Self-Disclosure and Digital Privacy Awareness and Knowledge among University Students in Malaysia

Siew Weng Yew, Abdul Hafiz AB Rahman, Sarina Yusoff

Centre for Research in Development, Social and Environment, Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia

DOI: https://dx.doi.org/10.47772/IJRISS.2024.8100255

Received: 15 October 2024; Accepted: 22 October 2024; Published: 21 November 2024

ABSTRACT

In the digital era, social media has become an integral communication tool, particularly for university students who frequently engage in high levels of self-disclosure. While social media offers numerous benefits, it also presents significant concerns about digital privacy, as students often share personal information without fully understanding the associated risks. This study investigates self-disclosure behaviors and evaluates digital privacy awareness among students at Universiti Kebangsaan Malaysia (UKM). A quantitative approach through the distribution of questionnaires was used to obtain responses from 123 students at UKM. The findings reveal that although 66.7% of respondents frequently use their real names and profile pictures on social media, only a small fraction share highly sensitive information, such as their residential address (17.1%) or phone numbers (16.3%). The study further indicates that while 85% of students are aware of basic privacy threats like phishing and 78% understand the risks of identity theft, awareness of more advanced threats remains limited. Only 45% of respondents are familiar with data mining techniques, and 40% are aware of algorithmic profiling, highlighting significant gaps in students' understanding of how their personal data can be exploited. These results demonstrate the urgent need for educational initiatives to strengthen digital privacy literacy and promote more effective protective behaviors. This study contributes to digital sociology by providing insights into students' privacy practices and highlighting the need for more comprehensive digital privacy education.

Keywords: digital privacy, self-disclosure, university students, social media, privacy risks, digital literacy

INTRODUCTION

The advent of social media has revolutionized communication and self-expression across the globe, especially among younger generations. University students, in particular, are a significant demographic in this digital landscape. As digital natives, these students have grown up immersed in online technologies, relying on platforms like Facebook, Instagram, and Twitter to communicate, network, and even build professional profiles. However, this ubiquity of social media has not come without significant concerns, the most pressing of which revolves around digital privacy.

In Malaysia, the increasing dependence on social media has exposed users to a wide range of privacy risks. According to Hanifah Mahat et al. (2023), Malaysia is a rapidly digitalizing nation, and university students constitute one of the most active social media user groups. Despite this, there is a growing gap between students' frequent social media usage and their awareness of the potential privacy risks associated with disclosing personal information online. As digital technologies evolve, the nature of privacy threats becomes more complex, ranging from identity theft and phishing attacks to algorithmic profiling and unauthorized data harvesting by third parties (Padmavathi & Mohanlal, 2021).

This paper investigates how students at Universiti Kebangsaan Malaysia (UKM) engage with social media, focusing on their levels of self-disclosure, awareness of digital privacy risks, and knowledge of measures to protect their personal data. The study aims to fill gaps in the literature on digital privacy awareness and seeks to contribute to ongoing discussions about digital privacy education and the development of more effective

strategies to safeguard the privacy of young people online.

Self-Disclosure in the Digital Age

Self-disclosure, which refers to the process of sharing personal information, is central to how individuals present themselves in both offline and online environments. According to Jourard's (1971) foundational work on self-disclosure, revealing personal details helps build trust and strengthen interpersonal relationships. However, the shift from face-to-face interactions to digital platforms has altered the nature of self-disclosure. Studies show that individuals tend to disclose more personal information online than they would in face-to-face interactions, driven by the perceived anonymity and distance afforded by the digital space (Luo & Hancock, 2020).

In the context of social media, self-disclosure can take many forms—users share photos, opinions, relationship statuses, locations, and even sensitive personal details such as political beliefs or health information. While these disclosures can enhance social bonding, they also create vulnerabilities. Users who engage in high levels of self-disclosure without considering the privacy settings of social media platforms risk exposing themselves to cyber threats, such as identity theft, cyberstalking, and unauthorized data harvesting (Petronio & Child, 2020). A key challenge lies in the balance between the desire for social connection and the need to protect one's privacy.

Awareness and Knowledge of Digital Privacy

Awareness of digital privacy encompasses an individual's understanding of the risks associated with sharing personal information online and the steps they can take to mitigate these risks. However, as the literature suggests, awareness does not necessarily translate into action. Many social media users, particularly younger ones, are aware of potential privacy threats but often fail to adopt appropriate protective measures (Padmavathi & Mohanlal, 2021).

