International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

INTERNATIONAL JOURNAL OF MODERN TRENDS IN SOCIAL SCIENCES (IJMTSS)
www.ijmtss.com

FOSTERING CYBERSECURITY CONSCIOUSNESS: ASSESSING AWARENESS AMONG STUDENTS AND STAFF IN A TECHNICAL INSTITUTION

Norshadila Ahmad Badela[1*]

[1] Department Of Information and Communication Technology, Politeknik Mersing, Johor, Malaysia
Email: norshadila@puo.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 12.03.2024
Revised date: 16.04.2024
Accepted date: 30.05.2024
Published date: 23.06.2024

To cite this document:

Badela, N. A. (2024). Fostering Cybersecurity Consciousness: Assessing Awareness Among Students And Staff In A Technical Institution. *International Journal of Modern Trends in Social Sciences, 7* (27), 26-39.

DOI: 10.35631/IJMTSS.727003

Abstract:

This research seeks to assess the level of cybersecurity awareness among both students and staff at Politeknik Mersing by means of a comprehensive survey study. The survey questionnaire encompassed a wide array of topics pertaining to cybersecurity knowledge and practices, ranging from email protocols and password management to recognizing phishing attempts and understanding various security concepts. A total of 136 respondents participated in the survey, offering valuable insights into their cybersecurity habits. The results unveiled a varied level of cybersecurity awareness among the participants, showcasing strengths in certain areas while also highlighting notable gaps in others. Particularly, the findings shed light on concerning behaviours such as the tendency to open emails from unfamiliar sources and the practice of using identical passwords across different platforms. These discoveries underscore the critical need for implementing thorough cybersecurity awareness initiatives at Politeknik Mersing, aimed at bridging the identified disparities and promoting safe online conduct. Tailored educational campaigns and continuous training initiatives are recommended to bolster cybersecurity knowledge and instil responsible behaviours. By fortifying cybersecurity awareness, Politeknik Mersing can effectively safeguard sensitive data and mitigate the inherent risks posed by cyber threats. It is advisable to conduct further research to assess the efficacy of specific cybersecurity education interventions and their enduring impact on individuals' attitudes and behaviours.

Keywords:

Cybersecurity, Security Awareness, Cyber Threat, Cybersecurity Practices

International Journal of Modern Trends in Social Sciences
IJMTSS
EISSN: 2600-8777
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

Introduction

In today's digital age, cybersecurity has become a paramount concern amidst rapid digitalization and technological advancements. The awareness of online dangers such as phishing attacks, data breaches, and identity theft is crucial for safe browsing, email communication, and online interactions (Koziol, 2022). Politeknik Mersing, as an academic institution, plays a significant role in managing and safeguarding valuable data. With the collection, storage, and processing of various data types, including student records, research findings, and administrative information, the institution faces significant cybersecurity challenges.

The sensitivity of the data held by academic institutions makes them prime targets for cyber threats. Cybercriminals often seek unauthorized access to such information for malicious purposes, including identity theft, financial fraud, and disrupting institutional operations. Therefore, fostering cybersecurity awareness among students and staff is essential to safeguard personal information and institutional data.

This research aims to assess the level of cybersecurity awareness among students and staff at Politeknik Mersing based on survey data collected during the Securetech Week from 7th to 13th May 2023. By analyzing responses to a survey questionnaire, this study seeks to understand the knowledge and behaviors of respondents regarding online security. Furthermore, the research aims to identify demographic factors influencing cybersecurity awareness and recommend tailored awareness programs for the Centre of Technology (COT) at Politeknik Mersing.

Literature Review

Cybersecurity Definition and Importance

Cybersecurity encompasses technologies, measures, and practices aimed at preventing cyberattacks or mitigating their impact (Oxford English Dictionary, n.d.). It protects individuals' and organizations' systems, applications, data, and financial assets against various cyber threats. With the rise of cyber threats, the importance of cybersecurity awareness has become evident. Continuous education and training on cyber threats and prevention measures are essential for individuals and organizations (Spanning Cloud Apps, 2022).

Phishing and Password Security

Phishing, a deceptive practice where attackers impersonate reputable entities to obtain sensitive information, remains a prevalent threat (Gillis, 2023). Password security is another critical aspect of cybersecurity awareness. Effective password management practices, such as using strong and unique passwords, are essential for online security (Adamu A. Garba, 2020).

Influence of Demographic Factors

Several demographic factors, including age, gender, and education, influence cybersecurity awareness. Research indicates that older users may exhibit lower tendencies to secure their devices but higher awareness of password security compared to younger users (Branley-Bell, 2022). Gender differences in cybersecurity awareness have also been observed, with females showing higher awareness of phishing than males (Daengsi, 2022). Additionally, educational backgrounds shape cybersecurity awareness, with higher levels of education correlating with increased awareness (Wilson Cheong Hin Hong, 2022).

