Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution

Rajeswari Raju[1]*, Nur Hidayah Abd Rahman[1], Atif Ahmad[2]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA,
UiTM Terengganu Kuala Terengganu Campus, 21080, Terengganu, Malaysia
rajes332@uitm.edu.my
hidayahrah97@gmail.com
[2] School of Computing & Information Systems
University of Melbourne, Parkville, Victoria, Australia
atif@unimelb.edu.au
*Corresponding Author

https://doi.org/10.24191/ajue.v18i3.18967

Received: 10 May 2022
Accepted: 15 July 2022
Date Published Online: 31 July 2022
Published: 31 July 2022

Abstract: As COVID-19 took hold, online learning became the norm as universities and classrooms worldwide were forced to close their doors. Education institute closures impacted more than 1.2 billion students across 186 countries as of April 2020. This pandemic, too, has shifted our Malaysian education sector as well. Academicians and students are adopting online learning via open and distance learning platforms. Education 5.0 is the revolution of human intelligence and cognitive computing. When the world is moving towards this, the major challenge one will face is the challenges in this digitalisation era, the challenges on cyber security and the risk associated with it. This study uses a digital learning platform to examine the cyber security awareness among UiTM Terengganu Faculty of Computer and Mathematical Sciences students. The study is significant to focus on the weakness and to educate the students about being cyber victims. The data was collected using a set of questionnaires among 110 students. Numbers and statistics from open-ended and closed-ended questions helped obtain data. Descriptive analysis shows that many students have awareness and knowledge of cyber security, cyber-attack, and cyberbullying.

Keywords: Cyber Security, Awareness, Digital Learning

1. Introduction

The COVID-19 pandemic and the lockdown have taken the world and Malaysia by storm. As a result, higher education institutions face instructional challenges, particularly in courses requiring physical contact. According to UNESCO, this pandemic has affected more than half of the world's student population in more than 160 nations (UNESCO, 2020). Despite the challenging situations amid the pandemic, educational institutions' services must continue to run as learning processes should never stop. Furthermore, cyber-attacks show an increase in number and act as a weapon against countries due to the dominance and extensive growth of dependency on cyberspace. Several security standards, guidelines and frameworks have been implemented by the Malaysian government, such as MS ISO/IEC 27001:2007 or ISO/IEC 27001:2005 and Cyber Security Framework for the public sector.

Successful online education supported by a national-level exploration of issues and strategies helps during a crisis (Rahiem, M. D., 2021). In the 2022 endemic situation, higher education institutions (HEIs) need to tighten access to their network infrastructure and caution users to be more vigilant in

protecting their data and privacy when engaging in online and distance learning. Large-scale online learning was implemented rushedly in educational institutions in the country due to the sudden disruption of traditional in-classroom activities by the Covid-19 pandemic, leaving campus networks open to vulnerabilities and fears over cyber threats.

During open and distance learning (ODL), students and lecturers rely on technology to assist the learning process. Online learning delivery has allowed instructors and learners to incorporate flexibility into their lesson plans (Md Noh et al., 2021). Undergraduate students, usually aged 20 to 26 years old, are active Internet users. They depend on information seeking via the internet and spend longer hours online browsing, downloading, and uploading information via the web. As a result, university students are in a vulnerable condition in which they are highly exposing themselves to online risks, such as cyber threats, bullies, and attacks in this situation. This study, therefore, aims to investigate UiTM Terengganu university students' knowledge and awareness of cybersecurity and cyber-attacks. With this information, students can be educated and given proper focused guidance to avoid being cyber victims.

2. Literature Review

2.1 Malaysia Cyber Security Strategy 2020-2024

Cybersecurity has become a general concern for all citizens, professionals, politicians, and decision-makers. It has also become a severe concern for societies that must protect against cybersecurity attacks, with preventive and reactive measures requiring much monitoring. It must simultaneously preserve freedom and avoid general surveillance. Cybersecurity is equivalent to computer security, also known as cyber security or IT security. It protects computer systems from damage to their hardware, software or information and disruption or misdirection of their services (Roca et al., 2019).

