Data Security Awareness in Online Learning

Rosilah Hassan[1]
Center for Cyber Security
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
Bangi, Malaysia

Wahiza Wahi[2]
School of Liberal Studies (CITRA-UKM)
Universiti Kebangsaan Malaysia
Bangi, Selangor

Nurul Halimatul Asmak Ismail[3]
Department of Computer Science and Information
Technology, Applied College
Princess Nourah bint Abdulrahman University
Riyadh, Kingdom of Saudi Arabia

Samer Adnan Bani Awwad[4]
Deanship of Information and Communication Technology
Imam Abdulrahman Bin Faisal University
Dammam, Kingdom of Saudi Arabia

***Abstract*—The Covid-19 pandemic has intensified the online learning activities, which have becoming the most crucial platforms for learning sessions. With these online learning activities, a major concern arises particularly on the security of educators and students' data. Every element in an online learning system can be a potential target of hacking or attack. Therefore, this paper examines students' awareness of data security in online learning. Google forms have been used to gather the students' feedback. Forty-two (42) students, involving the secondary school, pre-university and university students, responded to the survey questions. The results show that most of the respondents are well aware of how to keep their data safe in online learning. It is discovered that the level of awareness about data security in online learning amongst the students is commendable. The findings of this study indicate there are various ways to secure students' data especially during online learning.**

***Keywords*—Covid-19; IR4.0; education 4.0; online learning; data security**

I. Introduction

The massive spread of Covid-19 virus has disrupted many human activities all around the globe. One common daily activity, which has been significantly affected by Covid-19, is education. The Covid-19 pandemic has caused UNICEF, WHO, and IFRC to appeal when the virus situation spreads rapidly, schools must be closed in the 'Prevention and Control of Covid-19' spreading in schools [1]. On 8th April 2020, it was reported that 220 million post-secondary students across 175 countries [2] had experienced severe disruptions to their education given that their colleges and universities were forced to shut down in order to stop the spread of the virus [3]. This represents 13 percent of the total number of students affected globally [4]. Hence, most educational institutions have opted for online learning platforms to ensure that learning sessions continue to operate within the pandemic [5, 6].

Online learning is "a type of delivery method used in distance education that allows synchronous and asynchronous exchanges of resource over a communication network" [7] by using various devices with internet access such as mobile phone, laptops, and computer [8, 9]. Online learning is seen as a tangible form of technological development that is not restricted to the current 4.0 Industrial Revolution (4IR) only [10]. Haseeb (2018) denotes that online learning is one of the important aspects for future education or Education 4.0 to produce highly creative graduates [11]. The Education 4.0 is a global framework introduced by the World Economic Forum (2020) to ensure a high-quality education within the context of the 4IR and the future of the new global economy and society [12]. For example, the 4IR has observed that learners play a critical part in their learning activities, as well as a flexibility in the method and ambience of learning provided to them in many online classes given by higher learning institutions [13].

It is apparent that the current and future of education relies greatly on the use of advanced technology and automation whereby online learning plays a central role [14]. Fig. 1 illustrates the major trends of Education 4.0.

In fact, the Covid-19 pandemic has brought about tremendous challenges on students having to go through online learning sessions [15]. According to Chung et al. [16], the pandemic's quick shifts have had a significant impact on students and lecturers at higher education institutions critically. Many lecturers and students in schools all around the world have expressed their frustrations with adopting online learning platforms for teaching and learning. The ramifications of this epidemic are unexpected, according to Shahzad et al. [17], and it has transformed the education system into a new teaching and learning paradigm.

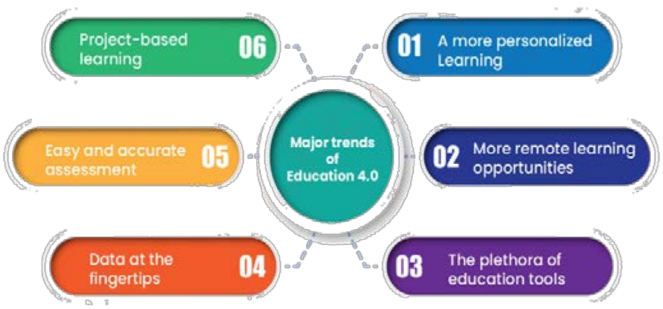
Project-based learning
06
01
A more personalized Learning
Easy and accurate assessment
05
Major trends of Education 4.0
02
More remote learning opportunities
Data at the fingertips
04
03
The plethora of education tools

Fig. 1. Major Trends of Education 4.0.

