International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 6, Nov-Dec 2024
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Examining Students' Awareness and Behaviors in Safeguarding Personal Information on Social Media Platforms

James L. Cabatuan Jr[1] , Raffy P. Carreon[2] , Siti Sheena K. Mediana[3], Markdy Y. Orong[4]
*(College of Computer Studies, Misamis University, Ozamiz City
Email: jamesjrcabatuan@gmail.com)
**(College of Computer Studies, Misamis University, Ozamiz City
Email: raffycarreon23@gmail.com)
***(College of Computer Studies, Misamis University, Ozamiz City
Email: sitisheena2@gmail.com)
****(College of Computer Studies, Misamis University, Ozamiz City
Email: markdy.orong@mu.edu.ph)

----------**********----------

Abstract:

This study examines the awareness and behaviors of undergraduate students at Misamis University in safeguarding their personal information on social media platforms. Using a descriptive research design, the study surveyed 310 students across various colleges to assess their levels of awareness and behavioral practices. Results revealed that students are generally aware of privacy and security measures, such as verifying website credibility and being cautious with privacy settings. However, gaps in awareness, such as reading terms and conditions, were identified. Behavioral practices like avoiding public Wi-Fi for sensitive activities and limiting information sharing were frequently observed, although certain habits, like regular password changes, were less common. A very strong positive correlation ($r = 0.855$, $p < 0.01$) was found between students' awareness and their behaviors, emphasizing the critical role of awareness in promoting secure online practices. The findings highlight the need for targeted educational interventions to enhance digital literacy and strengthen students' protective behaviors online.

Keywords — **Social Media Privacy, Online Security Awareness, Undergraduate Behavior, Personal Information Protection, Digital Literacy.**

----------**********----------

I. INTRODUCTION

The widespread integration of social media into daily life has revolutionized the way individuals communicate, connect, and share information (Achmad, 2021; Bayer et al., 2020; Hysa et al., 2021; Karamat & Farooq, 2020). Platforms such as Facebook, LinkedIn, and Twitter have become pivotal for maintaining relationships, exchanging ideas, and engaging with global communities (Cheng et al., 2020; Hruska & Maresova, 2020; Liang et al., 2021; Zulli et al., 2020). For university students, these platforms serve as essential tools for both academic and social interactions, encouraging the frequent sharing of personal experiences and opinions (Dutta, 2020; Kircaburun et al., 2020; Martzoukou et al., 2020; Thomas et al., 2020). However, this increased activity has also raised significant privacy concerns, as sensitive information may be accessed by unintended audiences, leading to risks such as misuse and data breaches (Al-Busaidi et al., 2022; Arpaci & Bahari, 2023; Hysa & Spalek, 2019; Kwon & Park, 2022).

As social media usage continues to grow, the need to address privacy risks has become more pressing (Cheng et al., 2022; Ismagilova et al., 2022; Jain et al., 2021; Onu et al., 2024). Research suggests that while many young adults are digitally active, they often lack adequate awareness of cybersecurity threats, particularly those associated with social media platforms (Akrami et al., 2024; Zwilling et al., 2022). University students, in particular, are vulnerable to privacy violations and cybercrimes, as

they may neglect privacy settings or fail to recognize the implications of sharing personal information online (Brands & Van Doorn, 2022; Carvalho et al., 2020; Kröger & Müller, 2021; Nkongolo & Sewnath, 2024). Understanding the awareness and behaviors of this demographic is critical for developing strategies to mitigate these risks.

This study aims to evaluate the level of awareness of Misamis University undergraduate students regarding the risks associated with sharing personal information on social media platforms. It also seeks to assess their behaviors in protecting personal information and to determine if there is a significant relationship between their awareness and their online security practices. Given the increasing importance of data privacy and digital safety in today's society, this research addresses the urgent need to identify gaps in knowledge and practices to enhance students' online security behaviors.