Fig. 1.1 displays the cybercrime statistics in 2018 and 2019. The Cyber Security Strategy authors analysed that the Royal Malaysia Police had to deal with 10742 cases related to cybercrime, with an estimated loss amounting to almost RM400 million in 2018. In just one year, in 2019, the number has increased to 11875 cases with an estimated loss of nearly RM500 million (n.a Malaysia Cyber Security Strategy, 2019).

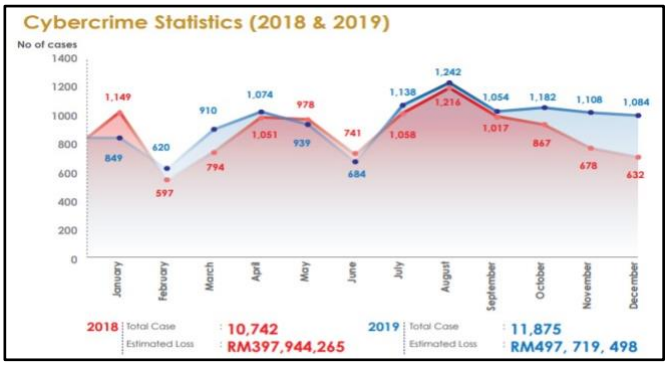

Fig. 1.1 The 2018 & 2019 Cybercrime Statistics (n.a, Malaysia Cyber Security Strategy, 2019)

The digital products that focus on speed and convenience have been developed more by financial institutions creating additional points of vulnerability that fraudsters could exploit online (Yun, T. Z., 2021). The Movement Control Order (MCO) in 2020 presented a shot up of 82.54% cybercrime, according to a report by CGC (Abrar Anwar, 2020). Moreover, the surge in the pandemic has led to a significant increase in cyber threats, phishing campaigns, business email compromises, ransomware, and denial-of-service attacks (Abrar Anwar, 2020).

Global studies on cyber aggression found that online aggressed youths reported feeling depressed, anxious, and afraid. It also contributes to poor academic performance, eating disorders, alcohol, drugs, and substance abuse (Yusuf, S, 2021). Fig. 1.2 shows the most challenging factors in

expanding new digital products in Malaysia by global fraud specialist GBG, demonstrating the highest number in fraud prevention for new digital products.

2.2 Digital Learning

Malaysia has moved into the digital age with the rest. Education 5.0 already being in place. Today, broadband connectivity has become a necessity for education, businesses, services, and the citizens of Malaysia. The standard learning method is Digital Learning which depends on the internet. Students use the internet the entire day for their classes and to finish their assignments. There are also addicted to technology and hooked to cyberspace. Socialising is to portray what others want you to be displayed, and if you cross the line, you will face cyberbullying. Hardly any person or thing is unconnected to cyberspace (Johan, Z. J, 2021).

Information and Communications Technology (ICT) has been widely used in Malaysian public sectors since the 60s to improve efficiency and effectiveness when dealing with internal and external entities. As a result, the Malaysian government introduced two initiatives to increase the reputation of ICT, namely the Technology Action Plan, which highlights the importance of microelectronics and enables Malaysia to become a developed country. However, by then, ICT had been utilised extensively for more strategic purposes (Hatimtai & Hassan, 2018).

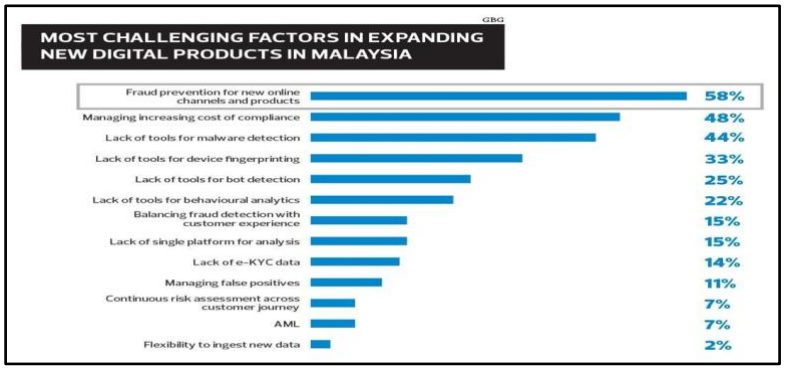

Fig. 1.2 The Most Challenging Factors in Expanding New Digital Products in Malaysia (Yun, T. Z., 2021)

