Exploring Chinese college students' awareness of information security in the COVID-19 era

Xinran Wang

University of Malaya

Abstract

The focus of this research was to look into the information security awareness of Chinese university students during the COVID-19 pandemic and make recommendations based on the survey's findings and research literature. The quantitative method is applied in this study. 111 Chinese college students were randomly sampled and requested to answer a Likert information security awareness questionnaire. The descriptive analysis of the data in this study is also done with SPSS. The findings revealed that the vast majority of college students know the significance of information security awareness and have basic information security awareness, based on the data collected.However, some students have not participated in relevant training courses, and many college students do not pay enough attention to personal information security, resulting in poor performance in areas such as files and passwords. As a result, effective solutions such as information security training projects are required to address the current deficiencies. The findings of this study have implications for university administrators and policymakers in terms of how to raise students' awareness of the security of their online learning information. The study should use mixed methods and large sample sizes in the future to provide more detailed and comprehensive survey data, and more credible evidence of college students' information security awareness.

Keywords: Information security awareness; College students; Information security

1. Introduction

On March 11, 2020, the Director-General of the World Health Organization (WHO) declared COVID-19 a global pandemic. The spread of covid-19 has put pressure on all sectors of society, for example, the use of telemedicine has greatly increased as the pressure on traditional medicine has increased(HealthCare & Somerville). Similarly, in education, the covid-19 pandemic affects more than 91% of students worldwide(Henaku, 2020). As a result, many schools and universities around the

world have adopted online learning and use many online learning platforms and online communication software(Crawford et al., 2020).

Although many schools are transitioning from face-to-face to online learning promptly, various schools are actively using online communication and learning platforms, and the education system is striving to provide quality education to students, however, online teaching is a completely different teaching experience for many teachers and students compared to traditional teaching methods, and different populations have different adaptations to online learning(Pokhrel & Chhetri, 2021). As a result, more and more problems are identified in the process of online learning (Dumford & Miller, 2018). Specifically, many students' academic performance decreases due to the lack of consultation with teachers(Subedi et al., 2020). There are also many developing countries where students have difficulty affording the equipment to study online, for example, in Colombia, only 34% of students have access to computers for online learning at home(Henaku, 2020). Less than 50% of households in rural areas of Georgia have access to computers(Subedi et al., 2020). Another issue that should not be overlooked is the exposure of the online learning environment to ongoing Internet security threats, which may involve risks such as the destruction of educational assets or unauthorized changes to the information(Chen & He, 2013).

Graf (2002) mentioned that the security of student information in online learning is frequently at risk, such as the loss and exposure of critical information. Online learning programs usually employ security protection mechanisms, yet problems such as manipulation and theft of information by outsiders still occur at times(Graf, 2002). Some researchers have explained the information security threats of online learning from the user perspective and the management perspective, where reckless human behavior is one of the main causes of information security threats in online learning(Chen & He, 2013). For example, when interacting with one another, college students frequently unintentionally exchange personal information that should be protected, and they share student ID numbers and passwords with their friends on social media, demonstrating a lack of awareness of personal information security that may stem from a "childish" student culture(Allen, 2011). Because students are generally nomadic and have less credit history than more mature individuals, college students are regarded to be a group at more risk for information security(Marks, 2007).

The main reason for e-learning security problems involves users not knowing the rules of information security very well, which results in wrong security behaviors and at the same time lack of appropriate guidance(Chen & He, 2013). Moreover, research has revealed that human mistake is regarded as one of the most serious concealed dangers to the security of information assets in businesses(Whitman & Mattord, 2021). The cost of user misbehavior can be higher than the cost of building a security system (Gómez Cárdenas & Sánchez, 2005). Therefore students must consider the

security of their personal information and raise awareness of information security when conducting online learning(Chen & He, 2013). Developing an IT security awareness program is critical to ensuring the security of student, faculty, and academic data(Ellison, 2007).

As a result, the goal of this study is to assess college students' present degree of information security awareness. Also, make recommendations on how to improve college students' information security awareness in order to serve as a reference for the construction of college information security programs.

