -2 and $+ 2$ and kurtosis between -7 and 7 were considered normally distributed. Mean knowledge (skewness $= -0.270$, kurtosis $= -0.393$), mean attitude (skewness $= -0.263$, kurtosis $= -0.783$), and mean behaviour (skewness $= -0.342$, kurtosis $= 0.351$) were all within the normal range.

4.3 Demographic information

According to the range provided by the questionnaire, grades were segmented into six sequential levels (year 1, year 2–3, postgraduate students, young working graduates, experienced working graduates, and final year). Ages (18–25, 26–35, 36–45, 46), disciplines (liberal arts and social sciences, natural sciences, technology and engineering), and genders (male, female) were also used as classification variables.

4.4 Multicollinearity

Next, a multicollinearity test was performed on the data. Correlation tests were conducted for variables such as knowledge, attitude, behaviour, grade, age, discipline, and gender (see Table 2 for correlation results). The mean knowledge, attitude and behaviour were discovered to be significantly positive and highly correlated ($p < 0.001$). There was a significant positive correlation between grade and age ($p < 0.001$), and they showed significant negative correlations with mean knowledge, attitude, and behaviour ($p < 0.001$). Therefore, grade and age as independent variables were considered covariables. To test the effect of grade, age has to be controlled.

Table 2 Correlation analysis for variables

	Mean knowledge	Mean behaviour	Mean attitude	Grades	Age	Discipline	Gender
Mean knowledge	1.000						
Mean behaviour	.780**	1.000					
Mean attitude	.765**	.823**	1.000				
Grades	−.500**	−.415**	−.443**	1.000			
Age	−.437**	−.352**	−.422**	.636**	1.000		
Discipline	−.135**	−.138**	−.152**	.102**	.404**	1.000	
Gender	.097**	.154**	.160**	−.028	−.074**	−.333**	1.000

**Correlation was significant at the .01 level (2-tailed)

As a result, the regression analysis hypothesis was completely satisfied. Therefore, the data and residuals were normally distributed, with no heteroscedasticity or correlation between regression residuals. The potential collinearity between grade and age was identified, but it could be accommodated in the proposed regression model by controlling for the latter.

4.5 Data analysis

A multivariate regression model was used to examine the effects of different grade levels and levels of work exposure on mean score of knowledge, attitude, and behaviour, with gender, age, and discipline controlled, as detailed below according to the corresponding assumptions. For simplicity, the changes are illustrated in Figs. 2, 3, and 4).

H1 University students of different years of study, postgraduate students and working graduates will display differing cybersecurity knowledge.

H1 was verified. There were significant differences between the knowledge of postgraduate students (M = 3.53, SD = 0.47) and non-final-year university students including year 1 students (M = 3.72, SD = 0.78) and year 2-3students (M = 3.64, SD = 0.77). Moreover, the knowledge of postgraduate students was found to be different from final-year ones (M = 3.57, SD = 0.77). At the same time, the knowledge of postgraduate students was also found to be visibly different from working graduates that contained young working graduates (M = 2.63, SD = 0.47) and experienced working graduates (M = 2.65, SD = 0.47). For simplicity, the differences in mean values of the three dimensions are illustrated in Table 2.

H2a Postgraduate students will score significantly higher in attitudes than final-year students.

H2a was rejected. The attitude of postgraduate students (M = 3.73, SD = 0.69) was found to be significantly lower than final-year students (M = 3.80, SD = 1.00).

H2b Postgraduate students will score significantly higher in attitudes than working graduates.

H2b was verified. The attitude of postgraduate students was found to be significantly higher than young working graduates (M = 2.73, SD = 0.32) and experienced working graduates (M = 2.73, SD = 0.36).

H2c Postgraduate students will score significantly higher in attitudes than non-final-year students.

H2c was rejected. The attitude of postgraduate students was found to be significantly lower than year 1 students (M = 3.88, SD = 1.00), and year 2–3students (M = 3.77, SD = 1.02).

H3a Postgraduate students will score significantly higher in behaviours than final-year students.

H3a was verified. The behaviour of postgraduate students (M = 3.54, SD = 0.47) was found to be significantly higher than final-year ones (M = 3.39, SD = 0.82).

H3b Postgraduate students will score significantly higher in behaviours than working graduates.

H3b was verified. The behaviour of postgraduate students was found to be significantly higher than working graduates containing young (M = 2.83, SD = 0.28) and experienced (M = 2.88, SD = 0.28).

H3c Postgraduate students will score significantly higher in behaviours than non-final-year students.

H3c was partially verified. The behaviour of postgraduate students was found to be significantly lower than year 1 students (M = 3.62, SD = 0.82), but significantly higher than that of year 2–3students (M = 3.50, SD = 0.85).

