INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 9.47]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 11, Issue - 03, March - 2025

DOIs:10.2015/IJIRMF/202503007 --:-- Research Paper / Article / Review

Security Concerns of Social Networking Sites: A Study on Student Awareness

Dr. A. Anandhiprabha,
Assistant Professor, Department of Commerce – Banking and Insurance
Nallamuthu Gounder Mahalingam College, Pollachi, Coimbatore, Tamilnadu.
Email: anandhiaruchamy@gmail.com

Abstract: *Social networking sites (SNS) have become integral to students' daily lives, offering platforms for communication, collaboration, and information sharing. However, their widespread usage raises significant concerns regarding privacy, data security, and cyber threats. This study investigates students' awareness of security issues associated with social networking platforms, focusing on their understanding of risks such as data breaches, phishing, identity theft, and privacy violations. The findings highlight varying levels of awareness among students, the factors influencing their knowledge, and the measures they adopt to protect themselves online. Recommendations are provided to improve students' cybersecurity awareness and promote safer online practices.*

Key Words: *Students, social networking sites, security concerns, cyber security awareness, privacy, online safety, data breaches, phishing, identity theft.*

1. INTRODUCTION:

Internet technology has facilitated global communication and information sharing, even among individuals with minimal technical expertise **(Zeebareea et al., 2020).**As social media platforms continue to amass vast quantities of user data, they become increasingly attractive targets for malicious actors seeking to exploit this information for personal gain. Furthermore, the widespread use of social media for marketing presents additional security risks if not properly managed **(Jain et al. 2021)**. Therefore, SNSs security must be taken seriously to safeguard against potential threats and protect confidential data.

2. LITERATURE REVIEW:

Martin, S., & Martin, M. (2023), conducted a study entitled "**Privacy Settings and Security Awareness on Social Media Among College Students".** This study focuses on the awareness of privacy settings and the overall security measures among college students using SNS like Instagram, Facebook, and TikTok. The researchers found that while students were generally aware of privacy settings, many still had incomplete or inadequate security configurations on their accounts. Specifically, the study revealed that a significant proportion of students did not regularly update their privacy settings or were unaware of tools to control who can access their personal information. The authors emphasized the need for universities to offer more targeted workshops and tutorials to increase awareness about effective privacy protection on social platforms.

In their study "Cyber security Awareness in the Age of Social Media: A Study on College Students' Practices" **Anderson, D. L., & Williams, R. (2022)** investigated cyber security practices among college students, specifically examining behaviours such as password strength, use of multi-factor authentication (MFA), and awareness of phishing schemes on SNS. The study highlighted a concerning lack of cyber security knowledge among students. Although many students were familiar with the term "phishing," a large portion did not recognize phishing attempts on social media platforms. The study also noted that students often used simple, easily guessable passwords and did not employ MFA, making their accounts vulnerable to hacking. The authors recommended that universities integrate cyber security training into their curricula to improve students' practical knowledge and self-protection strategies.

Schmidt, C., & Zhang, J. (2021) conducted a study entitled "**The Role of Social Media Literacy in Enhancing Students' Security Practices" they** focused on the concept of social media literacy, which includes both an understanding of how to use SNS securely and awareness of the potential risks. The study revealed that students who received training on the risks of oversharing, the dangers of location tagging, and the impact of personal data leaks were more likely to practice good security habits, such as adjusting privacy settings and avoiding risky behaviours. However, the study found that there was still a significant portion of students who lacked sufficient social media literacy. The authors suggested that social media literacy courses should be part of university programs, particularly in fields related to communication, digital media, and information technology.

Gupta, P., &Verma, R. (2023) conducted a study on "Social Media Security: A Study on Perceptions and Practices Among University Students" to explored the perceptions and practices of university students regarding SNS security, focusing on common issues such as data breaches, identity theft, and cyber talking. They found that students were often complacent about the potential security risks of social media. While most students were aware of the dangers of sharing personal information publicly, they did not consider the risk of data collection by third-party apps or advertisers. Furthermore, many students were unaware of the extent to which their data could be used or sold. The study emphasized the importance of teaching students about the broader implications of their digital footprints and the significance of controlling third-party access to personal data.