2.0 Literature review

2.1 Information Security

Information security is defined by McDaniel and McDaniel (1994) as concepts, skills, technological solutions, and administrative measures used to prevent unauthorized access, destruction, exposure, manipulation, modification, and loss of information assets. Software, hardware, data, users, processes, and networks are the six elements of information systems; however, users and processes are sometimes overlooked when it comes to information security (Dlamini et al., 2009; Maconachy et al., 2001).

Information security is defined as the capacity of authorized users to access learning resources without being compromised in online learning (Adams & Blanford, 2003). Confidentiality, integrity, and availability are the three essential prerequisites for security (Weippl & Ebner, 2008). Confidentiality refers to the fact that information is not accessible to unauthorized individuals and is not vulnerable to an unlawful disclosure; Integrity refers to the fact that information is accurate and complete and is not subject to unauthorized manipulation or destruction. Availability refers to the ability for already authorized users to access and use information whenever they need it, guaranteeing that it is available.

Many academics have been concerned about information security as the Internet has grown(Höne & Eloff, 2002), In the sphere of education, information security is one of the most significant aspects of education digitization, which necessitates extensive preparation and investment. Due to the stability and public welfare of the education industry, the leakage of its data does not lead to direct economic loss by losing a large number of customers like financial and other industries, but precisely because of the low cost of data leakage of individuals in the education industry, to a certain extent, it will weaken the importance of schools to the information security of online education and may further trigger a crisis of public trust in the information security of online education.

2.2 Information security awareness in the context of education

Information security awareness is defined as the user's realization of the importance of information security (Siponen, 2000) It mainly changes the security behavior of individuals(Taha & Dahabiyeh, 2021). With the increasingly digital educational

environment and the widespread use of online courses during the covid-19 period, it has become particularly important to create a safe and secure online learning environment(Taha & Dahabiyeh, 2021).

Several previous researchers have highlighted the importance of information security awareness(Hadlington et al., 2021; Wiley et al., 2020). Some studies have focused on the information security challenges faced by online learning, including malware attacks, unauthorized access to learning content, etc(Kambourakis, 2013; Shonola & Joy, 2014). Furthermore, the usage of cloud computing services (for example, Google Drive) in education creates information security vulnerabilities because educational institutions have no control over these cloud computing service platforms(Kambourakis, 2013). And schools also have no security control over the personal devices used by students in the learning process (Monrad, 2019). In other words, in the process of online learning, educational institutions are faced with many information security risks that they cannot control. In addition, nowadays, there are many students and teachers who use social media sites (e.g., Facebook, Twitter, etc.) to support teacher-student collaboration in online courses, etc.(He, 2011), however, many teachers and students are careless, so these sites are a major source of information security risks, and personal data posted on social media may be misused(Patel et al., 2012).

Therefore, many scholars have further studied the security awareness of users in educational institutions so that users can reduce the occurrence of insecure times such as information leakage in terms of their own use(Gharieb, 2021). Specifically, Kim (2014) suggests the need for universities to provide information security awareness training to students. a study by Yoon et al. (2012) also shows that both security awareness education and awareness of the seriousness of information security issues have an impact on students' information security awareness. Therefore, schools need to strengthen information security education for students and develop good security habits (Yoon et al., 2012), however, early studies found that only a few universities give information security awareness training to students (North et al., 2006).

With advances in technology and concepts, many developed countries, including the United States, are making efforts to strengthen public awareness of information security and are urging university leaders to take appropriate measures to protect the university's information network (Roach, 2001). For example, in 2014, California enacted the "Eraser Law" - the Student Online Personal Information Protection Act - which classifies content generated by students on social media, online services, and mobile software as personal data privacy, and online service operators are required to remove information posted on web pages by minors within a specified time frame(Wang, 2016). This statute was later borrowed by several U.S. states as a reference for legislation on educational information security (Molnar & Boninger, 2015). In addition, the EU adopted the General Data Protection Regulation in 2016,

which has had a global impact and can be applied to institutions that process student data as well as third-party service providers to provide clear regulation of their data operations, organizations are required to collect and use personal data lawfully and to provide appropriate privacy protections. (Steiner et al., 2015). However, studies have shown that the development of information security awareness may face more obstacles in developing countries, and the lack of socio-cultural environment and resources, and knowledge may create a gap between the development of this area and developed countries(Rezgui & Marks, 2008). Therefore more feasible measures are needed to narrow these gaps.

