Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

CYBERSECURITY AWARENESS AMONG STUDENTS: PROMOTING A SECURE DIGITAL ENVIRONMENT

Muhammad Faris Hami Mohd Zahibi [1*]
Muhammad Fathi Tarwan Mansur [2]
Mohd Akmal Faiz Osman [3]
Khadijah Abdul Rahman[4]
Huda Hamidon[5]

[1] Universiti Teknologi MARA; School of Information Science; (Email: farishami@uitm.edu.my)
[2] Universiti Teknologi MARA; School of Information Science; (Email: fathitarwan@gmail.com)
[3] Universiti Teknologi MARA; School of Information Science; (Email: mafaiz77@gmail.com)
[4] Universiti Teknologi MARA; School of Information Science; (Email: khadijah10@uitm.edu.my)
[5] Universiti Teknologi MARA; School of Information Science; (Email: huda685@uitm.edu.my)
* Correspondence: farishami@uitm.edu.my; 09-9763027.

Article history
Received date : 15-8-2024
Revised date : 16-8-2024
Accepted date : 7-9-2024
Published date : 15-10-2024

To cite this document:
Mohd Zahibi, M. F. H., Mansur, M. F. T., Osman, M. A. F., Abdul Rahman, K., & Hamidon, H. (2024). Cybersecurity awareness among students: Promoting a secure digital environment. *Journal of Islamic, Social, Economics and Development (JISED)*, 9 (66), 950-959.

Abstract: *The increased reliance on digital technologies in educational settings has created a need for high security awareness among university students. Potential risks, such as the exploitation of sensitive information, online scams, and the need for responsible behaviour, have been reported as problems for modern university students. This study explores the cybersecurity awareness of 100 Malaysian public university students enrolled in an information management course using a quantitative survey. The results revealed that students have high security awareness. However, this might be attributed to their enrolment in an IT-based course, which gradually exposes them to cybersecurity issues. Further studies in other courses are encouraged to identify and enhance cybersecurity awareness, ensuring that students complete their studies smoothly and successfully.*

Keywords: *Cybersecurity awareness, Digital technologies, University students.*

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

Introduction

The rapid growth in modern ICT technologies has dramatically revolutionized university students' lives, as various communication channels have been widely used to seek, analyze, and disseminate information (Alharbi & Tasaddiq, 2021). Thereupon, both public and private universities have adopted various modern technologies to aid teaching and learning process by providing access to information and learning materials. In relation to this, university students nowadays must possess ICT skills regardless of any course they enrolled in university. The ICT skills are needed to allow them to find, locate, evaluate, and access learning materials via online. Compared to 20 years ago, university students would need to find materials in the library, from lecturers, or by conducting field study. Despite the outrageous benefits offered by modern technologies in education, however, it is widely reported that the number of hackers and cybercrime are exponentially growing (Alharbi & Tasaddiq, 2021). To make matters worse, these cybercrimes and hackers are conducted and handled by organized units. Moreover, these criminals often adopt modern technologies to carry out their operation with the ultimate objective to take advantage of the technologies to steal private information such as username and password, bank account, phone number, and address. The interesting part and motivational factors behind this crime are to gain outrageous financial benefits. According to New Straits Times (2023), Malaysia faces enormous and increasing cybersecurity threats, as the number of crimes related to cyber technology increases exponentially. Although Cybersecurity Malaysia has provided guidelines in relation to avoiding cybercrime, the number of cases is still arousing and worrying. According to the cyber incident report for the first quarter of 2024, the Malaysia Computer Emergency Response Team (MyCERT) has identified 142 data breach cases. This highlights the urgent need to enhance cybersecurity awareness, particularly among students, who are becoming more susceptible to digital threats (MyCERT, 2024)

