Internet Usage and Cybersecurity Awareness Among Students at Politeknik Tuanku Syed Sirajuddin

N. N. S. Ismail[1]*, T. K. Tunku Norizan[2] and N. L Hashim[3]

[1]Kolej Komuniti Bandar Darulaman,
06000 Jitra, Kedah, Malaysia.

[2]Politeknik Tuanku Syed Sirajuddin,
Pauh Putra, 02600 Arau, Perlis, Malaysia

[3]Universiti Utara Malaysia.
06010 Sintok, Kedah, Malaysia.

*Corresponding Author's Email: naematul@kkbda.edu.my

Article History: Received 7 April 2024; Revised 13 Mei 2024;
Accepted 13 Jun 2024

Abstract

As the number of Internet users is rapidly growing, everyone uses the Internet for various purposes, such as e-commerce, online learning, or connecting with friends and family. Besides the benefits of the Internet, there are always risks, especially considering cybersecurity issues like keeping information safe online. This study looks at how students of the Commerce and Information Technology Department at Politeknik Tuanku Syed Sirajuddin (PTSS) use the Internet and whether they are aware of cybersecurity threats that might occur. Information was gathered through the involvement of 92 samples from first- and second-semester students from both departments. The results show how often they use the Internet and how they act while browsing it. By understanding how students use the Internet and what they know about staying safe online, we can figure out ways to help them stay even safer. This study gives us a good starting point for ensuring students at PTSS know how to keep their information secure while enjoying all the benefits the Internet offers.

Keywords: Cybersecurity Awareness; Cybersecurity in Education; Internet Usage; Tertiary Education;

1.0 Introduction

Over the past five years, Malaysia has witnessed a rapid increase in Internet users, with the current count at approximately 33.47 million. Forecasting has been done, suggesting that this number will increase to 33.98 million by 2024 (Statista, 2024). However, alongside this surge in Internet usage, there has been a corresponding rise in cybersecurity incidents, posing significant risks to users nationwide. According to (MyCERT, 2024), there were 1027 general reported cybersecurity incidents in the previous two months alone. These incidents encompass intrusion attempts, content-related vulnerability reports, denial of service, intrusion, malicious codes, spam, and fraud. Within the educational landscape, institutions like Politeknik Tuanku Syed Sirajuddin (PTSS), face unique challenges in safeguarding their network infrastructure.

However, the pervasive use of the internet among students poses inherent risks. As principal stakeholders in the institution, students' behaviors and habits concerning internet usage significantly impact PTSS's network security. Despite being avid users of technology and the internet, students often exhibit tendencies towards negligence and even aggression in their computing practices. The human element becomes the weakest link in cybersecurity, typically the target of the growing number of online criminals committing an ever-widening range of cybersecurity threats (Chandarman & Van Niekerk, 2017). Students were slightly more prone to open the email offering free concert tickets than the phishing email sending a PDF. Also, in both situations, students were more likely to use mobile devices to open the harmful link in the phishing email (Maimon et al., 2021). Frauenstein (2019) found that many participants allegedly replied to phishing emails from Facebook and other educational contexts. This supports the notion that users seem to fall for phishing if the content is interesting or pertinent to their situation.

In a recent conversation with the Head of the Information Technology and Data Center Unit at PTSS, it was highlighted that the network firewall has successfully blocked several attempts by PTSS users to access malicious external links. This preventative measure is crucial, as allowing such access could potentially compromise the PTSS network (Khadzir, 2023). Therefore, this study is purposely to determine the cybersecurity awareness level among students of PTSS. This paper is organized as follows: related works, methodology explains details of the research approach, and data collection procedures. At the same time, the next section presents the analysis of results on cybersecurity awareness among students. In the last section, conclusions and recommendations are discussed.

2.0 Related Works

Mohd Zaharon et al. (2021)performed a study to identify awareness among Generation Y (Gen Y) in Malaysia. They found three factors that affect awareness: social engineering, anti-phishing knowledge, and security concerns. Data collection has been performed by providing a set of questionnaires. The result of their study concluded that phishing significantly influences factors. Thus, GenY should be informed about phishing techniques and anti-phishing expertise by reading more phishing materials to be aware of the influence of social engineering. They should also install anti-virus software and use strong passwords to protect their data. Researchers believed their study would help Gen Y become aware and better understand phishing. The study can also help businesses and government organizations educate staff members and implement appropriate anti-phishing tactics. (Alshboul & Streff, 2017) were performed an analysis that adapted the Innovation Diffusion theory to determine the predecessor of information security policy (ISP) awareness and the satisfaction that impacts security practices.