In their study "**The Influence of Digital Trust on Social Networking Site Usage and Security Practices Among Students" Lee, J., & Kim, H. (2024),** assessed the relationship between digital trust and students' security practices on social networking platforms. The study found that students who had a high level of trust in SNS platforms were less likely to engage in secure behaviours such as updating privacy settings or using strong passwords. Conversely, students who were more skeptical of the platforms' security policies took more precautions. The research suggests that the perceived trustworthiness of SNS providers heavily influences students' engagement with security practices. The authors proposed that SNS platforms need to take more responsibility for user education and transparency about data security policies to foster more secure behaviours among users.

3. OBJECTIVES / AIMS :

The study's objectives are listed as follows:

1. To measure how much college students know about security concerns when using social networking sites.
2. Gauge how well students understand the privacy settings and security features available on popular social networking platforms.
3. Investigate the security practices and behaviors that students engage in when using social media, such as password management, enabling two-factor authentication (2FA), and using strong passwords.

4. RESEARCH METHOD / METHODOLOGY :

The present investigation is mainly based on the primary data which have been collected from the college students in various arts and science colleges through the issue of structure questionnaire. The questionnaire comprises questions relating to the personal profile and the usage of social networking sites by the college students. The study consists of 840 students which have been collected from arts and science colleges using snowball sampling method. The data gathered from the college students have been analyses by using Percentage Analysis and weighted average score analysis.

5. FINDINGS :

The findings of the study are segregated into four sections namely, nature of relationship of select variables with students' use of SNSs, determinants of usage of SNSs by college students, and the variables associated with their level of usage of social networking sites by the college students.

SECURITY ISSUES IN SOCIAL NETWORKING SITES

Security is protection from, or resilience against, potential harm (or other unwanted coercion) caused by others by restraining the freedom of others to act. Social media security is analyzing active social media data to safeguard against security and threats. Table 1.1 shows security issues in SNSs.

Table 1.1

Security Issues in Social Networking Sites

Variables	Student	Percentage
Accept Unknown Persons Friend Request		
Never	372	**44.30**
Rarely	174	20.70
Often	26	3.10
Sometimes	162	19.30
Always	106	12.60
Parents Aware		
No	186	22.10
Yes	654	**77.90**
Total	**840**	**100.0**

a) Accept Unknown Persons Friend Request

Of the 840 students, 372 (44.30%) students never accept an unknown person’s friend request, 174 (20.70%) students rarely, 26 (3.10%) students often, 162 (19.30%) students sometimes, and106 (12.60%) students are always.

Thus, most of the 372 (44.30%) students never accept an unknown person’s friend request.

b) Parents’ Awareness

Of the 840 students, 186 (22.10%) students’ parents are unaware of social networking activities, and 654 (77.90%) students are aware of social networking activities.

Thus, most 654 (77.90%) students’ parents know about social networking activities.

AWARENESS OF THE SECURITY ISSUES

Table 1.2 Awareness of the Security Issues

S.No.	Security Options	Awareness		Total
		Yes	No	
1	Security and Privacy Threats	695 (82.74%)	145 (17.26%)	840 (100.%)
2	Identity Theft Issues	528 (62.86%)	312 (37.14%)	840 (100.%)
3	Malware Issues	505 (60.12%)	335 (39.88%)	840 (100.%)
4	Spamming Attacks	472 (56.19%)	368 (43.81%)	840 (100.%)
5	Internet Fraud	542 (64.52%)	298 (35.48%)	840 (100.%)
6	Privacy Settings	662 (78.81%)	178 (21.19%)	840 (100.%)
7	Spam Detection	489 (58.21%)	351 (41.79%)	840 (100.%)
8	Phishing Detection	429 (51.07%)	411 (48.93%)	840 (100.%)
9	Botnet Attacks	394 (46.90%)	446 (53.10%)	840 (100.%)

The table above shows that out of the 840 students, 695 (82.74%) are aware of security and privacy threats. 662 (78.81%) students are aware of privacy settings. 542 (64.52%) students are aware of internet fraud.528 (62.86%) students are aware of identity theft issues. 505 (60.12%) students are aware of malware issues. 489 (58.21%) students are aware of spam detection. 472 (56.19%) students are aware of spamming attacks. 429 (51.07%) students are aware of phishing detection, and 394 (46.90%) are aware of botnet attacks.

