Education and Information Technologies (2023) 28:439–470
https://doi.org/10.1007/s10639-022-11121-5

The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates

Wilson Cheong Hin Hong[1] · ChunYang Chi[2] · Jia Liu[3] · YunFeng Zhang[4] · Vivian Ngan-Lin Lei[5] · XiaoShu Xu[6]

Received: 25 January 2022 / Accepted: 17 May 2022 / Published online: 30 June 2022

Abstract

A multitude of studies have suggested potential factors that influence internet security awareness (ISA). Some, for example, used GDP and nationality to explain different ISA levels in other countries but yielded inconsistent results. This study proposed an extended knowledge-attitude-behaviour (KAB) model, which postulates an influence of the education level of society at large is a moderator to the relationship between *knowledge* and *attitude*. Using exposure to a full-time working environment as a proxy for the influence, it was hypothesized that significant differences would be found in the *attitude* and *behaviour* dimensions across groups with different conditions of exposure and that exposure to full-time work plays a moderating role in KAB. To test the hypotheses, a large-scale survey adopting the Human Aspects of Information Security Questionnaire (HAIS-Q) was conducted with three groups of participants, namely 852 Year 1–3 students, 325 final-year students (age = 18–25) and 475 full-time employees (age = 18–50) in two cities of China. MANOVA and subsequent PROCESS regression analyses found a significant negative moderating effect of *work exposure*, which confirmed the proposed model. However, the effect was more pervasive than expected and moderation was found in the interaction between *work exposure* and all three ISA dimensions. The social influence does not only reshape the cybersecurity *attitude* of the highly educated, but also *knowledge* and *behaviour*. Findings contribute theoretically, methodologically and practically, offering novel perspectives on ISA research and prompting new strategies to respond to human factors.

Keywords National Education Level · Internet security · Work exposure · KAB model · HAIS-Q

✉ XiaoShu Xu
Lisaxu@wzu.edu.cn

Extended author information available on the last page of the article

1 Introduction

Cybersecurity is becoming a major concern and one of the most challenging issues as digital technology is evolving rapidly in recent years. However, this issue has never been so critical and urgent as it is during the current COVID-19 pandemic when working and learning online become the only plausible solution wherever the Internet is available. Such an unprecedented switch from offline to the online environment might generate great threats to privacy and protection of personal data, especially for online teaching and learning. Recent statistics show the education sector accounted for 7.2% of total breaches reported, which means attacks in higher education are growing significantly as cybercriminals target new online-learning models (Risk Based Security, 2020). As an efficient counter-measure, it is advised to increase Internet security awareness (hereafter ISA) by educating internet users to be sensitive to the various cyber threats and the vulnerability of computers and data (Siponen, 2000), in order to induce behavioural changes to tackle the ever-expanding digital society and culture. According to China Internet Network Information Center annual report (2021), until December 2020, China, with nearly one billion netizens, had formed the world's largest digital society. The COVID-19 epidemic has accelerated the wave of social digital transformation in China from individuals, enterprises to governments in an all-around way (Wu et al., 2020). At the same time, cybersecurity problems emerged as urgent issues in this country, which accounts for one-fifth of global internet users. Under such a context, it is worthwhile to explore the cybersecurity awareness of Chinese internet users, especially considering the enormously diverse educational background of the general public (National Bureau of Statistics of China, 2021; Ministry of Education of the People's Republic of China, 2020) who formed the netizen population.

Although studies related to ISA are plenty, existing literature shows empirical research on cybersecurity risks in higher education is scarce (Ulven & Wangen, 2021). To the authors' best knowledge, there has not been an attempt to understand behavioural changes of the highly educated as they graduate and work in society. Nevertheless, the abundant literature has provided a number of methods to assess cybersecurity awareness (Rahim et al., 2015). Among all, the knowledge-attitude-behaviour (KAB) model has been used to explain cybersecurity awareness and behaviours (Parsons et al., 2014; Zwilling et al., 2020), and the HAIS-Q is a relatively new and comprehensive scale to investigate internet security *knowledge*, *attitude* and *behaviours*, which has been confirmed to have high internal consistency and external reliability (McCormac et al., 2017; Parsons et al., 2014). However, like many other emerging models, KAB is subject to further improvements, as Parsons et al. (2014) rightly acknowledged. One factor that has been suggested is social influence, which past studies found to be a salient predictor of cybersecurity behaviours (Das, 2016; Elkhannoubi & Belaissaoui, 2016; Heirman et al., 2016; Rader et al., 2012; Watson et al., 2020). However, impacts from the external environment were rarely the focus of investigation (Kam et al., 2020) and barely any researchers examined the effect of the average education level of a society on an individual's ISA. A case in point is China, despite being the second-largest economy (International

Monetary Fund, 2021), the average national education level is much lower than most developed countries (United Nations Development Programme, 2020). As the comparatively better-ISA-informed and more highly-educated internet users (e.g., university students) come out into the society, there is a good chance their ISA would be influenced by other less-educated co-workers, since peers have tremendous impact on one another's ISA (Hwang et al., 2017). To evaluate this social influence, respondents of similar educaton backgrounds (i.e., higher-education level) were recruited, and three levels of *full-time work exposure* (hereafter *work exposure*) were considered, from no exposure to prolonged exposure. They are used to approximate the levels of influence of social education level (SEL), defined as the average education level of society, on university students/graduates' cybersecurity *knowledge*, *attitude* and *behaviour*. With the assumption that more social contact at work implies a higher influence of lower SEL, an extended KAB model was proposed; the influence of SEL is taken as a moderating variable between *knowledge* and *attitude*. A large-scale survey was then conducted to test the extended KAB model. Considering the relatively few large-scale studies on ISA and scarcely any attempts to compare university students with working graduates, this study may contribute in theoretical, methodological and practical respects, refining the KAB model, providing a novel method to quantify social influence and offering further insights into its impact on ISA.

2 Literature review

2.1 KAB framework and HAIS-Q

The knowledge-attitude-behaviour (KAB) model was first proposed by Kruger and Kearney (2006) to measure information security awareness. It is based on the three interrelated components of the social psychological model, namely, affect, behaviour and cognition (Eifert & Craill, 1989; MacKinnon & Hoey, 2021), which correspond to *attitude*, *behaviour* and *knowledge* respectively. The KAB model has been widely adopted to explain cybersecurity *awareness* and *behaviours* (Parsons et al., 2014; Zwilling et al., 2020). The main proposition of KAB is while *knowledge* can change *behaviours*, *attitude* is often a necessary mediator between the two factors. In other words, increased knowledge improves attitude, which then results in better information security behaviours (Parsons et al., 2014). *Knowledge* concerns knowing *what* (declarative), *how* (procedural), *when* and *why* (conditional) (Schrader & Lawless, 2004). *Attitude*, in this study, is defined as *beliefs* and *perceptions*. Finally, *behaviours* are referred to as *observable actions* under varied circumstances. The current study occasionally mentions the term *awareness*, as past studies have vaguely and at times inconsistently used it to refer to *knowledge* (e.g., Berki et al., 2017), *knowledge* and *attitude* (e.g., Zwilling et al., 2020), or a combination of *knowledge/attitude* and *behaviours* (e.g., Chandarman & Van Niekerk, 2017). For the purpose of this study, *awareness* is defined as a mix of *knowledge* and *attitude*.

The KAB model has received much attention due to earlier research finding that knowledge alone is insufficient to cause behavioural changes (Valente et al., 1998; Worsley, 2002). Attitude is a necessary mediator to mitigate the cognitive dissonance between knowledge and action. To measure the relationship between the three variables, Parsons et al. (2013) conceptualized the Human Aspects of Information Security Questionnaire (HAIS-Q) based on the KAB model. Before the emergence of HAIS-Q, survey questionnaires tended to have a narrow focus on ISA, such as the use of passwords (Carstens et al., 2004) and smartphone applications (Mylonas et al., 2013). Consisting of seven dimensions, the HAIS-Q is more comprehensive in capturing the most typical internet behaviours. The questions are relatively "neutral" in that they do not highlight deliberate positive behaviours or intentional malicious behaviours (Parsons et al., 2014), which can reduce social desirability bias. In addition, each sub-area of the dimensions, such as "opening attachments" under the aspect of "email use", is phrased to fit the definition of knowledge (*"I am allowed to open email attachments from unknown senders"*), attitude (*"It's risky to open an email attachment from an unknown sender*") and behaviour (*"I don't open email attachments if the sender is unknown to me"*) respectively (p. 168). Hence, a clear distinction can be observed between awareness and behaviours. Finally, studies have shown that HAIS-Q has high internal consistency and external reliability (McCormac et al., 2017; Parsons et al., 2014), making it a valid and reliable measurement tool for internet security perceptions and actions.