Two theoretical frameworks guide this study: Privacy Calculus Theory and Social Cognitive Theory. Privacy Calculus Theory posits that individuals evaluate the perceived benefits of sharing personal information—such as increased social interaction and self-expression—against potential privacy risks (Schomakers et al., 2022). This cost-benefit analysis plays a significant role in influencing online behavior, particularly on social media platforms. Understanding how students balance these considerations provides valuable insights into their privacy-related decisions.

Social Cognitive Theory further emphasizes the role of observational learning and self-efficacy in shaping behaviors. Students often model their privacy practices based on peers' behaviors or societal norms. Bandura's concept of self-efficacy suggests that individuals who believe in their ability to manage their online privacy are more likely to engage in protective behaviors (Tao et al., 2020). This underscores the need for a supportive environment that promotes positive privacy practices through education and peer influence.

By examining Misamis University undergraduate students' awareness and behaviors concerning personal information security, this research contributes to the broader discourse on digital privacy. The findings may inform the development of targeted educational initiatives, awareness campaigns, and institutional policies aimed at fostering safer online practices among students. Ultimately, this study seeks to empower students with the knowledge and skills needed to navigate the challenges of the digital age responsibly and securely.

II. METHODOLOGY

This study employed a descriptive and correlational research design to examine Misamis University undergraduate students' awareness and behaviors in protecting personal information on social media. The descriptive component assessed students' levels of awareness and specific security practices, while the correlational aspect explored the relationship between these factors. A cross-sectional survey was used to gather data from a broad sample of students at a single point in time, providing a snapshot of their current online security behaviors. Convenience sampling was employed to select readily accessible participants, focusing on regular social media users to ensure the relevance of the data. Although convenience sampling limited full representativeness, it offered valuable insights from a diverse group of students.

Data collection occurred online via a Google Forms survey, distributed through familiar social media channels such as Facebook groups and Messenger chats among Misamis University undergraduate students. This approach promoted accessibility and aimed to boost participation by leveraging platforms that students commonly used. The survey was divided into sections covering demographics, privacy awareness, and behaviors related to safeguarding personal information. Descriptive statistics summarized awareness and behaviors, while Pearson's correlation coefficient was used to assess the relationship between awareness and behaviors, offering insights that could inform recommendations for improving students' cybersecurity practices.

III. RESULTS AND DISCUSSION

A total of **310 undergraduate students** participated in the study, representing diverse academic programs across Misamis University.

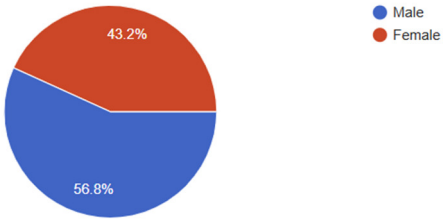

Figure 1. Sex Distribution

Among the respondents, **56.8% (176 students)** identified as male, while **43.2% (134 students)** identified as female. This distribution highlights a slightly higher representation of male students compared to female students in the sample population. The nearly balanced proportion ensures a diverse perspective on awareness and behaviors related to protecting personal information on social media, providing a well-rounded basis for analysis. Such representation is crucial for examining potential gender-based differences in cybersecurity awareness and practices, though the study primarily focuses on the overall trends within the student population.

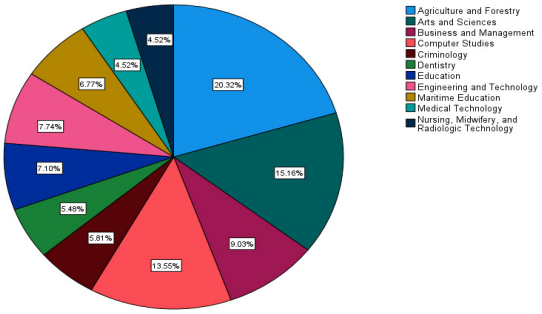

Figure 2. Colleges Represented

Participants were distributed across different colleges, with the largest representation from the **College of Agriculture and Forestry (20.3%)**, followed by the **College of Arts and Sciences (15.2%)** and the **College of Computer Studies (13.5%)**. Smaller groups of participants came from colleges like **Medical Technology (4.5%)** and **Nursing, Midwifery, and Radiologic Technology (4.5%)**, reflecting the diverse academic backgrounds of the student population. The broad distribution across colleges provides valuable insights into the awareness and behaviors of students from various academic backgrounds. This diversity ensures that the study captures differences in cybersecurity awareness and practices that may arise from varying educational environments and professional orientations. Moreover, the representation of multiple fields enriches the analysis, enabling a more comprehensive understanding of how students from distinct academic domains approach the safeguarding of personal information on social media platforms.