This paper is granted under the Dana Impak Perdana UKM DIP-2018-040.

Indeed, various aspects of the new education system such as the curriculum, the role of educators, student positions as well as assessments have been modified to cope with current trends [18, 19]. For instance, educators need to fill in students' data and update them constantly. Students, on the other hand, need to access their online learning platform persistently to obtain information and instructions related to their assignments and exercises. When everything is done online, the data security of educators and students has becoming a crucial concern. This is especially true when the users commit malicious acts and access the data illegally. These malicious acts include instilling viruses and malicious code such as worms and Trojan horses into the device with the intent to steal users' information. Every component of an online learning system is vulnerable to hackers or attacks.

Data security is to protect valuable and sensitive personal data such as email and bank information. Valuable data comprise of educational information that collected, stored and managed by universities as well as confidential information such as financial data, phone numbers, and sensitive personal information about students' personal life and family data are the goldmine for hackers. In data security, the processes and technologies should be used to safeguard the data is a crucial element in protecting personal data at best. The created, collected, stored, and exchanged data is a valuable asset. Safeguarding data from corruption and unauthorized access by internal or external hackers protects individual's data from being stolen and used without his or her consent and knowledge.

Researchers have devised a number of remedies and methods to increase security in online learning in response to rising dangers, particularly during current epidemic. This paper reports on a study that investigated students' understanding on data security as they are taking online learning during the Covid-19 pandemic. The reminder of this paper is organized as follows; Section II presents related works on online learning and data security, Section III describes methodology, Section IV depicts results and discussion, and Section V concludes the paper.

II. Related Work

A. Online Learning

Online learning refers to the teaching and learning method carried out in a web-based environment [20]. With access to the internet, the learning process can be conducted anywhere and anytime with the use of gadgets or online platforms which are accessible by any users. There are various teaching and learning applications available on the internet such as Google Classroom, Google Meet, Microsoft Teams, Skype, WhatsApp, and Zoom. Most educators and students depending on their own teaching and learning needs utilize these applications.

The occurrence of the Covid-19 pandemic has instigated the implementation of online learning on a vast scale worldwide. Interactions between educators and their students have now changed from a face-to-face to screen mode. This unexpected transition has led to many challenges encountered by both the educators and students. Some students are facing internet connectivity problems and lack of digital devices for their virtual learning [21]. Likewise, most lecturers are experiencing various challenges including financial, physical, and mental issues [22]. Most of them are grappling with the demands of online learning lessons and the advanced technologies in their attempt to ensure that learning takes place without disruption [20].

B. Security in Online Learning

Security in online learning relates to the safeguarding of resources against deliberate or unintentional usage [23]. According to previous research, there are three main needs for security: confidentiality, integrity, and availability [24], as shown in Fig. 2.

Confidentiality refers to the protection of sensitive information against unauthorized access as well as the absence of illegal dissemination [25]. Many online learning environments have a huge number of users (among them students, visitors, instructors, tutors, and administrators). To protect access to the proper user, both a login mechanism and a robust delimitation designating registered users and user groups are necessary [24]. Security precautions such as authentication and encryption are widely used to secure personal information.

Integrity, a critical element of security, refers to "the protection of data from intentional or accidental unauthorized changes" [24]. It also denotes "the absence of improper system alterations" [25]. It assures that "information and data have not been accidentally or maliciously modified or destroyed, and are in accurate, correct, and complete original form" [26]. Access control is the key to maintaining integrity in the online learning environment [24].

Availability means the readiness for correct service [24]. It connotes that any authorized users whenever needed can access an online learning system [24]. Additionally, it assures that "information and communication resources are readily accessible and reliable in a timely manner by authorized persons" [26]. Availability can be destroyed mainly by denial of service and/or loss of data processing capabilities [24].