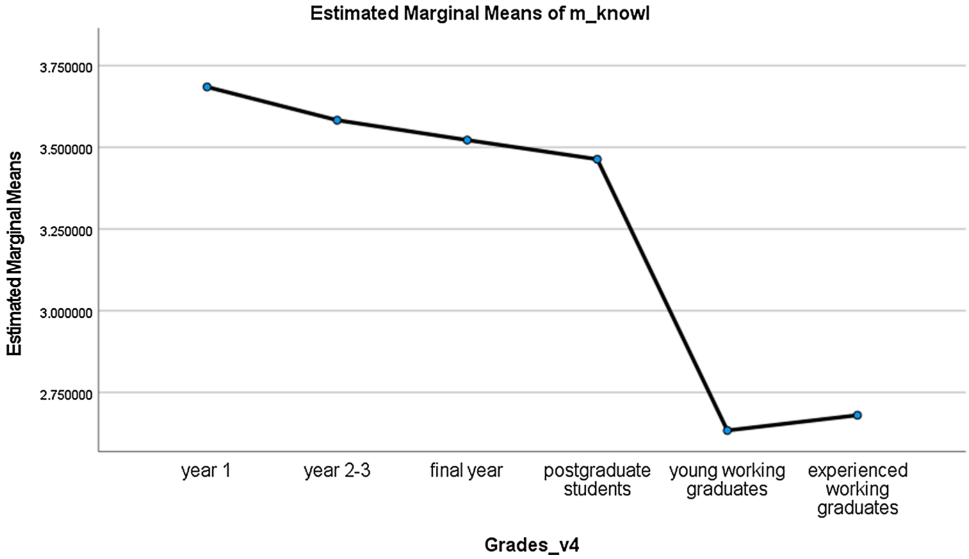

Fig. 2 Means of cybersecurity knowledge across groups

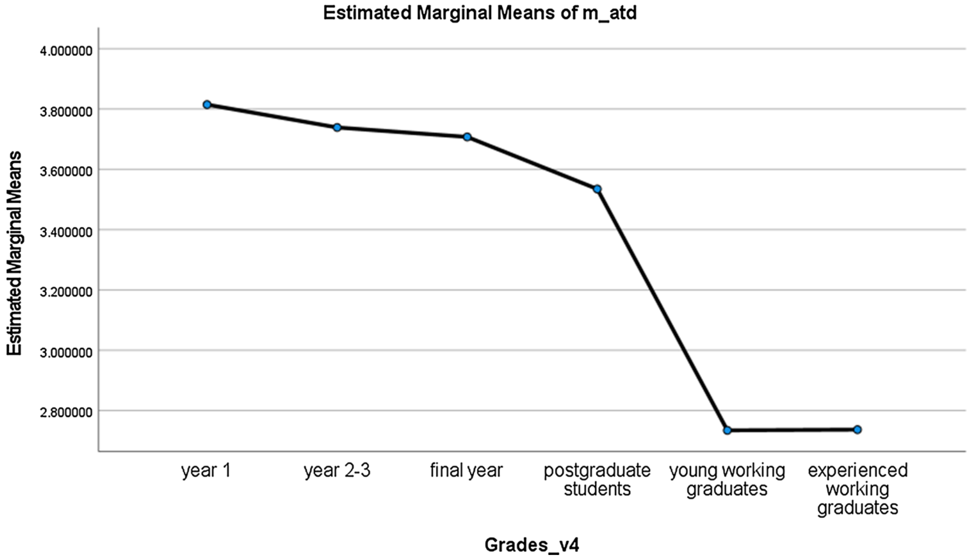

Fig. 3 Means of cybersecurity attitude across groups

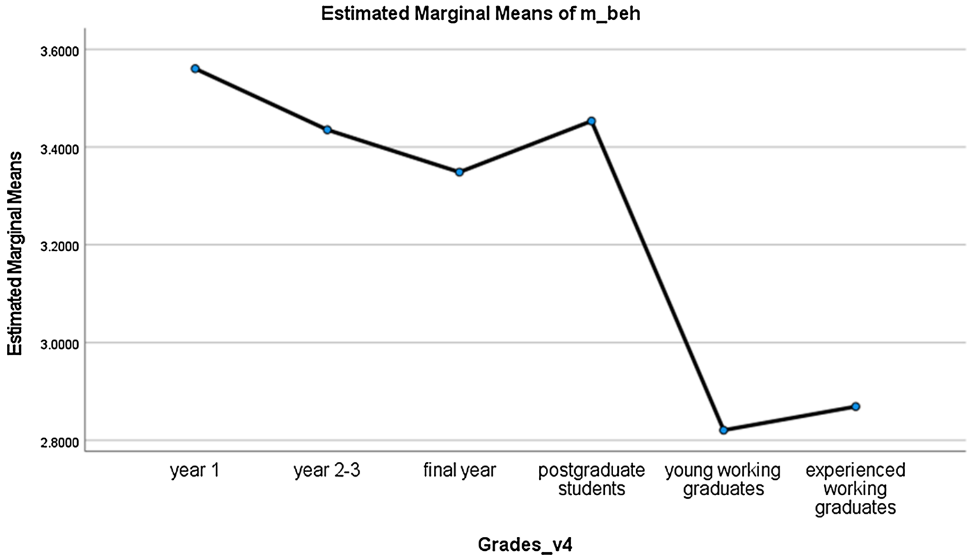

Fig. 4 Means of cybersecurity behaviour across groups

In terms of knowledge, as students advanced to higher levels, their cybersecurity knowledge deteriorated. Their cybersecurity knowledge also dropped significantly at work. As graduates gained more work experience, their knowledge seemed to rebound a little. In terms of behaviour, postgraduate students performed similarly to year 2–3 students but not as well as year-1 students. Working graduates performed similarly poorly, but slight improvements could be seen after gaining more work experience. In terms of attitude, as students advanced to higher levels as postgraduate students, or went to work, their cybersecurity attitudes deteriorated. Even inexperienced employees showed no improvement.

4.6 Gender difference

Many studies have hypothesised that personal factors such as gender influence behavioural decisions [37, 41]. The analysis revealed that the hypothesis was statistically supported. Females' knowledge ($M = 3.44$, SD $= 0.78$) was found to be significantly higher than males' ($M = 3.27$, SD $= 0.78$), as was their attitude ($M = 3.66$, SD $= 0.94$ vs $M = 3.32$, SD $= 0.99$). The same was true for female and male behaviour ($M = 3.44$, SD $= 0.70$ vs $M = 3.19$, SD $= 0.81$). As a result, females had higher ISA scores than males in all three dimensions.

4.7 Significant predictors

A multivariate regression model was also run to see if age, discipline, grade, or gender were significant predictors of ISA. Previous research suggested that age was a significant predictor of ISA (e.g. [55]), but a recent study found that age was not a significant predictor [7]. Pillai's Trace was used to evaluate the sum of the matrix's eigenvalues, and Roy's Largest Root statistic, to test the maximum value in a matrix's eigenvalues, have been used. And the greater the magnitude of these values, the greater the contribution of this effect to the model. Wilk's Lambda was also used, with a value between 0 and 1. In Wilk's Lambda, the smaller the value, the greater the contribution. As a result of the above analysis, the results showed that overall, grade and gender were significant predictors of ISA, whereas age and discipline were not.

