INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 3, (2024) E-ISSN: 2222-6990

Beyond Bytes: Unveiling Cybersecurity Literacy and Individual Responsibilities in Malaysian University Settings

Muhammad Firdaus Aziz[1], Yusnaini Md. Yusoff[1], Nurul Hanis Aminuddin Jafri[1], Aubrienne Chelsie Wong Houe Leng[2], Subah Sree Subramaniam[2], Haarshwaran Kumar[2], Hanis Sofiah Hisamudin[2], Nor Najla' Yusof[3], Salma 'Asyiqin Azlan[3], Ahmad Firdhaus Arham[1]

[1]Pusat Pengajian Citra, Universiti Kebangsaan Malaysia, Malaysia, [2]Faculty of Law, Universiti Kebangsaan Malaysia, Malaysia, [3]Faculty of Islamic Studies, Universiti Kebangsaan Malaysia, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i3/19757 DOI:10.6007/IJARBSS/v14-i3/19757

Published Date: 16 March 2024

Abstract

In an era where cybersecurity plays a pivotal role in safeguarding digital landscapes, the escalating incidence of cybercrime in Malaysia, particularly among university students, underscores the urgent need for enhanced awareness and knowledge in this domain. This study aims to assess the level of awareness and understanding of cybercrime among Malaysians, focusing on the responsibilities of individuals in fostering a secure digital environment. Conducted in the Klang Valley, the pilot survey engaged 202 participants from diverse backgrounds enrolled in tertiary education, utilizing an online survey platform. The results of the study reveal a consensus among participants regarding the importance of strong passwords, emphasizing the significance of cybersecurity, and acknowledging the individual's role in maintaining a secure digital environment for online safety. Notably, participants expressed a collective sense of responsibility, with a mean score of agreement exceeding 3.58. The surveyed participants strongly assert that regularly changing passwords, educating family members, keeping electronic devices updated, avoiding public WiFi, implementing two-factor authentication, and exercising caution to steer clear of unknown or suspicious websites are integral aspects of their responsibility to ensure online safety. The significance of this research lies in its exploration of factors contributing to cybercrime, shedding light on the intricate landscape of digital risks and vulnerabilities. The study, centring on tertiary students, holds significance beyond academia, acknowledging their potential to significantly influence Malaysian society, particularly in the realm of technological advancements. The

findings offer valuable insights for designing educational programs, shaping policies, and conducting awareness initiatives aimed at mitigating cyber threats.
Keywords: Cybersecurity, Awareness, Individual Responsibility, Students

Introduction

The significance of cyber security practices is increasing in our interconnected digital world. With the progress of information and communication technology, our reliance on digital devices and networks for several aspects of our lives, such as work, communication, banking, and online shopping, is increasing. Nevertheless, the advantages and ease offered by modern technology are counterbalanced by a significant peril that demands our attention, specifically the cyber threat. FortiGuard Labs reported that Malaysia experienced 61.1 million virus detections, 50.2 million botnet attacks, and 7.5 billion exploit detections in the fourth quarter of 2022 (Santos,2023). On a global scale, cyber threats reached approximately 200 billion attacks per day during the same period.

While governments and corporations take measures to safeguard systems and data against cybercrime assaults, individuals also have a crucial role in enhancing cyber security awareness and practices to shield themselves from cyber risks. These cybercrimes frequently arise as a result of users' insufficient knowledge and awareness of security measures. A multitude of individuals disclose sensitive personal information over the internet, including credit card numbers, identifying details, and financial condition (Cohen, 2019). Unauthorized possession of this information can lead to its misuse for activities such as identity theft, financial fraud, or other illicit acts (Smith, 2013). The Malaysian Cyber Security Landscape study reveals that cyber dangers, including online fraud, ransomware, data breaches, cyber espionage, dissemination of fake news, and hate speech, have experienced a surge in Malaysia throughout 2020 (Rasip et al., 2023). This is likely a result of the Covid-19 pandemic, which has led to an increased demand and reliance on the internet in consumers' daily lives. Hence, to mitigate cyber dangers, it is crucial to implement cyber security measures that enhance user knowledge regarding online information security and safeguard personal data against theft or misuse.