Traditionally, the issue of ISA had been widely explored using models developed from well-established psychological theories such as the Theory of Planned Behaviour (TPB) (Ajzen, 1991) and Protection Motivation Theory (PMT) (Rogers & Prentice-Dunn, 1997). However, these models were criticised for not being able to capture the complexity and the specific phenomenon in cybersecurity (Karjalainen & Siponen, 2011; Moody et al., 2018; Roberts, 2021). PMT, for example, emphasises personal threat, which is a less relevant concept in many contexts where ISA is essential (e.g., workplace) (Warkentin et al., 2016). Further, there are major differences in terms of the necessity of subject knowledge between internet behaviours and other health or environmental-related motivation studies where TPB and PMT were initially developed. In some of the latter studies, the risky behaviours being examined might be largely known by the public, such as the risk of smoking to one's body or the problem of plastic products to the environment. In others, such as the effect of wine on health or humanity's carbon emission on global warming, information can be controversial or even contradicting. However, knowledge in cybersecurity is unambiguous (Parsons et al., 2014) but may differ largely from person to person. Hence, the knowledge construct is an indispensable element, and the KAB model, which is based on social psychology and specifically developed to explain ISA (Kruger & Kearney, 2006), appears to be a more appropriate model for the purpose of this study.

2.2 Factors affecting cybersecurity behaviours

One major criticism of the KAB model is that the relationship between *knowledge*, *attitude* and *behaviour* is overly simple (Aikins et al., 2010; van der Linden, 2014) as studies have found knowledge and attitude alone can only account for some

behavioural changes. The model may fail to explain, for example, why certain countries have similar levels of cybersecurity awareness but differing reported behaviours (Zwilling et al., 2020), despite a significant relationship between awareness and behaviours. For this reason and others, many studies have hypothesized *personal* and *social factors* that affect behavioural decisions, such as age (Cain et al., 2018), gender (Chaudhary et al., 2015), self-efficacy (Choi et al., 2013), stress level (McCormac et al., 2018), cultural beliefs (Wiley et al., 2020) and work environment (Hadlington and Parsons, 2017); these studies focus on behavioural differences at an individual or interpersonal level in a confined context. Other studies examine cybersecurity differences from a cross-national perspective (Berki et al. 2017; Chen & Zahedi, 2016; Sawaya et al., 2017, Zwilling et al., 2020). To name but a few, Berki et al. (2017) investigated cloud services security knowledge, attitude and usage of higher institute students from Greece, Finland, Nepal, the UK and China. Chen and Zahedi (2016) compared perceived cybersecurity threats and coping behaviours of university students and their friends and family in the United States and China, while Zwilling et al. (2020) surveyed undergraduate and graduate students in Turkey, Israel, Poland and Slovenia on cybersecurity knowledge, awareness and behaviours. These studies found safer cybersecurity behaviours are related to higher GDP or better development of a country, but exceptions often exist.

It is known that an individual's education level correlates with his/her ISA (Aivazpour & Rao, 2020; Chua et al., 2018; Wiley et al., 2020). In particular, education on information and communication technology (ICT) can positively benefit one's ISA (Bostan & Akman, 2015; Brilingaitė et al., 2020; Sheng et al., 2010). Related studies have predominantly focused on the education received by an internet user. However, the impact of an individual being exposed to a social environment where most people have low education background and inadequate ICT education is seriously under-investigated. Different from the education at a personal level, SEL concerns how the general education level of an internet user's immediate circle, such as family, friends and colleagues, impacts the user's cybersecurity behaviours. Existing literature has found social influence to be a critical factor that motivates or demotivates cyber security behaviours (Das, 2016; Elkhannoubi & Belaissaoui, 2016; Heirman et al., 2016; Kam et al., 2020; Rader et al., 2012; Watson et al., 2020). Kam et al. (2020), for example, examined the relationship between industry type and information security awareness (ISA). The study found varied institutional environments produced unique security practices. They became social norms that affected employees' perceptions of organizations' ISA and pressure them into complying with safe internet practices. A structural model analysis was adopted to confirm the moderation effect of social norms on the formation of employee ISA. Workplace aside, Rader et al. (2012) found that most people learned lessons from stories about security incidents informally from family and friends. These stories impact the way people think about security, and their subsequent behaviour when making security-relevant decisions. Findings of Das (2016) echoed such peer influence. He found that "observing others" was a main trigger for safe internet practices. For example, a participant reported he only started to set passcodes for his phone because he noticed others in his circle set passcodes. Das commented that a change of behaviours is likely when there is "social proof" that others are doing the

same. Conversely, if a well-educated internet user is surrounded by under-educated users, whose security awareness is not as high (Bostan & Akman, 2015), the well-educated individual may reduce safe practices over time. These studies suggest that social influences from workplace, family and friends can affect individuals' attitudes and behaviours towards cybersecurity. At a national level, Elkhannoubi & Belaissaoui (2016) argued that social influence plays a key role in safe internet behaviours, especially in developing countries. They proposed a framework to assess and promote ISA in developing countries, which consists four variables: (public) awareness, social media, government and business influence. Governments are advised to consider these factors and mobilise social networks and businesses to develop an environment that can reshape internet users' opinions regarding cybersecurity. All in all, the external environment appears to play a key role in one's ISA but systematic investigations of its impact are lacking (Kam et al., 2020). SEL is an objective dimension that can quantify social influences on an individual's internet security practices.

2.3 Education level of China and its potential influence on ISA

Despite being the second-largest economy in the gross domestic product (GDP) (International Monetary Fund, 2021), with the latest Education Index of 0.58 (United Nations Development Programme, 2020), China's adult education level is still very far from all other developed countries. This echoes the latest census published in the 2020 China Statistical Yearbook, which reveals that 14.58% of the sampled population (N = 1,016,417) received post-secondary education, while 30.39% only received primary education or below,[1] and the adult illiteracy rate is 4.59% (National Bureau of Statistics of China, 2021). On the other hand, the proportion of secondary school students who entered higher institutes is relatively high, at 51.6% (Ministry of Education of the People's Republic of China, 2020), meaning that one out of two secondary school graduates is receiving higher education. This creates a split of two worlds in the education environment and the working environment. Hence, university graduates are likely to work with colleagues who do not possess a university degree or even a senior secondary school diploma. Such a dramatic change of social circle may reshape one's cyber security awareness and behaviours. A recent large-scale study on organizational ISA of several Asia-Pacific economies, including Mainland China, Hong Kong and Taiwan, found that employees generally underestimated company vulnerability to cyber-attacks (PwC's Threat Intelligence Centre, 2020). The research team surveyed 1133 management-level or information-technology employees. 84% of respondents were confident about their companies' internet security measures. However, 57% of the surveyed corporates had been attacked in the previous two years, with the majority being assaulted more than once. Among the malicious intents, viruses and malware, web-based attacks and phishing were the most common forms. With 47% of surveyed corporates not

[1] The survey included a population of six years old or above.

having even installed anti-virus software, the researchers noted a large discrepancy between respondents' beliefs and the actual situation and recommended boosting security awareness of employees.

To the authors' knowledge, there is no direct comparison between the ISA of university students and employees, and investigations comparing the ISA of different year-levels of university students are scant. Li et al. (2014) were one of the few studies that examined the change of information ethics awareness of university students in China. By splitting 171 student respondents into the junior group (year 1–2) and senior group (year 3–4), Li et al. found that the senior group exhibited significantly less awareness than the junior groups. Senior-level students were more prone to risky and illegal online behaviours. Li et al. suggested that social influence was the major cause for students' reversion to poorer behaviours, but did not expound on the source of such social influence. Nevertheless, it is known that senior-level students have more exposure to society through work and out-of-school activities than the lower-level students. Another larger-scale ISA study was conducted by Sun (2018), who surveyed 655 university students across seven higher institutes in Dalian, China. Sun found that final-year students consistently scored the lowest in preventative (cybersecurity) awareness, risky behaviours and responses to risks when compared to other year-levels of students, although statistically only preventative awareness was found to be significantly different between the groups. Sun suspected that the final-year thesis, internship and job applications were the main causes of reduced ISA, as students are exposed to more social circles where deceptions and risky behaviours are more common. These results echoed other safety-related studies in China (e.g., Huang et al., 2014), where upper-year students were found to display more risky behaviours and result in more safety incidents. These findings may sound counterintuitive at first glance, as an individual's education level is known to positively correlate with his/her ISA (Aivazpour & Rao, 2020; Chua et al., 2018; Wiley et al., 2020). Hence, senior-level students should not have lower ISA than junior-level students. However, as students promote to their senior year, they will also experience increased exposure to the society. In China, the low social education level implies a low ISA for the general public, who may affect university students' ISA negatively. To investigate if an increased exposure to society affects ISA, there is a need to compare the ISA of lower-level students, interns and full-time working graduates to understand if changes happen over time, and a larger sample is needed for better generalisability.

2.4 Inadequate large-scale studies

A search for existing literature suggests large-scale studies are far from adequate despite the plethora of research on ISA. A recent systematic review paper on higher education ISA reveals that the majority of the existing ISA surveys have small sample sizes (Ulven & Wangen, 2021). To name but a few, Nyblom et al. (2020) administered questionnaires to 72 respondents who had been cyber-attacked. Kwaa-Aidoo and Agbeko (2018) surveyed 180 respondents to elicit perceived security threats. Kim (2013) sampled 196 college students to examine their ISA. Understandably,

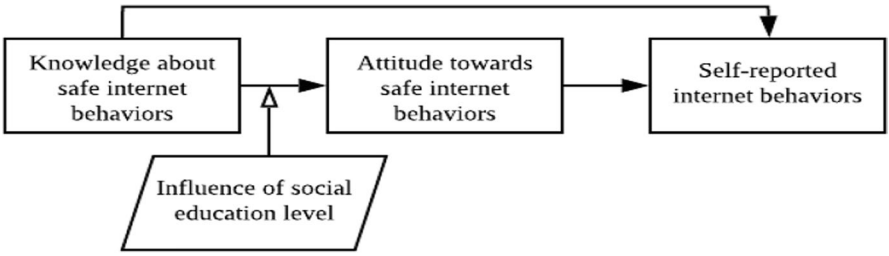

Fig. 1 An extended KAB model

each survey study comes with its limitations. Nevertheless, "small sample" is not a relative concept but rather a statistical deficiency. Considering random sampling in ISA studies are mostly improbable due to practical limitations, and that the size of a typical target population is quite large, a sample size of 333 to 400 for each group of respondents is the minimum for the data to be safely generalizable (Israel, 1992; Lipsitz & Parzen, 1995). However, not many have met such criteria. Larger-scale studies, therefore, appear to be valuable in the field of ISA, and the current studies attempt to contribute in this respect.