4.8 Significant correlations

In addition, tests of between-subjects effects were examined further, with mean knowledge, mean attitude, and mean behaviour as the dependent variables.

Significant correlations were discovered between grades, discipline, and gender.

According to the Sum of Squares, the grade had the greatest impact on knowledge (112.96), attitude (123.35), and behaviour (70.33), in that order. (See Table 3.)

4.9 Discipline differences

To the best of the authors' knowledge, ISA research in higher education rarely focuses on discipline. Thus, Fisher's LSD was used in this study for inter-group multiple comparisons to compare disciplines. The analysis found no difference between the disciplines of natural sciences and technology and engineering, but there was a difference between the above two disciplines and the discipline of liberal arts and social sciences. That could be because, in Chinese universities, the disciplines of natural sciences, technology, and engineering had at least two advanced information and communication technology (ICT) courses and one professional computer application course, whereas students majoring in liberal arts and social sciences only took the common course on basic ICT skills in the first year, according to the Computer Basic Curriculum System and the actual investigation [55, 56].

5 Summary of results

The current survey was one of the few initial studies that used students' year-level as a proxy for the impact of education level as an internal aspect, and work exposure for the influence of social education level as an external factor, both of which we consider being quantifiable sources of impact. We compared the impact of (personal) education and social education levels on year-1 university students, year-2 and year-3 university students, final-year students, postgraduate students, young working graduates and experienced working graduates. The context of this study was in China, where university graduates were more likely to work with colleagues who received less education than themselves. Differences have been found among university students, postgraduate students, and working graduates, which could suggest changes in online security knowledge, attitudes, and behaviour among individuals.