Due to the lengthy time spent on the Internet, students are exposed to cyber threats. This is due to their activities, like massively relying on free downloadable things, and some may not have any antivirus protection

software on their gadget. This will make them more vulnerable to threats. Meanwhile, the human factor is the weakest link in the cyber range. Even though students are adapting to new technology as they are always accessing their learning management systems, their cybersecurity knowledge is still unknown. Thus, (Subramaniam, 2017) researched cybersecurity awareness among pre-university students. The author found that male students had better cyber security awareness than female students. Students with better computing skills who use computers for extended hours tend to have more cyber security awareness.

The three studies presented offer diverse approaches to assessing and enhancing cybersecurity awareness among undergraduate students. The first study conducted at Imam Abdulrahman bin Faisal University in Saudi Arabia used a comprehensive methodology to evaluate students' knowledge, skills, attitudes, and self-perceptions regarding cybersecurity. By focusing on password security, browser security, and social media usage, the study aimed to provide a holistic understanding of students' awareness levels. However, it would be beneficial for future research to delve deeper into the effectiveness of various educational interventions in improving cybersecurity awareness and practices among students (Aldawood & Skinner, 2019).

The study performed by (Qasaimeh et al., 2021) took a more creative approach by utilizing humorous internal movies to deliver security awareness messages to newcomer students at Virginia Commonwealth University. While the initiative was well-received and demonstrated students' enthusiasm, the long-term impact of such an approach remains uncertain. Although engaging content can enhance students' receptiveness to cybersecurity education, it is essential to ensure that the lessons are effectively retained and translated into practical behaviors. Lastly, the study mentioned by (Alqahtani, 2022) highlights the importance of cybersecurity awareness programs in mitigating cyber risks faced by digital-native students. Given the prevalence of cyber threats targeting educational institutions, investing in cybersecurity education and training can empower students to protect themselves and their organizations against potential attacks. From the above studies conducted at the university, there is a need for a similar awareness study at PTSS as well. While students today are increasingly exposed to online threats, their awareness of cyber security risks often does not translate into taking concrete protective measures. This highlights the need for improved cybersecurity education and practical guidance to help children navigate the digital world safely.

3.0 Methodology

In this study, the researchers have used descriptive quantitative research. The non-probability sampling technique specifically purposive sampling that has been used in this study which involved a total of approximately ninety-two samples from the Department of Information Technology and Department of Commerce at PTSS, involving the first and second semesters, will participate in this study. By targeting the initial semesters, the study aims to gauge early cybersecurity awareness and threat perception as students begin their programs.

Questionnaires based on the PTSS population will be distributed to the samples to gather information for this study. There are two sections involved in the survey which are demographic element and awareness level identification, the survey instruments were adapted from (Garba et al., 2020) into a 20-item questionnaire that asked samples about their awareness level. Conducted in an unguided online format, the survey link was distributed by academic advisors and course lecturers. Participation in the survey was voluntary, ensuring samples were not forced to complete it. Quantitative analysis will be implemented to facilitate the identification of trends and patterns in the samples' awareness levels, as the awareness questions were close ended with dichotomous data.

4.0 Result

Table 1 below indicates the number of samples for this survey. Samples from four programs across two departments participated. 68% of samples are from the IT department, while the other 32% are from the Commerce department.

Table 1 : Samples' Program Distribution

Program	**Number of Samples**
Diploma in Business Studies	3
Diploma in Secretarial Science	26
Diploma in Digital Technology	15
Diploma in Information Technology	48
Total	92

4.1 Analysis of Demographic Elements

This analysis involved sample background characteristics, internet access preferences, and common internet issues and reporting mechanisms.

From the sample, the distribution of program study and their current semester shows that 3.26% are Diploma in Business Studies (DBS) students, while Diploma in Secretarial Science (DSS) makes up 28.26%. Meanwhile, students of Diploma in Digital Technologies (DDT) and Diploma in Information Technology (DIT) bring 16.30% and 52.17%, respectively. Furthermore, the percentage for semester 1 students is 16.3% while the percentage for semester 2 students is 83.7%.

