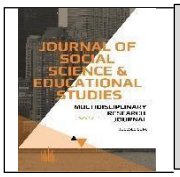

Journal of Contemporary Social Science and Education Studies
E-ISSN: 2785-8774
Vol 3, Issue 2 (2023)

Data Security Knowledge On Social Media Among University Students In Malaysia

***Nur Suhaili Mansor[1], Hapini Awang[2], Ramlan Mustapha[3] &**
Nurul Izzah Mohamad Ghozali[4]
[1,2,4] Institute for Advanced and Smart Digital Opportunities (IASDO), School of Computing, Universiti Utara Malaysia, 06010, Malaysia.
[3]Akademi Pengajian Islam Kontemporari Universiti Teknologi MARA Pahang Raub Campus, 27600, Malaysia.

Article Info

Article history:

Received: 2 July 2023
Revised: 30 July 2023
Accepted: 25 August 2023
Published: 1 September 2023

Keywords:

Data security, knowledge, social media

ABSTRACT

This study explores the current understanding of data security among students within the Malaysian higher education system. The focus is on evaluating how well the respondents grasp two critical aspects: knowledge related to securing social media platforms and a broader comprehension of data security measures. To gather insights, a meticulously designed questionnaire was administered to students enrolled at a reputable university college located in the northern region of Peninsular Malaysia. This particular institution was selected carefully to ensure a diverse representation of students across various academic disciplines. Upon thoroughly examining the gathered responses, the aim was to discern the level of familiarity Malaysian students have with data security. Unfortunately, the results underscore a significant deficiency in the respondents' understanding of both dimensions of data security knowledge that were scrutinized in this study. The findings emphasize the urgent necessity for improved educational initiatives in the realm of data security awareness for higher education students in Malaysia. This study highlights the importance for educational institutions and policymakers to acknowledge these existing gaps and take proactive steps to bolster students' comprehension of data security. This, in turn, can contribute to cultivating a more secure digital landscape for the entire nation.

Corresponding Author:

*Nur Suhaili Mansor

Institute for Advanced and Smart Digital Opportunities, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia

Email:nursuhaili@uum.edu.my

INTRODUCTION

Social media, a virtual platform for sharing thoughts, information, and content through digital networks, has gained prominence globally (Li et al., 2021). It facilitates the swift sharing of personal data, documents, videos, and images via web-based applications on various devices. While the prevalence of social media is evident in the United States and Europe, it is particularly widespread in Asian countries like Malaysia. The nation's internet usage has steadily risen, substantially increasing social media users since 2000. According to (Muniandy et al., 2017), Malaysia witnessed a significant surge in internet users, from 0.1 percent in 1995 to 37.9 percent in 2005. Reports from the Malaysian Communications and Multimedia Commission (2015) reveal a 66.6 percent internet penetration rate in Q1 2014, equivalent to around 20.1 million users. Especially in challenging times of physical separation, social media connects students more than ever (Alharbi & Tassaddiq, 2021), offering avenues for creative expression, learning (Khamali et al., 2018), and communication (Pekkala & van Zoonen, 2022). Nevertheless, while advantageous, it also poses potential negative consequences. In this context, trust becomes a prevailing assumption in the virtual realm.

However, the control users perceive within the virtual social media space can be misleading. Often, users are unaware of the exact location and sources of their data, which ranges from public to highly sensitive information (such as social security numbers) with varying security levels. As documented by (Gan et al., 2008), the proliferation of phishing attacks and identity theft has hindered the growth of Internet banking in Malaysia, with cyberattacks on financial institutions escalating since 2000. Notably, Malaysia ranked sixth globally for cybercrime vulnerability in the Sophos Security Threat Report 2013, resulting in reported losses of RM1 billion. Furthermore, Malaysia's cybercrime incidents surged from 9,986 in 2012 to 10,636 in 2013, as per data from the Malaysia Computer Emergency Response Team, known as MyCERT.

LITERATURE REVIEW

Social media platforms like Facebook, Twitter, WhatsApp, and Instagram are popular avenues for social interaction, and Malaysia stands out as an active user of such platforms in Asia. Notably, university students in Malaysia are recognized as enthusiastic social media users, with a study revealing that over 62.5% are heavy Internet users. Given this context, understanding data security within social media becomes crucial. Data security safeguards information from unauthorized access and corruption across various applications and platforms. Focusing on information disclosure on social networks among Malaysian university students, this study aims to address the prevalent issue and propose solutions. Specifically, the study delves into concerns like password practices and phishing as it scrutinizes data security behaviors in social media among this demographic. Social media platforms often provide privacy controls, such as profile visibility settings and content blocking. In recent years, Facebook has adjusted its privacy settings due to user complaints, defaulting to private profiles with the option to make posts public (Tatjana et al., 2010). In other words, everything can be shared in a blink around the world.