Then, there was little difference in overall ISA between graduate students and college students, implying that EL had little impact on these students. In the current context of China, the most important reason was probably that there were few computer-related courses at the higher levels of undergraduate and postgraduate study in most Chinese universities. The findings showed that above undergraduate education, the education level had minimal positive effect on postgraduates' cybersecurity behaviours, but with a negative impact on postgraduates' Internet security knowledge and attitude. To be more specific, only a few universities provided optional computer-related courses or computer-common courses to postgraduate students [56, 57], implying that the majority of them did not receive better ICT education at the postgraduate level, despite taking the basic ICT course at their first year as undergraduate students [55, 56]. As a result,

Table 3 Tests of between-subjects effects

Source	Dependent variable	Type III sum of squares	Mean square	F	Sig	Partial eta squared
Grades (year-levels)	Mean_knowledge	122.955	30.739	67.265	< .001	.127
	Mean_attitude	123.345	30.836	44.605	< .001	.088
	Mean_behaviour	70.330	17.582	38.507	< .001	.077
Age	Mean_knowledge	.195	.097	.213	.808	.000
	Mean_attitude	1.108	.554	.802	.449	.001
	Mean_behaviour	.175	.087	.191	.826	.000
Discipline	Mean_knowledge	4.237	2.119	4.636	.010	.005
	Mean_attitude	2.856	1.428	2.065	.127	.002
	Mean_behaviour	2.948	1.474	3.229	.040	.003
Gender	Mean_knowledge	.038	.038	.083	.773	.000
	Mean_attitude	5.386	5.386	7.791	.005	.004
	Mean_behaviour	4.352	4.352	9.531	.002	.005

higher levels of undergraduate and postgraduate students' information and communication technology (ICT) knowledge could not be enriched, and thus could not positively influence their attitudes. After all, ICT education could be beneficial to one's ISA [35, 36]. This also explains the differences between students majoring in disciplines of natural sciences/technology/engineering and liberal arts/social sciences, as liberal arts/social sciences students may have only taken one basic ICT course. Furthermore, females had higher ISA scores than males in all three dimensions, while age was not a significant predictor of ISA.

6 Discussion and implications

6.1 Discussion

To our surprise, there was little difference in overall ISA between graduate students and college students, implying that EL had little impact on these students. What we did not expect was that education level had no positive effect on postgraduates' cybersecurity behaviours, while it had a negative impact on postgraduates' Internet security knowledge and attitude. This result differed from previous international findings that individuals with higher education had higher ISA scores [9, 51] but was consistent with previous findings in the Chinese context [7, 10, 11]. Among past studies that investigated both undergraduate and postgraduate students [58–60], very few compared them as separate groups. However, our results echo findings that undergraduate and postgraduate students had similarly inadequate ISA [60] or that the postgraduates had slightly weaker awareness than the undergraduate group [58]. ICT education is known to benefit to one's ISA [35, 36], but computer-related courses are typically not provided at higher undergraduate levels and postgraduate study in most Chinese universities. Many tertiary-level students in China were only required to take a basic ICT course in year-1 [55, 56], the lack of ICT education in subsequent years and postgraduate programmes might have led to ISA deterioration. In fact, similarly inadequate training/education was found in non-Chinese institutes [60]. Although this is one of the few studies that investigated comprehensive ISA changes among university students and graduates, other studies have indicated that senior-year students were more prone to risky online behaviours [61] and weak preventative awareness of cyber-threats [62]. Increasing involvement in social activities such as interest groups and part-time jobs is potentially a major contributor to such peer-level changes, as argued by researchers [7, 62]. This social influence reaches a high point upon complete detachment from tertiary education, while others who choose to continue/return to their studies at postgraduate level may receive a less negative impact.

We also argue one major reason for existing ISA studies to yield contradicting results was that they only examined individual factors [34, 35, 40, 41], which should be considered alongside the influence of social forces [7, 12, 47] to paint a fuller picture. This study found that when all the factors (i.e. grades, age, discipline, and gender) were analysed together, age did not show significant correlations with any ISA dimensions. Our results indicated that year-levels/work exposure and age were highly correlated, which makes sense as the higher one's education level and work experience are, the older they typically are. In past studies, age alone seemed to predict ISA [34, 37, 41]. However, it is evident in this study that age is not the cause for changes in ISA, but rather, a co-founder or covariate of other directly related factors such as education levels. In particular, social influence is found to be more important than an individual's level of education. Although this study has provided further evidence of social influence [19, 21], much has yet to be done to examine how the external environment impacts one's ISA as studies beyond individual factors are relatively few [12, 45, 47]. This also explains why the results of previous studies that used GDP and country development to predict citizens' ISA were inconsistent [37, 57, 63], suggesting that the educational level of the whole country (SEL) plays a crucial role. Previous studies have argued that social influence may be more pronounced in developing countries than developed ones [12, 64, 65]. Apart from weaker cybersecurity infrastructure [65], the general lack of basic knowledge in ICT [64], added to the rampant access to pirate software [66], shaped people's risk-prone attitudes in developing countries. Despite the high GDP, China is a developing country, where people's education level and ICT knowledge vary largely [7, 49]. University students, graduates and postgraduates are undoubtedly under constant but varying levels of negative social influence, which, if strong enough, can result in a critical downturn of ISA.