Table 2 below describes computing skills. The computing skills were leveled very good, good, fair, and poor. 13.3% of samples in semester one from the DIT program admitted that they have excellent computing skills, while the other 46.67%, 33.33%, and 6.67% have claimed to have good, fair, and poor skills. All DBS students from semester two claimed to have good computing skills. While 7.69% of DSS programs have very good skills, 50% have good skills and 42.31% of them have fair skills. Meanwhile, for the DDT program,

none of them have very good or poor skills. Besides, 33.33% have good skills and 66.67% have fair skills. And lastly, for DIT students, 15.15% of them have very good skills, 30.30% have good skills, 48.48% have fair skills, and the rest 6.06% have poor skills.

Table 2 : Samples' Computing Skills.

Semester and Program	Skills Level				Grand Total
	Good	Poor	Very Good	Fair	
Semester 1	7	1	2	5	15
Diploma in Information Technology	7	1	2	5	15
Semester 2	31	2	7	37	77
Diploma in Business Studies	3				3
Diploma in Secretarial Science	13		2	11	26
Diploma in Digital Technology	5			10	15
Diploma in Information Technology	10	2	5	16	33
Grand Total	38	3	9	42	92

The bar chart in Figure 1 below depicting how they currently access the Internet directly reflects the responses to question 5, which asked “How do you currently access the Internet”. Most of the samples chose to use their mobile data. This might be a convenient method for them to access the Internet.

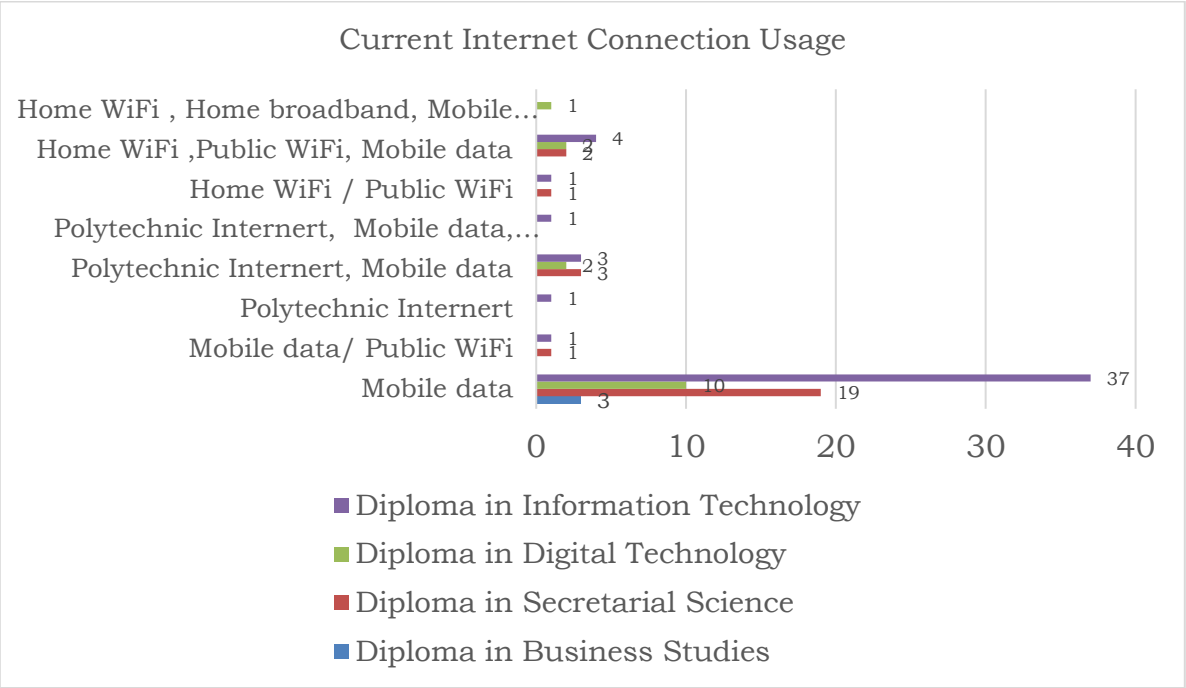

Figure 1 : Respondent's Current Internet Access Method

For their Internet access preferences, refer to the question: Which of the following is your preference? The data has been broken down based on the program of study. Only 3 samples from Diploma in Business Study and they prefer to use mobile data, public Wi-Fi, and home broadband. These preferences might be based on their location while answering the survey.