Furthermore, the internet has afforded cybercriminals a degree of anonymity due to its global connectivity, which facilitates swift and effortless access to information and interpersonal communication (Ojolo, 2020). However, this also presents a chance for malevolent individuals to engage in nefarious activities without being constrained by geographical boundaries. They possess the capability to conceal their identities and employ advanced tools and procedures to obfuscate their digital traces, so complicating the process of apprehension and legal proceedings. CyberSecurity Malaysia (CSM) recognizes that it encounters difficulties in managing cybercriminal activities as a result of the rapid and unrestricted nature of the internet. Fauzi Suhaimi, the Chief Executive Officer of CSM, stated that the ability to safeguard personal identification requires a combination of technological knowledge, online proficiency, and criminal experience. With the continuous advancement of technology, it is crucial for security and cyber security to adjust and accommodate these progressions. However, it's worth noting that individuals, including university students, can be vulnerable to cyber threats due to factors such as a lack of awareness, inadequate cybersecurity practices, or being targeted by cybercriminals (Alharbi & Tassaddiq, 2021). Educational institutions are often targeted for various reasons, including the potential for accessing sensitive information and the prevalence of technology use among students.

Ensuring cyber security awareness and adherence to best practices is crucial for sustaining robust security and safeguarding privacy in the realm of digital technology. Cyber security encompasses the techniques and measures employed to safeguard humans against cybercriminal assaults, achieved by the development of technologies, practices, or processes aimed at protecting hardware (Perwej et al., 2021). Cybersecurity, furthermore, refers to safeguarding computer systems against unauthorized access and theft of information, ensuring the security of internet users (Le et al., 2019). By acquiring knowledge and implementing effective security protocols, individuals can safeguard their online activities, sensitive information, monetary resources, and computer networks in order to counteract the menace of cybercrime.

The challenge of combating cybercrime is formidable due to its capacity to rapidly transcend national boundaries. Due to the increased freedom in internet usage, individuals have engaged in inappropriate activities such as cyber bullying, dissemination of pornographic material, email phishing, and online transaction fraud. Kritzinger & von Solms (2010) argue that the lack of understanding and awareness regarding internet security poses a threat to internet users in the context of cybercrime. It is imperative for individuals to comprehend the potential hazards linked to their digital endeavours, such as utilizing the internet, social networks, or engaging in online transactions. It is essential for individuals to possess a comprehensive comprehension of cyber security knowledge and protocols in order to safeguard their devices. This includes employing robust passwords, consistently upgrading them, and being able to identify indicators of a potential cyber-attack.

Cybercrime will have severe repercussions for both individuals and pose risks to essential national infrastructure. In order to address the issue of cybercrime, it is necessary to adopt a comprehensive strategy that encompasses public security education and awareness, workforce training in the field of cybersecurity, international collaboration in law enforcement, and the advancement of more robust security technologies. Through comprehension in this particular context, doing research on cyber security knowledge and practices can assist individuals in adopting enhanced security measures, hence contributing to the enhancement of overall cyber security at both the individual and community levels.

Hence the objectives of this study are to determine the extent of knowledge regarding cybercrime among Malaysians and to explore the responsibility of individuals in upholding a secure digital environment.

Methodology

This section presents a concise summary of the study's design, the individuals involved, the research instruments utilized, the methods employed for data collection, and the approach adopted for data analysis. This study uses cross-sectional designs to carry out population-based surveys in order to provide detailed descriptions. The survey involved a sample of 202 respondents from both public and private higher education institutions in Malaysia who were aged 18 and above. The purpose of this study was to determine the extent of awareness of cybercrime and analyse the responsibilities of individuals in ensuring a secure digital environment. Nevertheless, due to the study's primary focus on individual from tertiary education institutes in Malaysia, the findings cannot be extrapolated to other groups of citizens.

This study utilizes a quantitative research methodology. A sample of Malaysian citizens was selected to receive a questionnaire using Google Forms on social media. To address the impact of sampling bias, the sample selection strategy utilized a method called simple random

sampling. To achieve more accurate results, participants were given a two-month timeframe to diligently complete the questionnaire. The study obtained the respondents' explicit agreement and voluntary involvement, while ensuring their anonymity. The gathered data was entered into the SPSS software to do descriptive and inferential analysis.

The survey comprises three sections. The elements in Section A pertain to the personal information of the respondents. Section B aims to assess the level of awareness regarding cybercrime. Section C investigates the role individuals must fulfil in order to uphold a secure digital environment. In Part B of this study, the nominal scale is employed, where respondents select either "Yes" or "No" as their answer. In Part C, the Likert scale method is utilized, where respondents choose from options such as "Strongly disagree," "Disagree," "Not sure," "Agree," or "Strongly agree" for each issue.