Further, as expected, females had better attitudes and behaviour than males, which was consistent with previous findings [37, 40]. Another expected outcome was that there was a significant difference between liberal arts, social sciences and natural sciences, technology, and engineering which was rarely focused on in the previous studies. The reason was that different levels and amounts of ICT curriculum were designed among these disciplines, which also proved the previous finding that ICT education could be beneficial to one's ISA [35, 36].

6.2 Implications

An important methodological implication for the future was that, with readily available figures of national education level, the year-level (education level) and length of time at work (SEL) were quantifiable measures, similar to existing cross-national findings (e.g. [23, 58, 59]). As a result, it addresses the issue that GDP and nationality are inconsistent predictors of national ISA.

Because of the influence of SEL, the fact that the average difference in ISA between working graduates and the other two student groups was significant provided insight into the importance of conducting a survey on working postgraduates and working PhDs, given that the SEL of the working environment for working postgraduates may be better. Nonetheless, the behaviour of postgraduate students was significantly higher than that of final-year students, indicating that the negative effects of society (SEL) were offset by the positive effects of the university environment (education level). With this in mind, an ISA survey of PhD students was undoubtedly a worthwhile topic worthy of further investigation.

This study recommends that a greater effort is needed to be made to educate the general public, particularly while they were still in school. With 95.41% of the population in China having received an education, cybersecurity awareness training at the school level was critical to improving the national ISA and SEL. What was more important was the higher education group's knowledge of ICT. The ICT knowledge that remained only in the freshmen stage could no longer meet the current era of extensive and in-depth popularization of the Internet, and thus the ICT knowledge needed to be provided according to the needs of students at various stages, including the postgraduate stage. Simultaneously, because teachers' ICT knowledge can influence the younger generation, the quickest and most effective strategy was to train the teacher population on ICT knowledge [67].

Meanwhile, companies should consider providing more training for employees with lower education, who make up 48.8% of the workforce in China, as well as maintaining young graduates' better ISAs, to ensure that all employees have a broad range of ICT knowledge. Simultaneously, it was critical for the government to take actions to promote safe Internet behaviours among citizens, such as broadcasting knowledge and the importance of ISA via social media, online advertising, television, government-led talks, establishing network security policies, and collaborating with businesses to initiate social transformation.

7 Limitations and conclusions

7.1 Limitations

The study collected a larger sample in the hope that a larger sample would increase generalizability and thus mitigate the problem of non-random sampling. However, due to the varying difficulty of data collection in each group, the number of respondents in each of the six groups varied.

We attempted to understand changes in ISA and behaviour from year-1 to postgraduate studies to graduated employees. However, the change is not observed longitudinally, but it was obtained through a cross-sectional survey. Therefore, factors such as generation difference cannot be duly represented in the data. Readers are forewarned of this potential confounder.

Future research could also conduct longitudinal and cross-country studies to investigate the influence of education level and SEL on ISA using this extended model to further our understanding of education level and SEL.

7.2 Conclusions

This study used an extended KAB model, which proposed that year-level (grade) could act as a moderator in the relationship between knowledge and attitude. As a result, three main hypotheses and three sub-hypotheses were proposed based on the respondents' various conditions. The postgraduate student group has the highest education level, while the final-year students and non-final-year students decrease in order. These conditions represent various levels of educational influence. At the same time, postgraduate students return to the university environment after having had some contact with work, representing the group that has been influenced by both education level and SEL.

On this basis, the Human Aspects of Information Security Questionnaire (HAIS-Q) was used to assess the extended KAB model. The effect of grade and work exposure on mean knowledge, attitude, and behaviour scores was investigated. The findings confirmed that education level and SEL had a statistically significant effect on variables.

Three major hypotheses were found to be correct. *H1-University students of various years of study, postgraduate students, and working graduates will demonstrate varying levels of cybersecurity knowledge* was confirmed. There were significant differences in knowledge among university students of various years of study, postgraduate students, and working graduates.

H2a–H2c examined whether there would be statistically significant differences in attitudes among four groups of respondents. Non-final-year students performed better than the other three groups. Furthermore, final-year students had higher scores than postgraduate students, and postgraduate students had higher scores than working graduates.

H3a–H3c examined whether the behaviours of four groups of respondents will differ. Postgraduate students were found to score higher than final-year students and working graduates, but their scores were comparable to non-final-year students.

The current study was one of the first to compare postgraduate students with university students and working graduates in order to examine the cognitive and behavioural changes of well-educated individuals. It contributed to methodology and practice guidance. The findings of this study need to be confirmed by additional research, but it could serve as a starting point for future investigations.

Acknowledgements We are thankful to Dr. ChanFai Man (ORCID: 0000-0002-2458-1992) who provided expertise that greatly assisted the research.