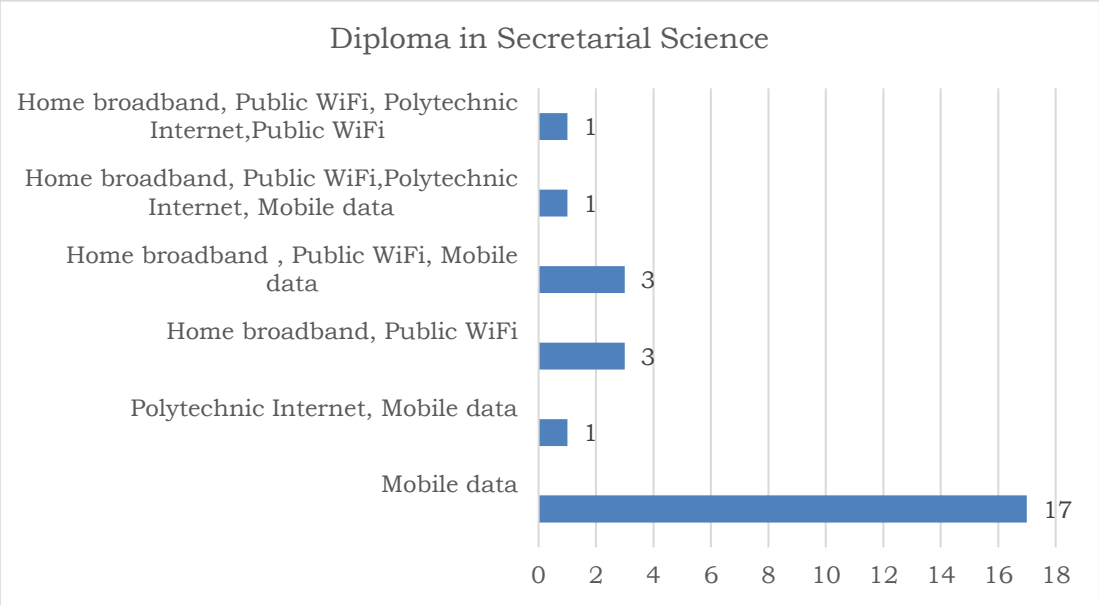

Figure 2 : Diploma in Secretarial Science Samples' Preferences.

Meanwhile, for the DSS samples, most of them prefer to use their mobile data. Most of them prefer to use a combination of home broadband, public Wi-Fi, and polytechnic internet. There is also a combination of home broadband, public Wi-Fi, mobile data, and polytechnic internet and mobile data, as referred to in Figure 2 above.