Table 1. Level of Awareness among Undergraduate Students

Statements	Mean	Standard Deviation	Interpretation
Before visiting a website, I will verify its credibility.	*3.58*	*.92*	*Aware*
I construct a password that includes my personal information (for example, last name, date of birth).	*3.37*	*.97*	*Somewhat Aware*
I am conscientious about the privacy settings on my social media accounts.	*3.55*	*.94*	*Aware*
Social media platforms safeguard my personal information.	*3.43*	*.88* .	*Aware*
Before using any social media, I carefully read the terms and conditions.	*3.38*	*93*	*Somewhat Aware*
I am cautious when clicking on links in social media posts.	*3.48*	*.94*	*Aware*
I constantly update my social media passwords.	*3.41*	*.92*	*Aware*
When I use public Wi- Fi, I feel safe.	*3.29*	*.94*	*Somewhat Aware*
I feel my social media has no value to hackers, and they do not target me.	*3.36*	*.95*	*Somewhat Aware*
Overall	*3.43*	*.93*	*Aware*

Note: 4.20-5.0 (Very Aware); 3.40-4.19 (Aware); 2.60-3.39 (Somewhat Aware); 1.80-2.59 (Not Aware); 1.0-1.79 (Unsure)

The findings indicate that the majority of students are **"Aware"** of essential privacy practices. For example, verifying website credibility had a mean score of 3.58 (Standard Deviation = 0.92), signifying a strong awareness of this security measure. Similarly, students demonstrated high awareness of privacy settings and the importance of restricting public access to personal details.

However, certain areas showed **lower levels of awareness**. One notable example is reading and understanding the terms and conditions of websites and applications, which scored as **"Somewhat Aware."** This highlights a critical gap in students' attention to often overlooked but essential aspects of digital safety. These findings suggest that while students are generally knowledgeable about fundamental privacy practices, targeted efforts are necessary to address specific areas where awareness is lacking.

The findings also reveal that students' behaviors align with established theories of decision-making and self-regulation. For instance, students frequently avoided using public Wi-Fi and limited the sharing of sensitive information, supporting the principles of **Privacy Calculus Theory**. This theory suggests that individuals weigh the perceived risks of sharing personal information against the potential benefits. Students who recognize the risks of insecure practices prioritize protective actions, highlighting the critical role of awareness in decision-making.

Moreover, the **Social Cognitive Theory** explains how personal awareness influences behavior through self-regulation and perceived self-efficacy. This was evident in students' proactive habits, such as taking measures to safeguard their privacy online.

Nevertheless, gaps in awareness, such as the low frequency of reading and understanding terms and conditions, remain concerning. This implies a lack of attention to hidden risks, leaving students vulnerable to privacy breaches. These findings emphasize the need for **targeted educational interventions** to address specific knowledge gaps and promote comprehensive online safety habits.

Table 2. Level of Behaviors among Undergraduate Students

Statements	Mean	Standard Deviation	Interpretation
I change my social media passwords regularly to enhance security.	*3.32*	*.88*	*Sometimes*
I avoid sharing sensitive personal information (e.g., address, phone number) publicly on social media.	*3.48*	*.90*	*Often*
I only connect with people I know personally on social media to protect my privacy.	*3.43*	*.86*	*Often*
I use multi-factor authentication on my social media accounts.	*3.39*	*.89*	*Sometimes*
I regularly review and update the privacy settings on my social media accounts.	*3.39*	*.90*	*Sometimes*
I avoid using public Wi-Fi when accessing sensitive accounts or personal information.	*3.41*	*.87*	*Often*
I log out of social media accounts after each session, especially on shared devices.	*3.42*	*.92*	*Often*
I carefully assess links and attachments before clicking or downloading on social media.	*3.43*	*.87*	*Often*
I disable location services or sharing my location on social media posts to limit exposure.	*3.46*	*.90*	*Often*
I monitor and delete old posts or content that may expose personal information.	*3.41*	*.91*	*Often*
Overall	*3.41*	*.89*	*Often*