2.5 Extension of the KAB model

In the initial proposition of HAIS-Q, Parsons et al. (2014) acknowledged that other *social factors* should be considered when adopting the KAB model or HAIS-Q, recommending further investigations. In other ISA studies where TPB is used (e.g., Chandarman & Van Niekerk, 2017; Heirman et al., 2016; Ifinedo, 2012; Ong & Chong, 2014), *social influence* has been consistently found to moderate personal engagements in safe internet practice. However, there is no easy way to quantify social influence. Hence, we take *China's national education level* as a bigger influencer at play and suggest that more social contact at work implies a decrease in *SEL*. In other words, as university students progress through their years of education and subsequently graduate to work full-time, they are in increasingly closer contact with average citizens in China. Their internet security awareness and behaviour may deteriorate as a result. Thus, an extended model of KAB is proposed as follows (see Fig. 1):

The extended KAB model anticipates that university students will have similar cybersecurity *knowledge* owing to similarly high education background and adequate ICT knowledge (Bostan & Akman, 2015). However, their *attitude* towards cybersecurity will be influenced by the external environment, which ultimately changes their internet *behaviours*. Hence, the following hypotheses are proposed:

H1: Full-time working graduates and university students of different years of study will not display differing cybersecurity *knowledge*.
H2: Full-time working graduates and university students of different years of study will display differing cybersecurity *attitudes* and *behaviours*.

Table 1 A cross-tabulation of participants' demographic information

		Education / working status				
Variable	Categories	Year 1	Year 2–3	Final year	Working graduate	Percentage
Age range	18–25	480	372	325	151	80.4%
	26–35	0	0	0	192	11.6%
	36–45	0	0	0	90	5.4%
	≥ 46	0	0	0	42	2.5%
Gender	Male	184	119	123	207	38.3%
	Female	296	253	202	268	61.7%
Place of residence	Macao	65	48	108	59	16.9%
	Wenzhou	415	324	217	416	83.1%
Total (per variable)		*480*	*372*	*325*	*475*	

H2a: Non-final-year students will score significantly higher in *attitudes* and *behaviours* than final-year students.
H2b: Non-final-year students will score significantly higher in *attitudes* and *behaviours* than full-time working graduates.
H2c: Final-year students will score significantly higher in *attitudes* and *behaviours* than full-time working graduates.
H3: The level of full-time *work exposure* will display a significant moderation effect between the *knowledge* and *attitude* dimensions

3 Research method

3.1 Sample and sampling method

The current study employed snowball sampling and criterion sampling methods. A total of 1652 valid responses were collected from five higher institutes and 110 companies in Wenzhou (n = 1372) and Macao (n = 280), China. Among them, 852 are year 1–3 students, 325 final-year students (Age range = 18–25) and 475 full-time employees (Age range = 18- ≥46); 633 were male and 1019 were female. The descriptive information of participants can be found in Table 1.

As participatory criteria, all undergraduate participants were first screened for having received training on cybersecurity during their tertiary education and having a compulsory component of a half-year or full-year full-time internship in their final year of study. Full-time internship is believed to be highly similar to full-time employment, which allows for comparisons among different levels of work exposure (i.e., prior, short and prolonged work exposure). University students were invited to fill in the survey via email or personal contact. They then contacted their peers to take part. Although researchers initially expected to collect a similar number of valid responses from each group, responses from final-year students turned out to be quite low, and reaching them was even harder. Thus, extra effort was spent to boost

the number of responses to over 300. Some respondents commented that final-year students were too busy with their internship and studies, and therefore showed little interest in the survey. On the other hand, the working participants were invited through personal contact only, and many were alumni of the sampled institutes. They were required to have obtained a higher education degree, need to use a computer at work, have received cybersecurity training at work, have been working full-time for at least one year before taking part and have colleagues who do not possess a university degree. These criteria created extra difficulty in securing a greater number of working respondents. Nevertheless, the criteria were necessary to control for participants' education background and ensure they have frequent access to computers in order to align with the background of the undergraduate respondents. Meanwhile, it was necessary for them to have longer work exposure than the final-year group, and that there was potential "downward" influence from colleagues who did not possess a higher-education degree. All respondents were informed of the background of the research project, the anonymity of participation, data confidentiality and their rights to withdraw their data up to four weeks after the survey. They clicked the "consent to proceed" button to proceed to the survey.

The participants were divided based on our hypotheses that prolonged working exposure can negatively affect one's ISA. Therefore, an internship is considered the first near-full-time exposure to a working environment, which we use as a proxy for a general and social education level that is typically lower than that of the respondents. Note that in the current sample, some respondents studied in three-year programs, where the internship happened in Year-three (i.e., their final year). However, as we take non-final years of study as one category, the total length of the program should not be an issue. Thus, we conceived that non-final-year students were minimally influenced by the SEL at large as they were not exposed to a full-time working environment, while final-year students were mildly influenced and working graduates strongly influenced by the lower SEL owing to the work exposure.

3.2 Instrument

The Human Aspects of Information Security Questionnaire (HAIS-Q) was adopted and translated into Chinese. A bilingual language specialist was consulted to ensure the Chinese version is faithful to the original English version and meanwhile comprehensible. It was then face validated by two Information Technology experts and three other faculty members. The HAIS-Q contains 63 items, which cover dimensions of *knowledge*, *attitude* and *behaviour*. In each of the dimensions, participants are given 21 statements regarding internet use, email use, social media use, password management, incident reporting, information handling and mobile computing. The HAIS-Q for students was slightly adapted. For instance, the question "It's acceptable to use my social media passwords on my work accounts" is changed to "…my study accounts". Participants respond to each of the items by indicating a score on a five-point Likert scale ("5 = strongly agree", "1 = strongly disagree"). With a total of 31 reverse question items, the HAIS-Q have been consistently found to be a reliable and valid instrument for measuring ISA (McCormac et al., 2017;

Parsons et al., 2017; Pattinson et al., 2017). The questionnaire was created and distributed online using one of the biggest local survey platforms, Wenjuanxing,[2] also known as Sojump (Mei & Brown, 2018).

3.3 Piloting testing

The Chinese version of the HAIS-Q was then piloted with 124 student participants. The average time taken to complete the questionnaire was 406.15 s (SD = 197.74). Each of the three dimensions of the HAIS-Q consisted of 21 items. The *knowledge* dimension reported a Cronbach's Alpha of .84, attitude .91, and behaviour .79. They indicated good to excellent levels of internal consistency in the subscales.

After checking for pilot data normality, the proposed model was analysed using the PROCESS macro v.3.5 developed by Andrew F. Hayes. The Model 7 moderated mediation was used. This preliminary analysis confirmed the moderation effect of *work exposure* between *knowledge* and *attitude*. Further, the mediation of *attitude* between *knowledge* and *behaviour* was also verified (see Appendix A for the analysis results).

3.4 Data analyses

The collected data (N = 1652) were analysed using IBM SPSS25. As the setting of the online questionnaire disallows blank answers, respondents had to fill in everything to submit their responses. An obvious advantage of such a setting is there was no missing data, ensuring more smooth data analyses. However, some respondents might decide to give up if they did not wish to respond to certain questions. Nevertheless, as the questionnaire only takes around 10 minutes to complete, most respondents showed a high willingness to finish it all.

3.5 Internal reliability

Each of the three dimensions ($n_{question} = 21$) was checked for internal reliability. The *knowledge* dimension reported a Cronbach's Alpha of .85, while *attitude* and *behaviour* had an alpha value of .91 and .78 respectively, which was similar to the pilot results and indicated good to excellent levels of internal consistency in the subscales.