Thus, the majority of 695 (82.74%) students are aware of the security and privacy threats, followed by privacy settings 662 (78.81%) and internet fraud 542 (64.52%).

PROBLEMS FACED BY STUDENTS WHILE USING SOCIAL NETWORKING SITES (WEIGHTED AVERAGE SCORE)

To find out the most prominent factor that leads to problems faced by students while using SNSs, weighted mean score analysis is applied by considering twelve variables, and the analysis findings are given in Table 1.3.

Table 1.3

Problems Faced by Students While Using Social Networking Sites (Weighted Average Rank)

Reason	Maximum Extent	Some Extent	Not at all	Weighted Average	Weighted Average Rank
Aware of the change in privacy settings	254 (30.24%)	340 (40.48%)	246 (29.29%)	1.01	1
Privacy of personal information	262 (31.19%)	282 (33.57%)	296 (35.24%)	0.96	2
I'm familiar with data protection and security while using the Internet	225 (26.79%)	327 (38.93%)	288 (34.29%)	0.93	3
Interruption in the study	209 (24.88%)	327 (38.93%)	304 (36.19%)	0.89	4
Faced any privacy and data security issues	207 (24.64%)	289 (34.40%)	344 (40.95%)	0.84	5
Fear of anonymous people online	183 (21.79%)	311 (37.02%)	346 (41.19%)	0.81	6
Internet addiction	168 (20.00%)	295 (35.12%)	377 (44.88%)	0.75	7
Secrecy of credentials while using it with mobile phone	158 (18.81%)	309 (36.79%)	373 (44.40%)	0.74	8
E-crime, e.g. identity theft, theft of valuable data, interruption of business, financial loss	143 (17.02%)	242 (28.81%)	455 (54.17%)	0.63	9
Bad impact on society	131 (15.60%)	260 (30.95%)	449 (53.45%)	0.62	10
Illegal activities	139 (16.55%)	205 (24.40%)	496 (59.05%)	0.58	11
Confidentiality of credit card number	107 (12.74%)	268 (31.90%)	465 (55.36%)	0.57	12

(i)Aware of the Change of Privacy Settings

Of the 840 students, 254 (30.24%) are at maximum extent faced 'aware of the change of privacy settings'. 340 (40.48%) students are to some extent, and the remaining 246 (29.29%) do not face the privacy settings change.

Thus, most of the students, are some extent, face the change of privacy settings, and it holds the first rank with the mean score value of 1.01.

(ii) Privacy of Personal Information

Of the 840 students, 262 (31.19%) are at maximum extent faced with 'privacy of personal information'. 282 (33.57%) students to some extent, and the remaining 296 (35.24%) are not at all face privacy of personal information.

Thus, most students are not at all faced with the privacy of personal information, and it holds the second rank with a mean score of 0.96.

(iii) Familiar with Data Protection and Securing While Using the Internet

Of the 840 students, 225 (26.79%) are, to a maximum extent, familiar with data protection and security while using the Internet. 327 (38.93%) students were to some extent, and the remaining 288 (34.29%) did not face data protection and security while using the Internet.

Thus, most students are somewhat familiar with data protection and security, and it holds the third rank with a mean score of 0.93.

(iv) Interruption in the Studies

Of the 840 students, 209 (24.88%) are maximum extent faced 'interruption in the study'. 327 (38.93%) students are to some extent, and the remaining 304 (36.19%) do not face interruption in the study.

