VoA
2025
Volume 21 Issue 2

اونيۏرسيتي تيکنولوݢي مارا
UNIVERSITI
TEKNOLOGI
MARA

Voice of Academia

Academic Series of Universiti Teknologi MARA Kedah

ISSN: 2680-7840

DR. FARAH SYAZRAH BINTI MOHD GHAZALLI,
UNIVERSITI SULTAN ZAINAL ABIDIN (UniSZA), TERENGGANU.

DR FARYNA MOHD KHALIS,
UNIVERSITI TEKNOLOGI MARA (UiTM) SHAH ALAM, MALAYSIA

DR. MOHAMAD IDHAM MD RAZAK,
UNIVERSITI TEKNOLOGI MARA (UiTM) SEREMBAN 3 BRANCH, MALAYSIA

DR. MOHD FAIZAL JAMALUDDIN,
UNIVERSITI TEKNOLOGI MARA (UiTM) KEDAH BRANCH, MALAYSIA

DR NOR ARDYANTI AHMAD,
UNIVERSITI TEKNOLOGI MARA (UiTM) KEDAH BRANCH, MALAYSIA

DR NOR AMIRA SYAZWANI,
UNIVERSITI TEKNOLOGI MARA (UiTM) PAHANG BRANCH, MALAYSIA

DR NOR RAIHANA ASMAR MOHD NOOR,
UNIVERSITI TEKNOLOGI MARA (UiTM) KELANTAN BRANCH, MALAYSIA

DR RAZLINA RAZALI,
UNIVERSITI TEKNOLOGI MARA (UITM) SEREMBAN 3 BRANCH, MALAYSIA

DR RIZAL ZAMANI IDRIS,
UNIVERSITI MALAYSIA SABAH (UMS), SABAH, MALAYSIA

DR. SAKINATUL RAADIYAH ABDULLAH,
UNIVERSITI TEKNOLOGI MARA (UiTM) KEDAH BRANCH, MALAYSIA

DR. SALIMAH YAHAYA,
UNIVERSITI TEKNOLOGI MARA (UITM) TERENGGANU BRANCH, MALAYSIA

DR. SITI NORFAZLINA YUSOFF,
UNIVERSITI TEKNOLOGI MARA (UiTM) KEDAH BRANCH, MALAYSIA

DR. SURITA HARTINI MAT HASSAN,
UNIVERSITI TEKNOLOGI MARA (UiTM) PAHANG BRANCH, MALAYSIA

DR. SHAHIRAH SAID,
UNIVERSITI TEKNOLOGI MARA (UiTM) PERMATANG PAUH,
PULAU PINANG BRANCH, MALAYSIA

PROFESOR MADYA TS DR MOHD NOR MAMAT,
UNIVERSITI TEKNOLOGI MARA (UiTM) SHAH ALAM, MALAYSIA

PROF. MADYA DR. WAN NOR JAZMINA BINTI WAN ARIFFIN,
UNIVERSITI SULTAN ZAINAL ABIDIN (UniSZA), TERENGGANU.

LANGUAGE REVIEWER

A&N ACADEMIC AND SCIENTIFIC EDITING SERVICES

DR. NURAINI ABDULLAH,
ACADEMY LANGUAGE STUDIES,
UNIVERSITI TEKNOLOGI MARA (UiTM) PERLIS BRANCH, MALAYSIA

FAHAROL ZUBIR,
ACADEMY LANGUAGE STUDIES,
UNIVERSITI TEKNOLOGI MARA (UiTM) PERLIS BRANCH, MALAYSIA

MATHS PROOFREAD SDN BHD

MAJDAH CHUAN,
ACADEMY LANGUAGE STUDIES,
UNIVERSITI TEKNOLOGI MARA (UiTM) PERLIS BRANCH, MALAYSIA

NOR ASNI SYAHRIZA BINTI ABU HASSAN,
ACADEMY LANGUAGE STUDIES,
UNIVERSITI TEKNOLOGI MARA (UiTM) KEDAH BRANCH, MALAYSIA

NURUL HAMIMI BINTI AWANG JAPILAN,
UNIVERSITI MALAYSIA SABAH (UMS), SABAH, MALAYSIA

e-ISSN: 2682-7840

9 772682 784004

© Voice of Academia is jointly published by the
Universiti Teknologi MARA (UiTM) Kedah Branch,
Malaysia and Penerbit UiTM (UiTM Press),
Universiti Teknologi MARA (UiTM) Malaysia,
Shah Alam, Selangor.

The views, opinions and technical recommendations expressed by the contributors and authors are entirely their own and do not necessarily reflect the views of the editors, the Faculty or the University.

TABLE of CONTENTS

TABLE of CONTENTS

Voice of Academia
Academic Series of Universiti Teknologi MARA Kedah

Voice of Academia Vol.21 Issue (2) 2025

Voice of
Academia

e-ISSN: 2682-7840

ASSESSMENT OF CYBERSECURITY AND PRIVACY AWARENESS AMONG NON-COMPUTER SCIENCE STUDENTS IN HIGHER LEARNING INSTITUTIONS

Satria Arjuna Julaihi[1]*, Norizuandi Ibrahim[2], Lenny Yusrina Bujang Khedif[3] & Neelam Amelia Mohamad Rejeni[4]

[1,2,3] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Sarawak, Kampus Samarahan 2
[4] Jabatan Teknologi Maklumat dan Komunikasi, Politeknik Kuching, Sarawak

ARTICLE INFO

Article history:

Received Jan 2025
Accepted May 2025
Published July 2025

Keywords:

Awareness, cybersecurity and privacy, pre-quiz, post-quiz & intervention

Corresponding Author:
satria@uitm.edu.my

ABSTRACT

This article focuses on using a pre-quiz and post-quiz methodology to evaluate students' awareness of cybersecurity and privacy among non-computer science students in higher education institutions. The study's main goals are to gauge students' prior knowledge of cybersecurity and privacy issues before any kind of intervention and to assess how well an educational intervention raises students' awareness levels. Students are given a pre-quiz survey as part of the study to see how well-versed they are in cybersecurity and privacy principles. An educational intervention is then carried out, and any changes in students' knowledge, attitudes, and practices regarding cybersecurity and privacy are evaluated using a post-quiz survey. The methodology's goals are to shed light on how well educational programs raise students' knowledge of cybersecurity and privacy issues and to guide the development of future for fostering digital literacy and online safety among higher education institution students. The results show that students' comprehension of cybersecurity and privacy concepts significantly improved after the intervention, demonstrating a successful knowledge transfer and emphasizing the value of educational initiatives in raising students' awareness and preparing them for life in the digital age.