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

Methodology

The study employed a cross-sectional survey design to assess cybersecurity awareness among students and staff at Politeknik Mersing. A survey questionnaire, distributed during the Securetech Week 2023 event, collected responses from 136 participants. The questionnaire included demographic questions and specific cybersecurity-related inquiries.

Research Design and Approach

This study employed a cross-sectional survey design to collect data on cybersecurity awareness among the participants. The survey was carefully crafted to evaluate the respondents' understanding and actions regarding various aspects of cybersecurity. The cross-sectional approach enabled data collection at a specific point in time, providing a snapshot of the cybersecurity landscape within the targeted population.

Sample Selection and Data Collection Procedure

The participants in this study were selected from Politeknik Mersing, encompassing both students and staff members. The sampling process involved a combination of convenience and random sampling techniques. The survey questionnaire was distributed during the Securetech Week 2023 event, organized by the Cyber Range Academy Politeknik Mersing. Questionnaires were disseminated to the participants, and a total of 136 individuals voluntarily completed the survey, ensuring their willingness to contribute and provide accurate responses.

Description of the Survey Questionnaire

The survey questionnaire comprised a series of inquiries designed to gauge the respondents' level of cybersecurity awareness. It covered a wide range of topics, including email management practices, responses to requests for personal information, online shopping behaviors, understanding of password characteristics, familiarity with phishing, habits regarding password reuse, awareness of user agreements, comprehension of HTTP and HTTPS, usage of debit/credit cards at outdoor payment terminals, knowledge of social engineering, computer usage in the workplace, understanding of DoS and DDoS attacks, downloading of free software/programs, utilization of encryption methods, regular updating of antivirus software, use of backup software, attitudes toward technology-dependent security, responses to requests for sensitive information via phone, importance of privacy policies and procedures, and accountability for information security awareness. These survey questions were carefully selected based on existing research instruments in the field of cybersecurity, considering their relevance to various factors affecting cybersecurity awareness (Alharbi, 2021).

Demographic Information

In addition to cybersecurity-related inquiries, respondents were also asked to provide demographic information, including age, gender, position, academic qualifications, and department. This demographic data facilitated the examination of potential correlations or distinctions in cybersecurity awareness based on these demographic variables.

Through this methodological approach, the study aimed to gain valuable insights into the cybersecurity awareness levels among participants at Politeknik Mersing, thereby contributing to a better understanding of their current cybersecurity knowledge and behaviors.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

Results and Analysis

Demographic Characteristics of the Respondents

The survey included a total of 136 respondents from Politeknik Mersing. The age distribution of the respondents was as follows:

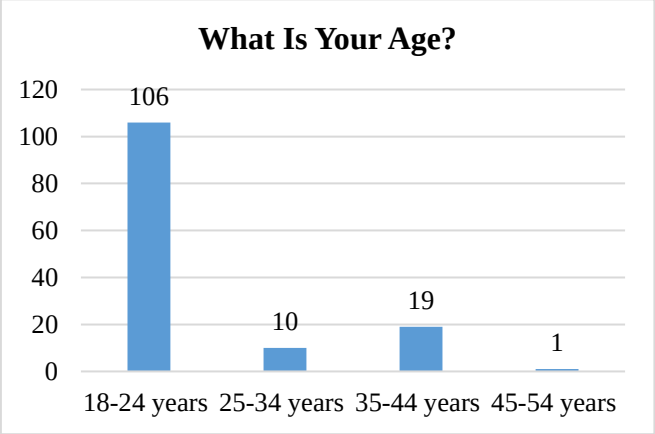

Figure 1: The Number of Respondents Dividing by Age.

Figure 1 shows 106 respondents aged from 18 to 24 years old, 10 respondents aged from 25 to 34 years old, 19 respondents age from 35 to 44 years old, and 1 respondent age 45 to 54 years old.

In terms of gender of respondents, the result is as follow:

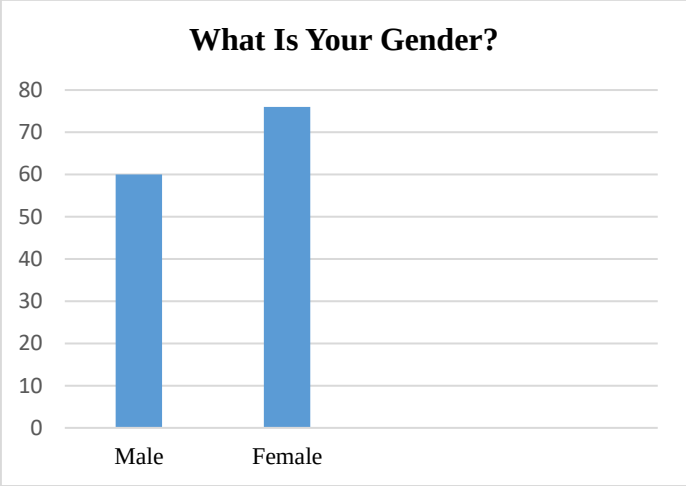

Figure 2: The Number of Respondents Dividing by Gender

From **Figure 2**, showing that, most of the respondents were female 76, while the remaining respondents were male 60.