Siponen (2000) mentioned that despite the general recognition of information security awareness, there are fewer studies with depth, probably because of the momentary non-technical nature of information security awareness. Thus the number of studies considering information security awareness is currently relatively limited, especially in higher education settings(Rezgui & Marks, 2008). Overall, scholars have proposed various information security risks, and solutions to mitigate online learning risks, but there is currently a lack of attention and research on increasing students' information security awareness.

3.0 Research method

3.1 Research Design

The purpose of this study was to explore college students' awareness of information security during their online learning process during the New Crown. A quantitative research method was selected for this study. This is because its purpose is to ask narrow objective questions and generate quantitative data that can be analyzed using statistics (Weippl & Ebner, 2008).

3.2 Participants

The study used a quantitative method. Students' security information awareness was considered as a variable that could be measured by a questionnaire. A convenience sampling technique was used in this study and 111 students from different universities in different regions of China participated in this questionnaire. The researcher used an online questionnaire to conduct the survey and it was conducted in March 2022. In terms of ethical considerations, an information sheet was added before completing the questionnaire to clarify the main purpose of the survey and to seek students' consent to participate in the study. It was also emphasized that participation was completely voluntary and anonymous and that withdrawal from the study was possible at any time.

3.3 Research Instruments and Procedures

In this study, a questionnaire was distributed to investigate the information security awareness of college students. A questionnaire consisted of two parts, the first part was demographic information including the age and gender of the participants and whether they had attended security awareness training, and the second part was questions related to the participants' information security awareness. The questionnaire in this study was designed using the questionnaire established in the study of Kim (2014). These 17 items were tested on students using a Likert scale, and a Likert-type 5-point scale ranging from strongly disagree (1) to strongly agree (5) was supplied as answer possibilities for all items, with just one response allowed for each item. Data were collected and then analyzed using descriptive statistics. In this study, 17 items were selected for a questionnaire survey based on previous scholars' studies(Kim, 2014), including：

- Require the usage of an anti-virus program;
- Require the frequent upgrading of virus definitions;
- Require the regular scanning of a computer and storage media;
- Require the use of a personal firewall;
- Require the installation of software patches;
- Require the use of pop-up blockers;
- Be aware of the risks of downloading files or programs.
- Recognize the dangers of peer-to-peer (P2P) file-sharing;
- Recognize the dangers of clicking on links in e-mails;
- Be aware of the dangers of e-mailing passwords;
- Be aware of the dangers of e-mail attachments;
- Back up vital files regularly;
- Be aware of the dangers of smartphone viruses;
- The requirement for a smartphone anti-virus application;
- Understand the features of a strong password;
- Use various passwords for various systems;
- Change your passwords on a frequent basis.

3.4 Reliability and validity of the study

Reliability describes the precision of the measurement, and reliability will be assessed by the Cronbach alpha coefficient, and the reliability result of the questionnaire used in this study was 0.859, so the questionnaire has high reliability and is suitable for distribution to respondents(Cronbach, 1957).

The validity was further evaluated, and the KMO and Bartlett coefficient tests of the sample data using factor analysis in SPSS 26.0 in this study showed a result of 0.796, which to some extent indicates the high validity of the measurement model.

3.5 Data analysis

The data was analyzed using SPSS version 26 to produce a descriptive analysis of the results, including mean and standard deviation scores, to determine the level of students' information security awareness.