3.6 Checking the assumptions for regression analyses

This study investigates the moderating effect of *work exposure* on people's cybersecurity *attitude*, which acts as a mediator between *knowledge* and *behaviour* as dependent variables. *Work exposure* was categorised into three levels (non-final-year = low exposure, final-year = intermediate exposure, working-graduates = high exposure). Cumulative mean values of ISA (i.e., *attitude*, *knowledge* and *behaviour*)

[2] The platform can be found at https://www.wjx.cn/

Table 2 Correlation analysis for variables

	Mean attitude	Mean behaviour	Work exposure	Age	Gender	Place of residence
Mean knowledge	.805**	.803**	−.670**	−.485**	.076**	−.012
Mean attitude	1	.857**	−.591**	−.443**	.135**	−.084**
Mean behaviour		1	−.572**	−.398**	.112**	−.021
Work exposure			1	.756**	−.076**	−.003
Age				1	−.051*	.081**
Gender					1	−.097**

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

*. Correlation is significant at the .05 level (2-tailed)

were used for further analysis. No outliers were identified considering 3 inter-quartile range above/below boxplots, while 1.5 inter-quartile range was not considered owing to its inaccuracy (Hoaglin & Iglewicz, 1987). The ISA variables were then checked against normality. As both Kolmogorov-Smirnov and Shapiro-Wilk are designed for smaller sample sizes ($n < 50$) (Razali & Wah, 2011), direct hypothesis testing is not recommended. Instead, the value of skewness and kurtosis were manually evaluated. It was suggested that a larger sample with skewness between −2 and +2 and a kurtosis between −7 and 7 to be considered normally distributed (Byrne, 2013; Hair et al., 2010). Mean *knowledge* (skewness = −.168, kurtosis = −.897), mean *attitude* (skewness = .39, kurtosis = −.841) and mean *behaviour* (skewness = .260, kurtosis = −1.33) were all found to be safely within the thresholds and were therefore normally distributed. Then, taking *behaviour* as the dependent variable, and *knowledge* and *attitude* as the independent variable, standardised residuals of regression were calculated. Same was done with *work exposure* (IV) against *attitude* (DV). Homoscedasticity of the residuals was checked by plotting the residuals with P-P plot and scatterplot, which show good conformity with the theoretical residual distribution, and no apparent curvature nor funnelling in the data points. Meanwhile, significant differences were found among all the regression residuals ($p < .001$).

Next, the data were checked for multicollinearity. A correlations test was conducted for the variables of *knowledge, attitude, behaviour, work exposure, age, gender* and *place of residence* (see Table 2 for correlation results). *Age* was categorised into four ordinal levels according to the ranges provided in the questionnaire (18–25, 26–35, 36–45, ≥ 46); *gender* (male, female) and *place of residenc*e (Macao, Wenzhou) were treated as categorical variables. Mean *knowledge*, *attitude* and *behaviour*, were found to be significantly positively and strongly correlated ($p < .001$). *Work exposure* and *age* were also significantly positively and strongly correlated ($p < .001$) and they show significant negative correlations with mean *knowledge*, *attitude* and *behaviours* ($p < .001$). Hence, the independent variables of *work exposure* and *age* were considered covariates, meaning that to test the effect of *work exposure*, *age* has to be controlled.

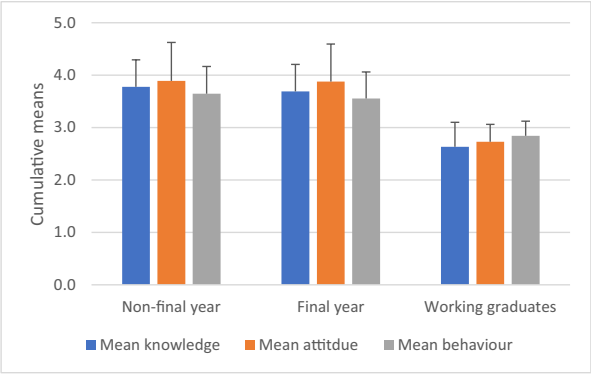

Fig. 2 Cumulative Means of knowledge, attitude and behaviour among non-final-year students, final-year students and working graduates

Hence, the assumptions for regression analyses were adequately met. They are, normal distribution of the data and the residuals, linear relationship between IVs and the DV, no signs of heteroscedasticity of nor correlation between regression residuals. Potential collinearity between *work exposure* and *age* was identified, but it can be accommodated in the proposed regression model by controlling for the latter.

3.7 Main analysis

A multivariate ANOVA was conducted to analyse the effect of different levels of *work exposure* on the mean scores of *knowledge*, *attitude* and *behaviour.* Box's M value was recorded at 527.003 ($p < .001$), meaning to reject the null hypothesis that the observed covariance matrices of the dependent variables are equal across groups. Therefore, Pillai's Trace, which is the most powerful and robust multivariate test (Anderson & Walsh, 2013), was taken for the MANOVA. A significant multivariate effect for the three latent variables was reported (Pillai's Trace = .53, F (6, 3296) = 197.15, < .001), and the effect size was .264. Subsequent ANOVA's of each dependent variable, *knowledge* (F (2, 1649) = 847.75, $p < .001$, partial $\eta^2 = .51$), *attitude* (F (2, 1649) = 227.42, $p < .001$, partial $\eta^2 = .4$) and *behaviour* (F (2, 1649) = 489.65, $p < .001$, partial $\eta = .37$) indicate they are all statistically significant. Fisher's LSD was used as a post-hoc comparison across groups, as detailed below in light of the corresponding hypotheses.

H1: Full-time working graduates and university students of different years of study will not display different cybersecurity *knowledge*.

H1 is rejected. The *knowledge* of non-final year students (M = 3.78, SD = .51) was found to be significantly different from final-year ones (M = 3.69, SD = .52) ($p = .008$), and significantly different from working graduates (M = 2.63, SD = .47) ($p < .001$). Final-year students were also found to be significantly different from working graduates ($p < .001$). See Fig. 2 for an illustration of mean differences.

H2a: Non-final-year students will score significantly higher in *attitude* and *behaviour* than final-year students.

H2a is partially verified. There is no statistically significant difference in *attitude* between non-final year students (M = 3.89, SD = .73) and final-year students (M = 3.88, SD = .72). However, the *behaviour* of non-final year students (M = 3.65, SD = .52) was found to be significantly different from final-year ones (M = 3.55, SD = .51) ($p = .002$).

H2b: Non-final-year students will score significantly higher in *attitude* and *behaviours* than full-time working graduates.

H2b is verified. There is a significant difference in *attitude* between non-final-year students and working graduates (M = 2.73, SD = .33) ($p < .001$). The same is true for *behaviour* between non-final-year students and full-time working graduates (M = 2.84, SD = .28) ($p < .001$).

H2c: Final-year students will score significantly higher in *attitudes* and *behaviours* than full-time working graduates.

H2c is verified. The *attitude* of final year students was found to be significantly different from working graduates ($p < .001$), and so is *behaviours* ($p < .001$). For simplicity, the differences in mean values of the three dimensions are illustrated in Figs. 2.

H3: The level of *work exposure* will have a significant moderation effect between *knowledge* and *attitude* dimensions

To test if exposure to full-time working environments moderates the relationship between the *knowledge* and *attitude* dimensions, a series of regression analyses using the PROCESS macro v3.5 was adopted. Moderation, in this study, is how the independent variable (X = *knowledge*), the moderating variable (W = *work exposure*) and the interaction between the two variables affect or predict the outcome (mediator) variable (M = *attitude*). These all create an interactive effect on the dependent variable (Y = *behaviour*). *Age* has been added as a controlled variable to remove the effect of the potential covariate. Past studies also indicated age to be a salient predictor of ISA (e.g., Cain et al., 2018; Grimes et al., 2010).

Results from the analysis show that the hypothesized model is statistically significant ($R^2 = .67$, F (6, 1645) = 556.12, $p < .001$), meaning the model can explain 67% of all cases. Specifically, *knowledge* is a significant predictor of *attitude* ($p < .001$). *Work exposure* is a categorical variable. Hence, PROCESS coded it into W1 (comparing average to low exposure) and W2 (comparing high to low exposure). W1 is not significant, while W2 is a positive predictor ($p < .001$). The interaction between *knowledge* and W2 is a significant negative predictor of *attitude* ($p < .001$), but *age* itself is not significant (see Table 3).

Table 3 Moderation analysis of variable effects on *attitude*

Variables	b	se	t	p	LLCI	ULCI
Knowledge	.940	.032	29.652	.000	.878	1.002
W1	.098	.226	.434	.665	−.345	.541
W2	1.075	.175	6.156	.000	.733	1.418
Knowledge*W1	−.008	.060	−.140	.889	−.127	.110
Knowledge*W2	−.435	.056	−7.733	.000	−.545	−.325
Age	−.016	.024	−.663	.507	−.062	.031

W1 = comparison between average and low *work exposure*

W2 = comparison between high and low *work exposure*

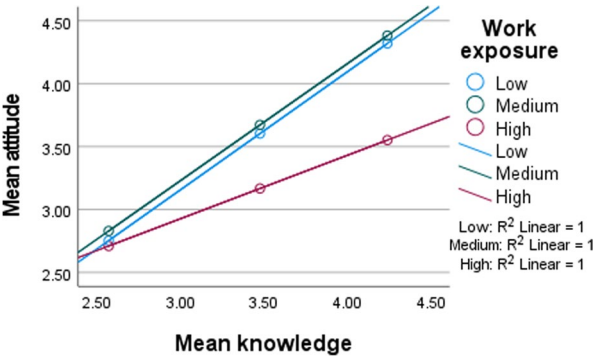

Fig. 3 An interaction plot of the moderating effect of work exposure on attitude at different levels of knowledge

An illustration of the interaction plot reveals the negative effects that high expo-

Table 4 Mediation analysis of variable effects on *behaviour*

Variables	b	se	t	p	LLCI	ULCI
Knowledge	.270	.017	16.328	.000	.238	.303
Attitude	.422	.014	30.150	.000	.394	.449
Age	.025	.011	2.196	.028	.003	.047

sure to full-time work has on ISA attitude at varied levels of ISA knowledge (see Fig. 3). The same effect is not found when work exposure is low or medium.