Regarding the position of the respondents, to know whether the respondents is a student, staff, the result are as follow:

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

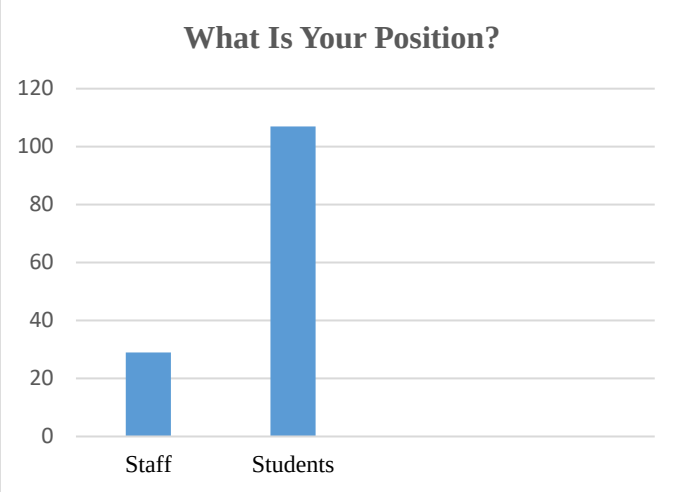

Figure 3: The Number Of Respondents Dividing By Position

From **Figure 3**, showing that 29 of the respondents were staff members, and the majority, that are 107 were students.

In terms of respondents' academic qualification, the outcome areas follow:

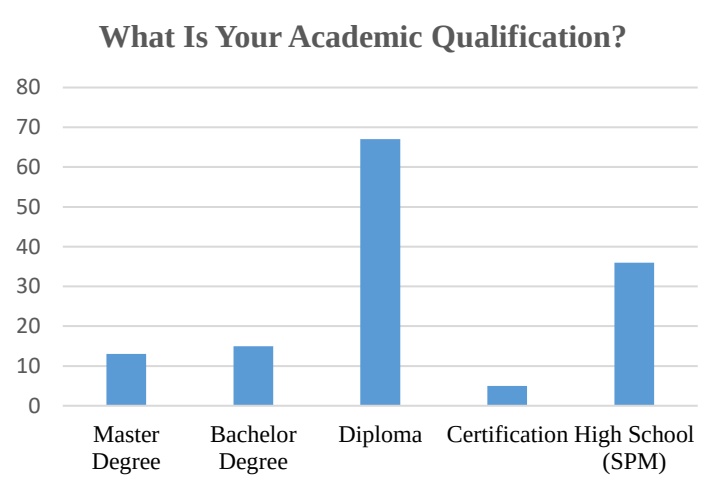

Figure 4: The Number of Respondents Dividing By Academic Qualification

Figure 4 portrays that the respondents had diverse backgrounds, with 15 respondents holding a bachelor's degree, 5 respondents having a Certificate, 36 respondents with a High School qualification, 67 of respondents holding a Diploma, and balance of 13 respondents having a master's degree.

The respondents represented various departments and the result is as follow:

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

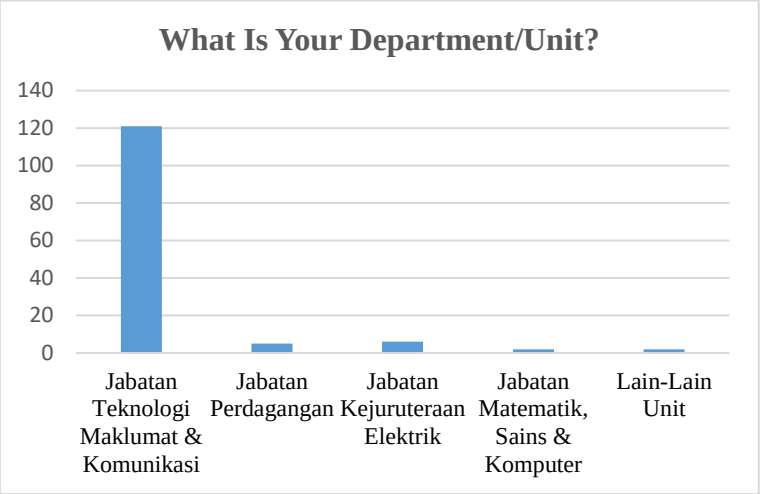

Figure 5: The Number Of Respondents Dividing By Department/Unit

Figure 5, showing that majority of the respondents comes from Jabatan Teknologi Maklumat & Komunikasi (JTMK), with 121 respondents. Jabatan Perdagangan (JP) have recorded 5 respondents, Jabatan Kejuruteraan Elektrik (JKE) with 6 respondents, and both Jabatan Matematik, Sains & Komputer (JMSK), Lain-lain Unit, with 2 respondents.