1. Introduction

As we progress further into the digital age, the knowledge regarding cybersecurity and privacy has become increasingly important. As individuals, we do a lot of online activities including socializing and e-commerce, which often involve exposing a lot of our personal information online and making us potential targets for cybercriminals. If we look at the students' community, being young and having their own devices, they would be eager to engage in online activities. Thus, making university students, attractive targets for cybercriminals due to the large amounts of sensitive data they possess and the diverse range of devices they use. Therefore, students in universities must be aware of cybersecurity and privacy issues. Including having the knowledge and skills to protect themselves and their information.

2. Literature Review

2.1 Various Approach in Increasing the Cybersecurity Awareness

Several studies have investigated methods for assessing cybersecurity awareness among students. A study by Du & Chintakovid (2023) explored the cybersecurity awareness of university students, finding that while they were aware of general cybersecurity concepts, they lacked specific knowledge and skills to protect themselves online. It is important to determine the target audience and coverage when selecting an assessment method for gauging cybersecurity awareness as done by Chaudhary, Gkioulos & Katsikas (2022) and Rohan et al. (2023). Esteve-Gonzalez et al. (2023) indicated that education, awareness, and training in cybersecurity increase the target participants capacity in dealing with the cybersecurity and privacy issues.

2.2 Difference in Demographics and the Difference of Awareness Level

Further research explores awareness across different student demographics. Huraj (2023) investigates potential differences in awareness levels between students in technical versus non-technical fields. This comparative approach highlights the importance of tailoring awareness programs to the specific needs and knowledge bases of diverse student groups.

2.3 Factors Influencing Cybersecurity Awareness

Various factors can influence students' cybersecurity awareness levels, Alharbi et al. (2021) found that students often engage in risky online behaviour due to a lack of knowledge about cybersecurity threats and consequences. Khalid et al. (2018) revealed that while students may demonstrate awareness in certain areas like cyberbullying and internet banking, they often lack knowledge in other areas. These findings underscore the need for comprehensive cybersecurity education intervention that addresses various threats and vulnerabilities. Raju (2022) also highlighted the importance of equipping students with knowledge to navigate the digital world safely, while promoting responsible online behaviour.

2.4 Impact of Training and Intervention Programs

Various research has explored the impact of training and intervention programs to increase the level of awareness. Zukarnain (2020) examines the effectiveness of targeted training programs in improving students' understanding of cybersecurity threats and best practices. Peker (2018) explores the potential of online modules as a scalable and accessible approach to cybersecurity education. These studies provide valuable insights into the design and implementation of effective awareness programs.

The influence of demographic factors on cybersecurity awareness has also been a subject of investigation. Daengsi (2022) examines the role of age and gender in shaping individuals' susceptibility to phishing attacks. While this study focuses on employees, the findings regarding demographic influences on awareness can be insightful when considering student populations as well.

2.5 Importance of Awareness Programs

Rehman (2023) emphasizes the importance of developing awareness programs that cater to the needs of non-technical audiences. This aligns with the focus of the current study, which aims to assess cybersecurity and privacy awareness among students from non-computer science backgrounds.

Overall, the existing literature highlights the importance of a multifaceted approach to cybersecurity awareness, considering the diverse needs and characteristics of student populations.

2.6 Assessment method

This study will employ a pretest-posttest design, using the quantitative approach of data analysis. The survey method will be used to collect data from students, focusing on their knowledge and behaviors related to cybersecurity and privacy as done by Lallie et al. (2023), Alyami et al. (2023), Persadha et al. (2016), Nkongolo et al. (2023) and Li et al. (2014).

The survey instrument will be designed based on the existing literature and will cover topics such as awareness of common cybersecurity threats (e.g., phishing, malware, social engineering).

3. Methodology

This study aims to assess the level of knowledge regarding cybersecurity and privacy awareness among students in higher learning institutions, specifically those from non-computer science backgrounds, namely the Diploma in Science and Office Management in UiTM Sarawak. The research will use the pretest-posttest design, where respondents are asked to answer the same sets of quiz questions before and after a sharing session (Nagahawatta et al., 2020). The quiz questions comprise of 3 sections. Section A on Demographics, collecting information about the respondents' gender, and their field of study. Section B on the Level of Understanding, the respondents need to answer three questions regarding their understanding of cybersecurity, its importance and threats. These questions are presented with a Likert scale ranging from "Strongly Understand" to "Not Understand." Section C on the Level of Awareness, where the respondents need to respond to 5 multiple choice questions regarding privacy, importance of cybersecurity for business and organizations, type of cyber-attacks, personal security measures and right of protection in today's digital landscape. The question in this section is based on the sharing session (Lallie et al., 2023) (Omar et al., 2021).

The quiz will be conducted through an online survey platform. Respondents will be given 15 minutes to complete the quiz. The pre-quiz will be conducted before the sharing session, and the post-quiz will be done right after the session. The sharing session covered the topics like Definition of Privacy and Cybersecurity, Importance of Privacy and Cybersecurity, Cyberattack, Precautions and Best Practices. The pre-quiz and post-quiz will see if there is any improvement in the students' awareness and understanding, after listening to the sharing session.

4. Results and Discussion

We aimed to analyse the complete group of students, known as the population, with the respondents serving as a subset of the population. We planned to conduct a survey of students at the UiTM Sarawak Branch, Samarahan Campus, with an emphasis on their level of understanding of cybersecurity and protection. To achieve these research goals, we analysed the data in three sections: Section A (demographics), Section B (students' awareness of key cybersecurity topics), and Section C (knowledge transfer).

4.1 Section A (Demographic)

The pie chart in Figure 1 depicts the demographic distribution of respondents by group and program of study. The largest portion, 23.10%, comes from BM1324A group. Following that, the AS1204E and AS1204F groups comprises for 17.20% of all respondents. There are 14.20% respondents from BM1324B and 10.40% from AS1204B. Finally, the BM1324G group comprises for 17.90% of all participants. Overall, 55.20% of the respondents are enrolled in the Diploma in Science (AS1204B, AS1204E, and AS1204F), and 44.80% are from the Diploma in Office Management (BM1324A, BM1324B, and BM1324G).