The information concentration of the 17 question items was explored first using factor analysis, and the SPSS output revealed that the KMO value was 0.796, which was more than 0.6, satisfying the prerequisite requirements for factor analysis and implying that the data could be used for factor analysis study. The data also passed the Bartlett sphericity test ($p<0.05$), indicating that it was suitable for factor analysis(As illustrated in the table).

KMO and Bartlett's Test			
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.796	
Bartlett's Test of Sphericity		Approx. Chi-Square	763.111
		df	136
		Sig.	.000

Fig. 1.KOM and Bartlett's test

In this study, factor analysis was used to obtain five factors (factor loading coefficients > 0.4) based on the criterion of eigenvalue one, and only those factors with eigenvalues greater than one were considered significant.

The first five components can explain 67.3 percent of the variation with eigenvalues greater than one, according to the findings. A single factor accounts for 16.46% of the variance, a second factor for 13.95% of the variance, a third factor for 13.64% of the variance, and the fourth factor for 12.71% of the variance, and the fifth factor for 10.54% of the variance. To identify the relationship between the factors and the study items, the final data of this study was rotated using the varimax approach. The correspondence between the factors and the study items was then assessed after confirming that the factors could extract the majority of the information content of the study items. By correlating the five factors with the question items, the five factors were named; factor one was email and mobile security, factor two was information system security awareness, factor three was the security of files and passwords, and factor four was cyberattacks, and factor five was browser security. These five aspects represent the current security awareness issues of the respondents.

4.0 Results and Discussion

This section provides the results of the study, which focuses on the analysis of the questionnaires collected from the online survey through descriptive statistics. The first part of the questionnaire consisted of demographic information and questions about whether or not they had attended an information security awareness course.

In terms of the gender of demographic information, 81 (73%) of the participants were female and 30 (27%) were male (As shown in Fig. 2). In terms of grade composition, 9 (8%) were first-year students, 25 (23%) were sophomores, 20 (18%) were juniors, 43 (39%) were seniors, and 13 (12%) graduate students, and 1 (0.9%) doctoral student participated in this questionnaire(As shown in Fig. 3).

	Frequency	Percent(%)
Female	81	73
Male	30	27
Total	111	100

Fig. 2. Gender

	Frequency	Percent(%)
Postgraduate	13	11.7
Fourth-year	43	38.7
Third-year	20	18
Second-year	25	22.5
First-year	9	8.1
Doctor	1	0.9
Total	111	100

Fig. 3. Grade Level

First of all, students were surveyed whether they had attended courses and training related to information security awareness (as shown in the table), and 80 (72%) respondents indicated that they had attended related courses, so it can be found that most college students are educated about information security awareness.

	Frequency	Percent(%)

Never attended	31	27.9
Attended	80	72.1
Total	111	100

Fig. 4. Attended or never attended

Furthermore, Figure 5 shows the means and standard deviations of the five dimensions of college students' information security awareness, and the data shows that students have a high level of awareness in terms of information system security perceptions but a poor level of security awareness in terms of files and passwords.

Dimensions	Mean	Std. Deviation
Information System Security Awareness	4.4204	0.63199
Email and Mobile Security	3.8198	0.75692
Browser Security	3.7568	1.07209
Cyber Attack	3.7538	0.87005
File and Password Security	3.3183	0.70157
Total	3.7334	.54301

Fig. 5. Mean and Std. deviation

Overall the level of information security awareness among college students is relatively high (M=3.73). Specifically, in the aspect of information system security awareness, the vast majority of students agreed that schools should install relevant information security procedures and the importance of information security knowledge, and the mean score of this dimension was 4.42, which was considered to be the highest mean score, indicating that students' information security awareness in this area is high.

The second dimension is email and mobile security, and the results of the study found that most students are already aware of the information risks of email and the virus risks of mobile devices. Also the average score for this dimension was 3.82, which is also a relatively high score, indicating that students are more aware of information security in this area. However, the score of one of the questions about the risk of email attachments was low, with only 66 (59%) students recognizing the information risk

of email attachments, indicating that many students are still very unfamiliar with the risk of email attachments.