Analysis of Survey Responses for Each Question

The survey questionnaire aimed to assess respondents' cybersecurity awareness and behaviours. The analysis of the survey responses revealed the following insights:

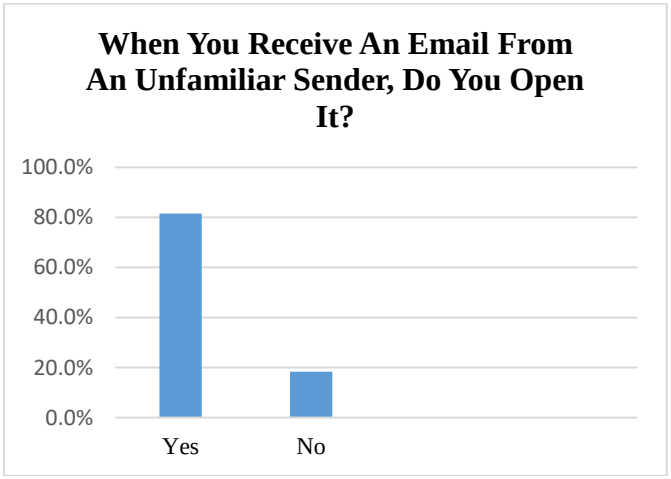

Figure 6: The Number Of Respondents Respond Towards Unfamiliar Email.

From **Figure 6**, showing that, when receiving an email from an unfamiliar sender, 81.6% of respondents indicated that they open it, while only 18.4% respondents do not open it.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

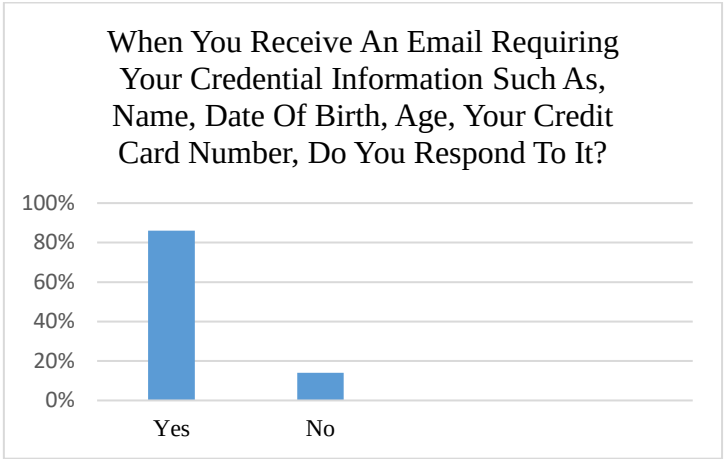

Figure 7: The Number Of Respondents Respond Towards Email That Requires Credential Information.

Figure 7, showing that when respondents receive an email requires credential information, such as name, date of birth, or credit card number, do they respond to it. 86% of respondents responded to it, while balance of 14% did not respond.

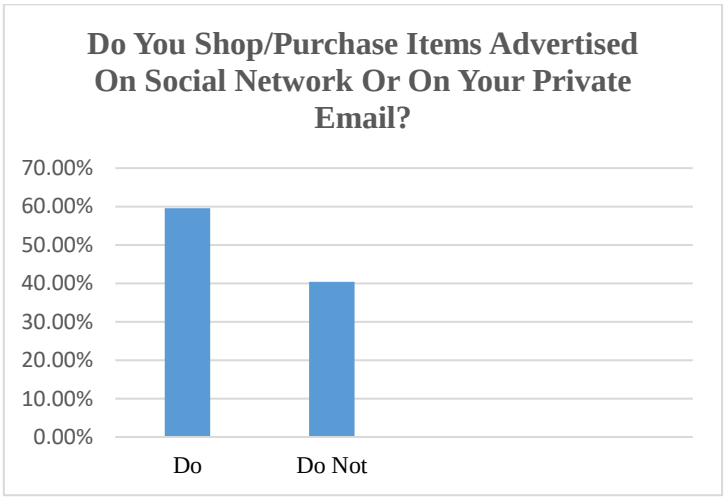

Figure 8: The Number of Respondents Respond On Shop/Purchase Items Advertised On Social Network Or On Private Email