The analysis also confirms *attitude* is the mediator between *knowledge* and *behaviour* ($R^2 = .77$, $F(3, 1648) = 1855.73$, $p < .001$). Both *knowledge* ($p < .001$) and *attitude* ($p < .001$) can significantly predict *behaviour*. *Age* is a significant predictor of *behaviour* ($p < .05$) (see Table 4). Depending on the level of *work exposure* moderation, different levels of indirect effect of X on Y are reported (see Table 5). Hence, the moderated mediation model is supported (Index = −.18, bse = .018, 95% CI = −.219; −.15), and H3 is verified.

Table 5 The indirect effect of the moderated mediation of *knowledge* on *behaviour*, mediated by *attitude* and moderated by *work exposure*

Work exposure	Effect	BootSE	BootLLCI	BootULCI
Low	.396	.021	.356	.439
Medium	.393	.029	.338	.449
High	.213	.012	.189	.237

Table 6 Moderation analysis of variable effects on *behaviour*

Variables	b	se	t	p	LLCI	ULCI
Knowledge	.319	.024	13.234	.000	.272	.366
Attitude	.422	.017	24.858	.000	.389	.455
Work exposure[1]	.902	.125	7.198	.000	.656	1.148
Knowledge*Work exposure	−.129	.045	−2.865	.004	−.217	−.041
Attitude*Work exposure	−.200	.056	−3.550	.000	−.311	−.090
Age	.034	.013	2.535	.011	.008	.060

[1]High VS low level work exposure

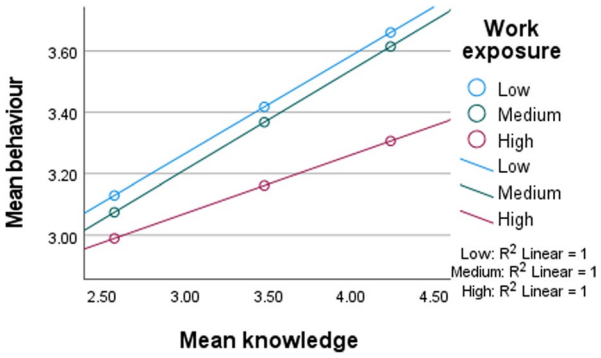

Fig. 4 An interaction plot of the moderating effect of work exposure on behaviour at different levels of knowledge

3.8 Further analysis

Based on the correlation analysis (Table 2), it seems possible that work exposure will also moderate the effect of *knowledge* on *behaviour*, as well as the effect of *attitude* on *behaviour*. Hence, a further analysis using Model 59 of the PROCESS macro was conducted, with behaviour as the outcome (Y) variable. The moderation for both was found to be statistically significant ($R^2 = .78$, $F(9, 1642) = 656.97$, $p < .001$). The interaction between of *work exposure* and *knowledge* ($p = .004$), and *work exposure* and *attitude* ($p < .001$) can both negatively predict *behaviour* (see Table 6).

Figure 4 illustrates how *work exposure* moderates the relationship between *knowledge* and *behaviour*, while Fig. 5 illustrates the effects of *work exposure* on the relationship between *attitude* and *behaviour*.

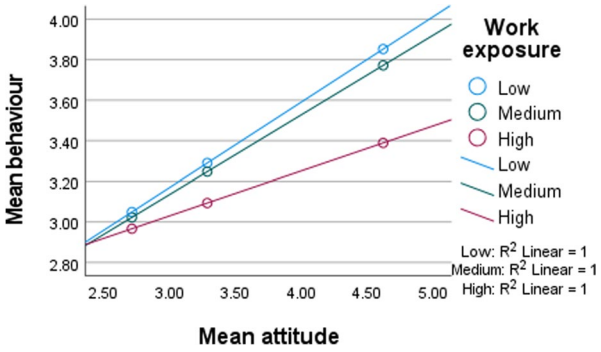

Fig. 5 An interaction plot of the moderating effect of *work exposure on behaviour* at different levels of attitude

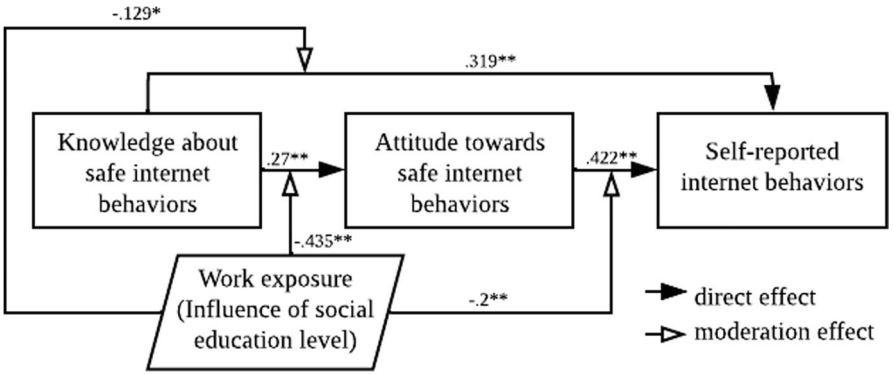

Fig. 6 Model analysis results and the final extended KAB model. *Significance at .01 level. **Significance at .001 level

In sum, a three-way moderation effect of *work exposure* was found. *Knowledge*work exposure* had a larger negative effect (b = −.435) on *attitude* than *knowledge*work exposure* (b = −.129) and *attitude*work exposure* (b = −.200) on *behaviour*. Overall, the impact of SEL influence is more pervasive than expected. Figure 6 illustrates the final extended KAB model.

4 Discussion

4.1 General discussion

The current investigation is one of the few, if not the first, studies that compare ISA between undergraduate students and working graduates, which can shed light on changes in cybersecurity *knowledge*, *attitude*, and *behaviours* of individuals with similar backgrounds. Further, we innovate in taking full-time *work exposure* as a proxy for the influence of SEL, which we argue is a quantifiable source of social influence. Past studies used GDP to predict citizens' ISA (e.g., Berki et al., 2017;

Chen & Zahedi, 2016; Zwilling et al., 2020), while national/social education level was never considered. This is possibly a reason for the conflicting predictions of ISA (e.g., Berki et al. 2017; Chen & Zahedi, 2016). China being the context of this study has a GDP higher than most developed countries (International Monetary Fund, 2021), but its national education indices are below many (United Nations Development Programme, 2020). Therefore, university graduates are likely to work with colleagues who possess lower education than them. With this in mind, a comparison was made between non-final years, final years and graduates who have worked full-time for at least one year to examine the effect of such social education exposure. Three main hypotheses, along with three sub-hypotheses, were proposed and all except one were verified. The rejected hypothesis concerns the differences in the *knowledge* dimension among the three groups. To our surprise, exposure to work does not only reshape participants' cybersecurity *attitudes*, which subsequently changed their *behaviours*, but it also negatively influences their *knowledge* of security. A closer look at the subscales reveals working graduates obtained the lowest scores for *email use* (M = 2.17) and *incident reporting* (M = 2.02). For example, many working participants agreed to click on a link or open attachments in emails from unknown senders. Moreover, they tend to turn a blind eye to suspicious behaviours or colleagues' risky behaviours. Interestingly, these are the exact two aspects that were scored the highest among non-final-year undergraduates (M = 4.06 & M = 4.01, respectively). Students have learned that they should not open links or attachments from unknown senders. The fact that both of these subscales are tightly associated with working environments offers insights into how and in what aspects a workplace or colleagues reshape one's understanding of ISA.

As expected, the full-time internship did affect respondents' cybersecurity *attitude* and ultimately *behaviour*, and the same is true for the full-time work. What is less expected is the extent of the influence on full-time graduates. While the decrease in ISA was moderate for interns, the drop was drastic for employees. This might be because the majority of the working respondents had worked for a number of years. Long-time exposure to work seems to deteriorate ISA seriously. Unfortunately, our sample does not support a deeper analysis of the effect of the length of work, as 80.4% of our respondents were aged between 18 to 25. Young working respondents were targeted to allow for better comparison among the studying, the interns, and the working population. However, the effect of prolonged work exposure is certainly a worthwhile topic that deserves further investigation.

Note that while undergraduates scored much higher than working graduates, their overall ISA is far from exceptional, with most subscales in the three dimensions below 4, the benchmark for adequately good ISA. The results align with previous findings on the internet security of higher education (Rezgui & Marks, 2008; Ulven & Wangen, 2021), suggesting a need for further effort on the young. Nevertheless, the situation for those who exited higher education is much more worrying and may

require a change of coping strategies for corporates and the government, to be discussed in 4.3.

4.2 Theoretical implications

This study adopted the KAB model as we believe that KAB makes better assumptions about ISA due to its emphasis on *knowledge* and item comprehensiveness. However, refinement of the model is necessary as there are certainly other factors at play (Parsons et al., 2014). Hence, an extended KAB model has been proposed, with the influence of SEL posited to moderate the relationship between *knowledge* and *attitude* (see Fig. 1). Results confirm the moderation is statistically significant and show a 67% goodness-of-fit, indicating the model is very good at explaining the stated relationship. However, smaller but significant moderation effects were also found in *knowledge*work exposure* and *attitude*work exposure* acting on *behaviour*, indicating very high pervasiveness of the proposed variable. In other words, SEL has a great negative impact on the formation of *attitude*, and it brings certain direct and indirect changes to *behaviour* too. It is evident that social influence must be incorporated into the KAB model for more accurate evaluation of ISA and the relationship between thoughts and actions. There are also important methodological implications for future research. First, the length of time at work is a quantifiable measure, while national education levels are readily available figures published regularly in many indices. Used together, researchers can objectively measure how society at large influences one's ISA. Along the same vein, the proposed model opens up possibilities for more convenient and accurate cross-national comparisons. It fits existing cross-national findings well (e.g., Berki et al., 2017; Sawaya et al., 2017; Chen & Zahedi, 2016; Zwilling et al., 2020) and can explain why GDP and nationality may fail to predict national ISA consistently.