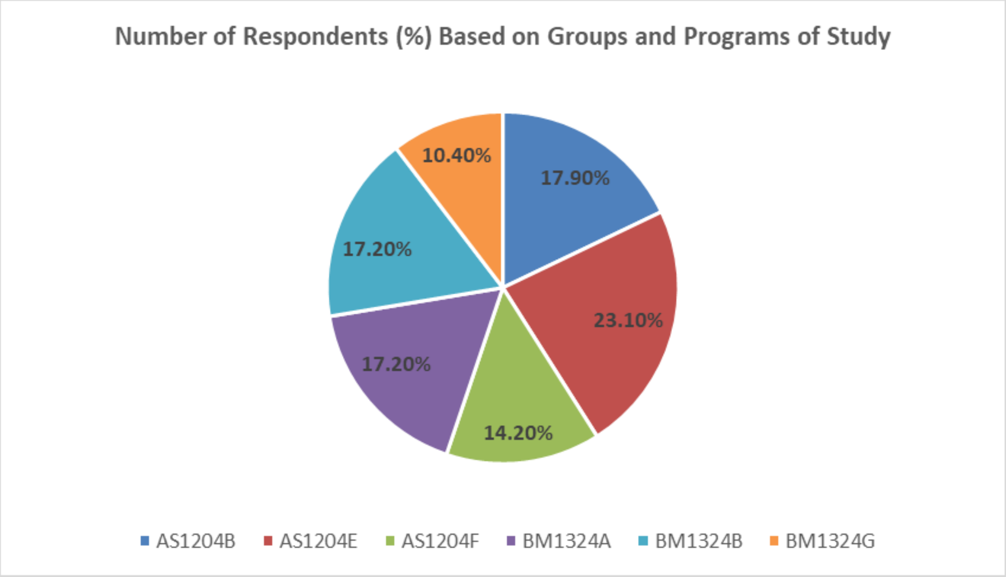

Figure 1: Number of Respondents based on Group and Program of Study

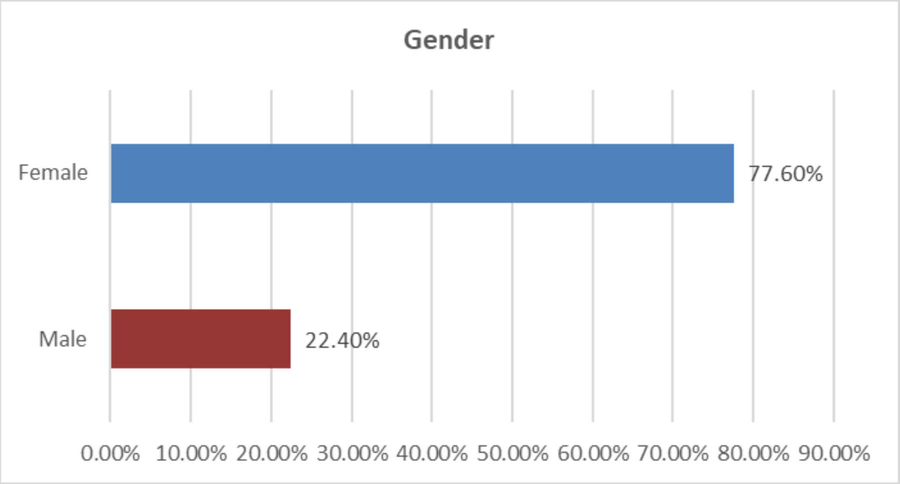

Figure 2: Gender Distribution

The bar chart (Figure 2) illustrates the gender distribution of the respondents. According to the chart, a substantial majority of the respondents are female, constituting 77.60% of the total. In contrast, male respondents make up 22.40%. This indicates a significant gender imbalance among the participants, with females being the predominant gender. The data suggests that any analysis or conclusions drawn from this group may be more representative of female perspectives, given their larger proportion in the sample.

4.2 Part B: Analysis on Level of Understanding using Pre-Quiz and Post-Quiz

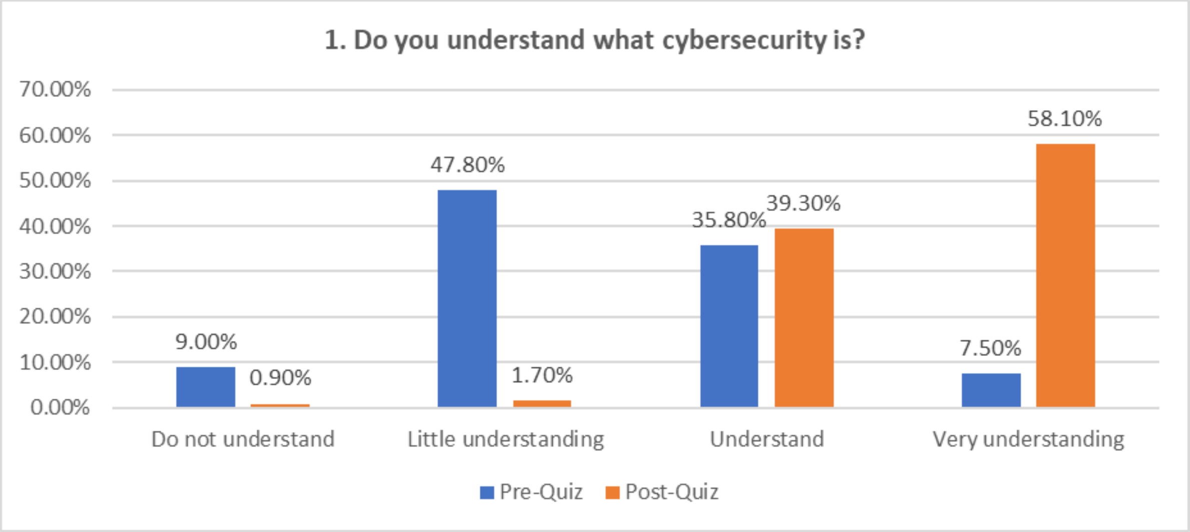

Figure 3: Level of understanding on What is Cybersecurity

The graph shown in the figure above compares the level of understanding of cybersecurity before (Pre-Quiz) and after (post-quiz) the sharing session. In terms of improvement in understanding, there is a significant increase in the percentage of participants with a "Very understanding" level of cybersecurity, from 7.50% in the pre-quiz to 58.10% in the post-quiz. The percentage of participants who have an "Understand" level also increased slightly from 35.80% to 39.30%. The reduction in low understanding shows in the percentage of participants who "Do not understand" cybersecurity dropped dramatically from 9.00% to 0.90%. Similarly, those with "Little understanding" decreased substantially from 47.80% to 1.70%.