Note: 4.20-5.0 (Always); 3.40-4.19 (Often); 2.60-3.39 (Sometimes); 1.80-2.59 (Rarely); 1.0-1.79 (Never)

The findings reveal that students often engage in **privacy-protective behaviors**, with an overall mean

score of 3.41 (Standard Deviation = 0.89), indicating that these practices are performed **"Often."** For instance, avoiding the use of public Wi-Fi for sensitive activities was among the most frequently observed behaviors, reflecting students' understanding of the risks associated with unsecured networks. Similarly, many respondents reported being cautious about sharing sensitive details on social media.

However, **less frequent behaviors** were also identified. Practices such as regularly updating passwords and reviewing app permissions scored lower, falling into the **"Sometimes"** category. These findings suggest that while students exhibit a proactive approach to protecting their personal information in some areas, there is still **room for improvement** in adopting consistent habits for enhanced online security.

Certain protective behaviors, such as avoiding public Wi-Fi, appear to be practiced more frequently. This may be influenced by **cultural or educational factors**, such as the emphasis on cybersecurity in university settings, which fosters these habits. In contrast, behaviors like regular password changes are less common, possibly due to a lack of awareness or prioritization of their importance.

The **university context** plays a critical role in shaping these practices. Integrating privacy education into the curriculum and offering workshops on online safety could significantly enhance students' knowledge and encourage the consistent adoption of secure behaviors.

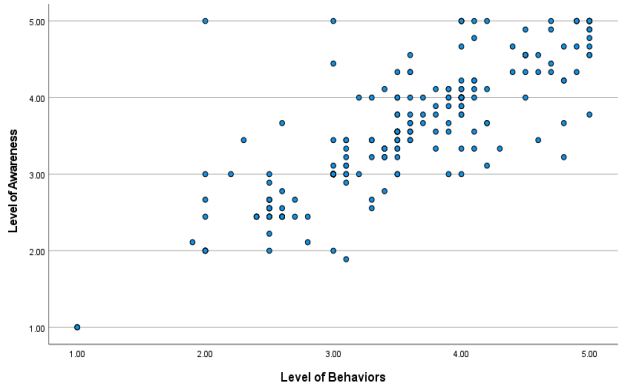

Figure 3. Scatterplot Showing the Relationship Between Level of Awareness and Level of Behaviors in Safeguarding Personal Information

The scatterplot shows the relationship between the level of awareness and the level of behaviors in safeguarding personal information. Each point represents an individual data observation, and the overall trend suggests a positive correlation between the two variables. This implies that individuals with higher levels of awareness tend to demonstrate more consistent safeguarding behaviors. The clustering of data points in the upper-right quadrant further supports this association, indicating that a strong understanding of cybersecurity concepts may lead to more proactive and protective practices. This visualization highlights the critical role of awareness in influencing behaviors related to personal information security.

Table 3. Significant Relationship between Students' Awareness and Their Behaviors

Variables	*r*	*p-value*	*Remarks*
Awareness	*.855***	*0.01*	*Highly Significant*
Behaviors	*.855***	*0.01*	*Highly Significant*

Probability Scale: p < 0.01 (Highly Significant); p < 0.05 (Significant); p > 0.05 (Not Significant)

Note: Relationship Strength Scale: 1.00 (Perfect); 0.80-0.99 (Very Strong); 0.60-0.79 (Strong); 0.40-0.59 (Average); 0.20-0.39 (Weak); 0.01-0.19 (Very Weak); 0.00 (No Relationship)

The analysis shows a **very strong positive correlation** between students' level of awareness and their behavioral practices in safeguarding personal information ($r = 0.855$, $p < 0.01$). This indicates that students with higher awareness levels are more likely to engage in secure online behaviors.