The current study further confirms normative/social influences (e.g., Heirman et al., 2016; Ifinedo, 2012) but they are approached by comparing differing work exposure conditions for participants with similar backgrounds. Not many ISA studies have focused on the effect of external influence (e.g., Das, 2016; Elkhannoubi & Belaissaoui, 2016; Kam et al., 2020) and evidence is typically flimsy due to methodological limitations (e.g., lack of effective tools to measure social influence, small samples). Further, there have not been any attempts to compare university students with working graduates. Although education as a personal factors has been widely studied (e.g., Aivazpour & Rao, 2020; Chua et al., 2018; Wiley et al., 2020), the same degree holder working in different countries may end up behaving very differently as the social "force" exerted on him/her is constant and powerful. Therefore, results from the predominant ISA studies on personal factors should be viewed in light of the society in case of missing the "bigger picture"; as such, conflicting results may also be better understood.

4.3 Practical implications

While ISA education to undergraduates is important, this study suggests a greater endeavour has to be committed to educating the public at large about cybersecurity and safe internet behaviours. In particular, effort should be put into training those who do not possess a higher-education degree, as they make up the majority of the population that could potentially reshape the ISA of the well-educated. For example, companies should consider offering more training to non-degree holders. They should understand that employees possess varied ICT knowledge. Hence, given their limited resources, a practical strategy would be to maintain the ISA of the better educated, and improve those who lack related ICT knowledge. Recent graduates, who presumably have better ISA, could be mobilised to bring positive ISA influence to experienced staff who might have formed bad cybersecurity habits over time. They may even assume responsibilities in educating colleagues safer ways of using the internet. This, however, would require immense organisation-level support as Chinese value seniority (i.e., length) at work very highly (Fu & Kamenou, 2013), which is also why without such conscious effort, graduates are bound to follow the way of work of the senior.

Given national education level can only improve over a long period of time, it would be unrealistic to expect quick remedies for better ISA. The current strategy of China is to target teacher population in ICT training (Wu, 2014; Zhao & Xu, 2010) so that they can influence the younger generation. However, it is important for the government to promote safe internet behaviours to the general public through social media, online advertisements, TV, government-led talks and workshops, etc. Existing promotional effort is inadequate, and risky online behaviours are common in China (Chen & Zahedi, 2016). Insecure actions, such as visiting unsafe websites for resources and accessing illegal content, are contagious. If many people in the society do the same, even the well-educated ones may follow suit. Elkhannoubi & Belaissaoui (2016) argued that social influence plays a larger role in developing countries than developed countries and suggested more proactive government intervention through promotions of ISA on social media, establishment of cybersecurity policies and cooperation with businesses to initiate a social transformation. Much has yet to be done in China.

4.4 Limitations and recommendations for future research

The current study attempted to collect a larger sample to mitigate the problem of non-random sampling. However, due to different difficulties of data collection, the number of respondents in the three groups ended up being different. Nevertheless, the sufficiently large sample can hopefully minimize any statistical implications. Second, full-time work is taken as an approximation for social education influence. However, the influence can potentially be due to corporate culture, which is hard to quantify. Assuming the 110 companies do not have a common culture, the effect should have been cancelled out by one another. Finally, it is noted that as students progress through their years of study, they may have more opportunities to do

part-time jobs. This factor is not considered because undergraduate part-time jobs are often different in nature, intensity and frequency from full-time internship or work. For example, one typical part-time job for undergraduates is being a cashier at convenience stores. They may not have as much interaction with as many colleagues; they may not even use a computer. Then, there is a problem with time; lengths of part-time jobs vary, unlike the typical 40-hour schedule of full-timers. These differences make it hard to consider part-time work for our purposes.

Apart from the suggestions to conduct multi-national research using the model, future research can investigate how different lengths of work change people's ISA and behaviours. It is hoped that the extended KAB model can add to our understanding of how society shapes people's ISA and be a useful tool of measurement for future investigations. As well, comparisons between high school students, undergraduate students and working individuals, especially in the form of longitudinal studies, are encouraged to understand the big picture and how changes happen.

5 Conclusions

The current study has proposed an extended KAB model, with the *influence of the education level of the society* at large posited to moderate the relationship between *knowledge* and *attitude*. Accordingly, three main hypotheses and three sub-hypotheses were conceived based on the different conditions of respondents. Namely, the non-final-year group represents those who have never been exposed to a full-time working environment, the final-year group have certain exposure, while graduates who are working have prolonged exposure to full-time work. The conditions represent different levels of influence of SEL.

The Human Aspects of Information Security Questionnaire (HAIS-Q) was then adopted to assess the extended KAB model. MANOVA was conducted to analyse the effect of internship and working full-time on the mean scores of *knowledge*, *attitude* and *behaviour.* Results confirm that the influence of SEL does have statistically significant effects on the variables.

Two of the main hypotheses, along with three sub-hypotheses, were confirmed. **H1**—Full-time working graduates and university students of different years of study will not display different cybersecurity *knowledge*—was rejected. The *knowledge* of non-final year students was found to be significantly different from final-year ones and working graduates as well. Final-year students were also found to be significantly different from working graduates.

H2a to **H2c** concerns whether there are significant differences of two variables—*attitude* and *behaviour*—among the three groups of respondents. Apart from *attitude* between non-final-year and final-year students, all other differences were found to be significantly different, with non-final years higher in score than final-years, and final years higher than working graduates.

H3 pertains to the moderation effect of *exposure to full-time working environments* between *knowledge* and *attitude* dimensions. This hypothesis was verified since *knowledge* was found to be a significant predictor of *attitude*, and the interaction between *knowledge* and full-time *work exposure* was also a significant predictor

of *attitude*. Higher exposure to a full-time work environment has a negative influence on ISA *attitude* at varied levels of ISA *knowledge*. However, moderation effect was found, but less strongly, in the interaction of *work exposure*knowledge* and *work exposure*attitude* acting upon *behaviour*. Data support a three-way moderated mediation model.

The current study is one of the first attempts to compare undergraduate students and working graduates and to examine the cognitive and behavioural changes of well-educated individuals. It contributes to methodology, innovates in theorization, and informs practice. The results of this study still require further confirmation from similar studies, but it can certainly provide a reference for future research endeavours.

Appendix A Pilot data regression analysis

Table 7 Overall moderation effect on *attitude* (N = 124)

R	R2	MSE	F	df1	df2	p
.868	.753	.172	71.898	5.000	118.000	.000

Table 8 Moderation analysis of variable effects on *attitude* (N = 124)

Variables	b	se	t	p	LLCI	ULCI
Knowledge	1.033	.100	10.358	.000	.835	1.230
W1	.083	.649	.128	.899	−1.203	1.369
W2	1.831	.607	3.014	.003	.628	3.033
Knowledge*W1	−.005	.174	−.030	.976	−.349	.339
Knowledge*W2	−.694	.205	−3.377	.001	−1.100	−.287

W1 = comparison between average and low work exposure

W2 = comparison between high and low work exposure

Table 9 Moderation effect at different levels of *work exposure* (N = 124)

Work exposure	b	se	t	p	LLCI	ULCI
Low	1.033	.100	10.358	.000	.835	1.230
Medium	1.028	.142	7.226	.000	.746	1.309
High	.339	.180	1.889	.061	−.017	.695

Table 10 Overall mediation effect on *behaviour* (N = 124)

R	R2	MSE	F	df1	df2	p
.895	.800	.068	242.383	2.000	121.000	.000

Table 11 Mediation analysis of variable effects on *behaviour* (N = 124)

Variables	b	se	t	p	LLCI	ULCI
Knowledge	.326	.063	5.181	.000	.202	.451
Attitude	.374	.054	6.876	.000	.266	.481

Table 12 The indirect effect of the moderated mediation of *knowledge* on *behaviour*, mediated by *attitude* and moderated by *work exposure* (N = 124)

Work exposure	Effect	BootSE	BootLLCI	BootULCI
Low	.386	.071	.263	.539
Medium	.384	.104	.212	.618
High	.127	.056	−.009	.221

Table 13 Questions in the employee and student versions of HAIS-Q

Ver.	Knowledge	Attitude	Behaviour
Focus area: Password management			
Employees	It's acceptable to use my social media passwords on my work accounts.	It's safe to use the same password for social media and work accounts.	I use a different password for my social media and work accounts.
	I am allowed to share my work passwords with colleagues.	It's a bad idea to share my work passwords, even if a colleague asks for them.	I share my work passwords with colleagues.
	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters.	I use a combination of letters, numbers and symbols in my work passwords.
Students	It's acceptable to use my social media passwords on my study accounts.	It's safe to use the same password for social media and study accounts.	I use a different password for my social media and study accounts.
	I am allowed to share my study passwords with classmates.	It's a bad idea to share my study passwords, even if a classmate asks for them.	I share my study passwords with classmates.
	A mixture of letters, numbers and symbols is necessary for study passwords.	It's safe to have a study password with just letters.	I use a combination of letters, numbers and symbols in my study passwords.
Focus area: Email use			
Employees	I am allowed to click on any links in emails from people I know.	It's always safe to click on links in emails from people I know.	I don't always click on links in emails just because they come from someone I know.
	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.
	I am allowed to open email attachments from unknown senders.	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Students	I am allowed to click on any links in emails from people I know.	It's always safe to click on links in emails from people I know.	I don't always click on links in emails just because they come from someone I know.
	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.
	I am allowed to open email attachments from unknown senders.	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.