2.3 Malaysian Education and Internet Users

In Malaysia, there is 21,056,126 Internet out of a population of 31,545,990 (Malaysian Digital Association, 2016). The Malaysian Council for Child Welfare (MKMM) has recently reported suicide and self-harm cases among youngsters due to cyberbullying and addiction to cyber gaming (Khalid, Fet. al, 2018).

Malaysian Education Blueprint Higher Education 2013-2025 was launched in 2013 Malaysian Education Blueprint Higher Education 2015-2025 (MEBHE). One of the shifting pillars is leveraging ICT to scale up quality learning across Malaysia (n.a, Education Blueprint, 2020). These 21st-century kids have been surrounded by digital technology since they were little. Technology development has remarkably benefited many industries, including the educational sector. The evolution of internet technology has complemented the delivery of lessons, regardless of primary, secondary, or tertiary levels of education (Raju R et al., 2021). Education is becoming deeply reliant on democratised technologies such as mobile, social, Big Data, Internet of Things (IoT), Artificial Intelligence (AI), and hyper-scale cloud that are all dependent on this connectivity (Malaysia Cyber Strategy, 2020). Critical National Information Infrastructure (CNII) Malaysia handles the escalation of vulnerabilities and risks. Also, it became a better place to meet technological advancement's challenges and opportunities (Hashim, 2011).

3. Methodology

110 students from Universiti Teknologi MARA, Kuala Terengganu Campus, took part in an online questionnaire for this study. The scope of the study was primarily focused on the responses from the Faculty of Computer and Mathematical Sciences students to analyse the level of awareness of cybersecurity. Significant principal advantages of the quantitative method helped in data collection and analysis. The target sample size representing the population (Aziz et al., 2020) took part in the questionnaire. Although the number does not resemble the whole population of students at the university, it is sufficient to carry out the study as stated by Ronán Michael Conroy in his technical report (Conroy, R. M.,2016).

The students are well exposed to computer technology and have computer security knowledge, which is a significant advantage of developing the fundamentals in studying at the faculty. Therefore, the objective of the survey was to analyse the awareness level of different groups of students varies according to their age and exposure to cyberspace. The questionnaires consist of three (3) sections, as stated in Table 1.

Table 1: Sections of the Questionnaire

Section	Title
Section A	Respondents' Background
Section B	Level of Awareness of Cybersecurity, Cyber Attack, Cyber Bully, and Cyber Insurance
Section C	Security Controls

The study duration, the variety of backgrounds, the program students were studying at the university, and their online awareness and engagement in cyberspace are the criteria for various purposes of this study. Google Form questionnaire, which contains close-ended and open-ended questions, measured the nominal scale of the study. A nominal scale is a scale of measurement used to assign events or objects into discrete categories. This form of scale does not require using numeric values or types ranked by class but simply unique identifiers to label each distinct category (Salkind, N. J., 2010). The questionnaire was pilot-tested with 25 second-year students from the same faculty. In addition, computer science educational programs selected students who knew to use computers.

3.1 Descriptive Analysis

Quantitative descriptive analysis characterises the world or a phenomenon by identifying patterns in data. Descriptive analysis is data simplification. Descriptive analysis can stand on its own as a research product, such as when it identifies phenomena or patterns in data that have not previously been recognised (Loeb et al., S, 2017). Frequency distribution and central tendency analysis were used to define the frequencies for each question as the data is nominal.

4. Findings and Analysis

Overall, this study examines cybersecurity awareness among the students of Universiti Teknologi MARA, Kuala Terengganu Campus. The 110 students from two programs took part in this survey (bachelor's degree in computer science and bachelor's degree in business computing).