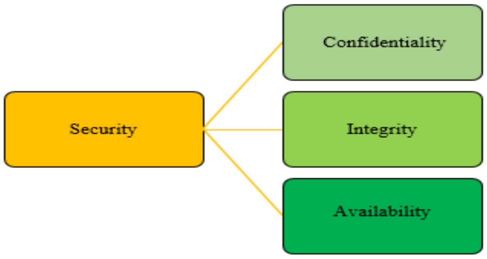

Fig. 2. Basic Requirements of Security.

III. Methodology

Google forms questionnaire was used to acquire feedback from students in this study. The questions were designed to measure the level of awareness among students on their understanding regarding data security in online learning. A total of 42 students responded the survey. The respondents include secondary school students, pre-university students, and university students. The methodology for conducting this research is shown in Fig. 3.

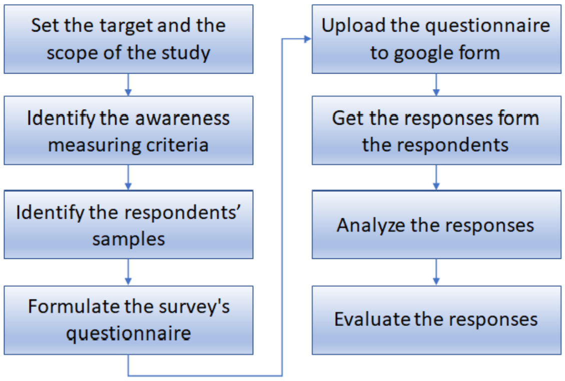
Set the target and the scope of the study
Identify the awareness measuring criteria
Identify the respondents' samples
Formulate the survey's questionnaire
Upload the questionnaire to google form
Get the responses form the respondents
Analyze the responses
Evaluate the responses

Fig. 3. Methodology.

This paper targets to measure the students' awareness level and practice of data security while they use online learning. The students' awareness level has been measured based on the following indicators:

- General awareness about online security.
- Using anti-virus on the device that they use for online learning.
- Using two factor authentications when logging in to the online learning application.
- Practicing logging out of online learning applications after using them.
- Using their own personal device individually or sharing the device with other students.
- Awareness about the confidentiality of the data that the student share in online learning.
- Using common information such as birthday, identity card (IC) number, matric number as the passwords for their online learning software.
- Using online learning platform on public computers or Wi-Fi such as in the library.
- Sharing the information in trusted website only.

IV. Result and Discussion

Forms Questionnaire. Fig. 4 shows the gender of the respondents. As the figure depicts, 71.4% of the respondents are male while the remaining 28.6% are female.

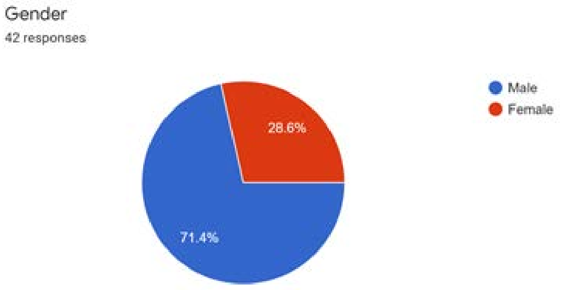

Fig. 4. Gender of the Respondents.

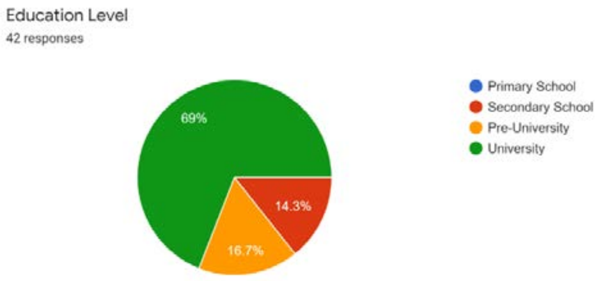

Fig. 5. Educational Level of the Respondents.

Fig. 5 exhibits the education level of the respondents whereby 69% of the respondents are university students, 16.7% are pre-university students, and 14.3% are secondary school students.