Specifically, students who are knowledgeable about key privacy measures, such as verifying website credibility and managing privacy settings, are more likely to adopt protective behaviors like avoiding public Wi-Fi for sensitive activities and limiting the personal information they share online. This suggests that awareness serves as the foundation for informed decision-making, enabling students to recognize potential risks and act accordingly to mitigate them.

The findings align with previous research, which emphasizes the strong link between awareness and behavior in online security. However, the study also reveals **unique patterns**, such as high awareness of basic security practices (e.g., avoiding public Wi-Fi)

and relatively low attention given to terms and conditions. This suggests that while students are knowledgeable about surface-level risks, their understanding of deeper aspects, such as data privacy policies, remains underdeveloped.

Conversely, **lower awareness levels** are linked to less frequent adoption of critical security practices, such as regularly updating passwords or reviewing app permissions. These findings underscore the importance of increasing awareness through education, as it directly influences students' ability to implement secure behaviors effectively, thereby reducing their vulnerabilities to online threats.

IV. CONCLUSION

This study assessed the awareness and behavioral practices of Misamis University students in safeguarding their personal information on social media platforms. The findings revealed that while students generally exhibit high levels of awareness about basic online privacy practices, gaps remain in specific areas, such as understanding terms and conditions. Similarly, students frequently engage in certain protective behaviors, such as avoiding public Wi-Fi and limiting sensitive information sharing, but practices like regularly updating passwords are less common.

The strong positive correlation **($r = 0.855$, $p < 0.01$)** between awareness and behaviors highlights the critical role of knowledge in fostering secure online habits. These results underscore the importance of comprehensive privacy education to address existing gaps and promote consistent protective behaviors. Ultimately, the study emphasizes the need for targeted interventions to improve digital safety among students, ensuring they are better equipped to navigate the risks of the digital age

V. RECOMMENDATIONS

To address the identified gaps in awareness and behaviors, universities should integrate privacy and cybersecurity education into their curricula, focusing on practical and actionable strategies for digital safety. Workshops, seminars, and awareness campaigns using accessible platforms like social media can further reinforce key messages and encourage proactive habits among students. Educators play a crucial role in this effort by incorporating case studies, guidelines, and resources that highlight real-world applications of privacy-protective practices. Students, on the other hand, should take the initiative to enhance their digital literacy by engaging with online resources and consistently adopting behaviors such as updating passwords, reviewing app permissions, and understanding terms and conditions. Future research should explore the effectiveness of these interventions and expand the scope to include diverse populations for a broader understanding of digital safety challenges. These collective efforts can promote a safer online environment and empower students to navigate the digital landscape responsibly.

REFERENCES

[1] Achmad, W. (2021). Citizen and Netizen Society: The Meaning of Social Change From a Technology Point of View. Jurnal Mantik, 5(3), 1564–1570.

[2] Akrami, K., Akrami, M., Akrami, F., Ahrari, M., Hakimi, M., & Fazil, A. W. (2024). Investigating the Adverse Effects of Social Media and Cybercrime in Higher Education: A Case Study of an Online University. Studies in Media, Journalism and Communications, 2(1), 22–33. https://doi.org/10.32996/smjc.2024.2.1.3

[3] Baker-Eveleth, L., Stone, R., & Eveleth, D. (2022). Understanding social media users' privacy-protection behaviors. Information and Computer Security, 30(3), 324–345. https://doi.org/10.1108/ICS-07-2021-0099

[4] Bayer, J. B., Triêu, P., & Ellison, N. B. (2020). Social media elements, ecologies, and effects. Annual Review of Psychology, 71, 471–497. https://doi.org/10.1146/annurev-psych-010419-050944

[5] Cheng, R., Wu, N., Chen, S., & Han, B. (2022). Will Metaverse Be NextG Internet? Vision, Hype, and Reality. IEEE Network, 36(5), 197–204. https://doi.org/10.1109/MNET.117.2200055