Table 13 (continued)

Ver.	Knowledge	Attitude	Behaviour
Focus area: Internet use			
Employees	I am allowed to download any files onto my work computer if they help me to do my job.	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done.
	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to.
	I am allowed to enter any information on any website if it helps me do my job.	If it helps me to do my job, it doesn't matter what information I put on a website.	I assess the safety of websites before entering information.
Students	I am allowed to download any files onto my study computer if they help me to do my job.	It can be risky to download files on my study computer.	I download any files onto my study computer that will help me get the job done.
	While I am at school, I shouldn't access certain websites.	Just because I can access a website at school, doesn't mean that it's safe.	When accessing the Internet at school, I visit any website that I want to.
	I am allowed to enter any information on any website if it helps my study.	If it helps my study, it doesn't matter what information I put on a website.	I assess the safety of websites before entering information.
Focus area: Social media use			
Employees	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings.
	I can't be fired for something I post on social media.	It doesn't matter if I post things on social media that I wouldn' t normally say in public.	I don't post anything on social media before considering any negative consequences.
	I can post what I want about work on social media.	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media.

Table 13 (continued)

Ver.	Knowledge	Attitude	Behaviour
Students	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings.
	I can't be fired for something I post on social media.	It doesn't matter if I post things on social media that I wouldn' t normally say in public.	I don't post anything on social media before considering any negative consequences.
	I can post what I want about study on social media.	It's risky to post certain information about my study on social media.	I post whatever I want about my study on social media.
Focus area: Mobile devices			
Employees	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute.	When working in a public place, I leave my laptop unattended.
	I am allowed to send sensitive work files via a public Wi-Fi network.	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network.
	When working on a sensitive document. I must ensure that strangers can' t see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Students	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute.	When working in a public place, I leave my laptop unattended.
	I am allowed to send sensitive study files via a public Wi-Fi network.	It's risky to send sensitive study files using a public Wi-Fi network.	I send sensitive study files using a public Wi-Fi network.
	When working on a sensitive document. I must ensure that strangers can' t see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Employees	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.	Disposing of sensitive print-outs by putting them in the rubbish bin is safe.	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place nothing bad can happen if I plug it into my work computer.	I wouldn't plug a USB stick found in a public place into my work computer.
	I am allowed to leave print-outs containing sensitive information on my desk overnight.	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there.

Table 13 (continued)

Ver.	Knowledge	Attitude	Behaviour
Students	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.	Disposing of sensitive print-outs by putting them in the rubbish bin is safe.	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
	If I find a USB stick in a public place, I shouldn't plug it into my study computer.	If I find a USB stick in a public place nothing bad can happen if I plug it into my study computer.	I wouldn't plug a USB stick found in a public place into my study computer.
	I am allowed to leave print-outs containing sensitive information on my desk in the dormitory overnight.	It's risky to leave print-outs that contain sensitive information on my desk in the dormitory overnight.	I leave print-outs that contain sensitive information on my desk in the dormitory when I'm not there.
Focus area: Incident reporting			
Employees	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	If I saw someone acting suspiciously in my workplace, I would do something about it.
	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague.	If I noticed my colleague ignoring security rules, I wouldn't take any action.
	It's optional to report security incidents.	It's risky to ignore security incidents, even if I think they' re not significant.	If I noticed a security incident, I would report it.
Students	If I see someone acting suspiciously in my school, I should report it.	If I ignore someone acting suspiciously in my school, nothing bad can happen.	If I saw someone acting suspiciously in my school, I would do something about it.
	I must not ignore poor security behaviour by my classmates.	Nothing bad can happen if I ignore poor security behaviour by a classmate.	If I noticed my classmate ignoring security rules, I wouldn't take any action.
	It's optional to report security incidents.	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Participants respond to each item on a five-point scale from"Strongly Disagree" to "Strongly Agree"

Funding This work was supported by 2021 Zhejiang Province Philosophy and Social Science Planning Project, "Research on the Integration Model of Industry and Education in Higher Vocational Education in the Yangtze River Delta Region from the Perspective of Industrial Collaborative Agglomeration" 2021 年度浙江省哲学社会科学规划课题 "产业协同集聚视角下长三角区域高职教育产教融合模式研究" [grant number 21NDJC308YBM]; and 2021 Research on the Development Model of "Overseas Chinese Enterprise Generalists" in the Post-epidemic Era后疫情时代"侨企通才"发展模式研究 [grant number RZWKZX-TS005P01].

Declarations

Conflicting interests The authors declare that there is no conflict of interest.

References

Aikins, A. D. G., Boynton, P., & Atanga, L. L. (2010). Developing effective chronic disease interventions in Africa: Insights from Ghana and Cameroon. *Globalization and Health, 6*(1), 1–15. http://www.globalizationandhealth.com/content/6/1/6. Accessed 21 July 2016.

Aivazpour, Z., & Rao, V. S. (2020). Information disclosure and privacy paradox: the role of impulsivity. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 51*(1), 14–36. https://doi.org/10.1145/3380799.3380803

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Anderson, M. J., & Walsh, D. C. (2013). PERMANOVA, ANOSIM, and the mantel test in the face of heterogeneous dispersions: What null hypothesis are you testing? *Ecological Monographs, 83*(4), 557–574. https://doi.org/10.1890/12-2010.1

Berki, E., Kandel, C. S., Zhao, Y., & Chaudhary, S. A. (2017). *Comparative study of cyber-security knowledge in higher education Institutes of Five Countries*. Proceedings of EDULEARN17 Conference 3rd-5th.

Bostan, A., & Akman, İ. (2015). Impact of education on security practices in ICT. *Tehnički Vjesnik, 22*(1), 161–168. https://doi.org/10.17559/TV-20140403122930

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, 88*, 101607. https://doi.org/10.1016/j.cose.2019.101607

Byrne, B. M. (2013). *Structural equation modeling with Mplus: Basic concepts, applications, and programming*. Routledge.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviours and knowledge. *Journal of Information Security and Applications, 42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Carstens, D., Sater, M. C.-B., Pamela, R., et al. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science, 7*, 67–85. http://s.dic.cool/S/qeUrlL1R. Accessed 20 July 2021.

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

Chaudhary, S., Zhao, Y., Berki, E., Valtanen, J., Li, L., Helenius, M., & Mystakidis, S. (2015). A cross-cultural and gender-based perspective for online security: Exploring knowledge, skills and attitudes of higher education students. *IADIS International Journal on WWW/Internet, 13*(1), 57–71. http://s.dic.cool/S/qOiTYTQw. Accessed 20 July 2021.

Chen, Y., & Zahedi, F. (2016). Individual's internet security perceptions and behaviours: Polycontextual contrasts between the United States and China. *Management Information Systems Quarterly, 40*(1), 205–222.

China Internet Network Information Centre. (2021). *The 47th Statistical Report on China's Internet Development* (Report). https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172744.pdf. Accessed 11 July 2021.

Choi, M., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*. https://www.researchgate.net/publication/318710121_The_Role_of_User_Computer_Self-Efficacy_Cybersecurity_Countermeasures_Awareness_and_Cybersecurity_Skills_Influence_on_Computer_Misuse

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Das, S. (2016). Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *It-information. Technology, 58*(5), 237–245. https://doi.org/10.1515/itit-2016-0008

Das, S., Kim, T. H. J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. In 1*0th Symposium On Usable Privacy and Security ({SOUPS} 2014)* (pp. 143–157). https://www.usenix.org/system/files/conference/soups2014/soups14-paper-das.pdfg/system/files/conference/soups2014/soups14-paper-das.pdf

Hoaglin, D. C., & Iglewicz, B. (1987). Fine-Tuning Some Resistant Rules for Outlier Labeling. *Journal of the American Statistical Association, 82*(400), 1147–1149. https://doi.org/10.1080/01621459.1987.10478551

Eifert, G., & Craill, L. (1989). The relationship between affect, behaviour, and cognition in Behavioural and cognitive treatments of depression and phobic anxiety. *Behaviour Change, 6*(2), 96–103. https://doi.org/10.1017/S0813483900007634

Elkhannoubi, H., & Belaissaoui, M. (2016). 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. https://doi.org/10.1109/SETIT.2016.7939834

Fu, Y., & Kamenou, N. (2013). The impact of Chinese cultural values on human resource policies and practices within transnational corporations in China. In *Society and HRM in China* (pp. 56–75). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203723456-7/impact-chinese-cultural-values-human-resource-policies-practices-within-transnational-corporations-china-yu-fu-nicolina-kamenou

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology, 36*(3), 173–192. https://doi.org/10.1080/03601270903183065

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, Behaviour and Social Networking, 20*(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

Hair, J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: Global edition, 7th edition*. Pearson Education International.