Author contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Qin Ana and Cheong Hin Hong. The first draft of the manuscript was written by Qin Ana and all authors commented on previous versions of the manuscript. Conceptualization: Qin Ana; Methodology: Xiaoshu Xu; Formal analysis and investigation: Cheong Hin Hong and Xiaoshu Xu; Writing - original draft preparation: Qin Ana; Writing - review and editing: Xiaoshu Xu, Kimberly Kolletar-Zhu; Resources: Yunfeng Zhang, Kimberly Kolletar-Zhu; Supervision: Cheong Hin Hong. All authors read and approved the final manuscript.

Funding National Social Science Foundation of China (NSSF) Postgrant Project (21FJKB013).

Data Availability Datasets are available in a funder-mandated or public (institutional, general, or subject-specific) repository that assigns persistent identifiers to datasets. A submission to the journal implies that materials described in the manuscript, including all relevant raw data, will be freely available to any researcher wishing to use them for non-commercial purposes, without breaching participant confidentiality. The datasets generated during and/or analysed during the current study are available in the Figshare repository, https://figshare.com/s/b840bda7b96e12ce93a7.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose. The authors have no competing interests to declare that are relevant to the content of this article. All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The authors have no financial or proprietary interests in any material discussed in this article. The authors declare no competing interests.

References

1. Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**, 606–622 (2015). https://doi.org/10.1108/k-12-2014-0283
2. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**, 179–211 (1991). https://doi.org/10.1016/0749-5978(91)90020-t
3. Rogers, E.M.: Diffusion of Innovations. Free Press, New York (2003)
4. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Comput. Secur. **25**, 289–296 (2006). https://doi.org/10.1016/j.cose.2006.02.008
5. McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., Pattinson, M.: A reliable measure of information security awareness and the identification of bias in responses. Australas. J. Inf. Syst. (2017). https://doi.org/10.3127/ajis.v21i0.1697
6. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. **42**, 165–176 (2014). https://doi.org/10.1016/j.cose.2013.12.003
7. Hong, W.C.H., Chi, C., Liu, J., Zhang, Y., Lei, V.N.-L., Xu, X.: The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Educ. Inf. Technol. (2022). https://doi.org/10.1007/s10639-022-11121-5
8. Ulven, J.B., Wangen, G.: A systematic review of cybersecurity risks in higher education. Future Internet **13**, 39 (2021). https://doi.org/10.3390/fi13020039
9. Wiley, A., McCormac, A., Calic, D.: More than the individual: examining the relationship between culture and information security awareness. Comput. Secur. **88**, 101640 (2020). https://doi.org/10.1016/j.cose.2019.101640
10. Li, Y.-L., Li, Y., Li, A.: A study on college students' internet information ethics cognition and influencing factors [大学生网络信息伦理认知与影响因素研究]. Inf. Doc. Work **35**, 10–16 (2014)
11. Huang, X., He, W., Hua, C., Shang, Y.: The Statistical Analysis about Status and Influencing Factors of University Students' Safety

Accidents. Statistical and Application [高校学生安全事故发生状况及其影响因素的统计分析]. 3, 57–67 (2014). https://doi.org/10.12677/sa.2014.32009