The data was examined using descriptive methods, which involved computing the total score, mean, and percentage. Subsequently, this study considers the average mean in order to ascertain the general level of agreement. The degree of consensus is categorized into two degrees, specifically "Disagree" or "Agree," in order to streamline the examination of each element encompassed in Section 3 of this study. A mean score ranging from 1.00 to 2.00 is categorized as "Disagree", while a mean score ranging from 2.01 to 3.00 is categorized as "Agree". The calculation of the mean is shown below:

$$Total\ Score\ =\ Frequency\ of\ Each\ Scale\ \times\ Score\ of\ Each\ Scale$$

$$Min\ (X) = \frac{Total\ Score}{Number\ of\ Respondents}$$

Results

Respondents' demographic

Table 1

Demographic frequency of 202 respondents.

Demographic factors	Attributes	Quantity (%)
Age		
	18	0.5
	20	7.4
	21	31.7
	22	43.1
	23	14.3
	24	2.0
	26	0.5
	28	0.5
Gender		
	Male	38.0
	Female	62.0
Race		
	Malay	26.0
	Indian	13.0
	Chinese	59.0
	Others	2.0
Year of study		
	First	34.0
	Second	51.0
	Third	14.0
	Fourth	1.0

According to the Table 1 above, most of the respondents are 21 to 23 years old and 62.0% of them are female. The table above also indicates that among the 202 participants, 53 individuals, accounting for 26.2% of the sample, are of Malay ethnicity, whilst Chinese participants constitute 58.9% of the total. The number of respondents who are Indian is 27, accounting for 13.4% of the total. Additionally, there are 3 respondents, representing 1.5% of the total, who belong to other nationalities. Given that this study was conducted among students at the tertiary education level, the majority of the participants are in their second year of study, accounting for 51.0% of the total responses. The first-year students make up 34.0%, forming a sizable portion, while third-year students represent 14.0%. Notably, the fourth-year student population is minimal, comprising only 1.0%.

Extent of cybercrime awareness

Table 2

Respondents' level of awareness on cyber security.

Question	Attributes	Quantity (%)
Cybercrime victim		
	Yes	27.0
	No	73.0
Enter personal information online		
	Yes	40.0
	No	60.0
Understanding "phising" meaning		
	Yes	45.0
	No	55.0
Secure digital account with a strong and regularly updated password		
	Yes	60.0
	No	40.0
Consider online privacy and cybersecurity crucial		
	Yes	92.0
	No	8.0
Individuals play a crucial role in maintaining a secure digital environment		
	Yes	93.0
	No	7.0

According to the data presented in Table 2, 23.0% of the participants have encountered cybercrime incidents at some point in their lives. 60.0% of individuals also regularly provided their personal information online, while 55.0% of them are unaware of the term "phishing," which is highly significant in the field of cybersecurity. Nevertheless, a significant majority of 60.0% of the participants take measures to protect their digital account by using a robust and frequently updated password. Additionally, 92.0% of them regard internet privacy and

cybersecurity as essential. Additionally, they hold the belief that individuals personally have a vital part in upholding a secure digital environment, with a consensus of 93.0% in agreement.

Individual Role in Maintaining a Safe Digital Environment

Table 3

Respondents role in maintaining a safe digital environment

Question	Attributes	Quantity (%)
Change passwords regularly		
	Strongly disagree	5.0
	Disagree	11.9
	Not sure	11.9
	Agree	62.4
	Strongly agree	8.9
Educate family members and friends about cyber security.		
	Strongly disagree	1.5
	Disagree	12.9
	Not sure	12.9
	Agree	42.1
	Strongly agree	30.7
Keeping electronics updated with security patches and operating systems		
	Strongly disagree	0.5
	Disagree	16.8
	Not sure	11.9
	Agree	51.0
	Strongly agree	19.8
Avoid using public WiFi without proper protection		
	Strongly disagree	2.5
	Disagree	13.4
	Not sure	11.4
	Agree	45.0
	Strongly agree	27.7
Have two-factor authentication for online account		
	Strongly disagree	2.5
	Disagree	13.9
	Not sure	13.9
	Agree	36.6
	Strongly agree	33.2

Take action to avoid visiting unknown or suspicious websites		
	Strongly disagree	0.5
	Disagree	8.4
	Not sure	8.4
	Agree	42.6
	Strongly agree	40.1

Based on the data presented in Table 3, the majority of participants concur that routinely changing passwords can effectively mitigate the risk of online scams, as indicated by a mean score of 3.58. The respondents also concur that they actively instruct their family members and friends on the subject of cyber security, with a mean average rating of 3.87. The respondents' mean score of 3.72 indicates their agreement with the responsibility of keeping electronics updated with security patches and operating systems in order to maintain a secure digital environment. In addition, they concur to refrain from utilizing public WiFi, as indicated by a mean score of 3.82, in order to ensure their online safety. They also concur that implementing two-factor authentication for online accounts is crucial for establishing a secure online environment, as indicated by a mean score of 3.84. Finally, the participants concur, as indicated by a mean score of 4.13, that their responsibility in upholding a secure digital environment involves refraining from accessing unfamiliar and dubious websites.