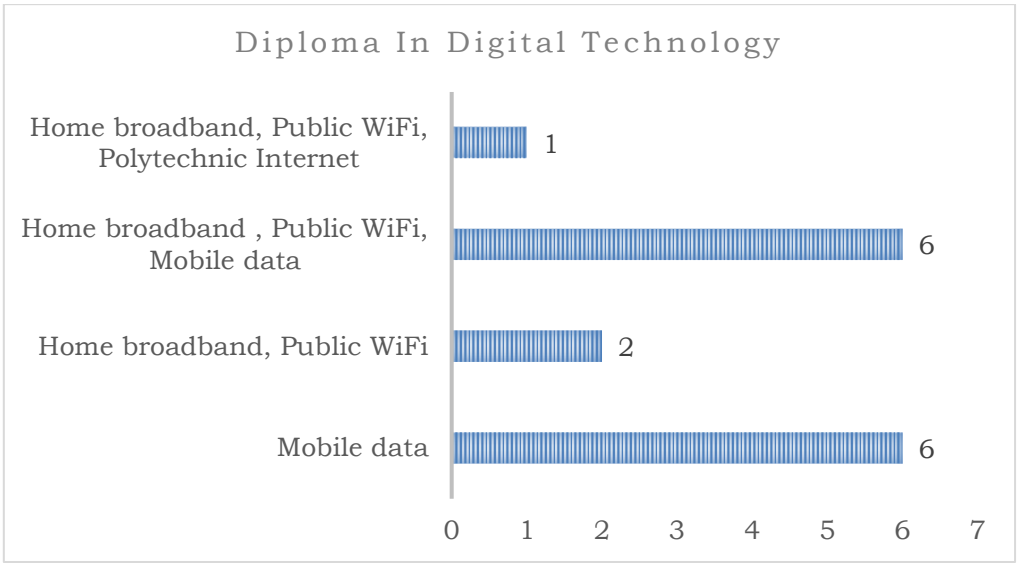

Figure 3 : Diploma in Digital Technology Samples' Preferences.

Figure 3 above shows the preferences of DDT samples. They preferred to use their mobile data and a combination of home broadband, public Wi-Fi, and mobile data.

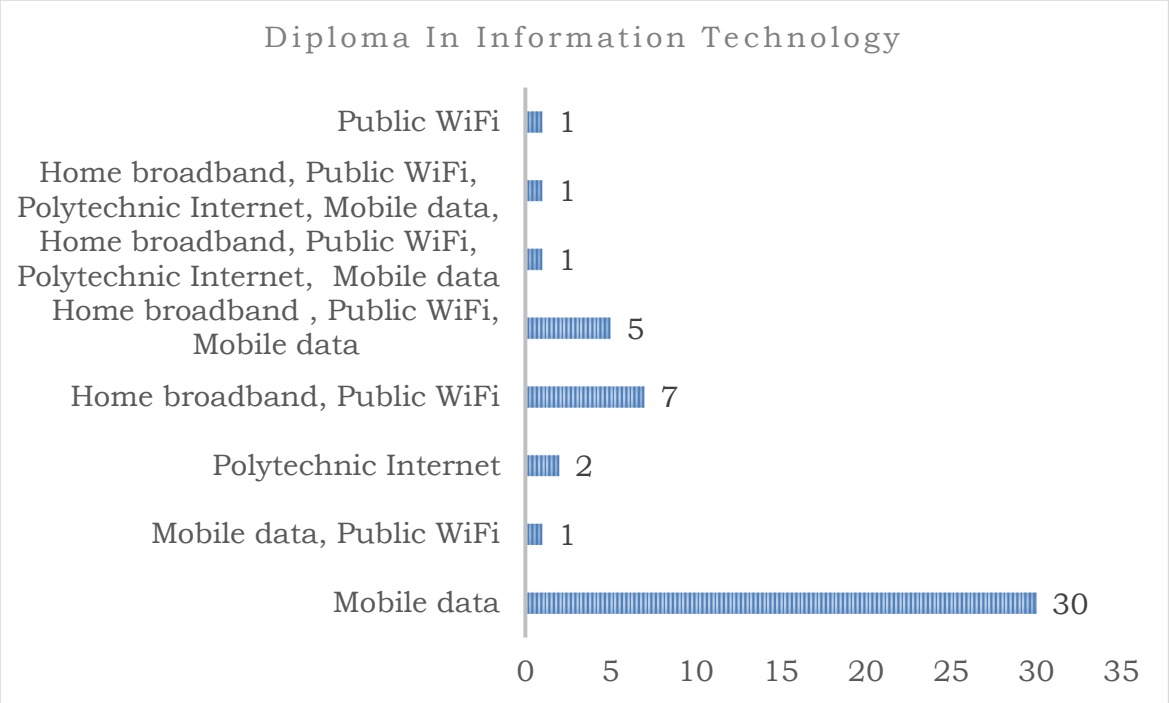

Figure 4 : Diploma in Information Technology Samples' Preferences.

Figure 4 above indicates the preferences of DIT samples. They preferred to use their mobile data and a combination of home broadband and public Wi-Fi. The survey found that 74.2% of samples felt extremely important, 20.4% said very important, and the rest, 5.4%, felt somewhat important regarding Internet connection reliability and stability. Samples alleged that they were experiencing Internet issues as follows: 78.5% responded that they experienced slow connection speed, and 67.7% faced unstable connection. While 33.3% of those who are using mobile data always faced limited data allowance, and 29% of the samples faced high cost. Meanwhile, only 1.1% never faced any difficulties. This finding was the response to the question: Have you ever experienced any of the following Internet issues? Hence, regarding the difficulties that the samples experienced, only 40.9% never made any complaints to the respective authorities. Meanwhile, 41.9% had made complaints via phone call, 10.8% reported via email, 15.1% reported by walking into the service center, and 17.2 % reported via the official social media of the respective authorities.