The sharing session appears to have been highly effective in improving participants' understanding of cybersecurity. The data shows a clear shift from lower levels of understanding to higher levels, indicating that the intervention successfully enhanced the participants' knowledge and comprehension of cybersecurity concepts.

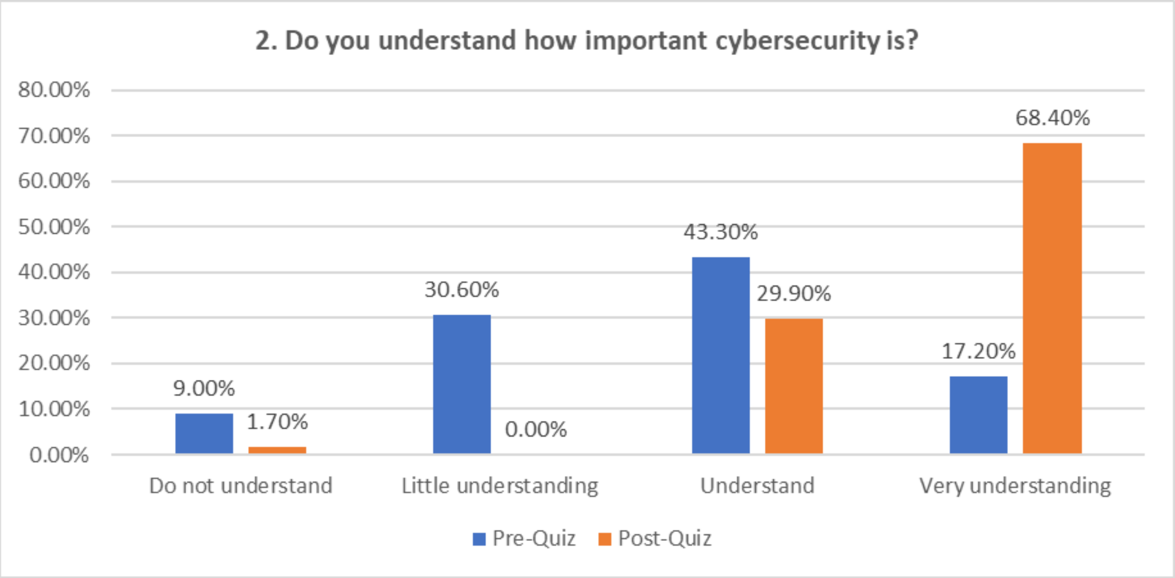

Figure 4: Level of Understanding on the Importance of Cybersecurity

This graph in Figure 4 compares the understanding of the importance of cybersecurity before (Pre-Quiz) and after (post-quiz) the sharing session. The finding shows a decrease in the low understanding region. There is a significant drop in the percentage of participants who "Do not understand" the importance of cybersecurity, from 9.00% to 1.70%. Similarly, those with "Little understanding" dropped from 30.60% to 0.00%. On the other hand, there is a shift to the higher understanding region. The percentage of participants who "Understand" the importance of cybersecurity decreased from 43.30% to 29.90%. This decrease is likely due to a shift of participants from the "Understand" category to the "Very understanding" category. The most significant change is seen in the "Very understanding" category, which increased substantially from 17.20% to 68.40%.

The sharing session was highly effective in enhancing participants' understanding of the importance of cybersecurity. The data shows a clear shift from lower levels of knowledge to higher levels, indicating that participants gained a better appreciation of cybersecurity's significance after the intervention. The marked increase in the "Very understanding" category is particularly noteworthy, demonstrating a significant improvement in awareness and comprehension.

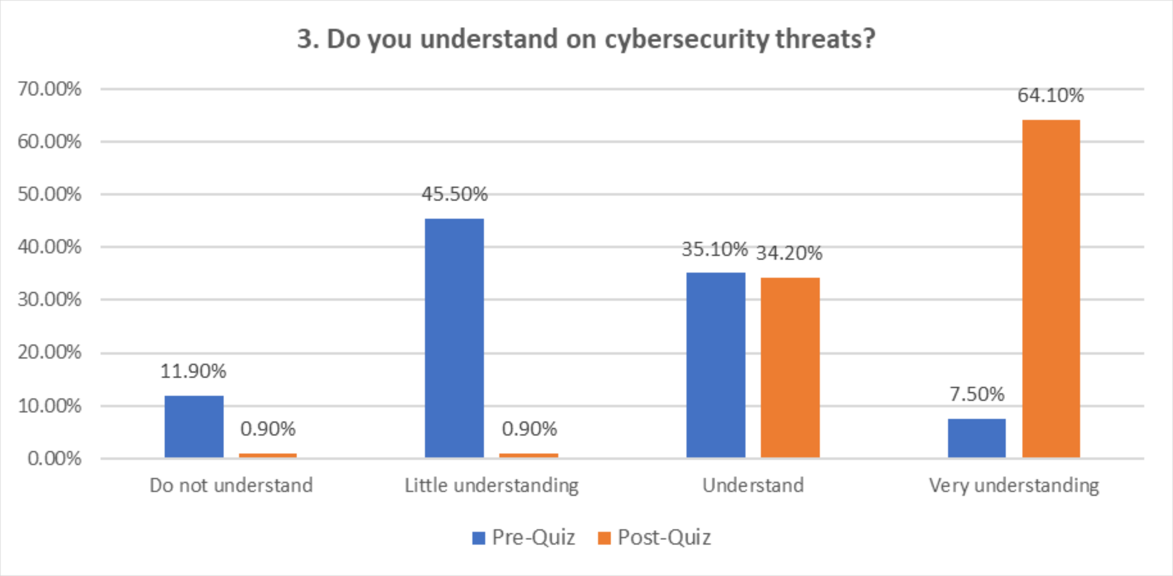

Figure 5: Level of Understanding on Cybersecurity Threats

The bar chart (Figure 5) above compares the respondents' understanding on cybersecurity threats before (Pre-Quiz) and after (post-quiz) the sharing session. There is a significant reduction in low understanding of cybersecurity threats. The percentage of respondents who "Do not understand" their cybersecurity threats dropped dramatically from 11.90% to 0.90%. Similarly, those with "Little understanding" decreased sharply from 45.50% to 0.90%. On the other hand, there is an increase in the higher understanding of cybersecurity threats. The percentage of respondents who "Understand" their cybersecurity threats remained relatively stable, with a slight decrease from 35.10% to 34.20%. The most notable change is in the "Very understanding" category, with a substantial increase from 7.50% to 64.10%.