Discussion

Cybersecurity is an essential foundation in our ever-interconnected digital realm. The significance of recognizing this issue cannot be exaggerated, as the widespread presence of the internet exposes individuals and organizations to numerous cyber risks. Appreciating the importance of cybersecurity extends beyond technical considerations and is a crucial obligation for society. It is imperative for us, as conscientious individuals, to fully grasp the prospective hazards and actively participate in endeavours to bolster cybersecurity in our everyday existence. The importance of strengthening cybersecurity cannot be overstated, since it encompasses protecting personal information, avoiding identity theft, and ensuring the reliability of digital systems. Adopting secure online practices, maintaining updated on emerging dangers, and promoting strong cybersecurity measures are crucial in creating a safer digital world for both present and future generations. By recognizing the significance of cybersecurity and implementing proactive measures, we enhance our own capabilities and contribute to the development of a more secure and resilient digital environment.

Factors that affect the level of Internet users' awareness of cyber security

The increasing use of the Internet and social media in Malaysia has led to a rise in cybercrime. Many cases result from a lack of awareness about cyber security among users. Most social media users are unaware that cybercrimes like bullying, fraud, and phishing originate from these platforms. Users often share sensitive information without realizing the risks, indicating a disregard for security and privacy. The prevalence of cybercrime due to personal information disclosure highlights the questionable awareness level among social media users. Various factors can influence Internet users' awareness of cyber security.

The level of Internet users' awareness of cyber security in Malaysia is influenced by

several key factors. Firstly, the knowledge factor is crucial, as users need to understand how to navigate social media platforms and be aware of potential cyber threats (Nagle, 2018). Lack of knowledge about security issues, such as malware on smartphones, can lead users to store sensitive information without encryption, making them vulnerable to cybercriminals. Therefore, enhancing users' knowledge about cyber security is vital for improving their awareness.

Attitudinal factors also play a significant role in shaping users' awareness of cyber security. Negative attitudes exhibited on social media, such as using offensive language, making threats, and ignoring permission messages, contribute to the exposure of personal information (Fire et al., 2014). Users need to adopt a responsible and cautious attitude towards their online activities to safeguard their digital security. Attitudinal factors, influenced by cultural, media, and personal elements, directly impact users' cyber security awareness and practices.

Furthermore, environmental factors, including parental guidance, peer influence, and workplace initiatives, contribute to the overall awareness of cyber security (Hsu et al., 2015). Parents play a crucial role in educating children about safe online practices, while peers can advise each other on using security software. Additionally, workplaces should prioritize cyber security by offering educational activities such as lectures and workshops (Wilson & Hash, 2003). The collaboration of these environmental factors is essential in fostering a culture of awareness and responsible cyber practices among Internet users.

Methods and personal approaches to protect against cybercriminals

In the present era, it is indispensable for individuals to have access to the internet, smartphones, and other contemporary technological advancements. Consequently, this circumstance has led to a substantial growth in cybercrime, thereby elevating the likelihood of individuals being exposed to cyber threats. Cybercrime is not solely the duty of the government; as citizens, we must also remain vigilant and take measures to protect ourselves against cyber thieves. Outlined below are a set of duties and tactics to safeguard oneself from engaging in a hazardous digital milieu.

a) Ensure that computer software is consistently updated

Consistently applying software updates, including patches and fixes, can effectively thwart potential attackers by mitigating software vulnerabilities that could be exploited to gain unauthorized access to computer systems (White, 2006). It is highly recommended for all computer owners to utilize the "automatic update" function in software, as it serves as an effective measure to ensure online safety. In addition, it is imperative to exclusively procure applications from reputable sources such as PlayStore. It is imperative that we install anti-virus software and employ a robust lock screen for enhanced security. Failure to do so would result in unrestricted access to all personal data stored on the phone.