Moreover**,** referring to **Figure 8**, is regarding shopping/purchasing items advertised on social networks or private emails, 59.6% of respondents indicated that they do, while 40.4% respondents do not shop/purchase items advertised on social network or on private email.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

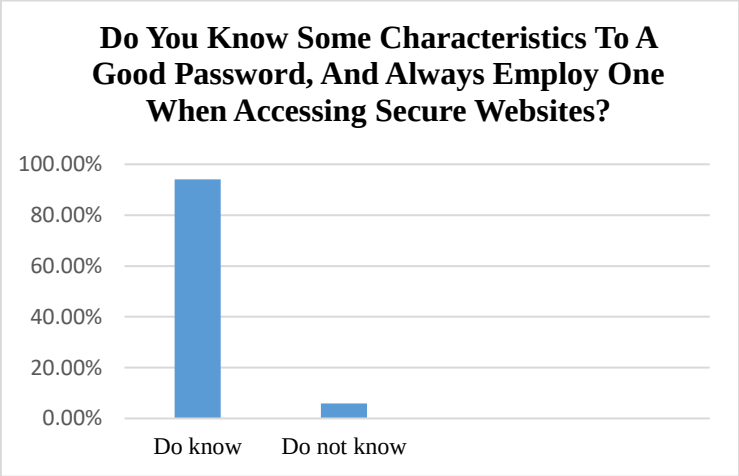

Figure 9: The Number of Respondents That Know Characteristics To A Good Password, And Always Employ One When Accessing Secure Websites?

Figure 9 shows the result when the respondents were asked about knowing the characteristics of a good password and employing one when accessing secure websites. 94.1% of respondents indicated that they do, while 5.9% respondents do not.

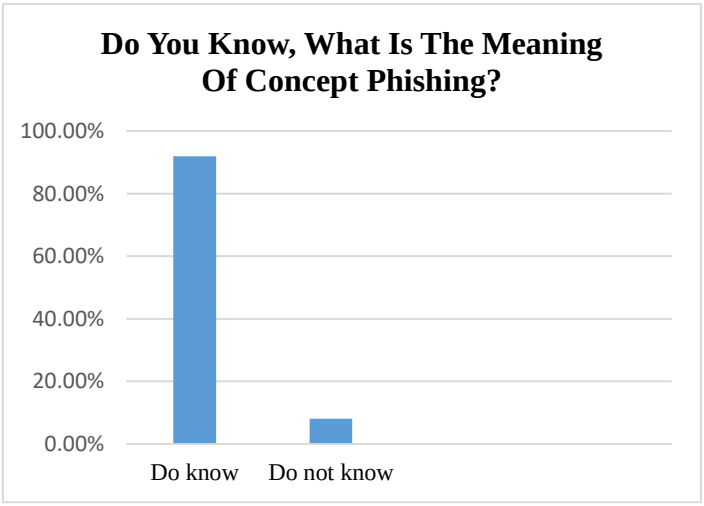

Figure 10: The Number of Respondents That Know Characteristics To A Good Password, And Always Employ One When Accessing Secure Websites?

From **Figure 10** is the result of respondents understanding the concept of phishing, 91.9% of respondents indicated that they do, while 8.1% do not understand.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

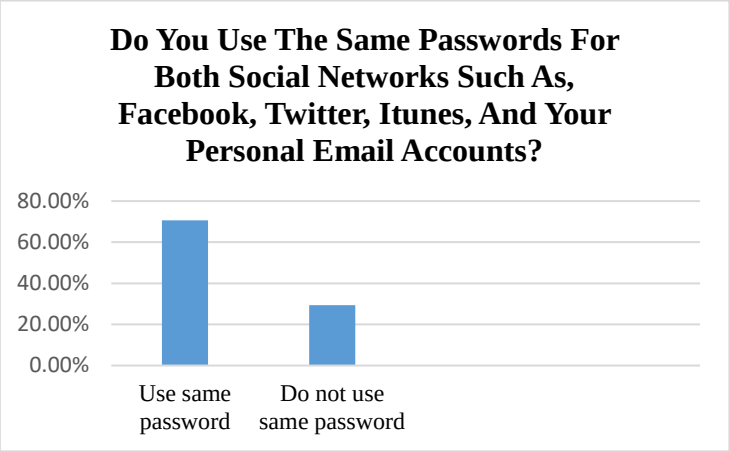

Figure 11: The Number of Respondents Divided by Knowing The Characteristics To A Good Password, And Always Employ One When Accessing Secure Websites.

Regarding password reuse for different social networks and personal email accounts, referring to **Figure 11**, 70.6% of respondents indicated that they use the same passwords, while 29.4% respondents do not.