The sharing session, as an educational intervention was highly effective in enhancing respondents' understanding of their cybersecurity threats. The data shows a significant shift from the lower levels of understanding to the higher levels. The substantial increase in the "Very understanding" category indicates that majority of the participants gained a much deeper comprehension of cybersecurity threats after the intervention. The decreases in the “Do not understand” and “Little understanding” categories further highlight the success of the educational efforts in improving cybersecurity awareness and knowledge.

4.3 Part C: Analysis on Knowledge Transfer using Pre-Quiz and Post-Quiz with espondents choose a correct answer

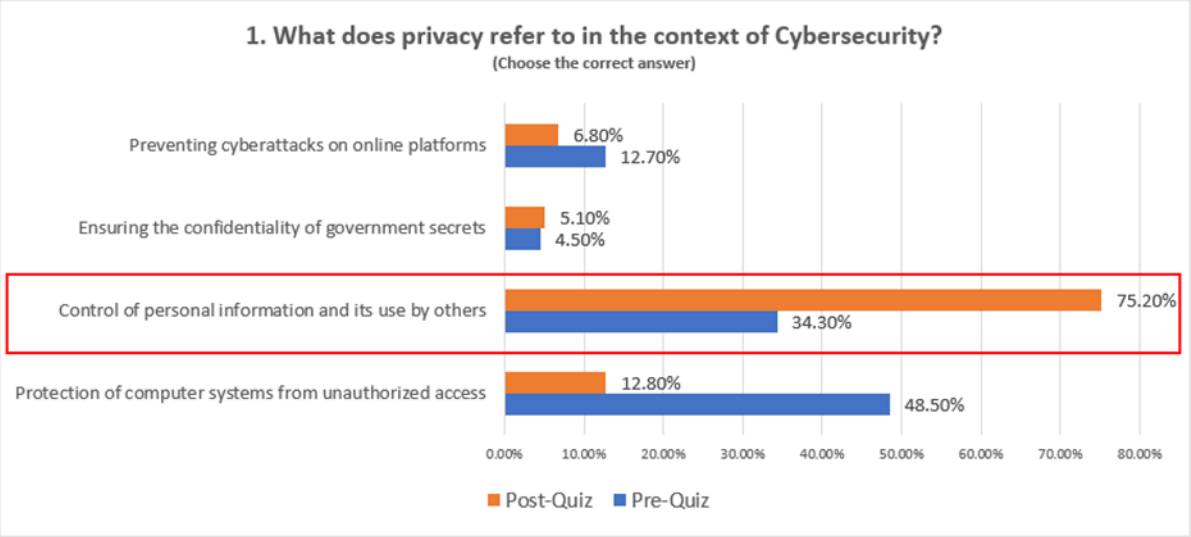

Figure 6: Analysis of Knowledge Transfer based on What does privacy refer to in the context of Cybersecurity?

The bar chart shows the responses of participants to the question "What does privacy refer to in the context of Cybersecurity?" before (Pre-Quiz) and after (post-quiz) an educational intervention. The correct answer, "Control of personal information and its use by others," is highlighted in a red box.

There is a substantial increase in the percentage of respondents who chose the correct answer, "Control of personal information and its use by others," from 34.30% (Pre-Quiz) to 75.20% (post-quiz). This indicates a significant improvement in understanding the correct definition of privacy in the context of cybersecurity after the educational intervention.

The percentage of respondents who chose "Preventing cyberattacks on online platforms" decreased from 12.70% (Pre-Quiz) to 6.80% (post-quiz). Similarly, those who selected "Protection of computer systems from unauthorized access" dropped significantly from 48.50% (Pre-Quiz) to 12.80% (post-quiz). The choice of "Ensuring the confidentiality of government secrets" saw a slight increase from 4.50% (Pre-Quiz) to 5.10% (post-quiz), indicating some confusion still exists, but it is relatively minor.

The educational intervention was highly effective in improving the respondents' understanding of what privacy refers to in the context of cybersecurity. The significant increase in the correct responses and the corresponding decrease in incorrect responses highlight the success of the knowledge transfer. Most participants correctly identified the control of personal information and its use by others as the key aspect of privacy in cybersecurity after the intervention.