Nowadays, university students are not only exposed to cybercrime during finding teaching and learning material as they often use online methods to buy groceries, coffee, communicate, and transfer money. University students also spend 4-5 hours per day on social media (Rahman et al., 2023). These alarming issues have led researchers, scholars, academicians to play their roles towards minimizing the damage. Senthilkumar and Easwaramoorthy (2017) have conducted a survey to analyse the cybersecurity awareness of university students in India. Tirumala et al., (2016) perform surveys among universities in New Zealand, while Garba et al., (2020) conduct surveys among Nigerian students. From these studies, it is found out that the awareness level of cybersecurity among university students is relatively low (Senthilkumar & Easwaramoorthy, 2017; Tirumala et al., 2016; Garba et al., 2020). The studies, however, offer meaningful insight for the community by highlighting the importance of high cybersecurity awareness among students to mitigate the rising number of cybercrimes that occurred involving university students (Bottyan, 2023). This is therefore highlighting the importance of conducting research to analyse the security awareness among students in order to trigger important measures such as providing security awareness workshops, campaigns, practice, or classes. The objective of this study is to analyse the cybersecurity awareness among public university students in east coast Malaysia, as it is found out that there are limitations and gaps in the literature.

Literature Review

Bottyan (2023) conducted a survey of students at the University of Dunaujvaros to address protective measures against cyber threats. The author argued that raising awareness about information security is the primary and most important way to prevent issues for students. Bottyan (2023) identified password management and performing sensitive activities on unfamiliar computers as the two main concerns that university students need to address to

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

reduce the risk of cyberattacks. Passwords need to be managed effectively by students as it allows access to many sensitive information such as personal information, banking details, and address. Failure to effectively manage and protect passwords allows unauthorized access to other individuals hence exposing the sensitive information to severe effects. Performing sensitive activities on other computers means that students sometimes need to do assignments or projects on other computers such as in the library, laboratory, or public place such as cyber cafes. It is important to note that most public cybercafe have pre-installed software that is able to steal sensitive information. This information later we sold to interested parties such as banks and insurance. The study of Bottyan (2023) found that the student information security awareness was relatively low.

Garba et al. (2020) investigated university students' awareness of cybersecurity at a university in Nigeria. The study used a survey of 367 valid responses to assess students' knowledge about protecting sensitive data and understanding cyber threats. The authors provided recommendations to reduce cybersecurity risks by enhancing students' knowledge about cyber threats and how to safeguard sensitive information. They found that while students had only basic knowledge of cybersecurity, they expressed a strong interest in learning more. The study encouraged the university and policymakers to organize more cybersecurity workshops to raise awareness and reduce cyber risks.

Senthilkumar and Easwaramoorthy (2017) conducted a survey of 500 college students to investigate cybersecurity awareness in Tamil Nadu. The authors highlighted the urgent issue of cybercrime, which poses concerns for national security, public safety, and personal privacy. They found that the level of cybersecurity awareness among students was relatively low. The authors argued that to prevent students from becoming victims, they must possess a strong understanding of safety measures. This necessity is underscored by the advanced techniques and methods used by cyber attackers, such as phishing. Senthilkumar and Easwaramoorthy (2017) recommended that university students should have a thorough understanding of security threats, including viruses, email scams, fake advertisements, pop-up windows, and phishing, to protect themselves effectively.

Tirumala and Sarrafzadeh (2017) explained that 93.8% of the population in New Zealand has used the internet while the cybersecurity attack cases are rising dramatically ever since. The author conducts a study to evaluate current knowledge on cybersecurity of students as more often the students have become a target because of their low knowledge. By providing the empirical data of low level of knowledge among students that stands at only 19% of them have satisfying knowledge regarding cybersecurity, coupled with majority of them are not familiar with cybersecurity terms and did not have enough awareness regarding rising threats such as web phishing, the author strongly suggests the policy maker to necessitate the workshop to increase cybersecurity awareness among students.