Thus, most of the students, are some extent, faced interruption in the study, and it holds the fourth rank with the mean score value of 0.89.

(v) Privacy and Data Security Issues

Of the 840 students, 207 (24.64%),to are maximum extent, faced any privacy and data security issues while using SNSs. 289 (34.40%) students are to some extent, and the remaining 344 (40.95%) do not face any privacy and data security issues.

Thus, most students do not face any privacy and data security issues, and it holds the fifth rank with a mean score of 0.84.

(vi) Fear of Anonymous People in Online

Of the 840 students, 183 (21.79%) are maximum extent faced 'Fear of anonymous people online' while using SNSs. 311 (37.02%) students to some extent, and the remaining 346 (41.19%) do not fear anonymous people online.

Thus, most of the students are not at all fear of anonymous people online, and it holds the sixth rank with a mean score value of 0.81.

(vii) Internet Addiction

Of the 840 students, 168 (20.00%) are, to the maximum extent, faced with 'internet addiction'. 295 (35.12%) students are, to some extent, and the remaining 377 (44.88%) are not at all faced with internet addiction.

Thus, most students do not at all face internet addiction, and it holds the seventh rank with a mean score value of 0.75.

(viii) Secrecy of Credentials While using it with Mobile Phone

Of the 840 students, 158 (18.81%) are maximum extent faced 'secrecy of credentials while using it with mobile phone'. 309 (36.79%) students are to some extent, and the remaining 373 (44.40%) do not face secrecy of credentials while using it with a mobile phone.

Thus, most students are not at all faced with the secrecy of credentials, and it holds the eighth rank with a mean score of 0.74.

(ix) E-Crime

Of the 840 students, 143 (17.02%) are maximum extent faced 'E-crime' while using SNSs. 242 (28.81%)students are some extent, and the remaining 455 (54.17%) not at all faced E-crime.

Thus, most students do not face E-crime issues, and it holds the ninth rank with a mean score of 0.63.

(x) Bad Impact on Society

Of the 840 students, 131 (15.60%), are maximum extent, faced a 'bad impact on society'. 260 (30.95%) students to some extent, and the remaining 449 (53.45%) do not negatively impact society.

Thus, most students do not negatively impact society; it holds the tenth rank with a mean score of 0.62.

(xi) Illegal Activities

Of the 840 students, 139 (16.55%) are maximum extent faced 'Illegal activities'.205 (24.40%) students are some extent, and the remaining 496 (59.05%) are not involved in illegal activities.

Thus, most students have not faced illegal activities, and it holds the eleventh rank with a mean score of 0.58.

(xii) Confidentiality of Credit Card Number

Of the 840 students, 107 (12.74%) are maximum extent faced 'Confidentiality of credit card number' while using SNSs. 268 (31.90%) students to some extent, and the remaining 465 (55.36%) not at all faced confidentiality of credit card numbers.

Thus, most students are not at all faced with the confidentiality of credit card numbers, and it holds twelve ranks with a mean score of 0.57.

The analysis infers that a large part of the students, is some extent, face the problems like privacy and data security issues, the confidentiality of credit card numbers, fear of anonymous people online, e-crime, e.g. identity theft, theft of valuable data, interruption of business, financial loss, the secrecy of credentials while using it with a mobile phone, I'm familiar with data protection and secure while using the Internet, the privacy of personal information, aware of the change of privacy settings, interruption in the study, internet addiction, bad impact on society, and illegal activities.

8. CONCLUSION:

The study highlights the varying levels of awareness among students regarding the security concerns associated with social networking sites. The analysis indicates that most students are aware of security and privacy threats, including privacy settings, internet fraud, identity theft, malware, spam detection, spamming attacks, phishing detection, and botnet attacks. The Weighted Mean Score reveals that a significant proportion of students have experienced problems such as changes to their privacy settings (ranked first with a mean score of 1.01), followed by concerns over the privacy of personal information (ranked second with a mean score of 0.96) and data protection and security (ranked third with a mean score of 0.93). The confidentiality of credit card numbers was ranked twelfth, with a mean score of 0.57. By fostering a culture of digital responsibility and proactive security measures, students can better protect their personal information and mitigate potential cyber threats.