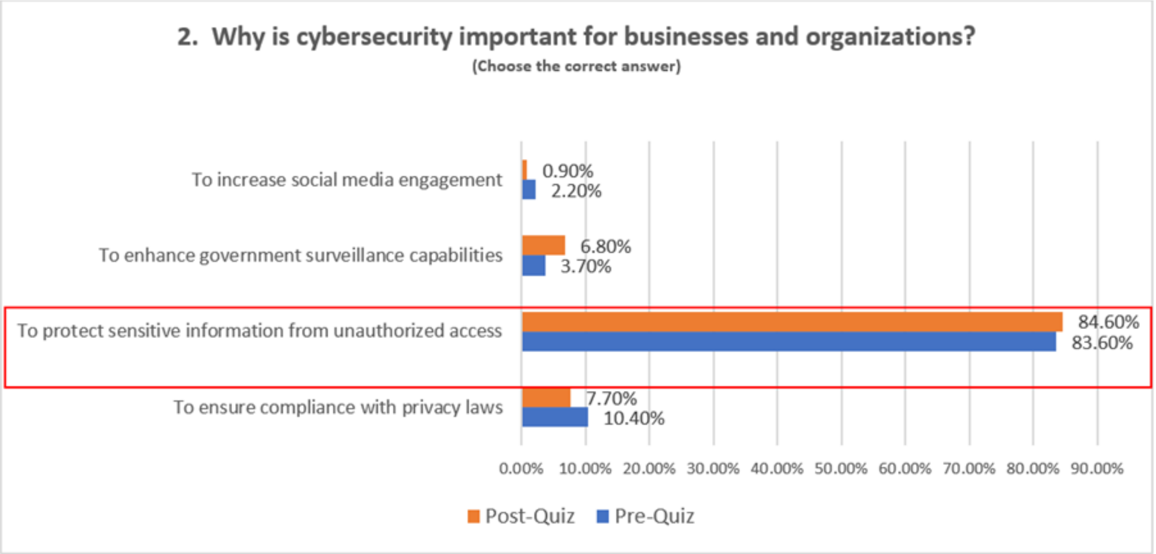

Figure 7: Analysis on Knowledge Transfer based on Why is cybersecurity important for businesses and organizations.

The bar chart in Figure 7 illustrates the responses of participants to the question "Why is cybersecurity important for businesses and organizations?" before (Pre-Quiz) and after (post-quiz) an educational intervention. The correct answer, "To protect sensitive information from unauthorized access," is highlighted in a red box.

The percentage of respondents who chose the correct answer, "To protect sensitive information from unauthorized access," was already high in the Pre-Quiz at 83.60% and increased slightly to 84.60% in the post-quiz. This indicates that most respondents were aware of the primary importance of cybersecurity even before the educational intervention, and this understanding was slightly reinforced after the intervention.

Meanwhile, there is a decrease in some incorrect answers. The percentage of respondents who chose "To increase social media engagement" decreased from 2.20% (Pre-Quiz) to 0.90% (post-quiz), indicating a reduction in this misconception. Similarly, those who selected "To ensure compliance with privacy laws" decreased from 10.40% (Pre-Quiz) to 7.70% (post-quiz).

However, the percentage of respondents who chose "To enhance government surveillance capabilities" increased from 3.70% (Pre-Quiz) to 6.80% (post-quiz). This suggests that there may have been some confusion introduced during the educational intervention regarding the role of cybersecurity in government surveillance.

The educational intervention had a mixed impact on the respondents' understanding of the importance of cybersecurity for businesses and organizations. While the recognition of the correct answer was already high and showed a slight increase, there was an unexpected rise in the misconception about enhancing government surveillance capabilities. This suggests that while the intervention successfully reinforced the primary purpose of cybersecurity, it may need to address and clarify other aspects to avoid introducing new misconceptions.

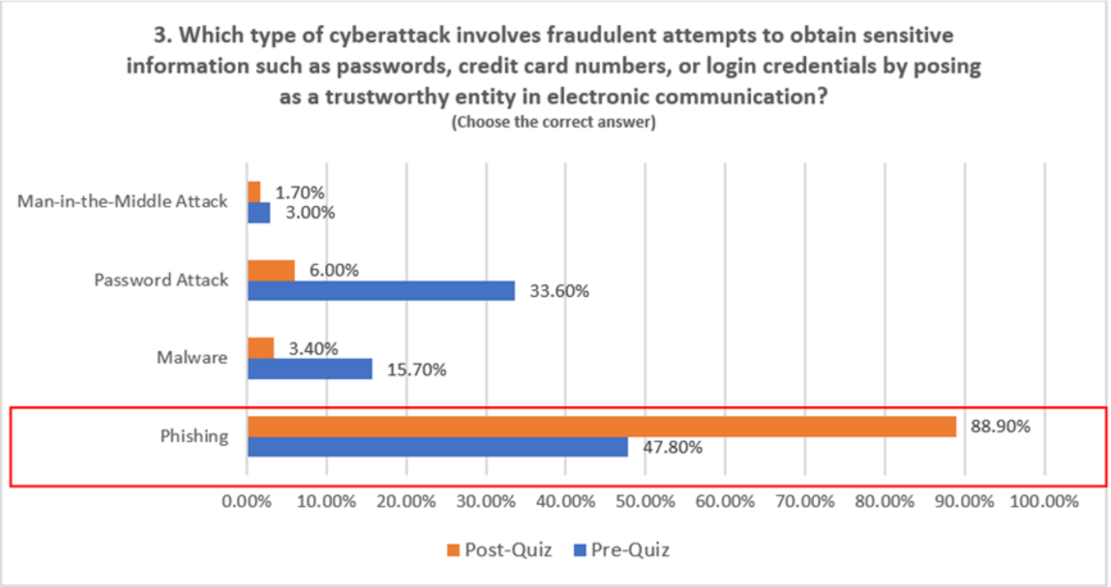

Figure 8: Analysis on Knowledge Transfer based on type of cyberattack involves fraudulent attempts

The bar chart in Figure 8 shows the responses of participants to the question " Which type of cyberattack involves fraudulent attempts to obtain sensitive information such as passwords, credit card numbers, or login credentials by posing as a trustworthy entity in electronic communication?" before (Pre-Quiz) and after (post-quiz) an educational intervention. The correct answer, "Phishing," is highlighted in a red box.

There is a substantial increase in the percentage of respondents who chose the correct answer, "Phishing," from 47.80% (Pre-Quiz) to 88.90% (post-quiz). This indicates a significant improvement in understanding which cyberattack involves fraudulent attempts to obtain sensitive information such as passwords, credit card numbers, or login credentials by posing as a trustworthy entity in electronic communication after the educational intervention.

The percentage of respondents who chose "Malware" decreased from 15.70% (Pre-Quiz) to 3.40% (post-quiz). Similarly, those who selected "Password Attack" dropped significantly from 33.60% (Pre-Quiz) to 6.00% (post-quiz). The choice of "Man-in the Middle-Attack" decreased from 3.00% (Pre-Quiz) to 1.70% (post-quiz).

The educational intervention was highly effective in improving the respondents' understanding type of cyberattack involves fraudulent attempts. The significant increase in the correct responses and the corresponding decrease in incorrect responses highlight the success of the knowledge transfer. Most respondents correctly identified the type of cyberattack involves fraudulent attempts after the intervention.