Bhatnagar and Pry (2020) argue that university students, while familiar with basic concepts such as phishing and password security, are generally unaware of more sophisticated privacy threats, including algorithmic profiling, where personal data are used by companies to create detailed consumer profiles for targeted advertising and data mining, where personal data is harvested and analyzed to predict behavior or influence decision-making (Acquisti & Grossklags, 2021). This knowledge gap is especially concerning given the increasing use of data-mining technologies by corporations and governments alike.

In Malaysia, the digital landscape has become increasingly complex, with a surge in cyber threats over the past few years. A report from CyberSecurity Malaysia recorded 4,741 cyber incidents in 2022 alone, including cases of phishing, identity theft, and data breaches (Bernama, 2023). The Malaysian government's efforts to address these issues include initiatives such as the National Scam Response Center (NSRC), which aims to educate the public about cyber threats. However, research suggests that many young people in Malaysia remain unaware of how to protect their personal information effectively (Adlina Kamalulail et al., 2022).

METHODOLOGY

This study adopts a quantitative research design to assess the digital privacy behaviours, awareness, and knowledge of UKM students. A structured questionnaire was developed and distributed to a sample of 123 undergraduate students from various faculties at UKM. The questionnaire contained 30 items divided into three sections: self-disclosure behaviours, awareness of digital privacy risks, and knowledge of privacy protection measures.

Sampling and Data Collection

Participants were selected using stratified random sampling to ensure a representative sample across different academic disciplines. The questionnaire was administered online, and respondents provided informed consent before participating. The data collection period spanned two weeks during the academic semester to allow for

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VIII Issue X October 2024

adequate responses. Participants were asked to rate their agreement with various statements using a five-point Likert scale which ranged from 1 (strongly disagree) to 5 (strongly agree), covering topics such as the types of information students disclose on social media, their understanding of digital privacy risks, and their use of privacy settings.

Data Analysis

The data were analyzed using IBM SPSS Statistics Version 29 to generate descriptive statistics and inferential analyses. Descriptive statistics were used to summarize students' self-disclosure behaviors, awareness of digital privacy threats, and use of privacy protection tools. Inferential statistics, including Pearson correlation analysis, were employed to examine the relationships between self-disclosure and knowledge of privacy risks.

RESULTS

A total of 123 university students participated in the study. The majority of respondents were female, with 68.3% (n = 84), while male respondents accounted for 31.7% (n = 39).

Personal Information Control

When it comes to controlling personal information on social media, the findings reveal that while students are cautious about sharing sensitive information, they still disclose identifiable details such as their real names and profile pictures. Specifically, 66.7% (n = 82) of respondents reported that they display their real names on their social media accounts, and an equal proportion (66.7%, n = 82) use their real profile pictures (Table 1). In contrast, more sensitive details, such as residential addresses and phone numbers, were shared by far fewer respondents. Only 17.1% (n = 21) of students displayed their actual place of residence, and just 16.3% (n = 20) shared their phone numbers on social media.

Adjusting privacy settings is an important part of personal information control, and 90.2% (n = 111) of respondents reported that they personally adjust the privacy settings on their social media accounts (Table 4). However, despite this proactive measure, some respondents still disclose potentially risky information. For example, 52.8% (n = 65) of students admitted to sharing their real birthdate, while 16.3% (n = 20) provided entirely accurate personal information on their social media profiles. These findings suggest that although most students take steps to control their online privacy, there remains a gap in fully understanding the risks of oversharing identifiable personal details.

Table 1: Types of Information Disclosed on Social Media

		Yes		No	
No.	**Item**	**n**	**%**	**n**	**%**
1	I display my real name on social media.	82	66.7	41	33.3
2	I display my real profile picture on social media.	82	66.7	41	33.3
3	I display my real gender on social media.	109	88.6	14	11.4
4	I display my real place of residence on social media.	21	17.1	102	82.9
5	I display my real phone number on social media.	20	16.3	103	83.7
6	I display my real birthdate on social media.	65	52.8	58	47.2
7	I display accurate information about myself on social media.	20	16.3	103	83.7
8	I adjust the privacy settings of my social media accounts myself.	111	90.2	12	9.8

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VIII Issue X October 2024

Self-Disclosure Behaviors

Self-disclosure behaviors were measured to understand how frequently students share personal information on social media. The findings suggest a mixed approach to sharing personal details online (Table 2). A significant proportion of respondents (67.5%, n = 83) reported that they often or almost always hesitate to share personal information on social media, while only 8.1% (n = 10) rarely hesitate. However, trust plays a crucial role in self-disclosure, with 86.9% (n = 107) stating that they only share personal information with close friends they trust.