The mean scores for cyber attacks and browser security are relatively close, at 3.75 and 3.76 respectively. However, some students did not seem to have a good understanding of some of these information security items. For example, out of 111 respondents, only about 61 would install software patches, 65 would use a personal firewall and 66 would use a pop-up blocker. This means that nearly half of the respondents are not aware of these items and they do not take effective actions to protect their personal information, which may bring many threats to information security. In addition, in the dimension of cyber attack, the question about checking and scanning electronic devices at regular intervals scored better, with only 7% of people having no relevant awareness. This may be because security software has developed better in recent years and it has become more convenient for users to check the security of their devices. According to the 2013 China Internet User Information Security Report released by the China Internet Network Information Center (CNNIC), 96.5% of users have installed security software on their computers and 70% of users have downloaded security software on their cell phones. This brings convenient conditions for checking and scanning electronic devices.

The lowest scoring dimensions were file and password security. One of the lowest scoring items was changing passwords for each software regularly, with only 24 people (21%) changing their passwords regularly. Students are also unaware of the dangers of P2P file sharing, with only 36 (32%) saying they are more aware of the risks of file sharing. Also just under half (44%) of respondents said they use different passwords for different software. In the file backup item, 33 (30%) individuals said they do not regularly back up their files. Knowledge of strong passwords and awareness of file downloading risks, which are also in this dimension, performed slightly better, with only 15% and 11% of people not having relevant security awareness, respectively.

In general, students are aware of general security threats and protection procedures. Nevertheless, they do not make sufficient efforts to protect their devices or information and do not follow good information security practices.

5.0 Recommendations

Although students score well in the awareness of information security system, there is still a certain percentage of students who lack the relevant awareness that cannot be ignored, and schools and relevant education policymakers should increase the dissemination of relevant knowledge. At the same time, information awareness education activities should be carried out to make students fully aware of the necessity of information security systems, and relevant knowledge should be updated and publicized at all times.

In the second place, the university should provide relevant information security awareness training to college students, and previous literature has suggested two ways to improve information security, including a sanctions-based approach and information security awareness training (Siponen et al., 2007). This study is concerned with information security awareness training(Siponen, 2000). The purpose of information security awareness training is to encourage and stimulate users to consider information security and the significance of information security measures(Gardner, 2006). In addition, lack of training is regarded as the leading cause of inadequate reaction plans(Coopers, 2013).If college students are not familiar with the school's information security policies and rules, they will not be aware of the potential information risks in the school and correctly maintain personal information security(Kim, 2014). Because problems might occur as a result of a lack of personal knowledge, abilities, and attitudes, training becomes an effective type of intervention(King et al., 2001). Planning, organizing, implementing, reviewing, and following up are the four processes of effective training(Vincent & Ross, 2001). In response to the current situation that students do not have a comprehensive understanding of e-mail risks, it is suggested that each university can carry out relevant thematic training, targeted training, and assessment of college students' general knowledge of e-mail information security, etc., to ensure that students can use online communication platforms such as e-mail under the premise of ensuring their own personal information security.

Furthermore, an effective security awareness campaign should concentrate on how users develop long-term security practices(Okenyi & Owens, 2007). What can be found from the survey is that respondents generally scored low on personal information security behaviors, such as using software patches, using personal firewalls, and pop-up blockers. This indicates that even though students have some awareness of security procedures, they still do not have enough security behaviors in their personal practices. Schools or education authorities should provide targeted training and teaching on the means of personal information protection to ensure that students are able to defend themselves against cyber attacks. Overall, security awareness efforts aim to change behaviors and reinforce good practices among students; awareness does not practice, and the purpose of strengthening information security awareness is simply to focus attention on security, while the skills students acquire during training are based on awareness(Wilson & Hash, 2003). Only by improving students' information security awareness through training can their information security behavior be further promoted.