4.2 Analysis of Cybersecurity Awareness

For this section cybersecurity awareness analysis involves instruments that fall under categories like those mentioned after this.

Online Privacy and Cybersecurity Practices

By referring to the question: Which tools do you use to secure your online privacy and protect against potential cybersecurity threats? Several tools can be used to secure online privacy and protect against potential cybersecurity threats such as Virtual Private Networks (VPN), antivirus software, firewalls,

and proxy servers. 25.8% of the samples never used any one of them. Meanwhile, the most selected tool is antivirus software, which accounts for 43% of the total. For firewall, proxy server, and VPN, 29%, 12.9%, and 36.6% each. The responses to the question: How often do you update your device's software and security settings? This shows that 55.4% of them sometimes update their device's software and security settings, while 19.6% regularly update their software and security settings, and 21.7% rarely update their device's software and security settings. Besides, 3.3% never care about the software and security settings.

Online Activities and Security Concerns

For daily Internet usage, 44.57 % spend more than 12 hours daily. This suggests that the Internet is central to many people's daily lives. 45.65 % of them spend 6 to 12 hours daily, which may show that they rely heavily on the Internet for various activities such as work, communication, entertainment, and information access. Only a tiny percentage (9.78%) spend less than 6 hours online daily. This group might have limited access, preferred offline activities, or had specific reasons for restricted internet use. For online banking activities, 98.91% of them have experience with online shopping or banking. These findings were responses to the question: How long have you used the Internet daily? Online banking and shopping offer significant convenience compared to traditional methods. People can access their accounts, make purchases, and manage finances from anywhere with Internet access. The widespread availability of smartphones and internet connections has made online banking and shopping accessible to a larger population. Apart from online shopping and online banking usage, 8.7% of them think that online security is quite important, 77.17% feel extremely important and 11.96% think that it is very important to have secure online banking and online shopping. This demonstrates a widespread understanding of the potential risks associated with online transactions. while only 2.17% do not prioritize online security for banking and shopping. This could be due to various reasons, such as a lack of awareness, overconfidence in their security practices, or a perception of low risk.

Four applications have been listed for instant messaging application preferences: WhatsApp, Telegram, and Snapchat. 56.62% of the samples chose WhatsApp, which shows that this application is a favorite. Telegram also enjoys significant popularity, as 36.96% of the samples chose this application. Snapchat seems to be the least preferred among these options, scoring only 1.09%. Additionally, the reasons behind their preferences could vary depending on individual needs, features offered by each app, and social circles using specific platforms. All samples have experience using video conferencing tools such as Google Meet, Microsoft Teams, Cisco Webex, and Zoom. The breakdown usage will be explained further as follows; Google Meet is the most popular choice. It is used either alone or in combination with other platforms by 91 users (98.91%). Zoom is the second most preferred option used by 48 users (52.17%), mostly in conjunction with Google Meet. Meanwhile, Microsoft Teams and Webex have lower adoption as they are mainly used alongside Google Meet and Zoom, with very few users choosing them exclusively.

Social media is also among the famous applications that are widely used nowadays. The social media that is mostly used by the samples has been broken down in Table 3 below. The most common engagement platforms are TikTok and Instagram. Nearly one-third of users prefer TikTok exclusively. Facebook, X, and Twitter are the least commonly used platforms. This might be based on the younger generation's preference.

Table 3 : Social Media Platform Preferences

Social Media Platform	**Number of Samples**	**Percentage (%)**
TikTok only	30	32.61
Instagram only	10	10.87
TikTok + Instagram	32	34.78
TikTok + Instagram + Facebook	7	7.61
TikTok + Instagram + X/Twitter	5	5.43
TikTok + Instagram + Facebook + X/Twitter	5	5.43
Instagram + Facebook + X/Twitter	1	1.09
X/Twitter only	1	1.09
Facebook only	1	1.09

Cybersecurity Awareness

There are eighteen questions in this section to gather insight into samples' cybersecurity awareness level behaviors and attitudes, which can inform efforts to enhance cybersecurity education and practices. The questions can be classified into general cybersecurity knowledge, personal security habits, institutional security awareness, and **i**nterest in learning. Eighteen questions in this section were designed to get a yes or no answer from the samples.