Fig. 6 displays the respondents' awareness about online security. The highest percentage of students, 50% of them, is well aware about online security. On the other hand, the lowest percentage, 2.5% of them, represented respondents who are unaware about online security. Meanwhile, the chart shows that almost 4.8% of the respondents have little awareness, 16.7% have awareness, and 26.2% have excellent awareness about online security.

As can be depicted from the figure, the majority of respondents are aware about online security, which indicates a positive result. However, it will be a lot better if all the respondents are very well aware about online security since this will prevent them from any malicious actions such as data theft.

Fig. 7 shows whether or not the respondents have practiced online security in online learning. The highest percentage of the respondents, almost 42.9% of them, has practiced online security well. On the other hand, the lowest percentage of them, almost 2.4%, are unaware about practicing online security. Meanwhile, the chart shows that also 4.8% have practiced a little, 19% have practiced, and 31% have very well practiced the online security. An overall result indicates that most of the respondents have at least used an anti-virus in their electronic devices in order to protect their devices from virus such as Trojan [27]. However, it is speculated that half of the respondent have never practiced online security. For example, they do not used two factor authentications to secure third party platforms.

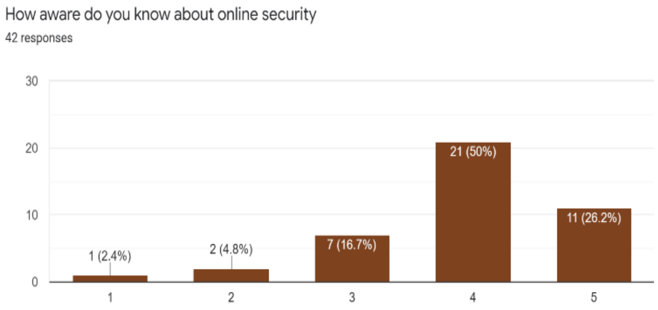

Fig. 6. Awareness about Online Security.

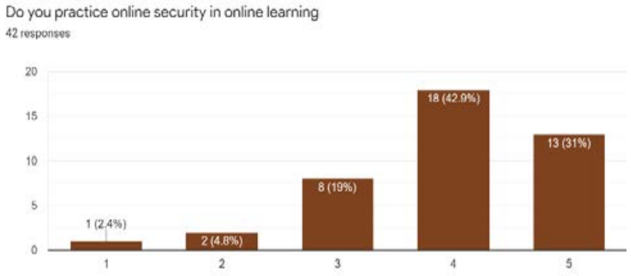

Fig. 7. Respondents Practice Online Security in Online Learning.

Fig. 8 shows that 83.3% of the respondents have used antivirus software during online learning. On the other hand, 16.6% respondents have not used any anti-virus software and that they are aware of the importance of it particularly in online learning. The pie chart clearly depicts that majority of the respondents have used anti-virus. This is due to the fact that anti-virus is a common software that can be easily installed in most devices.

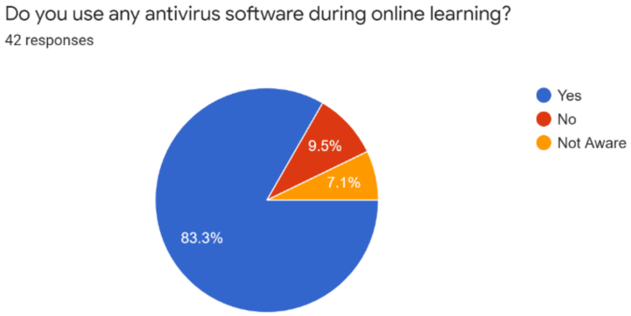

Fig. 8. Use Antivirus Software during Online Learning.

Fig. 9 shows whether the respondents log out of the online learning applications software after using them. It is obvious that half of the respondents log out of the applications software after using them while 40.5% of them do not. 9.5% of the respondents are not sure whether they log out after using the applications software or not.

It is important to note that 50% of the respondents, who log out from the applications software after using them, are those who are very much aware of online security and thus, logging out after using the applications has become a common practice to them. These respondents understand the risks of not logging out of the applications software. For example, they are aware of the risks when someone else uses their devices and gets an access to their personal information like e-mails. It can be concluded that another 50% of the respondents, who do not log out of the applications software, are less mindful and unconcerned of the effects of their actions.