12. Elkhannoubi, H., & Belaissaoui, M.: Assess developing countries' cybersecurity capabilities through a social influence strategy. In: 2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) pp.19–23 IEEE. (2016). https://doi.org/10.1109/SETIT.2016.7939834
13. Fishbein, M., Ajzen, I.: Belief, attitude, intention, and behavior: an Introduction to Theory and Research. Addison-Wesley Pub. Co, Reading, Mass. (1975)
14. Vance, A.: Why Do Employees Violate Is Security policies?: Insights from Multiple Theoretical Perspectives, http://urn.fi/urn:isbn:9789514262876
15. Ng, B.-Y., Kankanhalli, A., Xu, Y.: (Calvin): studying users' computer security behavior: a health belief perspective. Decis. Support Syst. **46**, 815–825 (2009). https://doi.org/10.1016/j.dss.2008.11.010
16. Fan, J., Zhang, P.: Study on e-government Information Misuse Based on General Deterrence Theory. In: ICSSSM11. pp. 1–6. IEEE Institute of Electrical & Electronic Engineers (2011)
17. Mathieson, K.: Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour. Inf. Syst. Res. **2**, 173–191 (1991). https://doi.org/10.1287/isre.2.3.173
18. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Inf. Manag. Comput. Secur. **8**, 31–41 (2000). https://doi.org/10.1108/09685220010371394
19. Heirman, W., Walrave, M., Vermeulen, A., Ponnet, K., Vandebosch, H., Hardies, K.: Applying the theory of planned behavior to adolescents' acceptance of online friendship requests sent by strangers. Telemat. Inform. **33**, 1119–1129 (2016). https://doi.org/10.1016/j.tele.2016.01.002
20. Chandarman, R., Van Niekerk, B.: Students' cybersecurity awareness at a private tertiary educational institution. Afr. J. Inf. Commun. (2017). https://doi.org/10.23962/10539/23572
21. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. **31**, 83–95 (2012). https://doi.org/10.1016/j.cose.2011.10.007
22. Anderson, C., Agarwal, R.: Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q. **34**, 613 (2010). https://doi.org/10.2307/25750694
23. Chen, Y., Zahedi, F.M.: Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. MIS Q. **40**, 205–222 (2016). https://doi.org/10.25300/misq/2016/40.1.09
24. Warkentin, M., Johnston, A.C., Shropshire, J., Barnett, W.D.: Continuance of protective security behavior: a longitudinal study. Decis. Support Syst. **92**, 25–35 (2016). https://doi.org/10.1016/j.dss.2016.09.013
25. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**, 106–125 (2009). https://doi.org/10.1057/ejis.2009.6
26. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. **47**, 154–165 (2009). https://doi.org/10.1016/j.dss.2009.02.005
27. Roberts, S.A.: Exploring the Relationships between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors, https://www.proquest.com/openview/c1c31d84698165e5843133986323a773/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y, (2021)
28. De-Graft Aikins, A., Boynton, P., Atanga, L.L.: Developing effective chronic disease interventions in Africa: insights from Ghana and Cameroon. Glob. Health (2010). https://doi.org/10.1186/1744-8603-6-6
29. Schrader, P.G., Lawless, K.A.: The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. Perform. Improv. **43**, 8–15 (2004). https://doi.org/10.1002/pfi.4140430905
30. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Comput. Secur. **66**, 40–51 (2017). https://doi.org/10.1016/j.cose.2017.01.004
31. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł, Cetin, F., Basim, H.N.: Cyber security awareness, knowledge and behavior: a comparative study. J. Comput. Inf. Syst. **62**, 1–16 (2020). https://doi.org/10.1080/08874417.2020.1712269
32. Worsley, A.: Nutrition knowledge and food consumption: can nutrition knowledge change food behaviour? Asia Pac. J. Clin. Nutr. **11**, S579–S585 (2002). https://doi.org/10.1046/j.1440-6047.11.supp3.7.x
33. Parsons, K., McCormac, A., Pattinson, M.R., Butavicius, M.A., Jerram, C.: An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations, In Furnell, S. M., Clarke, N. L. & Katos, V (Eds). Proceedings of the European Information Security Multi-Conference (EISMC 2013). 34–44 (2013)
34. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M.: The effect of resilience and job stress on information security awareness. Inf. Comput. Secur. **26**, 277–289 (2018). https://doi.org/10.1108/ics-03-2018-0032
35. Bostan, A., Akman, I.: Impact of Education on Security Practices in ICT. Tehnicki Vjesnik—Technical Gazette. 22, 161–168 (2015). https://doi.org/10.17559/tv-20140403122930
36. Brilingaitė, A., Bukauskas, L., Juozapavičius, A.: A framework for competence development and assessment in hybrid cybersecurity exercises. Comput. Secur. **88**, 101607 (2020). https://doi.org/10.1016/j.cose.2019.101607
37. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D.: Managing information security awareness at an Australian bank: a comparative study. Inf. Comput. Secur. **25**, 181–189 (2017). https://doi.org/10.1108/ics-03-2017-0017
38. Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput. Secur. **49**, 177–191 (2015). https://doi.org/10.1016/j.cose.2015.01.002
39. Hadlington, L., Parsons, K.: Can cyberloafing and internet addiction affect organizational information security? Cyberpsychol. Behav. Soc. Netw. **20**, 567–571 (2017). https://doi.org/10.1089/cyber.2017.0239
40. Chaudhary, S., Zhao, Y., Berki, E., Valtanen, J., Li, L., Helenius, M., Mystakidis, S.: A cross-cultural and gender-based perspective for online security: exploring knowledge, skills and attitudes of higher education students. IADIS Int. J. WWW/Internet **13**, 57–71 (2015)
41. Cain, A.A., Edwards, M.E., Still, J.D.: An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. **42**, 36–45 (2018). https://doi.org/10.1016/j.jisa.2018.08.002
42. Choi, M., Levy, Y., & Anat, H.: The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. In Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy. 1. December (2013)
43. Brilingaitė, A., Bukauskas, L., Juozapavičius, A.: A framework for competence developmentand assessment in hybrid cybersecurity exercises. Comput. Secur. **88**, 1–13 (2020). https://doi.org/10.1016/j.cose.2019.101607
44. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of

the SIGCHI Conference on Human Factors in Computing Systems pp. 373–382 (2010)