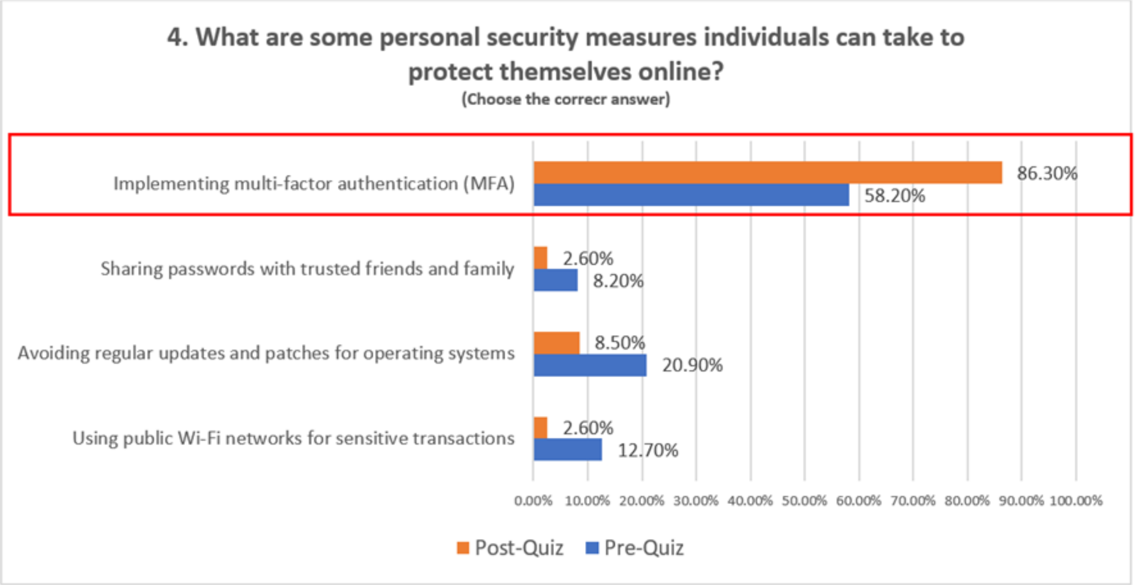

Figure 9: Analysis on Knowledge Transfer based on personal security measures individuals can take to protect themselves online

The bar chart in Figure 9 illustrates the responses of participants to the question " What are some personal security measures individuals can take to protect themselves online? " Before (pre-quiz) and after (post-quiz) an educational intervention. The correct answer, "Implementing multi-factor authentication (MFA)" is highlighted in a red box.

The percentage of respondents who chose the correct answer, " Implementing multi-factor authentication (MFA)" increased from 58.2% in Pre-Quiz to 86.30% in the post-quiz. This indicates a significant improvement in understanding implementation of multi-factor authentication (MFA) after the educational intervention.

The percentage of respondents who chose "Sharing password with trusted friends and family" decreased from 8.20% (Pre-Quiz) to 2.60% (post-quiz), indicating a reduction in this misconception. Similarly, those who selected "Avoiding regular updates and patches for operating system" decreased from 20.90% (Pre-Quiz) to 8.50% (post-quiz). In addition, there is also a decrease on "Using public Wi-Fi networks for sensitive transactions" from 12.70% (Pre-Quiz) to 2.60% (post-quiz).

The educational intervention was highly helpful in boosting respondents' comprehension of personal security measures individuals can take to protect themselves online. The considerable rise in accurate responses and the matching decrease in incorrect responses demonstrate the success of knowledge transfer. Most respondents accurately identified the personal security measures individuals can take to protect themselves online following the intervention.

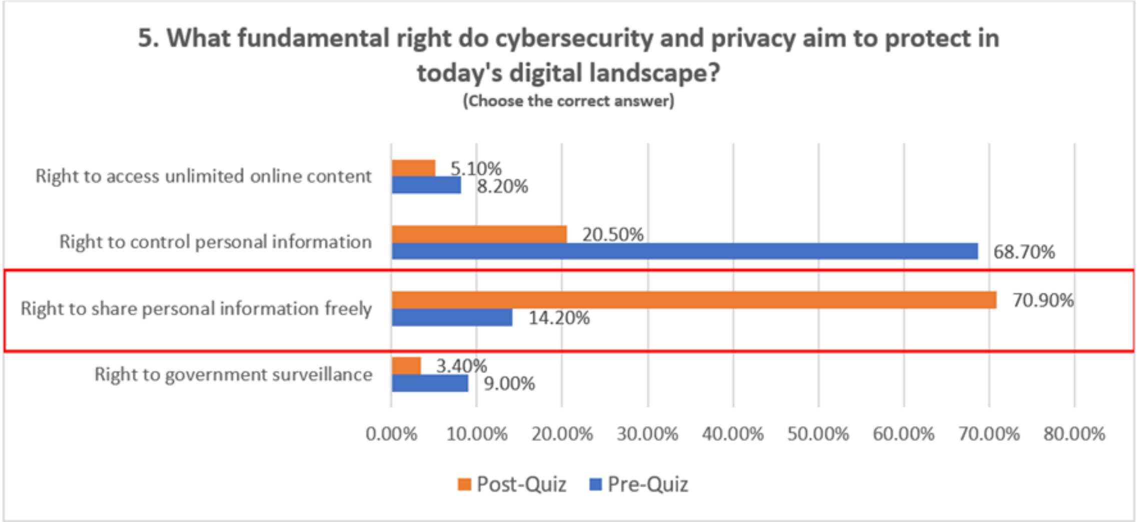

Figure 10: Analysis on Knowledge Transfer based on fundamental right do cybersecurity and privacy aim to protect in today's digital landscape

Participants' answers to the question, "What fundamental right do cybersecurity and privacy aim to protect in today's digital landscape?" both before (Pre-Quiz) and after (post-quiz) an educational intervention is displayed in Figure 10. "Right to freely share personal information" is the correct response, and it is shown by a red box.

There is a substantial increase in the percentage of respondents who chose the correct answer, "Right to freely share personal information," from 14.20% (Pre-Quiz) to 70.90% (post-quiz). This indicates a significant improvement on the fundamental right do cybersecurity and privacy aim to protect in today's digital landscape after the educational intervention.