The worst performing areas of file sharing and passwords need to be given sufficient attention. Few students pay much attention to the security of private passwords, often using one password for a long time and using the same password for multiple platforms at the same time, and without sufficient awareness of file downloading and sharing. This may be due to the popularity of social software, where it has become easy for students to share their information online, yet this may introduce some

computer viruses as well as violate copyright laws because the content shared is not in the public domain(Kim, 2014). To address these specific issues, schools should regularly measure students' security awareness levels to provide targeted training to provide students with the training content they need.

Since it is still during the covid-19 pandemic, information security awareness training does not need to use traditional face-to-face courses at all; virtual training (online courses or video-recorded training) can be used to allow students to attend the training more easily and to control training costs for both the organizers and the students. This is because budget constraints are also a significant barrier to information security awareness programs(Chen, 2009).

Schools should also encourage college students to read books, publications and other materials about network information security through school libraries, mobile phone electronic reading rooms, etc., or arrange online courses on related contents, etc., or provide relevant elective courses, so as to broaden the channels for college students to obtain knowledge about network information security.

In addition, schools need to take effective measures to truly engage students in training, such as making virtual training in information security awareness a graduation requirement, automatically alerting students to personal information security tips when they log into learning platforms or school programs, or holding regular webinars to promote information security knowledge. In addition, information security awareness training programs need to be updated as technology evolves and new security threats emerge so as to maximize the protection of teachers' and students' personal information.

6.0 Conclusion

It is a necessity that online instruction requires students to have a high level of information security awareness. The results of this study showed the level of information security awareness among Chinese college students. The analysis revealed that students generally have some awareness of information security and can take some basic precautions, but their personal practices are not sufficient, with a significant lack of security awareness in file sharing and password security, and a lack of personal awareness of the risks of cyberattacks.

In consideration of these findings, higher education institutions should provide targeted information security awareness to students, such as conducting information security training programs, updating relevant precautionary knowledge, and setting security tips on school websites, in order to help students improve their own information security awareness and prevent threats to their personal information.

However, there are limitations to this study. Firstly, this study was limited to the students' perspective, so future studies should also consider the teachers' and principals' perspectives. Secondly, the current study was limited to a quantitative

study with data from a random sample of 111 college students. Therefore future research could involve a larger sample size to ensure the presentability and generalizability of the data. In addition, interviews are needed to further explore and explain the possible reasons for these findings.

References

[1] Adams, A., & Blanford, A. (2003). Security and online learning: to protect and prohibit. In Usability evaluation of online learning programs (pp. 331-359). IGI Global.
[2] Allen, G. (2011). Hitting the ground running. Security, 48(12), 44-45.
[3] Chen, C. (2009). The Impact Of Information Richness On Information Security Awareness Training Effectiveness NC Docks].
[4] Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. International Review of Research in Open and Distributed Learning, 14(5), 108-127.
[5] Coopers, P. (2013). Key findings from the Global State of Information Security Survey 2013. Changing the game.
[6] Crawford, J., Butler-Henderson, K., Rudolph, J., Malkawi, B., Glowatz, M., Burton, R., Magni, P., & Lam, S. (2020). COVID-19: 20 countries' higher education intra-period digital pedagogy responses. Journal of Applied Learning & Teaching, 3(1), 1-20.
[7] Cronbach, L. J. (1957). The two disciplines of scientific psychology. American psychologist, 12(11), 671.
[8] Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. Computers & security, 28(3-4), 189-198.
[9] Dumford, A. D., & Miller, A. L. (2018). Online learning in higher education: exploring advantages and disadvantages for engagement. Journal of Computing in Higher Education, 30(3), 452-465.
[10] Ellison, N. (2007). Facebook use on campus: A social capital perspective on social network sites. ECAR Symposium, Boca Raton, FL,
[11] Gardner, H. (2006). Changing minds: The art and science of changing our own and other peoples minds. Harvard Business Review Press.
[12] Gharieb, M. E. (2021). Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah Al-Mukarramah-Saudi Arabia. International Journal of Computer Science & Network Security, 21(8), 360-368.
[13] Gómez Cárdenas, R., & Sánchez, E. M. (2005). Security challenges of distributed e-learning systems. International Symposium and School on Advancex Distributed Systems,
[14] Graf, F. (2002). Providing security for eLearning. Computers & Graphics, 26(2), 355-365.