Fig. 10 illustrates the respondents' answers on whether or not they have used two factor authentications during their online learning. The results depict that 52.4% of the respondents have used two factor authentications for their online learning platform. On the other hand, 35.7% of them have not used two factor authentications for online platform while the remaining 11.9% are not aware about using two factor authentications for online learning platform.

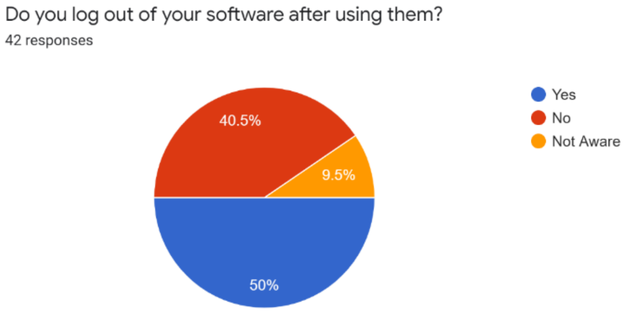

Fig. 9. Log out of Software after using them.

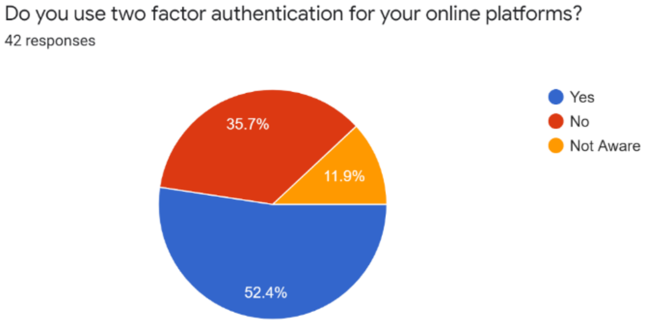

Fig. 10. Use Two Factor Authentications for Online Platforms.

This indicates that some respondents are totally not aware of the function of two factor authentications. This is rather dangerous as other users using their e-mail's accounts or passwords can easily access their accounts.

The respondents were asked whether they have individually used their own devices or they have shared their own devices with others during online learning. Fig. 11 presents the results in which approximately 69% of the respondents used their own personal devices, whilst, 23.8% indicated that they shared their devices with others during online learning. The remaining 7.1% of the respondents are not sure whether they have used their own device or they have shared devices with others during online learning.

The results indicate that it is better for the respondents to use their own personal devices instead of sharing the devices with others as this can avoid from sharing their data with others. By having their own devices, the respondents can also manage their files more strategically and efficiently. If the respondents share their devices with others, there is a possibility that they may unintentionally expose their confidential information.

Fig. 12 shows whether the respondents are aware about the data that they share in online learning including the privacy of the data like personal information, pictures and location. Majority of the respondents, 66.7%, are aware about the data their share in online learning. Conversely, 33.3% of the respondents are not aware about the of the privacy data they share in online learning.

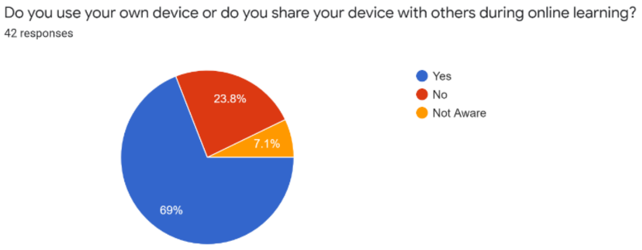

Fig. 11. Use Own Device or Share Device with others during Online Learning.

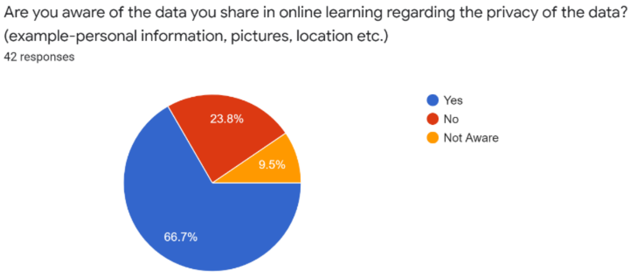

Fig. 12. Aware of the Data you Share in Online Learning.