REFERENCES:

1. Zeebaree, S., Ameen, S., &Sadeeq, M. (2020). Social media networks security threats, risks, and recommendation: A case study in the Kurdistan region. International Journal of Innovation, Creativity, and Change, 13, 349-365.
2. Jain, A. K., Sahoo, S. R., &Kaubiyal, J. (2021). Online social networks security, andprivacy: a comprehensive review, and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.
3. Martin, S., & Martin, M. (2023). Privacy concerns and awareness among college students using social media. Journal of Cybersecurity Education, 12(1), 45-60.
4. Anderson, D. L., & Williams, R. (2022). Cyber security and social media: Understanding the security practices of college students. International Journal of Cyber security, 9(4), 72-85.
5. Schmidt, C., & Zhang, J. (2021). Social media literacy and its role in enhancing security awareness among students. Journal of Digital Media Literacy, 8(3), 111-125.
6. Gupta, P., &Verma, R. (2023). Student awareness of data privacy risks on social networking sites. Journal of Information Security Education, 6(2), 61-75.
7. Lee, J., & Kim, H. (2024). Exploring social media security and the role of trust in student behavior. Cybersecurity and Privacy Journal, 14(1), 33-47.
8. Acquisti, A., John, L. K., &Loewenstein, G. (2015). What Is Privacy Worth?. Journal of Legal Studies, 42(2), 243-274.
9. Besmer, A., & Richter, S. (2014). Privacy Settings and Social Network Sites: A Longitudinal Study of Facebook Users. Computers in Human Behavior, 35, 158-167.

10. Boyd, D. (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press.
11. Florencio, D., &Herley, C. (2010). A Large-Scale Study of Web Password Habits. Proceedings of the 16th ACM Conference on Computer and Communications Security, 1-10.
12. Gbadeyan, B. T., and Delicеırmak, F. D. (2022). Analysis of social networking sites: a study on effective communication strategy in developing brand communication, SSRG International Journal of Humanities and Social Science, 9(1), 31-37.
13. Jagatic, T. N., Johnson, N. A., Jakobsson, M., &Menczer, F. (2007). Social Phishing. Communications of the ACM, 50(10), 94-100.
14. Kaviarasu, J., Mary, J & Dinesh, J. (2019). Impact of social media on the academic performance of undergraduate college students of Loyola College, Chennai City, International Journal of Innovative Studies in Sociology and Humanities,4(2).
15. Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2012). A Nutrition Label for Privacy. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1-12.
16. Koohang, A., Floyd, K., Yerby, J., &Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, 22(2), 133-145.
17. Mattioli, R., Kim, S. H., & Tedesco, J. (2019). User Attitudes and BehaviorTowards Social Media Security Features: A Student-Centric Study. International Journal of Human-Computer Studies, 124, 87-97.
18. Nawalagatti, A. (2022). Analysis of Security and Privacy Issues in Social Networks, International Journal of Creative Research Thoughts (IJCRT),10(3).
19. Patel, H., Green, P., & Kumar, A. (2014). Phishing Awareness Among College Students: A Study of Social Networking Sites. Journal of Computer Security, 22(3), 207-223.
20. Rawath, S. S., Satheeshkumar, D. R., & Kumar, V. (2019). A Study on Impact of Social Media on Youth. Journal of Management (JOM), 6(1), 89-96.
21. Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society, 28(1), 20–36.
22. Oorschot, P. C., &Stubblebine, S. P. (2016). On the Security of Two-Factor Authentication and Related Protocols. IEEE Transactions on Dependable and Secure Computing, 13(4), 456-467.

Acknowledgement

This article has been published using the **Seed Money** granted by the **Management of Nallamuthu Gounder Mahalingam College (Autonomous), Pollachi**.