Interestingly, despite hesitations about sharing personal information, a notable number of respondents (42.3%, n = 52) admitted to accepting friend requests from individuals they do not know, while fewer respondents (8.1%, n = 10) frequently send friend requests to strangers. This contradiction between trust in self-disclosure and risky social media practices such as accepting unknown contacts suggests a potential gap in students' understanding of the privacy risks associated with social media usage. Furthermore, 75.6% (n = 93) of respondents either rarely or never feel comfortable discussing personal challenges openly on social media, indicating a level of restraint in sharing sensitive personal information

The overall results show that while students may be cautious about sharing personal information with the public, they often engage in behaviors that may expose them to privacy risks, such as interacting with unknown individuals. This highlights the need for more robust educational initiatives focusing on online privacy and digital literacy.

Table 2: Level of Self-Disclosure on Social Media

No.	Item	Frequency (%)				
		Never	Rarely	Sometimes	Often	Almost always
1.	I hesitate to share my personal information on social media.	0 (0)	10 (8.1)	30 (24.4)	43 (35.0)	40 (32.5)
2.	I only share my personal information with friends I trust.	0 (0)	4 (3.3)	12 (9.8)	42 (34.1)	65 (52.8)
3.	I accept friend requests from people I do not know.	29 (23.6)	28 (22.8)	14 (11.4)	20 (16.3)	32 (26.0)
4.	I send friend requests to people I do not know.	61 (49.6)	40 (32.5)	12 (9.8)	8 (6.5)	2 (1.6)
5.	When facing challenges in life, I feel comfortable talking about them openly on social media.	41 (33.3)	52 (42.3)	24 (19.5)	6 (4.9)	0 (0)
6.	I often share personal issues on social media without hesitation.	77 (62.6)	28 (22.8)	14 (11.4)	0 (0)	4 (3.3)
7.	I limit the personal information I share on social media.	0 (0)	6 (4.9)	8 (6.5)	44 (35.8)	65 (52.8)
8.	If I feel the information I have shared on social media is too personal, I delete it.	2 (1.6)	4 (3.3)	8 (6.5)	36 (29.3)	73 (59.3)
9.	I avoid posting certain topics because I worry about who has access.	0 (0)	6 (4.9)	14 (11.4)	48 (39.0)	55 (44.7)
10.	I allow my main interests to be publicly known to gain friends on social media	27 (22.0)	20 (16.3)	32 (26.0)	22 (17.9)	22 (17.9)

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VIII Issue X October 2024

Knowledge of Digital Privacy Threats on Social Media

The respondents displayed a relatively high level of awareness regarding basic digital privacy threats, such as malware and phishing. For example, 67.5% (n = 83) of students agreed or strongly agreed that they know malware is a type of malicious software designed to collect user credentials and gain access to personal information (Table 3). Similarly, 67.5% (n = 83) understood that phishing is the act of impersonating an authorized person or organization to obtain sensitive personal information.

However, knowledge about more advanced privacy threats, such as social engineering and clickjacking, was notably lower. Only 31.7% (n = 39) strongly agreed that they are aware of social engineering tactics used to manipulate individuals into revealing confidential information, while 39.8% (n = 49) were familiar with clickjacking, a technique where users are tricked into clicking on deceptive links. These results suggest that while students have a basic understanding of common digital privacy risks, they may be less aware of more sophisticated and evolving threats, which may make them vulnerable to advanced cyberattacks.