Table 2: Respondent's demographic information

Variables	Sub Variables	n	%
Gender	Male	65	59.1
	Female	45	40.9
Programs	Computer Science	85	77.3
	Business Computing	25	25.7

As shown in Table 2 and Fig. 4.1, out of this number, 65 students (59.1%) are male students, and the rest are female students (n=45, 40.9%). The highest number of participants are from the Computer Science program (n=85, 77.3%), followed by the Business Computing program (n=25, 22.7%). This study investigates university students' awareness of cyber security elements consisting of personal information, cyberbullying, cyberattacks, cyber insurance, internet activities and do & don'ts in Cyber Space.

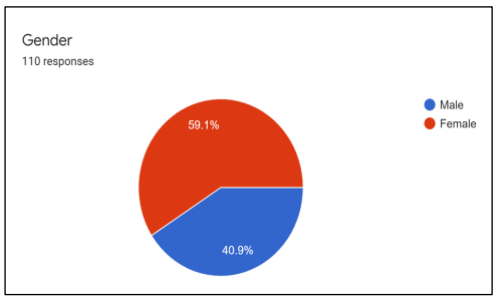

Fig. 4.1: Participants of students by Gender

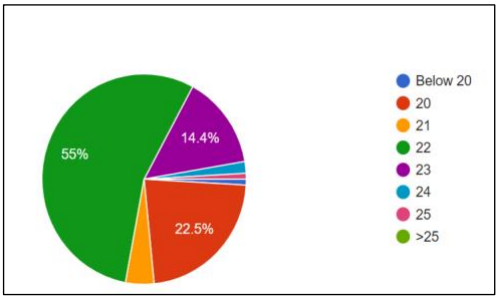

Fig. 4.2: Distribution of students by age

Fig. 4.2 shows that the enormous number of participants, 61 students are from the age group of 22 years old (55%), followed by the age 20 years old with 25 students (22.5%), 16 students of 23 years old (14.4%), five students of 21 years old (4.5%), two students of 24 years old (1.8%) and one student of 25 years old (0.9%). The variety of age groups can contribute to different thinking capabilities and experiences.

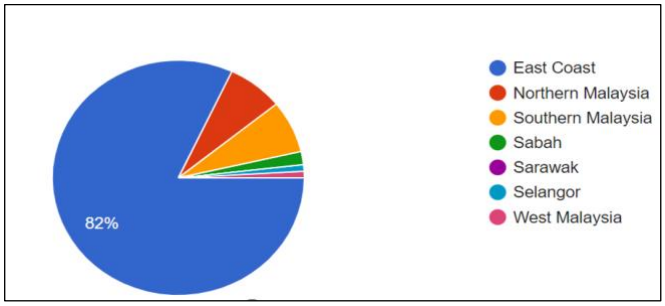

Fig. 4.3: Shows the distribution of students by Origin

Fig. 4.3 shows that the students come from different parts of Malaysia. The majority at 82% are from East Coast Region, which covers Pahang, Kelantan, and Terengganu, with 91 participants. Followed by 7.2% from Northern Region, which covers Kedah, Perlis, and Perak, with 8 participants. The figures reported for Southern Region (Johor) are 8 participants. Selangor and Sabah each have two respective participants contributing to 1.8% each.

Table 3 summarises the mean for each item in terms of students' views on the knowledge and awareness of cyber security, cyber-attack, cyberbullying, and cyber insurance. It shows that most students know cyber security and cyber-attack, 96.36% and 98.18%, respectively. All of them have answered that they are also aware of cyberbullying. It is good news as our students are well versed in the dangers they may face when online surfing. A computer science education improves awareness of cybersecurity and must practice safety precautions. A small minority of a few students (20.91%) indicated that they do not know about cyber insurance and how it can mitigate cyber risks.