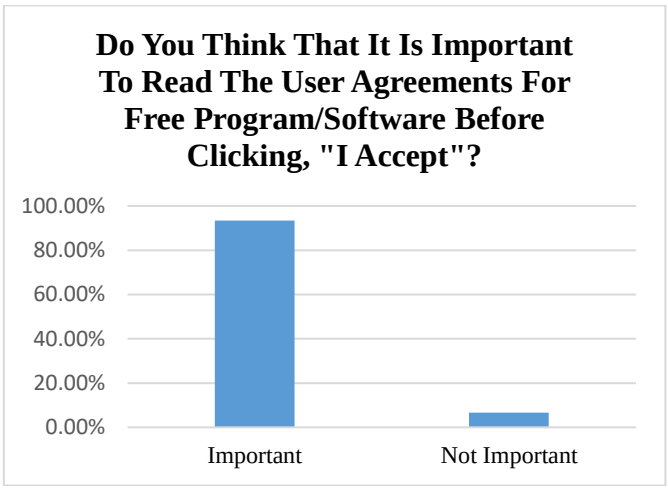

Figure 12: The Number Of Respondents Know The Importance To Read The User Agreements For Free Program/Software Before Clicking, "I Accept".

Referring to **Figure 12**, When it comes to reading user agreements for free programs/software, 93.4% of respondents indicated that they consider it is important, and while 6.6% of the respondents do not.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

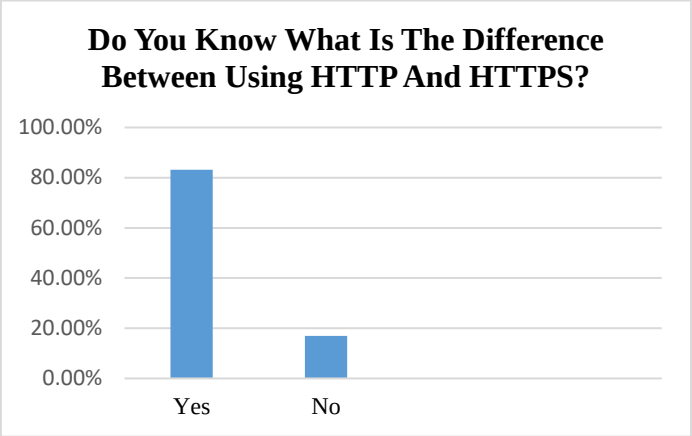

Figure 13: The Number Of Respondents Know The Difference Between Using HTTP and HTTPS

Regarding the difference between using HTTP and HTTPS by referring to **Figure 13**, 83.1% of respondents indicated that they know the difference, while 16.9% of respondents do not the difference between HTTP and HTTPS.

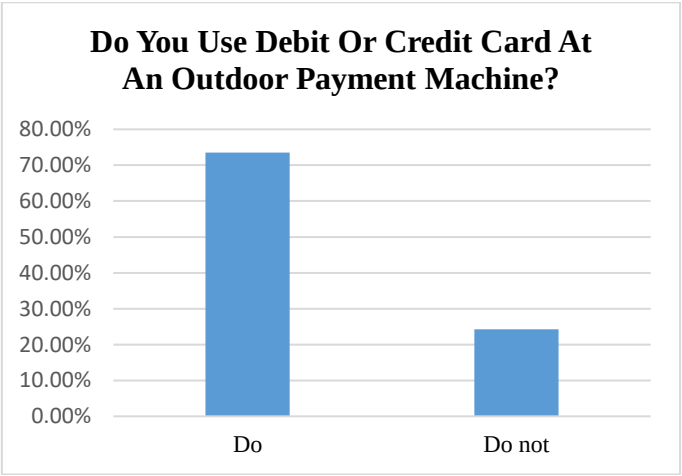

Figure 14: The Number Of Respondents Using Debit Or Credit Card At An Outdoor Payment Machine.

Referring to **Figure 14,** the survey is about using debit or credit cards at outdoor payment machines. 73.5% of respondents indicated that they do use it, and while 24.3% do not.