Table 3: Knowledge of Digital Privacy Threats

No.	**Item**	**Frequency**				
		Strongly Disagree	**Disagree**	**Not Sure**	**Agree**	**Strongly Agree**
1.	I know malware is malicious software that collects user credentials and gains access to personal information.	12	10	18	49	34
2.	I know malware can use credentials obtained to impersonate the user and send malware links to the user's online friends.	12	10	30	32	39
3.	I know malware is distributed on social media in the form of malvertising, hidden links in images, plugins, and digital media.	6	14	26	43	34
4.	I know phishing is the act of obtaining personal information such as user ID, passwords, and other sensitive data by impersonating an authorized person or organization.	2	14	24	40	43
5.	I know phishing occurs through email, text messages, or phone calls to trick people into sharing sensitive data, including passwords, banking information, or credit card details.	6	6	16	49	46
6.	I know phishing spreads among social media users by redirecting them to fake URLs.	4	8	24	42	45
7.	I know cyber fraud is the use of internet access to deceive or take advantage of individuals.	2	0	10	44	67
8.	I know cybercriminals build trust with victims and then exploit personal data displayed in their profile accounts.	2	2	10	44	65
9.	I know clickjacking is a malicious technique that tricks users into clicking on something other than what they intended to click.	8	14	26	26	49

10.	I know identity theft involves using someone else's photos and personal information to create fake social media accounts, either as a prank or for fraudulent purposes.	0	4	8	48	63
11.	I know identity thieves can extort money, contact friends to ask for money, or post political messages or hate speech through fake accounts.	0	4	10	50	59
12.	I know cyberstalking involves intensively and repeatedly searching for someone's information, then using it to threaten or cause harm.	0	2	10	48	63
13.	I know doxing involves exposing identifiable information about someone online, such as their real name, home address, workplace, phone number, and other personal details, without the victim's consent.	4	16	28	28	47
14.	I know social engineering is a technique of manipulating targeted victims to disclose data, spread malware, or provide access to restricted systems, both online and through personal interactions.	8	20	32	24	39

Awareness of Digital Privacy on Social Media

The majority of respondents demonstrated a high level of awareness regarding the potential threats posed by social media platforms and the security measures available to protect personal information (Table 4). For example, 93.5% (n = 115) agreed or strongly agreed that they are aware of personal information security issues on social media, while 87.0% (n = 107) acknowledged the risk of third parties misusing their personal information online.

Most respondents (89.4%, n = 110) reported that they are aware of security features that protect the confidentiality of social media users, and 91.9% (n = 113) knew about verification mechanisms that can help identify the personal information of social media users. However, fewer respondents (64.2%, n = 79) indicated that they know whom to contact in the event of a privacy threat on social media, highlighting a gap in practical knowledge about how to respond to security breaches. This points to the need for more education on digital safety protocols, not only to increase awareness but also to empower students to act when privacy concerns arise.

Table 4: Awareness of Digital Privacy on Social Media

No.	**Item**	**Frequency**				
		Strongly Disagree	**Strongly Disagree**	**Strongly Disagree**	**Strongly Disagree**	**Strongly Disagree**
1.	I am aware of the issue of personal information security on social media.	2	0	6	46	69
2.	I am aware of the potential digital privacy threats to myself.	2	0	6	56	59
3.	I am aware of with whom I share	2	4	2	58	57

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VIII Issue X October 2024

	information on social media.					
4.	I am aware of with whom I interact on social media.	0	2	6	52	63
5.	I am aware that third parties or other people can access my personal information on social media.	2	4	10	48	59
6.	I am aware of the risks of personal information being misused by irresponsible parties.	2	2	8	50	61
7.	I am aware that there are security features that protect the confidentiality of social media users' information.	0	6	10	52	55
8.	I am aware that there are security features that can verify and identify the personal information of social media users.	0	4	6	62	51
9.	I am aware that the appearance of advertisements and promotions (pop-up/spam) on social media can threaten privacy when users are online.	2	10	10	38	63
10.	I am aware of the security of personal information when involved with fake advertisements or promotions offered on social media.	2	4	4	48	65
11.	I am aware of whom to contact if there is a privacy threat on social media.	8	8	28	28	51
12.	I am aware that there are cybersecurity awareness programs.	2	6	14	44	57
13.	I am aware that there are authorities responsible for monitoring users and electronic media in Malaysia.	2	4	16	40	61
14.	I am aware of the existence of laws or acts related to electronic media in Malaysia.	0	2	16	32	73

DISCUSSION

The findings of this study highlight a significant gap between the self-disclosure behaviors of university students and their awareness of digital privacy risks. While students frequently use social media platforms to engage and share personal information, their knowledge of more sophisticated privacy threats, such as social engineering and clickjacking, remains inadequate. This discrepancy underscores a key issue in digital literacy: although students are generally aware of privacy concerns, they lack the in-depth understanding and practical skills necessary to protect themselves from evolving cyber threats.