[15] Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. Computers in Human Behavior, 114, 106557.
[16] He, W. (2011). Using wikis to enhance website peer evaluation in an online website development course: An exploratory study. Journal of Information Technology Education, 10, IIP236-IIP247.
[17] HealthCare, P., & Somerville, M. Telemedicine, Privacy, and Information Security in the Age of COVID-19.
[18] Henaku, E. A. (2020). COVID-19 online learning experience of college students: The case of Ghana. International Journal of Multidisciplinary Sciences and Advanced Technology, 1(2), 54-62.
[19] Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? Computers & security, 21(5), 402-409.
[20] Kambourakis, G. (2013). Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. International Journal of u-and e-Service, Science and Technology, 6(3), 67-84.
[21] Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security.
[22] King, S. B., King, M., & Rothwell, W. J. (2001). The Complete Guide to Training Delivery: A Competency-Based Approach. ERIC.
[23] Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). A model for information assurance: An integrated approach. Proceedings of the 2001 IEEE workshop on information assurance and security,
[24] Marks, A. A. (2007). Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research Salford: University of Salford].
[25] McDaniel, G., & McDaniel, G. (1994). IBM dictionary of computing.
[26] Molnar, A., & Boninger, F. (2015). On the Block: Student Data and Privacy in the Digital Age--The Seventheenth Annual Report on Schoolhouse Commercializing Trends, 2013-2014. National Education Policy Center.
[27] Monrad, J. (2019). Universities fall into the cross hairs of cyber attacks. Infosecurity-magazine. com. https://www. infosecuritymagazine. com/opinions/universities-attackers/(accessed Jan. 13, 2022).
[28] North, M. M., George, R., & North, S. M. (2006). Computer Security and ethics awareness in university environments: A challenge for management of information systems. Proceedings of the 44th annual Southeast regional conference,
[29] Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. Information Systems Security, 16(6), 302-314.
[30] Patel, A., Taghavi, M., Júnior, J. C., Latih, R., & Zin, A. M. (2012). Safety measures for social computing in wiki learning environment. International Journal of Information Security and Privacy (IJISP), 6(2), 1-15.

[31] Pokhrel, S., & Chhetri, R. (2021). A literature review on impact of COVID-19 pandemic on teaching and learning. Higher Education for the Future, 8(1), 133-141.
[32] Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & security, 27(7-8), 241-253.
[33] Roach, R. (2001). Ringing the alarm on campus computer security. Diverse Issues in Higher Education, 18(20), 50.
[34] Shonola, S. A., & Joy, M. (2014). Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)'. 6th International conference on education and new learning technologies,
[35] Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. IFIP International Information Security Conference,
[36] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security.
[37] Steiner, C. M., Kickmeier-Rust, M. D., & Albert, D. (2015). Let's talk ethics: Privacy and data protection framework for a learning analytics toolbox. Ethics and Privacy in Learning Analytics (# EP4LA), Poughkeepsie, NY.
[38] Subedi, S., Nayaju, S., Subedi, S., Shah, S. K., & Shah, J. M. (2020). Impact of E-learning during COVID-19 pandemic among nursing students and teachers of Nepal. International Journal of Science and Healthcare Research, 5(3), 68-76.
[39] Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721-1736.
[40] Vincent, A., & Ross, D. (2001). Personalize training: determine learning styles, personality types and multiple intelligences online. The Learning Organization.
[41] Wang, Z. (2016). U.S. Student Data Privacy Protection Legislation and Governance System in the Era of Big Data. Comparative Education Research(11), 28-33.
[42] Weippl, E. R., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education,
[43] Whitman, M. E., & Mattord, H. J. (2021). Principles of information security. Cengage Learning.
[44] Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & security, 88, 101640.
[45] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special publication, 800(50), 1-39.
[46] Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. Journal of information systems education, 23(4), 407-416.