International Journal of Modern Trends in Social Sciences
IJMTSS
EISSN: 2600-8777
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

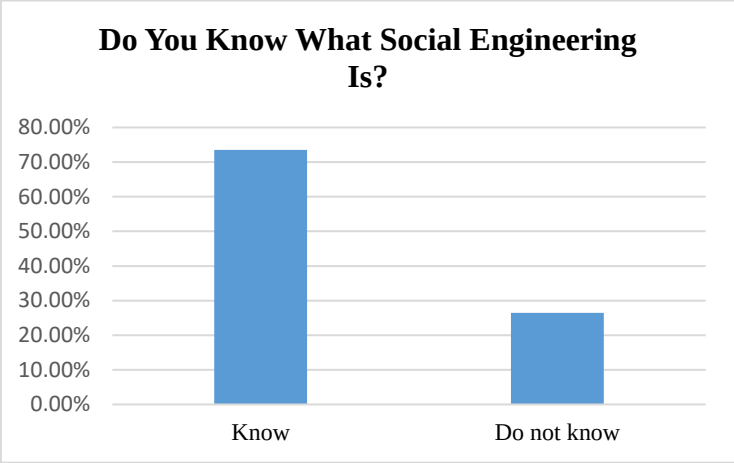

Figure 15: The Number Of Respondents Know About Social Engineering

Regarding **Figure 15**, respondents' knowledge of social engineering resulted for 73.5% of respondents indicated that they know about it, while 26.5% do not know about social engineering.

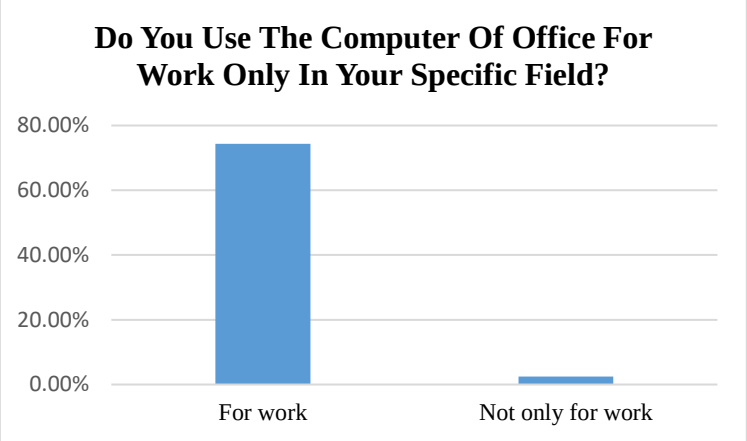

Figure 16: The Number of Respondents Only Use Computer of Office For Work.

When using computers at the office as shown in **Figure 16**, 74.3% of respondents indicated that they use them only for work in their specific field, while 25.7% do not use only for work.

International Journal of Modern Trends in Social Sciences
EISSN: 2600-8777
IJMTSS
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

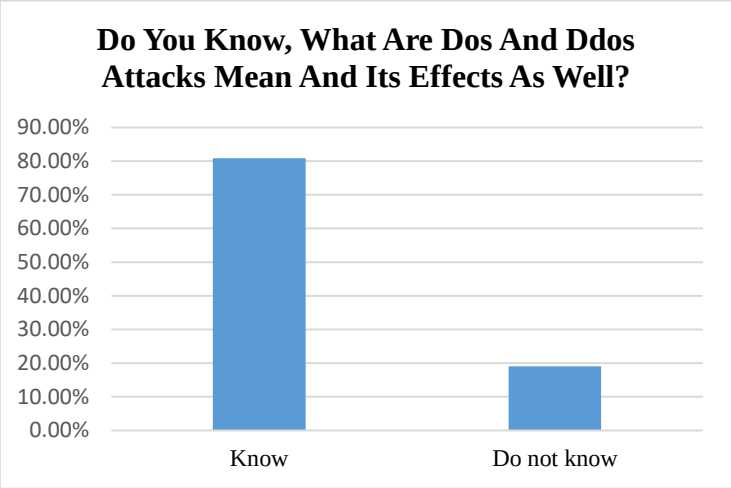

Figure 17: The Number of Respondents Know the Meaning of Dos and Ddos

Finally, referring to **Figure 17**, when asked about knowledge of DoS and DDoS attacks and their effects, 80.9% of respondents indicated that they know the meaning and effects, while 19.1% do not know the meaning.

Identification of Patterns and Trends in the Data

The survey results highlighted both positive trends and areas for improvement in cybersecurity awareness. While respondents showed understanding of certain cybersecurity concepts, risky behaviors such as opening emails from unknown senders and password reuse were prevalent.

Discussion

The findings underscore the importance of targeted cybersecurity awareness initiatives at Politeknik Mersing. Recommendations include addressing risky behaviours through educational programs and promoting a comprehensive understanding of cybersecurity concepts. Collaborative efforts between academic institutions, government agencies, and industry partners are crucial for enhancing cybersecurity awareness.

In addition to educational programs, integrating cybersecurity awareness into the curriculum across various disciplines can further reinforce the importance of cyber hygiene practices among students and staff. Furthermore, establishing regular cybersecurity training sessions and workshops can provide ongoing support and reinforcement of cybersecurity best practices. Encouraging participation in cybersecurity competitions, hackathons, and other hands-on activities can also foster a proactive approach to cybersecurity among the Politeknik Mersing community.