Aljohni et al. (2021) found that the awareness of cybersecurity levels has no significant gap between male and female students although the female shown a little bit higher in the awareness . The study was conducted in Saudi Arabia university students. Other demographic variables do affected the awareness level such as the origin of the students, the students who are from the city are more likely to have a higher cyber security awareness compared to the students that come from village. Other demographic variable that affected the level of awareness is studies major. Students that are from the IT related programmes are more likely to have a higher level of awareness compare to other students. Bognár & Bottyán (2024) also found that study major

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

do affected the awareness of cybersecurity, in the case of the study in University of Dunaújváros, Budapest Business School, Ludovika University of Public Service, and Óbuda University, they found the students from science and technology major are prone to have higher level of cybersecurity awareness compared to social science students.

The cybersecurity awareness also affected by how far the authorities' efforts in educating the students, study made in Kyrgyz-Turkish Manas University found that even the famous cybersecurity attacks occur, the students still have no knowledge about on how severe can it be and this also affected on lack of urgency in preventing it, including the unknowingly malicious software types and how are they distributed (Erendor & Yildirim, 2022). In other study shows that cybersecurity awareness lacking doesn't only focusing on one group of demographics, but varies Hossain et al. (2022). This indicates that the authorities or government need to do an intervention to minimize this problem. Other study in Pakistan found that the demographic factor of the student that does not aware of the cybersecurity is due to socioeconomic factors. The lack of cautious is vary indicates the need of targeted training Khan et al. (2023).

From these studies, there are several patterns that can be identified. First, most university and college students have relatively low levels of knowledge about cybersecurity measures (Garba et al., 2020; Bottyan, 2023), rising threats (Senthilkumar and Easwaramoorthy, 2017), data protection (Bottyan, 2023), cybersecurity terminology (Tirumala & Sarrafzadeh, 2017), demographic factors on the cybersecurity awareness level (Aljohni et al. 2021; Bognár & Bottyán 2024). Second, university students today are frequently exposed to cybersecurity threats due to their extensive use of the internet for assignments, classes, discussions, entertainment, and online purchases (Bottyan, 2023; Garba et al., 2020). Third, as suggested by Garba et al. (2020), universities should conduct cybersecurity workshops to educate students about emerging threats, security measures, and cybersecurity terminology (Bottyan, 2023; Tirumala & Sarrafzadeh, 2017; Senthilkumar and Easwaramoorthy, 2017; Khan et al. 2023). Therefore, by following these research trends and addressing existing gaps, this study aims to investigate the current level of information security awareness among students at public universities in the east coast region of Malaysia.

Method & Material

The research employed an online questionnaire survey for data collection. The objective of the research is to evaluate the information security awareness among public university students thus, by following the works of previous researcher (Senthilkumar and Easwaramoorthy; 2017; Bottyan, 2023; Tirumala & Sarrafzadeh; 2017; Rahman et al., 2022), online questionnaire survey was deemed as the best data collection method to achieve the research objective. The questionnaire was adapted and adopted from the works of Aljohani et al., (2020) due to similarities in objectives. SPSS version 28 software was used to analyze and present data in a meaningful way. For sampling, convenience purposive sampling was chosen due to researcher's access in public universities. The course selected is information management as the intent of the researcher is to measure information security awareness among IT related course students to fulfil the gaps in the literature. In total, 126 online questionnaires were collected, however, only 100 were found usable for data analysis due to incomplete and missing data. The analysis only comprises descriptive technique, as the research is not seeking to establish any relationships.

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

Findings

Demographic Information

The first component of the demographic data is represented by the age and gender of the students and is displayed in Figure 3.1 below. Gender statistics are projected in Figure 3.2. Ninety-five percent of the students are in the age range of 21 to 23. There are 64% female students and 36% male students in terms of gender. It is evident from these statistics that women predominate in information management courses, despite being an IT-based course. This information confirmed by Schoenberger (2018) that in high school and university, most women became involved in technology where the recruiters made male-centric references. However, there is a very limited number of studies on the gender disparity issue in students' actual choice of IT-related majors using objective assessments based on Zhang, et al (2021).