[6] Cheng, W. W. H., Lam, E. T. H., & Chiu, D. K. W. (2020). Social media as a platform in academic library marketing: A comparative study. Journal of Academic Librarianship, 46(5). https://doi.org/10.1016/j.acalib.2020.102188

[7] Dutta, D. A. (2020). Impact of Digital Social Media on Indian Higher Education: Alternative Approaches of Online Learning during COVID-19

Pandemic Crisis. International Journal of Scientific and Research Publications (IJSRP), 10(05), 604–611. https://doi.org/10.29322/ijsrp.10.05.2020.p10169

[8] Hruska, J., & Maresova, P. (2020). Use of social media platforms among adults in the United States—Behavior on social media. Societies, 10(1). https://doi.org/10.3390/soc10010027

[9] Hysa, B., Karasek, A., & Zdonek, I. (2021). Social media usage by different generations as a tool for sustainable tourism marketing in society 5.0 idea. Sustainability (Switzerland), 13(3), 1–27. https://doi.org/10.3390/su13031018

[10] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers, 24(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

[11] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex and Intelligent Systems, 7(5), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

[12] Karamat, A., & Farooq, A. (n.d.). Emerging Role of Social Media in Political Activism: Perceptions and Practices. In South Asian Studies A Research Journal of South Asian Studies (Vol. 31, Issue 1).

[13] Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2020). Uses and Gratifications of Problematic Social Media Use Among University Students: a Simultaneous Examination of the Big Five of Personality Traits, Social Media Platforms, and Social Media Use Motives. International Journal of Mental Health and Addiction, 18(3), 525–547. https://doi.org/10.1007/s11469-018-9940-6

[14] Kröger, J. L., & Müller, F. (2021). H Ow D Ata C an B E U Sed a Gainst P Eople : a C Lassification of P Ersonal D Ata M Isuses.

[15] Liang, X., Lu, Y., & Martin, J. (2021). A review of the role of social media for the cultural heritage sustainability. Sustainability (Switzerland), 13(3), 1–17. https://doi.org/10.3390/su13031055

[16] Mansor, N. S., Awang, H., Mustapha, R., & Ghozali, N. I. M. (Year). Title of the document. ERIC. https://files.eric.ed.gov/fulltext/ED639485.pdf

[17] Martzoukou, K., Fulton, C., Kostagiolas, P., & Lavranos, C. (2020). A study of higher education students' self-perceived digital competences for learning and everyday life online participation. Journal of Documentation, 76(6), 1413–1458. https://doi.org/10.1108/JD-03-2020-0041

[18] Nkongolo, M., & Sewnath, J. (2024). Data protection psychology using game theory. International Conference on Cyber Warfare and Security, 19(1), 240–250. https://arxiv.org/abs/2402.07905v1

[19] Onu, P., Pradhan, A., & Mbohwa, C. (2024). Potential to use metaverse for future teaching and learning. In Education and Information Technologies (Vol. 29, Issue 7). https://doi.org/10.1007/s10639-023-12167-9

[20] Schomakers, E. M., Lidynia, C., & Ziefle, M. (2022). The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance. International Journal of Human-Computer Interaction, 38(13), 1276–1289. https://doi.org/10.1080/10447318.2021.1994211

[21] Tao, D., Shao, F., Wang, H., Yan, M., & Qu, X. (2020). Integrating usability and social cognitive theories with the technology acceptance model to understand young users' acceptance of a health information portal. Health Informatics Journal, 26(2), 1347–1362. https://doi.org/10.1177/1460458219879337

[22] Thomas, L., Orme, E., & Kerrigan, F. (2020). Student Loneliness: The Role of Social Media Through Life Transitions. Computers and Education, 146(September 2019), 103754. https://doi.org/10.1016/j.compedu.2019.103754

[23] Zulli, D., Liu, M., & Gehl, R. (2020). Rethinking the "social" in "social media": Insights into topology, abstraction, and scale on the Mastodon social network. New Media and Society, 22(7), 1188–1205. https://doi.org/10.1177/1461444820912533

[24] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