Heirman, W., Walrave, M., Vermeulen, A., Ponnet, K., Vandebosch, H., & Hardies, K. (2016). Applying the theory of planned behaviour to adolescents' acceptance of online friendship requests sent by strangers. *Telematics and Informatics, 33*(4), 1119–1129. https://doi.org/10.1016/j.tele.2016.01.002

Huang, X., He, W., Hua, C., & Shang, Y. (2014). 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*(2), 57–67. https://doi.org/10.12677/SA.2014.32009

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*, 2–18. https://doi.org/10.1108/OIR-11-2015-0358

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

International Monetary Fund. (2021). *World Economic Outlook Database*. https://www.imf.org/en/Publications/WEO/weo-database/2021/April/. Accessed 11 July 2021.

Israel, G. D. (1992). *Determining sample size*. University of Florida, University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS.

Kam, H. J., Mattson, T., & Goel, S. (2020). A cross industry study of institutional pressures on organizational effort to raise information security awareness. *Information Systems Frontiers, 22*(5), 1241–1264. https://doi.org/10.1007/s10796-019-09927-9

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association forInformation Systems, 12*(8), 3. https://doi.org/10.17705/1jais.00274

Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective, 22*(4), 171–179. https://doi.org/10.1080/19393555.2013.828803

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kwaa-Aidoo, E. K., & Agbeko, M. (2018). An analysis of information system security of a Ghanaian university. *International Journal of Information Security Science, 7*(2), 90–99.

Li, Y.-L., Li, Y., & Li, A. (2014). 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. http://qbzl.ruc.edu.cn/EN/abstract/abstract669.shtml. Accessed 20 July 2021.

Lipsitz, S., & Parzen, M. (1995). Sample size calculations for non-randomized studies. *Journal of the Royal Statistical Society. Series D (The Statistician), 44*(1), 81–90. https://doi.org/10.2307/2348619

MacKinnon, N. J., & Hoey, J. (2021). Operationalizing the relation between affect and cognition with the somatic transform. *Emotion Review, 13*(3), 245–256. https://doi.org/10.1177/17540739211014946

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*. https://doi.org/10.3127/ajis.v21i0.1697

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security, 26*(3), 277–289. https://doi.org/10.1108/ICS-03-2018-0032

Mei, B., & Brown, G. T. (2018). Conducting online surveys in China. *Social Science Computer Review, 36*(6), 721–734. https://doi.org/10.1177/0894439317729340

Ministry of Education of the People's Republic of China. (2020). 毛入学率达*51.6%* 高等教育更普及了*[Gross admission rate at 51.6%, Tertiary Education is more prevalent]*. http://www.moe.gov.cn/fbh/live/2019/50340/mtbd/201902/t20190227_371425.html. Accessed 2 Aug 2021.

Moody, G. D., Siponen, M., Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security, 34*, 47–66. https://doi.org/10.1016/j.cose.2012.11.004

National Bureau of Statistics of China. (2021). *2020 China statistical yearbook*. China Statistics Press. http://www.stats.gov.cn/tjsj/ndsj/2020/indexeh.htm. Accessed 2 Aug 2021.

Nyblom, P. J. B., Wangen, G., Kianpour, M., & Østby, G. (2020). The root causes of compromised accounts at the University. In *ICISSP* (pp. 540–551). https://doi.org/10.5220/0008972305400551

Ong, L., & Chong, C. (2014). January). Information security awareness: An application of psychological factors–a study in Malaysia. In *2014 International Conference on Computer, Communications and Information Technology (CCIT 2014)*. Atlantis Press. https://doi.org/10.2991/ccit-14.2014.27

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M. R., Butavicius, M. A., & Jerram, C. (2013). In Furnell, S. M., Clarke, N. L. & Katos, V (Eds), *An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations* (pp. 34–44). https://www.researchgate.net/publication/286612263_An_analysis_of_information_security_vulnerabilities_at_three_Australian_government_organisations

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information & Computer Security, 25*(2), 181–189. https://doi.org/10.1108/ICS-03-2017-0017

PwC's Threat Intelligence Centre. (2020). *Cyber Security in Times of Crisis, Asia Pacific SME Survey* [危機時刻的網絡安全--亞太地區中小企業調查報告]. https://www.pwccn.com/zh/issues/cybersecur

ity-and-privacy/research-report-on-the-safety-of-small-and-medium-sized-enterprises-in-the-asia-pacific-region-aug2020.html. Accessed 11 July 2021.

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (pp. 1–17). https://doi.org/10.1145/2335356.2335364

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

Razali, N. M., & Wah, Y. B. (2011). Power comparisons of shapiro-wilk, kolmogorov-smirnov, lilliefors and Anderson-darling tests. *Journal of Statistical Modeling and Analytics, 2*(1), 21–33.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Risk Based Security. (2020). *The 2019 Year-End Report Data Breach QuickView* (Report). https://edtechmagazine.com/higher/article/2020/08/tips-reducing-key-remote-learning-security-risks-perfcon. Accessed 10 July 2021.

Roberts, S. A. (2021). *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors*. Doctoral dissertation, Northcentral University.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behaviour research 1: Personal and social determinants* (pp. 113–132). Plenum Press.

Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A., & Yamada, A. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behaviour. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 2202–2214). https://doi.org/10.1145/3025453.3025926

Schrader, P. G., & Lawless, K. A. (2004). The knowledge, attitudes, & behaviours approach how to evaluate performance and learning in complex environments. *Performance Improvement, 43*(9), 8–15. https://doi.org/10.1002/pfi.4140430905

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). 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).

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Sun, W. (2018). *i*nvestigation 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]. Master's thesis, Dalian University of Technology.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cyber security risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

United Nations Development Programme. (2020). *Human Development Report 2020—The next frontier: Human Development and the Anthropocene*. http://hdr.undp.org/sites/default/files/hdr2020.pdf. Accessed 12 July 2021.

Valente, T. W., Paredes, P., & Poppe, P. R. (1998). Matching the message to the process: The relative ordering of knowledge, attitudes, and practices in behaviour change research. *Human Communication Research, 24*(3), 366–385. https://doi.org/10.1111/j.1468-2958.1998.tb00421.x

Van der Linden, S. (2014). Towards a New Model for Communicating Climate Change. In Cohen, S. A. et al. (Eds) *Understanding and Governing Sustainable Tourism Mobility: Psychological and Behavioural Approaches* (pp. 243–275). http://s.dic.cool/S/FsDq5KQh. Accessed 18 July 2021.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Watson, H., Moju-Igbene, E., Kumari, A., & Das, S. (2020). We hold each other accountable: Unpacking how social groups approach cybersecurity and privacy together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp 1–12). https://doi.org/10.1145/3313831.3376605

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Worsley, A. (2002). Nutrition knowledge and food consumption: Can nutrition knowledge change food behaviour? *Asia Pacific Journal of Clinical Nutrition, 11*, S579–S585. https://doi.org/10.1046/j.1440-6047.11.supp3.7.x

Wu, D. (2014). An Introduction to ICT in Education in China. In Huang, R., Kinshuk, & Price, J. (Eds.), *ICT in Education in Global Context. Lecture Notes in Educational Technology* (pp. 65-84). Springer. https://doi.org/10.1007/978-3-662-43927-2_5

Wu, J., Zhang, F., Sun, Y., Zhu, Y. B., & Liu, C. X. (2020). Fight against COVID-19 promotes China's digital transformation: Opportunities and challenges [抗疫情助推我国数字化转型: 机遇与挑战]. *Journal of Chinese Academy of Sciences, 35*(3), 306–311. https://doi.org/10.16418/j.issn.1000-3045.20200229002

Zhao, J., & Xu, F. (2010). The state of ICT education in China: A literature review. *Frontiers of Education in China, 5*(1), 50–73. https://doi.org/10.1007/s11516-010-0006-1

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2020.1712269

Authors and Affiliations

Wilson Cheong Hin Hong[1] · ChunYang Chi[2] · Jia Liu[3] · YunFeng Zhang[4] · Vivian Ngan-Lin Lei[5] · XiaoShu Xu[6]

Wilson Cheong Hin Hong
wilsonhong@ift.edu.mo

ChunYang Chi
Chichunyang@wzpt.edu.cn

Jia Liu
amyliu@zmu.edu.cn

YunFeng Zhang
zhangyunfeng@ipm.edu.mo

Vivian Ngan-Lin Lei
vivianlei@ipm.edu.mo

1 Centre for Teaching and Learning Enhancement, Macao Institute for Tourism Studies, Colina de Mong-Ha, Macao, SAR, China

2 Editorial Department of Journal, Wenzhou Polytechnic, Wenzhou City, Zhejiang Province, China

3 Department of Foreign Studies, Zunyi Medical University Zhuhai Campus, Zhuhai City, Guangdong Province, China

4 Centre for Portuguese Studies, Macau Polytechnic University, R. de Luís Gonzaga Gomes, Macao, China

5 Macao Polytechnic University, Rua de Luís Gonzaga Gomes, Macao, China

6 School of Foreign Studies, Wenzhou University, Wenzhou City, Zhejiang Province, China