b) Employ a robust password

Passwords are a crucial aspect of online existence in contemporary society, as they are employed for a multitude of purposes. It is advisable for individuals to employ distinct combinations of passwords and usernames for various accounts, and refrain from storing their passwords on any computer device. To ensure security, it is imperative to utilize robust

passwords consisting of at least 8 characters, incorporating a blend of uppercase letters, lowercase letters, digits, and symbols (Bhana & Flowerday, 2022). Avoid using passwords that include the login name, personal information such as last name, or words that can be easily located in a dictionary. It is crucial to select a highly robust and distinctive password for every significant account, such as an electronic banking password, in order to safeguard all online activities. In order to enhance the security of the password and prevent unauthorized access, it is necessary to routinely modify it, preferably at intervals of no more than 90 days.

c) Safeguarding personal data

To fully utilize various online services, it is unavoidable that we must furnish personal information to facilitate the shipment of bought goods. There is an absolute certainty that all personal information will be disclosed. Nevertheless, it is imperative to consistently ensure the security of personal information when using the internet (Sicari et al., 2015). Caution must be exercised while disclosing personal identification details such as name, address, phone number, and financial information on the Internet. Furthermore, it is imperative to guarantee the website's security when engaging in online transactions. This entails activating our privacy settings while utilizing or accessing social media platforms. To safeguard personal information effectively, it is imperative to refrain from responding to email solicitations that request personal data, avoid accessing deceptive websites designed for the purpose of identity theft, and remain vigilant regarding the privacy policies of websites and applications (Youn, 2009).

Conclusion

In conclusion, the level of awareness and practice of cyber security is important in the rapidly growing digital world. Cyber security involves preventive measures to avoid threats from cyber criminals such as stolen personal information and financial fraud. Without proper cyber security awareness and practices, individuals are exposed to the risk of losing significant information and being hacked online. Therefore, cyber users need to be responsible to guarantee the security of their personal information by being equipped with knowledge and skills about the ethical use of computer technology.

The importance of this work resides in its investigation of circumstances that can result in cybercrime, illuminating the intricate terrain of digital risks and weaknesses. Researchers can provide vital insights to cybersecurity efforts by comprehending these aspects, thereby establishing a basis for targeted interventions and preventive actions. Although the study specifically targets tertiary education students, its wider influence on society is also apparent. The study suggests that tertiary education students, who are often at the forefront of technology advances, can have a significant impact on Malaysian society as a whole. The results can provide valuable insights for educational programs, policy formulation, and awareness efforts aimed at tackling cyber dangers. This will help ensure that the knowledge and responsible practices instilled in students are also spread to the wider community. Therefore, this study not only contributes to academic discussions but also provides practical benefits for improving cybersecurity practices in society, ensuring the digital security of Malaysians beyond the boundaries of tertiary education.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.

Bhana, B., & Flowerday, S. V. (2022). Usability of the login authentication process: Passphrases and passwords. *Information & Computer Security*, *30*(2), 280-305.

Cohen, M. C. (2018). Big data and service operations. *Production and Operations Management*, *27*(9), 1709-1723.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019-2036.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information systems research*, *26*(2), 282-300.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840-847.

Nagle, J. (2018). Twitter, cyber-violence, and the need for a critical social media literacy in teacher education: A review of the literature. *Teaching and teacher education*, *76*, 86-94.

Ojolo, T. L. (2020). *A criminological investigation into the lived experiences of cybercrime perpetrators in southwest Nigeria* (Doctoral dissertation).

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.

Le, D. N., Kumar, R., Mishra, B. K., Chatterjee, J. M., & Khari, M. (Eds.). (2019). *Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies*. John Wiley & Sons.

Rasip, O. M., Salleh, M. M., Abd Rahman, S., Taib, M. N. M. M., & Rozlan, A. M. (2023). Kesan Pandemik Covid-19 Terhadap Keupayaan Keselamatan & Pertahanan Negara: The Effect of The Covid-19 Pandemic on National Security & Defense Capabilities. *International Journal of Interdisciplinary and Strategic Studies*, *4*(6), 379-391.

Santos, D. J. P. dos. (2023). Key findings from the 1H 2023 FortiGuard Labs Threat Report: Fortiguard Labs. Fortinet Blog. https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-1h-2023

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146-164.

Smith, R. G. (2013). Identity theft and fraud. In *Handbook of internet crime* (pp. 273-301). Willan.

White, D. S. D. (2006). *Limiting Vulnerability Exposure through effective Patch Management: threat mitigation through vulnerability remediation* (Doctoral dissertation, Rhodes University).

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1-39.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, *43*(3), 389-418.