Their age range of 21–23 can be explained by the fact that 5 percent are now earning their diploma and the other 9 percent are pursuing their first degree. This information is in line with the population's level of education; figure 3.3 shows that 95% of the population currently has a degree, with the remainder people having a diploma. This demographic information, however, would have an impact on the findings of their awareness on information security level as degree level students usually have more experience and knowledge in relation to information security particularly for IT-based courses.

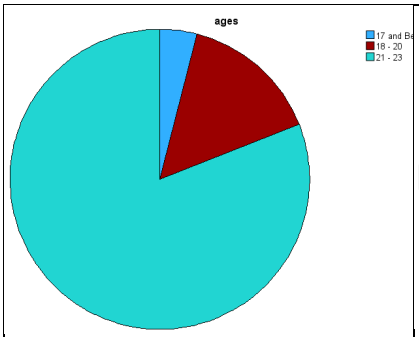

Figure 4.1. Age

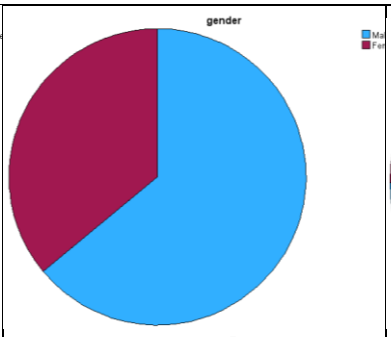

Figure 4.2 Gender

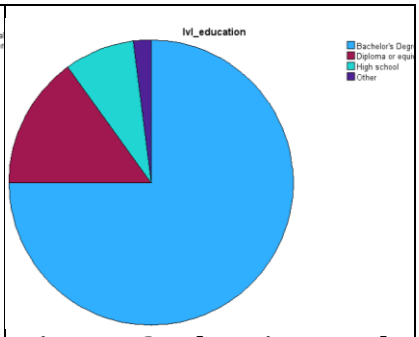

Figure 4.3 Education Level

Knowledge and Awareness on Cybercrime

In this section, students were asked regarding their knowledge and awareness of cybercrime. Figure 4.4 depicts the findings that clearly shown, majority of students are aware and have knowledge in relation to cybercrime cases and activities. 89% of students admit they are aware, followed by only 3% that admit to not having knowledge on cybercrime, while the other 8% answered maybe. From this finding, it can be said that students of this course have satisfying knowledge and awareness regarding cybercrimes. This finding is doubted to be influenced by the usage of social media as discussed by Rahman et al., (2023), where they found out that student spends more than 4 hours per day on social media for leisure, news, and other activities.

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

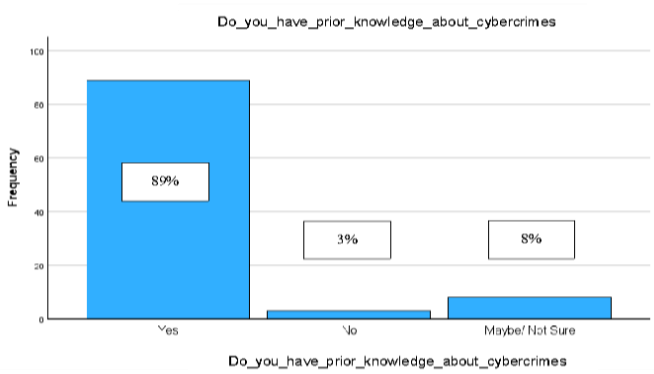

Figure 4.4. Knowledge and Awareness of Cybersecurity

Figure 4.5 below depicts the answer from students that shows most of them are not sure regarding this matter which stands at 40%. Thirty percent of the respondents answered YES, while the other 30% answered NO. Respondents have been probed with questions on their knowledge on whether the government is monitoring the cybersecurity issue that arose in the country. In this diagram, it is crystal clear that they are really sure. Other than that, respondents were asked whether the government is focussing on awareness and education to reduce cybercrime or not. To this question, 89% of them agreed, only 3% disagreed, while 8% were not really sure. The response is depicted in Figure 4.6.