General Cybersecurity Knowledge

67% of the samples consider themselves knowledgeable about cybersecurity. This can indicate a decent level of awareness. However, 41% of samples still feel insecure using computers and the internet; referring to the instrument "Do you feel safe while using the computer system and browsing the Internet" suggesting a need for further education and confidence building.

Email Security

Referring to the instrument "When you receive an email from an unfamiliar sender, do you open it?", 93% of them avoid opening emails from unfamiliar senders, demonstrating good practice against phishing attempts. While 98% of them refuse to share personal information via email, highlighting awareness of potential scams which can be referred to the instrument "When you receive an email requiring your personal information such as name, date of birth, age, and credit card number, did you send it?" This indicates that most of the samples were aware of email security.

Password Security

Referring to the samples' responses towards password security-related instruments. 89% use strong passwords for bank accounts and social media, indicating a positive approach to protecting their account based on “Do you use a harder-to-guess password to access your bank account and your social networking accounts?”. Meanwhile, only 57% of the samples are familiar with and use Two-Factor Authentication (2FA), demonstrating an understanding of additional security layers which can be referred to as “Do you know what Two-Factor Authentication (2FA) is?” and “Do you use Two-Factor Authentication (2FA)”. Therefore, another awareness regarding password security can be done later to enhance their cybersecurity knowledge.

Application and Data Security

For the application and data security response while using their devices, 80% have rejected app requests for unnecessary permissions, showing concern for data privacy referring to this instrument “Have you ever rejected a mobile app request for accessing your contacts, camera or location?”. While 66% believed they are being monitored online without consent, which referred to “Do you have reason to believe that you are being observed online without your consent?” shows that they are concerned about privacy while online. Lastly, 65% of them feel their data on the polytechnic system is secure, suggesting moderate trust in institutional data security which refers to the instrument “Do you think that your data on the polytechnic system is secure?”.

Online Shopping and Phishing

Referring to “Do you shop/purchase items advertised on social networks or your private email?”, 67% of the samples avoid shopping through social media or email ads, demonstrating caution against potential scams, while 57% of them understand the concept of phishing, indicating awareness of this cyber threat when responded to this instrument “Do you know the meaning of the concept of phishing?”.

Password Hygiene and User Agreements:

Based on Table 4 below, 68% of the samples avoid using the same password for multiple platforms, showcasing good password hygiene practices. That means they are aware that the attacker can pawn the account. While 91% believe reading user agreements is essential before accepting, reflecting a responsible approach to software usage and showing their alertness upon agreement.

Table 4 : Password Usage and User Agreement Alertness

Item	Number of Samples	
	Yes	No
Do you use the same passwords for social networks like Facebook, Twitter, iTunes, and your email accounts?	29	63
Do you think it is essential to read the user agreements for free programs/software before clicking, "I accept"?	84	8

HTTPS and Information Security Officer Necessity

Table 5 below shows that 51% of samples understand the difference between HTTP and HTTPS, this indicates that they have some awareness of secure web connections. While 94% of them believe academic institutions should have an information security officer, this would highlight the observed importance of dedicated cybersecurity personnel in educational institutions.

Table 5 : Secure Connection and Security Officer

Item	Number of Samples	
	Yes	No
Do you know what the difference is between using HTTP and HTTPS?	47	45
In your opinion, is it important that academic institutions should have an information security officer?	87	5

Desire for Further Learning

Lastly, 91% of the sample expressed their interest in learning more about cybersecurity, which indicates a strong willingness to improve their knowledge and skills effectively despite becoming an Information Technology student. Overall, the results show that samples from the IT department have a higher level of cybersecurity awareness than samples from the Commerce department. For instance, IT samples reported that they are knowledgeable about cybersecurity, do not open emails from unfamiliar senders, and use strong, unique passwords for their online accounts based on the percentage of the "Yes" answer. Despite that matter, there are also some areas where cybersecurity awareness can be improved for both programs. For example, a significant percentage of samples from both departments indicated that they do not know the meaning of the phishing concept. Thus, there is a need for more education and awareness-raising on this important cybersecurity-related topic.