The concept of self-disclosure on social media is a complex phenomenon. On one hand, it is essential for maintaining social bonds and expressing personal identity. On the other hand, excessive disclosure without appropriate privacy settings can expose users to risks like identity theft and data misuse. For university students, who are among the most active users of these platforms, such risks are particularly concerning.

Studies have consistently shown that individuals, especially younger demographics, tend to prioritize convenience and social engagement over security precautions (Mansour & Francke, 2021). This study confirms that while UKM students are relatively aware of basic threats like phishing, many are unaware of more advanced risks such as algorithmic profiling and how their data is commodified by third parties.

Despite high levels of concern about privacy, few students appear to adopt strong security measures. For instance, while the majority of respondents were aware of basic privacy features provided by social media platforms, fewer students were familiar with more advanced tools like VPNs and encryption software. This is consistent with findings from previous research which suggests that while awareness exists, practical knowledge on how to implement effective protective measures is often lacking (Abdullah Alabdulatif & Fahad Alturise, 2020). Therefore, it is crucial for universities to take a proactive role in addressing this gap. By integrating digital privacy education into the academic curriculum, institutions like UKM can equip students with the skills they need to navigate these platforms safely and securely.

In particular, the low percentage of students who knew whom to contact in the event of a privacy breach highlights the need for more comprehensive education on digital safety protocols. Practical measures, such as how to report privacy violations or steps to take when facing cyber threats, should be a core part of such programs. Previous studies have emphasized the importance of targeted interventions in raising awareness and improving privacy behaviors among young people (Bhatnagar & Pry, 2020).

CONCLUSION

The present study provides valuable insights into the digital privacy awareness, self-disclosure behaviors, and knowledge levels of university students at UKM. Although students demonstrate a high level of engagement with social media, there remains a substantial gap in their understanding of advanced privacy threats and how to effectively safeguard their personal information. The findings suggest that while students are aware of the basic risks associated with digital privacy, such as phishing and identity theft, they are less familiar with more complex privacy concerns like data commodification and algorithmic profiling.

This gap between awareness and action highlights the pressing need for more comprehensive digital privacy education. By fostering a culture of privacy awareness and providing students with practical tools to protect their information, universities can play a pivotal role in preparing students for the complexities of the digital age. In doing so, institutions like UKM not only protect the privacy of their students but also contribute to the development of a generation that is more digitally literate and resilient to the threats posed by the evolving online landscape .

REFERENCES

1. Abdullah Alabdulatif & Fahad Alturise. 2020. Awareness of data privacy on social networks by students at Qassim University. International Journal of Advanced Computer Research, 10(50): 194-205.
2. Acquisti, A. & Grossklags, J. 2005. Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, 3(1): 26-33.
3. Adlina Kamalulail, Nur Ezzatul Nadia Abdul Razak, Siti Aisyhah Omar & Noreha Mohamed Yusof. 2022. Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. e-Academia Journal of UiTM Cawangan Terengganu, 11(1): 1-13.
4. Bernama. 2023. Ancaman keselamatan siber meningkat di Malaysia.
5. Bhatnagar N. & Pry M. 2020. Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal (ISEDJ), 18(1): 48-58.
6. Hanifah Mahat, Siti Wardah Hussein, Yazid Saleh, Mohmadisa Hashim, Nasir Nayan, Zahid Mat Said & Edi Kurniawan. 2023. Social Media as a Medium for Disseminating Community Awareness of Environmental Issues in Malaysia. TEM Journal, 12(3): 1658-1667
7. Jourard, S. M. 1971. The Transparent Self.

8. Luo, M. & Hancock, J.T. 2020. Self-disclosure and social media: motivations, mechanisms and psychological well-being. Current Opinion in Psychology, 31: 110-115.
9. Mansour, A. & Francke, H. 2021. Collective Privacy Management Practices: A Study of Privacy Strategies and Risks in a Private Facebook Group. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), bil.360, hlm. 1–27.
10. Padmavathi J. & Mohanlal S.A.K. 2021. A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(3).
11. Petronio, S. & Child, J.T. 2020. Conceptualization and operationalization: utility of communication privacy management theory. Current Opinion in Psychology, 31: 76-82.