Table 3: Descriptive Analysis of Students' Awareness & Knowledge

Awareness & Knowledge	Yes (%)	No (%)	Not sure (%)	Mean	Median	Mode	Standard Deviation
Cyber Security	96.36	2.73	0.91	1.94	2.00	2.00	0.34
Cyber Attack	98.18	1.82	0.00	0.98	1.00	1.00	0.13
Cyber Bully	100.00	0.00	0.00	1.00	1.00	1.00	0.00
Cyber Insurance	20.91	77.27	1.82	0.44	0.00	0.00	0.82

Fig. 4.4 shows students' different types of attacks when dealing with an online platform (one student can choose multiple attacks). According to the survey respondents, the virus attack is the one that happened with higher frequency, with 83.8% agreeing that they face this issue, followed by spam emails that show 78.4%, malware with 51.4%. On the other hand, DNS Spoofing and Man of the middle attack are less-faced, according to the respondents.

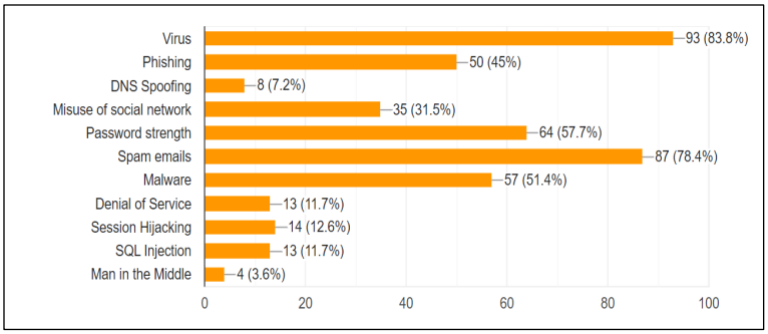

Fig. 4.4: Shows the different types of attacks they experience.

Most students admitted that they only change their passwords occasionally every six months. As shown in Fig. 4.5, 39.09% of them used to renew their password only when warned.

On the other hand, 19.09% of respondents acknowledged updating their password if the system tells them to do so. The data appear symmetrical, which explains why the mean is greater than the median in Table 4. Advice and education will improve this habit of students so that they are well-versed on the danger they may face when they are reluctant to change their password frequently.

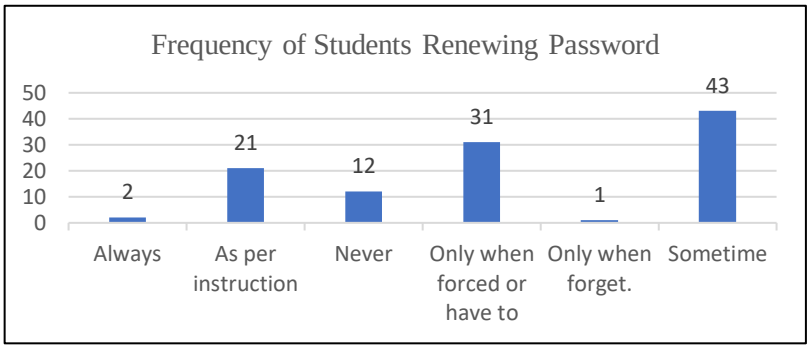

Fig. 4.5: Frequency of times students changed their Internet application password in 6 months

Table 4: Descriptive Analysis of Frequency of Students Renewing Password

Mean	Median	Mode	Standard Deviation	Skewness
3.25	3.00	5.00	1.60	-0.22

In response to a question about whether they have installed the anti-virus application, nearly all surveyed indicated that they have already installed it on their computers to be safe from cyber threats. Fig. 4.6 proves that only 19 students never renewed the anti-virus license, while 13 students did not install the anti-virus application. Table 5 portrays that the data are highly skewed, where the mean is 2.24, and the median is 3.00, respectively. It is essential to keep the anti-virus software up to date as one of the precautions against a cyber breach.