However, the rapid sharing nature of social media poses risks, as hackers can exploit shared information, including login credentials, for malicious purposes (Potgieter, 2019). Notably, a phishing campaign aimed at Instagram users has been observed (Soni et al., 2019). Instagram has become a famous medium platform for picture graphs and text-sharing. Most customers will use it as a digital diary to proportion regular sports and moments. A phishing assault should occur on Instagram (Zhang & B. Gupta, 2018), demonstrating how even

prominent platforms are susceptible. For example, hackers can create convincing fake pages to capture user credentials, granting unauthorized access.

Consequently, this research is driven by two main inquiries: the level of data security awareness among Malaysian university students and effective strategies to enhance this awareness. To achieve this, the study employs an extensive survey of Malaysian universities to gauge students' foundational data security understanding and offer practical recommendations to foster a culture of informed data security within the country's higher education institutions.

METHODOLOGY

This research was carried out in five major stages. The first phase involved the development of a questionnaire. In this phase, questionnaires were created using Google Forms based on our research title, Data Security Knowledge on social media Among Malaysian University Students. The questionnaire was divided into three sections: respondents' demographics, student knowledge of data security on social media, and student experience with data security leaks or threats.

The second phase of the study was a questionnaire blasting. In data collection, this study used a quantitative approach to online questionnaires, Google Forms. The type of respondent determined the structure of each questionnaire. This study included demographic profiles, social media usage, and level of awareness of data security knowledge on social media. Online survey methods were used because they would provide greater access to respondents and larger sample size. The Google Form was distributed to Malaysian university students via online platforms such as WhatsApp, Instagram, and Facebook. One hundred fifty people completed the survey.

The third phase was data collection. Once the target number of respondents was reached, all responses were entered into an Excel spreadsheet for analysis. Closed-ended questions were coded, and surveys were numbered. The data has been saved for use in this study.

Data analysis was the focus of the fourth phase. The results and findings were produced by analyzing the data collected from the surveys. For the open-ended questions that required a text response, a consolidation process was used to synthesize many responses into similar categories. The researcher started by going over all the responses given in response to a specific question. The responses revealed common themes designated as "categories" for classification purposes. Each response was reread, and A decision was made as to which category it should be placed in. This enabled the categorization of responses for analysis purposes. The modules would then be given recommendations for how to use social media. As a result, social media content and features will be utilized.

Lastly is Phase Five, the result presentation. In the result presentation phase, every result that was analyzed was presented in tables and graphical representations such as pie charts to show the data security knowledge on social media among university students in Malaysia, as in Figure 1.

Figure 1: Five Major stages

RESEARCH FINDINGS

In the this section, a comprehensive exposition of the research findings is dedicated to the demographic facets under investigation. This portion involves a detailed breakdown and elucidation of the multifaceted demographic variables that underwent scrutiny as integral components of this study. A thorough examination of these demographic findings unveils a nuanced and comprehensive understanding of the participants' diverse characteristics, backgrounds, and distinctive attributes that have influenced their involvement in the research. A holistic and detailed portrayal of the participants' profiles is constructed by delving into age distribution, educational attainments, geographical locations, and potentially other pertinent factors. These demographic insights enrich the overall comprehension of the respondent cohort and furnish the necessary contextual backdrop that underpins the subsequent analysis and discourse on the research outcomes. This exploration of the demographic dimensions contributes to the depth and breadth of understanding while ensuring a robust foundation for others to draw subsequent interpretations and implications from the research findings.

Demographic profile

The study's participant pool encompassed 59 male and 91 female students from diverse universities and regions across Malaysia. Examination of the questionnaire responses elucidated key aspects of the participants' profiles. Notably, most respondents fell within the age bracket of 19 to 24 years and were in academic semesters from 3 to 6 within their higher education journey. These demographic insights are visually represented in Table 1, which succinctly encapsulates the social media usage patterns exhibited by these 150 respondents.

Table 1: The usage related to social media of these 150 respondents

No	Questions	Response %	Response %	Response %	Response %	Response %
1.	Which social media channels are you most active on?	Instagram 33.3	Whatsap 38	Tiktok 14	Facebook 11.3	Snapchat 2.1
2.	How often did you use social media in a day?	Once 1.3	2-3 times 18	4-8 times 53.3	Nine and above 27.3	

3.	How long does the usage of social media last per session?	1-5 min 12.7	5-10 min 15.3	10-30 min 37.3	30 min above 34.7	
4.	What do you use social media for?	Networking 52.7	Business 13.3	Learning 27.3	Others 6.7	
5.	How many social platforms are you on?	1 0.00	2 18.7	3 28	4 33.3	Five and above 20
6.	How often do you post on social media?	Very often 18.7	Somewhat often 49.3	Rarely 32		