The respondents should be aware of the data that they share in online learning especially when it involves confidentiality of the data. This is because hacker could either use the respondents' information to blackmail them or sell their data to other parties. It is recommended that 33.3% of the respondents to take classes about data security or use self-reading to gain more information about the importance of protecting data especially during this pandemic.

Fig. 13 shows whether the respondents use common information such as birthday, identity card (IC) number, matric number as the passwords for their online learning software. 59.5% of the respondents have been using common information for their online learning software's password. This is probably because it is easier for the respondents to remember their password whenever they want to log in into their accounts. 26.2% of the respondents have not used common information for their online learning software's password.

This indicates that the respondents are alert that most hackers these days can easily guess users' password particularly their personal data such as birthdate or real name as their passwords. Next, 14.3% of the respondents are not aware or unsure if they use common information for their online learning software's password.

Fig. 14 shows whether the respondents have ever used online learning platform on public computers or Wi-Fi such as in the library. The figure shows that 54.8% of the respondents have not used online learning platform on public computers or Wi-Fi such as in the library. This is generally because of the pandemic that forces the students to do their online learning at home [28]. 38.1% of the respondents have used online learning platform on public computers or Wi-Fi such as in the library or even McDonald's.

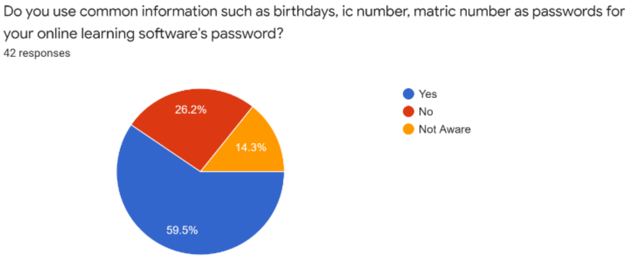

Fig. 13. Use Common Information as Passwords for Online Learning Software Password.

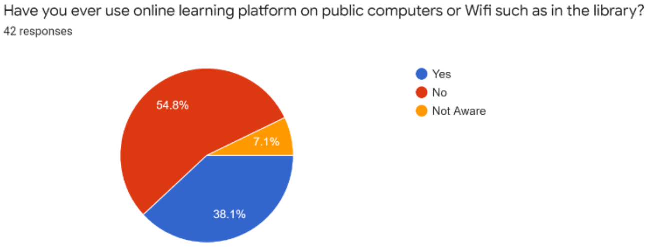

Fig. 14. Use Online Learning Platform on Public Computer or Wi-Fi.

This indicates that some of the respondents have been using the university Wi-Fi or even library during this pandemic. The remaining 7.1% of the respondents are not aware whether they have ever used online learning platform on public computers or Wi-Fi in public places such as in the library.

Fig. 15 presents the respondents' answers on whether or not the website in which they share their information is trusted and legitimate. The respondents' awareness helps to avoid sharing important information with irresponsible people.

The results show that 66.7% of the respondents are aware that the websites which they share information is secure and legit, while 33.3% of the respondents are not aware about it. This result is disturbing given that generally 1 out of 3 respondents is not aware about the danger of the websites that can be potentially a scam to steal important information, money, and private information.

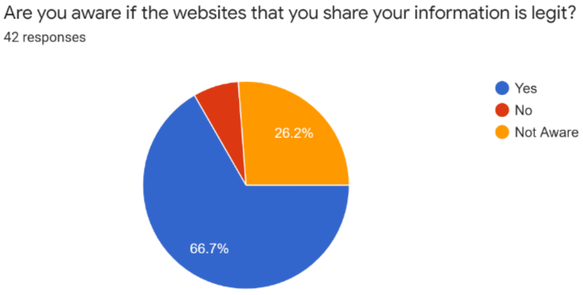

Fig. 15. Awareness if the Websites that you Share your Information is Legit.