45. Das, S.: Social cybersecurity: understanding and leveraging social influence to increase security sensitivity. It-inf. Technol **58**(5), 237–245 (2016). https://doi.org/10.1515/itit-2016-0008
46. Rader, E., Wash, R., & Brooks, B.: Stories as informal lessons about security. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, pp. 1–17 (2012). https://doi.org/10.1145/2335356.2335364
47. Kam, H.-J., Mattson, T., Goel, S.: A cross industry study of institutional pressures on organizational effort to raise information security awareness. Inf. Syst. Front. **22**, 1241–1264 (2020). https://doi.org/10.1007/s10796-019-09927-9
48. Watson, H., Moju-Igbene, E., Kumari, A., Das, S.: "We Hold Each Other Accountable": unpacking How Social Groups Approach Cybersecurity and Privacy Together. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. (2020). https://doi.org/10.1145/3313831.3376605
49. United Nations Development Programme. Human Development Report 2020—The next frontier:Human Development and the Anthropocene. (2020). http://hdr.undp.org/sites/default/files/hdr2020.pdf. Accessed 12 July 2021
50. National Bureau of Statistics of China. 2020 China statistical yearbook. China Statistics Press. (2021). http://www.stats.gov.cn/tjsj/ndsj/2020/indexeh.htm. Accessed 2 Aug 2021
51. Aivazpour, Z., Rao, V.S.: (Chino): information disclosure and privacy paradox. ACM SIGMIS Database DATABASE Adv. Inf. Syst. **51**, 14–36 (2020). https://doi.org/10.1145/3380799.3380803
52. Lipsitz, S.R., Parzen, M.: Sample size calculations for non-randomized studies. Statistician **44**, 81 (1995). https://doi.org/10.2307/2348619
53. Mei, B., Brown, G.T.L.: Conducting online surveys in China. Soc. Sci. Comput. Rev. **36**, 721–734 (2017). https://doi.org/10.1177/0894439317729340
54. Razali, N.M., Wah, Y.B.: Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests. J. Stat. Model. Anal. **2**, 21–33 (2011)
55. Jin, R.: Discussion on the Teaching Reform of Computer Fundamental Course for non-computer Majors in Applied Universities [应用型本科院校非计算机专业《计算机基础》教学改革探讨]. Fujian Comput. 10, 174–175 (2018). https://doi.org/10.16707/j.cnki.fjpc.2018.10.088
56. Chen, S.: Research on VC + + Curriculum Construction for Non-computer Major Postgraduate Students [非计算机专业研究生 VC + +课程建设研究]. J. Lanzhou Inst. Educ. 35, 80–81, 145 (2019)
57. A. Farooq, J. Isoaho, S. Virtanen and J. Isoaho, "Information security awareness in educational institution: an analysis of students' individual factors," IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 352–359 (2015) https://doi.org/10.1109/Trustcom.2015.394
58. Alqahtani, M.A.: Cybersecurity awareness based on software and e-mail security with statistical analysis. Comput. Intell. Neurosci. (2022). https://doi.org/10.1155/2022/6775980
59. Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S.: Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology. Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria, 5–7 April, 2022
60. Moallem, A.: Cyber security awareness among college students. In International conference on applied human factors and ergonomics, pp. 79–87. Springer, New York (2018) https://doi.org/10.1007/978-3-319-94782-2_8
61. Li, Y.-L., Li, Y., & Li, A. A study on college Students' internet information ethics cognition and influencing factors [大学生网络信息伦理认知与影响因素研究]. Information and Documentation Work, 35(2), 10–16 (2014). http://qbzl.ruc.edu.cn/EN/abstract/abstract669.shtml Accessed 10 June 2022
62. Sun, W.: Investigation of Safety Consciousness of University Students in Dalian City [大连市大学生网络安全意识调查研究]., (2018)
63. Berki, E., Kandel, C., Zhao, Y., Chaudhary, S.: Comparative study of cyber-security knowledge in higher education institutes of five countries. Educ. Comput. Sci. (2017). https://doi.org/10.21125/edulearn.2017.1591
64. Senali, M. G., Cripps, H., Meek, S., & Ryan, M. M.: A comparison of Australians, Chinese and Sri Lankans' payment preference at point-of-sale. Market. Intell. Plan. 40(1), 18–32 (2021). https://doi.org/10.1108/MIP-07-2021-0235
65. Mezzour, G., Carley, K.M., Carley, L.R.: An empirical study of global malware encounters. In: Proceedings of the 2015 Symposium and Bootcamp on the Science of Security. ACM, p. 8, (2015)
66. Gantz, J.F., Vavra, T., Lim, V.: Unlicensed Software and Cybersecurity Threats, BSA- The Software Alliance, January (2015)
67. Zhao, J., Xu, F.: The state of ICT education in China: a literature review. Front. Educ. China **5**, 50–73 (2010). https://doi.org/10.1007/s11516-010-0006-1

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.