5.0 Conclusion

This study examined the internet usage patterns and cybersecurity knowledge of Politeknik Tuanku Syed Sirajuddin (PTSS) students. Students use the internet frequently, and their primary way of accessing the internet is through mobile data. Many students exercise cautiousness by not responding to shady emails and by not disclosing personal information online, but some continue to use weak passwords and other unsafe behaviors. Regarding cybersecurity risks like phishing, safe web connections, and data privacy, there are differences in people's awareness. Students are interested in learning more about cybersecurity despite these gaps in their understanding.

The study essentially emphasizes how critical it is to fill in these knowledge gaps to improve PTSS students' online safety practices. To enhance students' awareness more effectively in cybersecurity, here are some suggestions that can be implemented, such as developing and implementing comprehensive

cybersecurity awareness programs, promoting the use of security tools and best practices, organizing workshops and training sessions, and collaborating with industry partners like Cyber Security Malaysia. Besides that, the population can be expanded to all students in both departments, not limited to semester one and semester two students only.

Acknowledgments
The authors would like to extend their sincere gratitude to Politeknik Tuanku Syed Sirajuddin, Kolej Komuniti Bandar Darulaman and Jabatan Pendidikan Politeknik dan Kolej Komuniti that have made significant contributions to various parts of this research endeavor.

Author Contributions
N.N.S. Ismail: Conceptualisation, Methodology, Writing- Original Draft Preparation; **T.K. Tunku Norizan:** Writing-Reviewing and Editing. **N.L. Hashim:** Proofread, Validation, Supervision.

Conflicts Of Interest
The manuscript has not been published anywhere else and is not being considered by other journals. All authors have authorized the review, agree with the submission, and state that they have no conflicts of interest in the work.

References
Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. In Future Internet (Vol. 11, Issue 3). MDPI AG. https://doi.org/10.3390/fi11030073

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences (Switzerland), 12(5). https://doi.org/10.3390/app12052589

Alshboul, Y., & Streff, K. (2017). Beyond cybersecurity awareness: Antecedents and satisfaction. *ACM International Conference Proceeding Series*, 85–91. https://doi.org/10.1145/3178212.3178218

Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, *20*, 133–155. https://doi.org/10.23962/10539/23572

Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. The African Journal of Information and Communication, 20, 133–155. https://doi.org/10.23962/10539/23572

Frauenstein, E. D. (2019). An Investigation into Students' Responses to Various Phishing Emails and Other Phishing-Related Behaviours. *Communications in Computer and Information Science*, *973*, 44–59. https://doi.org/10.1007/978-3-030-11407-7_4

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

Khadzir, N. H. (personal communication, August 8, 2023)

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2021). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. *Social Science Computer Review*, *41*(1), 286–304. https://doi.org/10.1177/08944393211046339

Mohd Zaharon, N. F., Mohd Ali, M., & Hasnan, S. (2021). Factors Affecting Awareness of Phishing Among Generation Y. *Asia-Pacific Management Accounting Journal*, *16*(2), 409–444. https://doi.org/10.24191/apmaj.v16i2-15

MyCERT. (2024). *MyCERT : Incident Statistics*. https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932

Qasaimeh, M., Al-Manaseer, H., Al-Manaseer, H., & Alghanim, F. (2021). Status Update on Phishing Emails Awareness: Jordanian Case. ACM International Conference Proceeding Series. https://doi.org/10.1145/3492547.3492565

Samaneh Tajalizadehkhoob. (2022, March 22). ICANN. Internet Corporation for Assigned Names and Numbers.

Statista. (2024). *Malaysia number of internet users 2023 | Statista*. Statista. https://www.statista.com/statistics/553752/number-of-internet-users-in-malaysia/

Subramaniam, S. R. (2017) Cyber Security Awareness Among Malaysian Pre-University Students. *E-Proceeding of The 6th Global Summit On Education*, 4 Dec. 2017, pp. 1–14. e-ISBN 978-967-0792-22-4