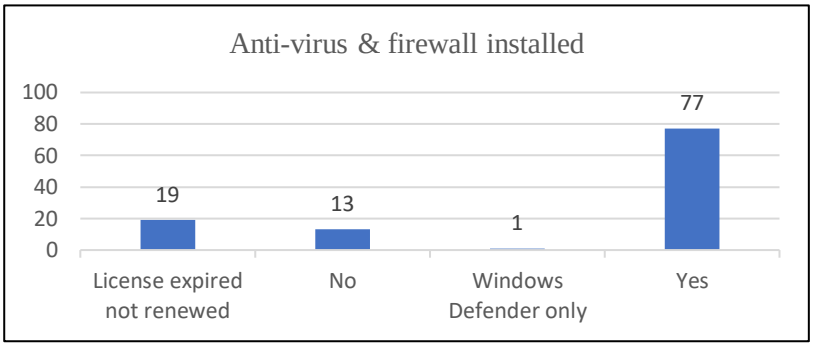

Fig. 4.6: Antivirus software of firewall application installed in access computer

Table 5: Descriptive Analysis of Students that Installed the Anti-Virus and Firewall

Mean	Median	Mode	Standard Deviation	Skewness
2.24	3.00	3.00	1.21	-1.07

Only 5 of the 110 students who participated in the survey frequently shared their passwords with their peers. Fig. 4.7 displays the number of students who never and occasionally shared the same password with their friends. The mean score for this question is 1.45, as shown in Table 6, which shows the data are symmetrical. It seems that the students were not concerned about security around friends and were quite happy to share their passwords.

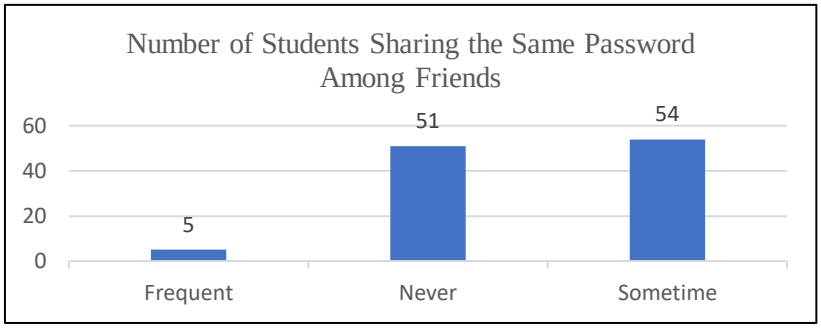

Fig. 4.7: Share or reveal internet or computer password access with friends

Table 6: Descriptive Analysis of Students that Shared the Same Password Among Friends

Mean	Median	Mode	Standard Deviation	Skewness
1.45	1.00	2.00	0.58	-0.49

As for the question about downloading from unlicensed or unknown sources, further analysis showed that 50% of the students highly agreed that they used to download unlicensed software applications illegally from unknown sites. The overall response to this question in Fig. 4.8 was surprisingly negative as it is unsafe and highly exposed to cyber threats or data theft. Table 7 proves the data are symmetrical as the mean score is 0.86 and the median equals 1, respectively. This result offered invaluable evidence for downloading software from unknown sites. Despite many students being aware of cybersecurity in Table 3, few students never downloaded any applications from unknown hosts.

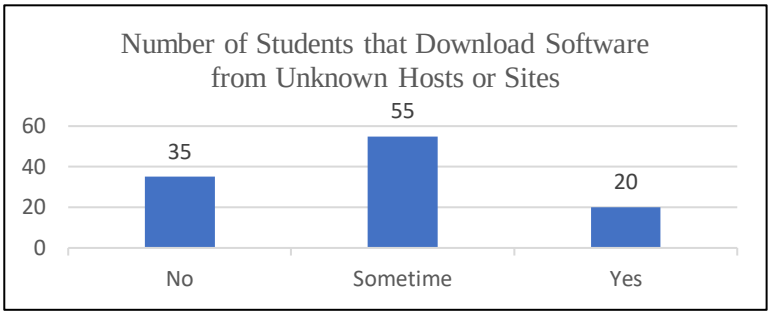

Fig. 4.8: Download software from an unknown host or sites

Table 7: Descriptive Analysis of Students that Download Software from Unknown Source

Mean	Median	Mode	Standard Deviation	Skewness
0.86	1.00	1.00	0.70	0.19

Table 8 shows the descriptive analysis data of accessing bank services websites using public wireless service. The result in Fig. 4.9 proved that the majority agreed that they do not use public WIFI when accessing online banking services. However, it is crucial to note that many people from different backgrounds can access public WIFI; it is possible to steal the data of online banking for personal benefits.