As delineated in Table 1, the analysis reveals a striking trend among higher education students with substantial internet engagement. They are active across many social media platforms, with Instagram and WhatsApp claiming the highest percentages at 33.3% and 38%, respectively. Furthermore, a considerable segment also engages with TikTok, Facebook, and Snapchat (27.4%). Their dependence on social media becomes evident through the sheer volume of daily usage and session duration. Remarkably, more than half (53.3%) engage with social media 4 to 8 times a day, while their most active sessions span between 10 to 30 minutes (37.3%) and beyond 30 minutes (34.7%), figures that nearly equate. Conversely, 12.7% exhibit infrequent social media usage, clocking 1 to 5 minutes sessions. Unveiling their motivations, networking emerges as the predominant drive (52.7%), followed by educational pursuits (27.3%), business activities (13.3%), and other factors (6.7%).

Shifting focus, the subsequent inquiry unveils the extent of their immersion. A substantial majority (33.3%) actively engage across at least four social media platforms, with others not lagging either—none use just one platform, each maintaining at least two accounts. Surprisingly, their enthusiasm wanes when it comes to posting; almost half (49.3%) post moderately, 32% do so infrequently, and 18.7% display a penchant for frequent posting. This behavior aligns with Malaysian students' broader inclinations in social networking, corroborated by (Muniandy et al., 2017), revealing that Internet users across various age groups in Malaysia exhibit a bias for active social networking engagement. This study further underscores the prevalence of students' consistent interaction with social networking sites, illustrating the multifaceted roles the Internet assumes in their academic journeys and beyond.

Table 2: The participant's security practices regarding data security

No	Questions	Do not know	Never	Rarely	Often	Always
1.	Before visiting a website, I will verify its credibility.	6%	34.7%	20%	16.7%	22.7%
2.	I construct a password that includes my personal information (for example, last name, date of birth)	7.3%	18%	11.3%	23.3%	40%

3.	I am conscientious about the privacy settings on my social media accounts	0%	0.7%	12%	26.6%	60.7%
4.	Social media platforms safeguard my personal information.	2.7%	5.3%	14%	22%	56%
5.	Before using any social media, I carefully read the terms and conditions.	2.7%	34.7%	12%	8.7%	56%
6.	I am cautious when clicking on links in social media posts.	22.7%	34.7%	12%	8.7%	22%
7.	I constantly update my social media passwords.	2.7%	5.3%	10.7%	20.7%	60.6%
8.	When I use public Wi-Fi, I feel safe.	13.3%	42%	19.3%	8%	48.7%
9.	I feel my social media has no value to hackers, and they do not target me.	4%	36.7%	18%	10%	31.3%

Presented in Table 2 are the findings related to participants' security practices concerning data security, offering insights into their awareness when utilizing social media. Various perspectives emerge concerning platform credibility, revealing a majority's apparent indifference; approximately 34.7% acknowledge never verifying platform credibility during internet browsing, while fewer than half display concern. Regarding passwords, over 60% tend to incorporate personal information despite the associated risks to their accounts. Notably, responses to question 3 reflect a pronounced concern for privacy on social media, yet translating this into proactive measures seems limited, mirroring observations from questions 1 and 2.

In addition to that, impressively, over 70% believe that social media platforms uphold their privacy, with merely 5.3% harboring skepticism. Predictably, a minority (30.7%) engages with terms and conditions when using social media, while a majority (69.3%) remains indifferent. A remarkable revelation lies in the heightened caution (about 90%) exercised while clicking social media links, indicative of awareness regarding the perils of phishing and malware. Conversely, the impetus to update passwords appears lacking, with only 48.7% consistently perceiving public Wi-Fi as safe, while around 20% disagree. Exploring perceptions of hackers and their targets, around half envisage themselves as potential targets due to their account's value. At the same time, the remaining half are less concerned, possibly owing to perceived insignificance.

This array of figures underscores a notable paradox: despite their youth and education, participants' familiarity with social media data security remains somewhat limited. Many evince a carefree stance

despite their significant daily engagement with social media. A heightened sense of concern typically emerges only when they become victims themselves. Yet, it's essential to acknowledge that not all participants are oblivious; a subset demonstrates a vigilant approach toward their use of social media platforms, exemplifying a more cautious and informed standpoint.

DISCUSSIONS

The ensuing sections delve into the vulnerabilities of the respondents' limited grasp of data security, exposing them to potential cyber security attacks. Addressing this deficiency could alleviate some of the associated risks. Initiating awareness campaigns to enlighten individuals about these concerns is one of the pivotal measures that can shield them from the escalating tide of cyber security threats. In essence, augmenting cyber security awareness becomes an imperative barrier against imminent cybercrimes and nascent cyber threats. Despite skepticism from some security professionals regarding the value of cyber security education, many researchers advocate for its indispensability in safeguarding cyber users from the perils of cyber security threats.