The percentage of respondents who chose "Right to government surveillance" decreased from 9.00% (pre-quiz) to 3.40% (post-quiz). Similarly, those who selected "Right to control personal information" dropped significantly from 68.70% (Pre-Quiz) to 20.50% (post-quiz). The choice of "Right to access unlimited online content" decreased from 8.20% (pre-quiz) to 5.10% (post-quiz).

The educational intervention was very successful in raising respondents' awareness of the fundamental rights that cybersecurity and privacy seek to uphold in the current digital environment. The success of the information transfer is demonstrated by the notable rise in accurate responses and the commensurate decline in incorrect responses. After the intervention, most respondents correctly identified the fundamental rights that cybersecurity and privacy seek to preserve in the current digital context.

5. Conclusion

This study aimed to assess the level of cybersecurity and privacy awareness among students in higher learning institutions, specifically those from non-computer science backgrounds. The findings reveal that prior to a cybersecurity and privacy awareness sharing session, the students exhibited significant gaps in their understanding of key concepts and best practices in this domain.

However, after the session, the students demonstrated a much stronger grasp of these topics, indicating the effectiveness of the awareness-raising intervention. These findings highlight the importance of providing targeted cybersecurity and privacy education to all students, regardless of their field of study, to ensure they are equipped with the knowledge and skills to navigate the digital landscape safely and responsibly.

Future research could explore the long-term impact of such awareness programs, as well as investigate the specific factors that influence cybersecurity and privacy awareness among diverse student populations.

Acknowledgments

The authors would like to thank to those who have contributed directly or indirectly to this research project.

Funding Details

The researcher received no financial support for the research, authorship or publication of this article.

Authors Contributions

- Author 1 is responsible for finalising the article's content and is involved in the data collection.
- Author 2 is responsible for designing the methodology and is involved in the data collection.
- Author 3 is responsible for revising the survey questionnaire, writing the analysis and discussion and being involved in the data collection.
- Author 4 is responsible for revising the survey questionnaire and being involved in the data collection.

Conflict of Interest

No conflicts of interest were disclosed in relation to the research, authorship, or publication of this article.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Multidisciplinary Digital Publishing Institute*, 5(2), 23-23

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model. *Emerald Publishing Limited,* 36(8), 94-125. https://doi.org/10.1108/itp-07-2022-0515

Chaudhary, S., Gkioulos, V. & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program, *Journal of Cybersecurity, Volume 8, Issue 1*, 2022, tyac006, https://doi.org/10.1093/cybsec/tyac006

Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. Cybersecurity (2022). Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Educ Inf Technol* 27, 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Du, X. & Chintakovid, T. (2023). A Survey of Cybersecurity Awareness Among Undergraduate Students at Yunnan University of Finance and Economics in China. https://doi.org/10.2991/978-94-6463-172-2_78.

Esteve-Gonzalez, P., Shillair, R., Dutton, W., Creese, S., Nagyfejeo, E. & Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*. 119. https://doi.org/10.1016/j.cose.2022.102756

Huraj, L., Lengyelfalusy, T., Lajcin, D. & Hurajova, A. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal*, 623-633. https://doi.org/10.18421/TEM122-05.

Khalid, F., Daud, M.Y., Rahman, M.J.A., & Nasir, M. (2018). An Investigation of University Students' Awareness on Cyber Security. *International Journal of Engineering & Technology*, 7(4.21), 11-14. https://doi.org/10.14419/ijet.v7i4.21.21607

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *Institute of Electrical and Electronics Engineers,* 8, 125140-125148. https://doi.org/10.1109/access.2020.3007867

Kshetri, N., Vasudha, V., & Hoxha, D. (2023). knowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students. Cornell University. https://doi.org/10.48550/arxiv.2310.12684

Lallie, H S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *Cornell University*. https://doi.org/10.48550/arxiv.2307.07755

Li, L., He, W., Xu, L D., Ivan, A., Anwar, M., & Yuan, X. (2014). Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. https://doi.org/10.1109/es.2014.66

Nagahawatta, R., Warren, M., & Yeoh, W. (2020). A Study of Cyber Security Issues in Sri Lanka. IGI Global, 10(3), 59-72. https://doi.org/10.4018/ijcwt.2020070105

Nkongolo, M., Mennega, N., & Zyl, I V. (2023). Cybersecurity Career Requirements: A Literature Review. *Cornell University*. https://doi.org/10.48550/arxiv.2306.09599

Omar, S Z., Kovalan, K., & Bolong, J. (2021). Effect of Age on Information Security Awareness Level among Young Internet Users in Malaysia. , 11(19). https://doi.org/10.6007/ijarbss/v11-i19/11733

Peker Y., Ray L. and da Silva S. (2018). Online Cybersecurity Awareness Modules for College and High School Students. *National Cyber Summit* (NCS). 24-33, doi: 10.1109/NCS.2018.00009

Persadha, P D., Waskita, A A., Fadhila, M I., Kamal, A., & Yazid, S. (2016). How inter-organizational knowledge sharing drives national cyber security awareness? A case study in Indonesia. https://doi.org/10.1109/icact.2016.7423468

Raju, R., Rahman, N., & Ahmad, A. (2022). Cyber Security Awareness In Using Digital Platforms Among Students in A Higher Learning Institution. *Asian Journal of University Education*, 18(3). https://doi.org/10.24191/ajue.v18i3.18967

Rehman, S. & Manickam, S. (2023). Towards a Cybersecurity Awareness Program for Non-Technical Audiences in Malaysia. In Vajjhala, N. & Strang K. (Eds), Cybersecurity for Decision Makers https://doi.org/10.1201/9781003319887-6.

Rohan, R., Debajyoti, P., Hautamaki, J., Funilkul, S., Chutimaskul, W. & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon. 9. e14234. https://doi.org/10.1016/j.heliyon.2023.e14234.

Tirumala, S S., Valluri, M R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. https://doi.org/10.1109/iccci.2019.8821951

Zukarnain, Z.A., Hashim, M.Z., Muhammad, N., Mansor, F. & Azib, W.N.H. (2020). Impact of training on cybersecurity awareness. *Gading Journal for Science and Technology*, 3(1), 114-120. https://ir.uitm.edu.my/id/eprint/31118

اونيۏرسيتي تيكنولوݢي مارا
UNIVERSITI
TEKNOLOGI
MARA

9 772682 784004

ISSN: 2680-7840