Moreover, leveraging technology-driven solutions such as gamification and interactive online modules can make cybersecurity awareness initiatives more engaging and accessible to a wider audience. Investing in state-of-the-art cybersecurity infrastructure and tools, coupled with continuous monitoring and assessment, is essential for staying ahead of emerging threats. Additionally, fostering a culture of information sharing and collaboration within the institution can facilitate the dissemination of cybersecurity knowledge and best practices.

Collaborative partnerships with government agencies and industry stakeholders can provide valuable insights and resources to enhance cybersecurity awareness initiatives. By sharing

International Journal of Modern Trends in Social Sciences
IJMTSS
EISSN: 2600-8777
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

expertise, best practices, and threat intelligence, Politeknik Mersing can strengthen its cybersecurity posture and contribute to the broader cybersecurity ecosystem. Ultimately, a multidisciplinary approach, combined with proactive engagement and collaboration, is key to building a resilient cybersecurity framework at Politeknik Mersing.

Conclusion

Continuous efforts are needed to enhance cybersecurity awareness at Politeknik Mersing. By identifying and addressing identified gaps in knowledge and behaviour, the institution can foster a culture of cyber vigilance among students and staff. Implementing targeted educational programs and awareness campaigns, tailored to the specific needs of different demographic groups, will play a crucial role in strengthening cybersecurity practices. Furthermore, collaboration with industry partners and government agencies can provide access to resources and expertise to develop comprehensive cybersecurity initiatives. Ultimately, prioritizing cybersecurity awareness will enable Politeknik Mersing to proactively mitigate the evolving threats landscape and safeguard its valuable data assets from cyber adversaries.

Acknowledegment

The authors would like to express sincere gratitude to the Cyber Range Academy at Politeknik Mersing for their invaluable support and resources provided throughout the course of this research. The expertise and assistance significantly contributed to the success of this study. Author is deeply appreciative of the commitment to fostering cybersecurity education and awareness among students and staff. Additionally, thanks to the departments members and staff who generously shared insights and experiences, without which this research would not have been possible.

References

Adamu A. Garba, M. M. (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach . *International Journal on Emerging Technologies 11(5): 41-49(2020)* , 41.

Alharbi, T. T. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*.

Alsulami, M., Alharbi, F., Almutairi, H., Almutairi, B., Alotaibi, M., Alanzi, M., . . . Alharthi, S. (2021). *MDPI and ACS Style*. Retrieved from https://www.mdpi.com/: https://www.mdpi.com/2078-2489/12/5/208

Branley-Bell, D. C. (2022). *Hindawi*. Retrieved from https://www.hindawi.com/: https://www.hindawi.com/journals/hbet/2022/2693080/

Daengsi, T. P. (2022, May). *https://link.springer.com/article*. Retrieved from https://link.springer.com/: https://link.springer.com/article/10.1007/s10639-021-10806-7#citeas

Gillis, A. S. (2023). *Tech Target*. Retrieved from https://www.techtarget.com/: https://www.techtarget.com/searchsecurity/definition/phishing

Hasani T, R. D. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. *International Journal of Engineering Business Management.*, 15.

Ismail, N. N. S. ., Fammy Rikzan, F. I. ., Katuk, N. ., Hashim, N. L., & Mohd Zulkefli , N. A. . (2023). Enhancing Information Security Awareness On Phishing Among It Students: A Pilot Test Case Study At Politeknik Tuanku Syed Sirajuddin. *Journal of Digital System Development, 1*, 12–23. https://doi.org/10.32890/jdsd2023.1.2

International Journal of Modern Trends in Social Sciences
IJMTSS
EISSN: 2600-8777
Volume 7 Issue 27(June 2024) PP. 26-39
DOI 10.35631/IJMTSS.727003

Jack Koziol, C. B. (2022, March 16). *Cybersecurity Awareness: What It Is And How To Start*. Retrieved from Forbes: https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/

Kathryn Parsons, D. C. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 40-51.

Orvila Sarker, A. J. (2024). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*.

Oxford English Dictionary. (n.d.). *https://www.oed.com/search*. Retrieved from https://www.oed.com/: https://www.oed.com/search/advanced/Meanings?textTermText0=cybersecurity&textTermOpt0=WordPhrase

Spanning Cloud Apps. (2022, June 30). *Cybersecurity Awareness: Definition, Importance, Purpose and Challenges*. Retrieved from Spanning: https://spanning.com/blog/cybersecurity-awareness/

Stephan Wiefling, M. D. (2020). More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. *In Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC '20)*, 203-218.

Wilson Cheong Hin Hong, C. C.-L. (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, 439-470.