Recognizing that data security concerns necessitate education, it becomes evident that the human factor constitutes the weakest link within information systems, an assertion frequently voiced by security experts. A multitude of security challenges, especially those intertwined with human interaction with information systems, mandate a focus on addressing the human dimension of cyber security.

Furthermore, academia has a robust consensus in favor of incorporating cybersecurity education into the curricula of Malaysian schools and higher education institutions. This resonates given the current void in explicit cyber security instruction. Although earlier research highlights the extensive internet usage by higher education students, the majority are not exposed to the intricacies of emerging data security threats. Furthermore, the research conducted by Rezgui and Marks underscores the heightened vulnerability of individuals aged 18 to 24 to cyber security attacks, exacerbated by the scarcity of tertiary institutions addressing this imperative aspect. Consequently, a clarion call for educating these individuals in data security emerges, positioning cyber security education as a critical preparation for safeguarding their virtual presence as they transition into the practical realm upon graduation.

The consensus voiced by (Saleh Zolait et al., 2014) reinforces the notion that students must be well-versed in security matters before embarking on their professional journeys. Additionally, echoing the sentiments of Teer, Kruck, and Kruck's stance is firm that risky computer security behavior should not permeate workplaces. Against this backdrop, the persistent theme that emerges strongly from these discussions is the imperative need for formal cybersecurity education to effectively address the escalating demands of data security in a dynamic digital landscape.

CONCLUSION AND RECOMMENDATION

In the contemporary landscape, university students find themselves more interconnected than ever, a phenomenon facilitated by social media, particularly in times of physical separation and challenging circumstances. The research journey was meticulously charted, encompassing five pivotal phases: questionnaire preparation, questionnaire distribution, data collection, data analysis, and result presentation. Additionally, our study uncovers a panorama of risky security behaviors exhibited by

participants, which have demonstrated consistency across similar investigations. Hence, it is unsurprising that the findings reported in this study align with prior research. This collective body of research highlights an intriguing paradox: despite being a demographic characterized by youth and education, participants exhibit a distinct lack of comprehension concerning social media data security. Remarkably, despite their substantial daily presence on social media platforms, a substantial proportion demonstrates an apparent lack of concern.

Nonetheless, some students display commendable prudence within this spectrum when navigating social media. In conclusion, the imperative remains to continually guide social media and internet users to heighten their consciousness of these precarious scenarios, nurturing their preparedness to undertake preventative measures as and when required. It is paramount to foster a well-informed student populace equipped with the knowledge necessary to safeguard themselves in the ever-evolving landscape of digital interactions.

ACKNOWLEDGEMENT

We would like to acknowledge Fadillah Teguh Rizka, Md Rayhan Uddin, Muhammad Aqil Haafiz Norhaziz and Nurul Idashazwaney Rosli for their contribution and assistance during the data collection, analysis and report preparation.

REFERENCES

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

Khamali, R., Thairu, & Wanja, R. (2018). Influence of Social Media on Knowledge Sharing Practices in Kenyan Universities: a Case of Strathmore University. *The Strategic Journal of Business&Change Management*, *5*(4).

Li, F., Larimo, J., & Leonidou, L. C. (2021). Social media marketing strategy: definition, conceptualization, taxonomy, validation, and future agenda. *Journal of the Academy of Marketing Science*, *49*(1). https://doi.org/10.1007/s11747-020-00733-3

Malaysian Communications and Multimedia Comission. (2015). *Malaysian Communication and Multimedia Malaysia (MCMC) Internet Users Survey 2014*. 1–52.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance & Cybersecurity*, *2017*, 1–13. https://doi.org/10.5171/2017.800299

Pekkala, K., & van Zoonen, W. (2022). Work-related social media use: The mediating role of social media communication self-efficacy. *European Management Journal*, *40*(1). https://doi.org/10.1016/j.emj.2021.03.004

Potgieter, P. (2019). *The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology*. *12*, 272–262. https://doi.org/10.29007/gprf

Saleh Zolait, A. H., Al-Anizi, R. R., Ababneh, S., BuAsalli, F., & Butaiba, N. (2014). User awareness of social media security: The public sector framework. *International Journal of Business Information Systems, 17*(3). https://doi.org/10.1504/IJBIS.2014.064973

Soni, Hafid, A., & Sudyana, D. (2019). Analysis of Security Awareness in using Technology and Social Media at Muhammadiyah University of Riau. *International Journal of Computer Applications*, *177*(18), 20–25. https://doi.org/10.5120/ijca2019919631

Tatjana, T., Elena, A., Georgina, S., Yiannis, L., & Aysu, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example. *International Journal of Media & Cultural Politics*, *6*(1), 81–101.

Zhang, Z., & B.Gupta, B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 914–925.