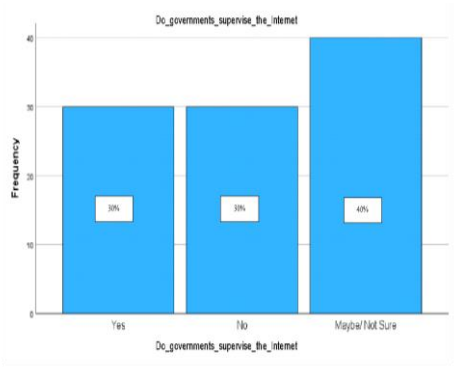

Figure 4.5. Knowledge on Government effort in monitoring cybercrime

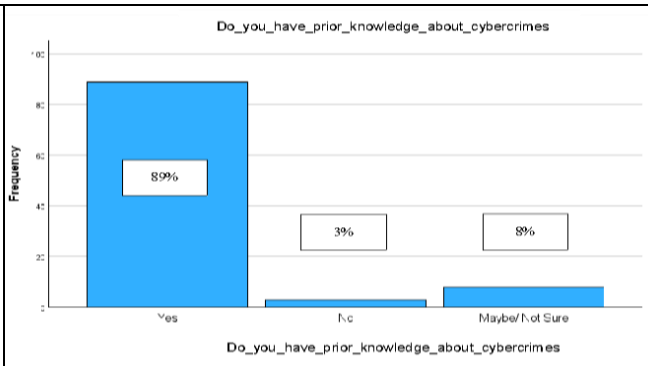

Figure 4.6. Knowledge on Government effort in promoting awareness and education on cybercrime

Awareness and Behaviour in Digital Environment

This section analysed respondents' awareness and behaviour that is related to cybercrime. The first question explores the password preference of students when signing up into a digital account. The question asked, "Do you use personal information as your password?" The instrument provides 5 likert-scale answers that stand at strongly disagree, disagree, neutral, agree, and strongly agree. The depiction of the answers was presented on figure 4.7 in which only 6% strongly agree in using personal information as password, while 22% of them answered

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

agree. However, more than 50% of the respondents strongly disagree, thus indicating that many students do not use personal information as a password on digital accounts.

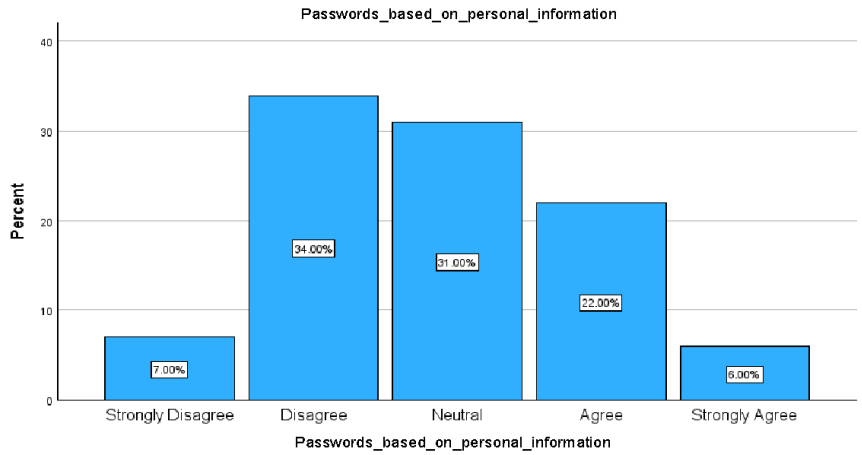

Figure 4.7. Behaviour of using password for digital account

The use of password hinting to control digital access has also been examined in the context of studying student behaviour in digital environments. The item's overall result is shown in Figure 4.8. From the figure, 14% of the students agree that they are using the password hint to remember their password, while 31% of them simply did not use the password hint at all. The rest of the respondents simply opted to answer unsure. According to Al-Janabi et al., (2016) the usage of password hint presents security risks, as cyber criminals would have a focus in trying to exploit any unauthorized use of access.