V. CONCLUSION

The demands of the use of technology, especially during the Covid-19 pandemic, have led to the growth of end user devices and the widespread of online learning around the globe. Indeed, these massive applications of online learning bring along with them various security risks to many users. Nevertheless, it is safe to say that online learning is still at its premature and impulsive phase because most educators and students alike are still struggling in getting themselves familiar with its applications and operations. Concurrently, its providers are still taking the security risks of online learning lightly although it has become the most vital means of learning in the world today. It is important to note that most providers had to opt for an impulsive execution of the information and communication technology without taking into consideration relevant security concerns such as two-factor authentications. This was deliberately done to ensure that learning continues regardless the challenges experienced by students and educators during the pandemic. Given this scenario, it is discovered that most of them are not concerned about the importance of online security. This is evidenced in the study in which students at various levels of education were found to be insensitive towards the crucial needs to protect data security when conducting online learning. It is recommended that the stakeholders, such as the Ministry of Higher Education and the university, to enforce on data security in online learning. Online talks and forums on the most effective ways of online learning security should be conducted for educators and students to enhance their awareness. Therefore, data security awareness among students is essential.

ACKNOWLEDGMENT

We would like to acknowledge the Network and Communication Technology Research Group for the assistance and support they have provided. This survey has been conducted by UKM Students from TK2133-Data Communication and Telecommunication class.

REFERENCES

[1] E. Budiman, U. Hairah, M. Wati, and H. Haviluddin, "Sensitivity analysis of data normalization techniques in social assistance program decision making for online learning," Advances in Science, Technology and Engineering Systems Journal, vol. 6, no. 1, pp. 49-56, 2021, doi: 10.25046/aj060106.

[2] N. Azman and D. Abdullah, "A critical analysis of Malaysian Higher Education Institutions ‘response towards Covid-19: Sustaining academic program delivery," Journal of Sustainability Science and Management, vol, 16, no. 1, pp. 70-96, 2021, doi:10.46754/jssm.2021.01.008.

[3] A. Obeidat, R. Obeidat, and M. Al-Shalabi, “The effectiveness of adopting e-Learning during Covid-19 at Hashemite University,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 11, no. 12, pp. 96- 104, 2020.

[4] UNESCO, 2020. COVID-19 educational disruption and response. Retrieved from https://en.unesco.org/themes/educationemergencies/coronavirus-school-closures. Accessed on 28 December 2021.

[5] D. F. Murad, R. Hassan, Y. Heryadi, and B. D. Wijanarko, "The impact of the Covid-19 pandemic in Indonesia (Face to face versus Online Learning)," 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE), pp. 1-4. 2020, doi:10.1109/ICVEE50212.2020.9243202.

[6] Q. Kharma, K. Nairoukh, A. Hussein, M. Abualhaj, and Q. Shambour, “Online learning acceptance model during Covid-19: an integrated conceptual model” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 5, 2021, http://dx.doi.org/10.14569/IJACSA.2021.0120561.

[7] B. H. Khan, "Web-based instruction (WBI): An introduction," Educational Media International, vol. 35, no. 2, pp. 63-71, 1998, doi: 10.1080/0952398980350202.

[8] S. Dhawan, "Online learning: A panacea in the time of Covid-19 crisis," Journal of Educational Technology Systems, vol. 49, no. 1, pp. 5-22, 2020, doi: 10.1177/0047239520934018.

[9] V. Singh and A. Thurman, "How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018)," American Journal of Distance Education, vol. 33, no. 4, pp. 289-306, 2019, doi: 10.1080/08923647.2019.1663082.

[10] B. M. Batubara, "The problems of the world of education in the middle of the Covid-19 pandemic," Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences, vol. 4, no. 1, pp. 450-457, 2021, doi:10.33258/birci.v4i1.1626.

[11] A. Haseeb, 2018. Higher Education in the Era of IR 4.0. New Straits Times. Retrieved from https://www.nst.com.my/education/2018/01/323591/higher-education-era-ir-40. Accessed on 28 December 2021.

[12] World Economic Forum. 2020. Schools of the Future, Defining New Models of Education for the Fourth Industrial Revolution. Geneva: World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf. Accessed on 4 January 2022.