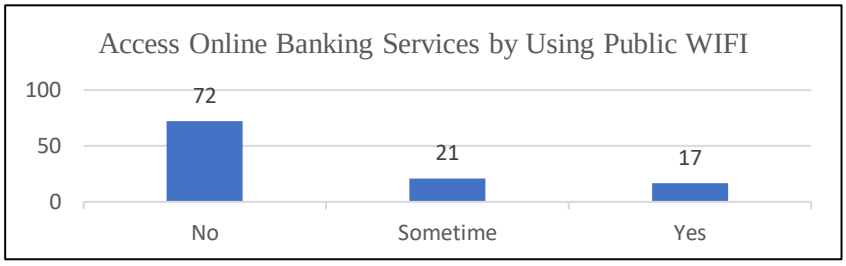

Fig. 4.9: Accessing bank services website using public WIFI

Table 8: Descriptive Analysis of Students that Access Bank Services Website Using Public WIFI

Mean	Median	Mode	Standard Deviation	Skewness
0.50	0.00	0.00	0.75	1.12

Interestingly, the last question revealed many students are interested in learning cybersecurity. Fig. 4.10 proved that 77.27% of the students agreed to study and dive deep into cybersecurity. As per Table 9, the descriptive analysis stated that the data collected for this question are highly skewed. This is in good agreement, as displayed in Table 3, where the students were interested in learning cybersecurity to build solid fundamentals and be prepared for unpredictable events such as cyber-attacks. In addition, students understood the exposure to cyber risk if they were negligent of the precautions.

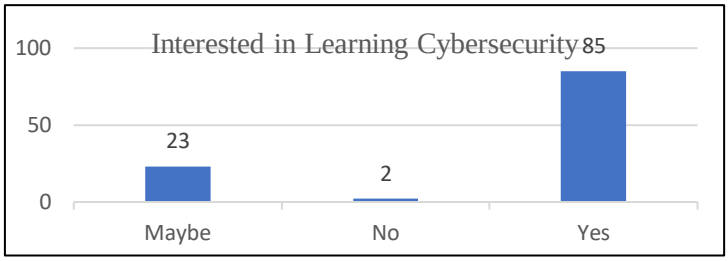

Fig. 4.10: Interested in Learning Cybersecurity

Table 9: Descriptive Analysis of Students interested in Learning Cybersecurity

Mean	Mediar	Mode	Standard Deviation	Skewness
1.56	2.00	2.00	0.82	-1.38

5 Conclusion

Cybersecurity awareness is essential in an organisation that is related to IT. The result of this study showed that even though Universiti Teknologi MARA (UiTM) Terengganu Faculty of Computer Science students demonstrated a decent level of awareness of some aspects of cyber security such as cyber-attack, cyberbullying, and personal information. However, there is still no appropriate depth of knowledge of cyber security. Although the students' awareness level is high of the attacks, survey results still show that students are involved in activities that can contribute to the security risk, such as sharing passwords and accessing unknown websites and ignorance in protecting their information or safety. The students are still unaware of how to protect their data and privacy. Exposure to the internet daily has positioned students to cyber dangers. Proper guidance and frequent knowledge transfer to the student can help to solve this issue. Currently, there is no active program for rising cybersecurity knowledge among the students. The only contribution to the mastery is taking computer and cyber security subjects. Other than that, students can attend external cyber security and awareness programs. Moreover, to spread awareness across all levels, the government should handshake with private entities to better educate our children.

6. Suggestions for Future Research

The conclusion cannot represent the entire population of UiTM since the sampling size only caters for the UiTM Terengganu Computer Science and Business Computing students. However, a more extensive sampling might help future research with a different branch campus of UiTM to ensure that the outcome can represent the population.