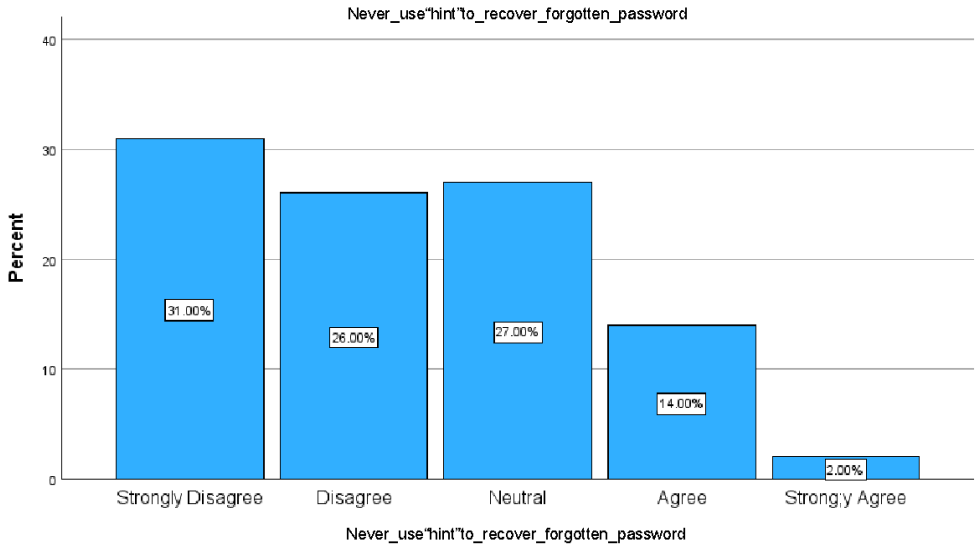

Figure 4.8. Behaviour of using password hint

The final metric used to examine student behaviour is the propensity to believe images shared online by strangers. The question, "Do you simply trust the pictures posted by unknown strangers on the internet?" was posed to the students. Figure 4.9 shows the depiction of the answer that is based on scale. 51% of the answers strongly disagree and disagree. This means that half of the respondents do not easily believe any pictures posted by unknown strangers on the internet. However, 49% of these answers fall either in the category of neutral, agree and

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

strongly agree. The trust towards any images and posting posed a high risk for students, as the number of digital cases rose dramatically since the post-covid 19 era.

Discussion

The findings have shown that respondents possess a quite low knowledge and awareness regarding cyber security. However, given that respondent was a university student, they are not really exposed to the real cyberthreat as they still do not have a sustainable amount of salary in their bank account. This in turn, evades them from being targeted by cyber criminals. Many cybercrime cases targeted people with substantial amounts of money in their bank account, and have made transactions (Bernama, 2023; Thiruchelvam et al., 2022). According to Thiruchelvam et al., (2022), the number of cybercrime cases rose dramatically from the year 2008 until 2022. The rise of cases is parallel to the advancement of ICT that causes loss of money, threats to organization and individual, and psychological trauma. University students should prepare themselves with adequate knowledge and awareness before they enter the workforce and have a salary (Muharram et al., 2022). Other than that, students also will work in organizations that handle large transactions. Thus, the knowledge and awareness in safeguarding both individual and organization assets is critical. The findings show that students even use a hint for password, which is a high risk of being exposed. Moreover, the data shows that they tend to use personal information as their password. Universities should play a role in educating students through awareness programs to boost their knowledge. This can be done through exposing students to cybercrime cases and conducting a workshop on how to safeguard themselves in a digital environment. Students need to equip themselves with substantial knowledge on cybersecurity through awareness programs and workshops. Although students are not the prime target of cybercriminals, the awareness and knowledge of cybercrime would ensure a smooth journey of their study.

Conclusion

This study employs a survey to explore university students' awareness, knowledge, and behaviour in the digital environment. The findings show that university student's awareness, knowledge and behaviour were not at a satisfactory level. Although students are not really exposed to cybercriminals, it is imperative for them to have substantial awareness and knowledge to safeguard their personal information and have secure behaviour while interacting online. This is because these students will work in an organization one day and receive a salary. They also are responsible for safeguarding the organization assets that they work for in the future. Universities should play a role in educating students regarding cyber security to enable them to safeguard their individual and organizational assets.