[13] D. F. Murad, R. Hassan, W. Wahi, and B. D. A. Wijanarko, "User-item collaborative filtering system to predict online learning outcome," Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 5, pp. 117-121, 2020, doi: 10.25046/aj050516.

[14] Creatrix Campus, 2020. Why should higher education institutions focus on Education 4.0? Retrieved from https://www.creatrixcampus.com/blog/Education-4.0. Accessed on 28 December 2021.

[15] E. J. Thandevaraj, N. A. A. Gani, and M. K. M. Nasir, "A review of psychological impact on students online learning during Covid-19 in Malaysia," Creative Education, vol. 12, no. 6, pp. 1296-1306, 2021, doi:10.4236/ce.2021.126097.

[16] E. Chung, N. M. Noor, and V. N. Mathew, "Are you ready? An assessment of online learning readiness among university students," International Journal of Academic Research in Progressive Education and Development, vol. 9, pp. 301-317, 2020, doi:10.6007/IJARPED/v9-i1/7128.

[17] A. Shahzad, R. Hassan, R., A. Y. Aremu, A. Hussain, and R. N. Lodhi, "Effects of Covid-19 in e-learning on higher education institution students: the group comparison between male and female," Quality & Quantity, vol. 55, pp. 805-826, 2020, doi:10.1007/s11135-020-01028-z.

[18] F. M. Kamaruzaman, N. A. Sulaiman, and N. A. N. Shaid, "A study on perception of student’s readiness towards online learning during Covid-19 pandemic," International Journal of Academic Research in Business and Social Sciences, vol. 11, no. 7, pp. 1536-1548, 2021, doi:10.6007/IJARBSS/v11-i7/10488.

[19] S. J. Daniel, "Education and the Covid 19 pandemic," Prospects, vol. 49, pp. 91-96, 2020, doi:10.1007/s11125- 020-09464-3.

[20] M. N .O. Sadiku, P. O. Adebo, and S. M. Musa, "Online teaching and learning," International Journals of Advanced Research in Computer Science and Software Engineering, vol. 8, no. 2, pp. 73 – 75, 2018.

[21] M. Mahyoob, "Challenges of e-learning during the Covid-19 pandemic experienced by efl learners," Arab World English Journal (AWEJ), vol. 11, no. 4, pp. 351 – 362, 2020, doi:10.24093/awej/vol11no4.23.

[22] C. T. Vu et al., "Dataset of Vietnamese teachers’ perspectives and perceived support during the COVID-19 pandemic," Elsevier, Data Brief 2020, vol. 31, p. 105788, 2020, doi:10.1016/j.dib.2020.105788.

[23] A. Adams, A. Blandford, "Security and online learning: To protect or prohibit," Usability Evaluation of Online Learning Programs, pp. 331-359, 2003, doi:10.4018/978-1-59140-105-6.ch018.

[24] A. Serb, C. Defta, N. M. Iacob, and M. C. Apetrei, "Information security management in e-learning," Knowledge Horizons, vol. 5, no. 2, pp. 55-59, 2013.

[25] E. Weippl and M. Ebner, "Security privacy challenges in e-learning 2.0," In World Conference on E-Learning in Corporate, Government,

Healthcare, and Higher Education, vol. 2008, no. 1, pp. 4001-4007, 2008.

[26] R. Raitman, L. Ngo, N. Augar, and W. Zhou, "Security in the online e-learning environment," In 5th Advanced Learning Technologies, 2005 (ICALT), pp. 702-706, 2005, doi:10.1109/ICALT.2005.236.

[27] K. G. Liakos, G. K. Georgakilas, S. Moustakidis, P. Karlsson, and F. C. Plessas, "Machine learning for hardware trojan detection: a review," 2019 Panhellenic Conference on Electronics & Telecommunications (PACET), 2019, pp. 1-6.

[28] N. A. N. Shaid, F. M. Kamruzaman, and N. A. Sulaiman, "Online Learning During Ongoing Covid-19 Pandemic: A Survey of Students' Satisfaction," International Journal of Academic Research in Business and Social Sciences, vol. 11, no. 7, pp. 924-937, 2021.