7. Acknowledgement

The authors would like to express gratitude to all students willing to take some time to participate in this study. The authors would also like to extend their appreciation to RCF Grant-600-UiTMCTKD (PJI/RMU 5/2/1)/RCF2020-ST (5/2020) Science and Technology, Universiti Teknologi MARA (UiTM), Terengganu for supporting and helping on the publication of this study and Malaysian Communications and Multimedia Commission for the reference of their documents and Cyber Security Malaysia.

8. References

Abrar, Anwar. (2020). Annual Report 2020. *CGC.* https://cgc.com.my/annual-report-2020/downloads/CGC-Annual-Report-2020.pdf

Aziz, A. A., Osman, S., Widyarto, S., & Marjudi, S. (2020). The Descriptive Data Analysis for E-learning Cloud-based Factor Adoption.

Conroy, R. M. (2016). *The RCSI Sample size handbook*. A rough guide.

Hashim, M. S. b. (2011). Malaysia's National Cyber Security Policy: The country's cyber defence initiatives. *2011 Second Worldwide Cybersecurity Summit (WCS).*

Hatimtai, M. H., & Hassan, H. (2018). The relationship between the characteristics of innovation towards the effectiveness of ICT in Malaysia productivity corporation. *Jurnal Komunikasi: Malaysian Journal of Communication, 34*(1).

Husni Rahiem, M. D. (2021). Indonesian university students' likes and dislikes about emergency remote learning during the COVID-19 pandemic. *Asian Journal of University Education (AJUE), 17*(1), 1-18.)

Johan, Z. J., Hafit, N. I. A., & Tusyanah, T. (2021). Technology Addiction among UiTM Puncak Alam and UNNES Semarang Students. *Asian Journal of University Education, 17*(4), 511-526.

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology, 7*(421), 11-14.

Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017). *Descriptive Analysis in Education: A Guide for Researchers*. NCEE 2017-4023. National Center for Education Evaluation and Regional Assistance.

Malaysia Cyber Security Strategy, 2020 – 2024. (2020), https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

Malaysian Digital Association. (2016). Malaysia Digital Landscape Exploring the Digital Landscape In Malaysiaboosting Growth For A Digital Economy. *The Digital Integration & Business Transformation Asia Con.*

Malaysian Education Blueprint Higher Education 2015-2025. (2013). https://jpt.mohe.gov.my/portal/index.php/en/corporate/development-plan/16-malaysia education-development-plan-2015-2025

Md Noh, N. H., Raju, R., Eri, Z. D., & Ishak, S. N. H. (2021). Extending technology acceptance model (TAM) to measure the students' acceptance of using digital tools during open and distance learning (ODL). *International Conference of Emerging Challenges in Engineering and Current Technology (ICECT III).*

Raju, R., Noh, N. H. M., Ishak, S. N. H., & Eri, Z. D. (2021). Digital Tools Acceptance in Open Distance Learning (ODL) among Computer Science Students during COVID-19 Pandemic: A Comparative Study. *Asian Journal of University Education, 17*(4), 408-417.

Roca, S. K.-L.-D.-V. (2019). *Cybersecurity Current Challenges and Inria's research directions*. Le Chesnay Cedex, France: Inria.

Salkind, N. J. (2010). *Research Methods*. Encyclopedia of research design (Vols. 1-0). https://dx.doi.org/10.4135/9781412961288

UNESCO, U. (2020). *COVID-19 Educational Disruption and Response*. https://en.unesco.org/covid19/educationresponse

Yun, T. Z. (2021). *Cybersecurity: Staying Ahead of Cyber Criminals*. The Edge Malaysia. https://www.theedgemarkets.com/article/cybersecurity/staying-ahead-cybercriminals

Yusuf, S., Mohamed Al-Majdhoub, F., Mubin, N. N., Chaniago, R. H., & Rahim Khan, F. (2021). Cyber aggression-victimization among Malaysians youth. *Asian Journal of University Education (AJUE)*, *7*(1), 240-260.