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data and Cognitive Computing, 5 (23). https://doi.org/10.3390/bdcc5020023

Al-Janabi, S., & AlShourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management. 15. 1650007. 10.1142/S0219649216500076.

Aljohani, W., & Mohamed, N. (2020). Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University. 9. 141-155

Bernama. (2023). Cybercrimes: Types & Tips. December, 13, 2023. https://www.bernama.com/en/thoughts/news.php?id=2253495

Bognár, S., & Bottyán, J. (2024). Evaluation of cybersecurity awareness scale for university students: A comparative analysis of online security behaviors. *Education Journal*, 14(5), 588-600. https://doi.org/10.3390/education-14-00588

Bottyan, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences*, *13*(3), ArtNo: 363. https://doi.org/10.24368/jates363

Cybersecurity Malaysia. (2020). Malaysia Cyber Security Strategy 2020 – 2024. National Security Council : Malaysia

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, 10, 52319-52329.

Garba, A., Siraj, M., Alhaji, M.., & Othman, S. (2020). A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach. 41-49. International Journal on Emerging Technologies, 11(5). 41-49.

Hossain, A., Tin, D., Chum, P., Taing, T., & Chhem, S. (2022). Cybersecurity readiness in developing countries: A survey to demonstrate potential risks of the Cambodians. *Proceedings of the 14th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, 309–313.

Khan, F. H., Ali, R., Khan, M., & Qureshi, S. (2023). Socioeconomic and digital inequalities affecting cybersecurity awareness among university students in Pakistan. *Journal of Cybersecurity Education and Research*, 5(3), 375-388.

Muharram, S.S., Suhaimi, M. Z., & Marcus, M. (2022). Cybercrimes In Malaysia. Journal of Education and Social Sciences, 22 (1). 34-38.

Mohamed, N. E., Jarajreh, M., Aljohni, W., & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia university students. *International Journal of Advanced Computer Science and Applications*, 12(3), 276-281.

MyCERT. (2024, May 2). Advisory SR-026.052024. MyCERT. https://www.mycert.org.my/portal/advisory?id=SR-026.052024

New Straits Times. (2023). Malaysia Faces increasing Cybersecurity Threats. March, 17, 2023. https://www.nst.com.my/news/nation/2023/03/890120/malaysia-faces-increasing-cybersecurity-threats-teo?utm_source=nst&utm_medium=mostpoplatest

Rahman, K. A., Osman, M. A. F., Ya'acob, W. M. Z. W., & Sapiai, N. S. (2023). The Impact of Social Media Addiction on Academic Performance among University Students. Journal of Islamic Social, Economics and Development (JISED*), 8*(56), 13-18.

Schoenberger, N. (2018). *Access to information in the age of Trump*. Emerging Library & Information Perspectives, 1: 6-33. https://doi.org.10.5206/elip.v1i1.360

Senthilkumar, K., & Sathishkumar, E. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, 263(4).

Volume: 9 Issues: 66 [September, 2024] pp. 950-959
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096680

Thiruchelvam, V., Tham, K. F., Hasan, M. S., Bastaki, B. B., Bosakowski, T. (2022), Recent Cyber Breaches in Malaysia And Possible Countermeasures. Journal of Engineering Science and Technology. Special Issue on SIET 2022, 297 – 306.

Tirumala, S., Sarrafzadeh, A. (2016). A survey on internet usage and cybersecurity awareness in students. 223-228. 10.1109/PST.2016.7906931.

Y. Zhang, T. Gros, and E. Mao, "*Gender Disparity in Students' Choices of Information Technology Majors*," in Business

Systems Research Journal, vol. 12, no. 1, pp. 80-95, Walter de Gruyter GmbH, 2021. doi: 10.2478/bsrj-2021-0006.