

A Study of Cybersecurity Awareness among University Students in the Age of Social Media

Harsha Mohan¹, Dr. R. Hemanth Babu²

¹Department of Psychology, Jain (Deemed-to-be) University, Bengaluru, Karnataka, India

Email: harshaachoo[at]gmail.com

²Supervisor, Assistant Professor, Faculty of Management, Jain (Deemed-to-be) University, Bengaluru, Karnataka, India

Email: hemanthbabu.r[at]jainuniversity.ac.in

Abstract: *This study examined cybersecurity awareness among university students in the context of rapidly increasing social media usage. Social media platforms have become integral to students' academic, social, and personal lives, offering opportunities for communication and learning while simultaneously exposing users to risks such as hacking, phishing, cyberbullying, and identity theft. Using a descriptive research design, the study employed convenience sampling with a final sample of 102 college students aged 18–29 in Kannur City. Data were collected through a self-structured online questionnaire assessing social media usage patterns, awareness of security measures, exposure to cyber risks, and perceived academic and health impact. Overall, respondents were more security-aware than the literature review anticipated: 64.7% reported understanding privacy settings and 81.4% correctly identified a phishing scenario. However, 25.5% had experienced an adverse cyber event, and among respondents who had faced online harassment, more than half did not report it. Statistical testing found no significant relationship between usage level and security awareness ($p = 0.749$) or between usage level and academic grades ($p = 0.874$). A significant relationship was found between age at first profile creation and phishing identification ($p = 0.015$), with earlier joiners showing higher accuracy. The study concludes that usage alone does not guarantee protective behaviour and recommends integrating digital safety education into academic curricula, supported by targeted awareness campaigns and clearer reporting channels.*

Keywords: Social media usage, cybersecurity awareness, college students, privacy settings, phishing, digital safety education

1. Introduction

Social media has become an integral part of everyday communication, learning, information access, and social connection. Over the past two decades, the rapid growth of smartphones and internet access has accelerated social-media use, particularly among young adults and students. Although social media supports socialising, self-expression, communication, and learning, it also creates exposure to hacking, phishing, identity theft, cyberbullying, online scams, and related psychological and physical concerns.

As technology increasingly shapes how information is accessed and shared, security literacy has become an important component of responsible digital participation. Protective practices include the use of complex and unique passwords, two-factor authentication, appropriate privacy settings, and caution with suspicious links. College students aged 18–29 are a particularly relevant group because they are frequent digital users while moving through a period of increasing independence.

The central issue addressed by the present study is the potential disconnect between high-frequency social-media use and actual knowledge of security protocols. The study therefore examines usage patterns, cybersecurity awareness, exposure to cyber risks, perceived academic and health effects, and the relationships among these variables.

2. Literature Review

2.1 Effects on Academic Performance

Research reviewed in the dissertation consistently identifies a relationship between high social-media consumption and academic outcomes. Uddin et al. (2022) reported substantial

daily networking-site use and a negative effect on overall performance. Owusu-Acheaw et al. (2015), based on 1,508 respondents, identified a link between social-platform use through cell phones and reduced academic success. Talaue et al. (2018) similarly noted that social-media applications can be beneficial but may also have detrimental effects on students' studies.

2.2 Cybersecurity Awareness

The reviewed literature highlights the need for formal education in digital safety. Nawalagatti (2022) emphasised training in complex passwords, authorised Wi-Fi, and updated antivirus software. Rajan (2013) reported that while most students used social media daily, a proportion had already experienced account compromise.

2.3 Privacy Concerns

Haneefa and Sumitha (2011) found that students identified privacy and security as important concerns while many continued to use real identities and photographs on social-network profiles. Borgohain and Gohain (2020) highlighted the challenges and opportunities created by smart devices as academic and private life increasingly intersect online.

2.4 Online Behaviour Risks

Stefanescu et al. (2018) identified chatting frequency and the type of personal information shared as predictors of risky internet behaviour. Umar and Idris (2018) concluded that social-media use can negatively affect not only grades but also psychosocial behaviour.

2.5 Summary and Positioning of the Present Study

Taken together, the literature establishes three themes: heavy social-media use is frequently linked to reduced academic performance; students may lack formal cybersecurity education despite daily exposure to digital risks; and stated privacy concerns do not always translate into protective behaviour. The present study builds on these themes by empirically testing relationships within a defined sample of college students in Kannur City.

3. Problem Definition

Despite the recognised benefits of social media, college students may remain vulnerable to hacking, phishing, unauthorised access, scams, cyberstalking, and online harassment. The study addresses the gap between usage patterns and security literacy by examining whether frequent use is associated with awareness and academic outcomes and whether age at first profile creation is related to phishing-identification ability.

Objectives of the Study

The study was guided by the following objectives: (1) To examine social-media usage patterns among college students, including platforms used, time spent, and habits of use. (2) To assess awareness of social-media security measures and identify common risks or security lapses. (3) To examine the relationship between social-media usage, security awareness, academic performance, and perceived physical and mental well-being.

Hypothesis

H1: There is no significant difference in security awareness between high and low social-media users. H2: There is no significant correlation between the frequency of social-media usage and the academic grades of students. H3: There is no significant relationship between the age at which a social-media profile was created and the user's current ability to identify online exploitation.

4. Methodology

4.1 Research Design

A descriptive research design was adopted to describe current social-media usage patterns and security awareness and to test hypothesised relationships between usage, awareness, and outcomes.

4.2 Sampling Method and Sample Size

Non-probability convenience sampling was used to recruit college students aged 18–29 residing in Kannur City. A final sample of 102 valid responses was obtained.

4.3 Research Instrument

A self-made 16-item online questionnaire was used. It covered demographic information; usage patterns; cybersecurity awareness; risky online behaviour and

experiences; perceived academic and health impact; and opinions regarding digital-safety education. The cybersecurity section included a privacy-setting awareness item and a multiple-choice phishing knowledge check.

4.4 Data Collection Procedure

The questionnaire was deployed through Google Forms and distributed via WhatsApp and college groups. Respondents participated voluntarily and anonymously, and collection continued until 102 responses were obtained.

4.5 Ethical Considerations

Participation was voluntary and anonymous. The data were used for research purposes and identifying information was not collected. Data-cleaning decisions were documented before analysis.

4.6 Statistical Analysis

Frequencies, percentages, and means were used for descriptive summaries. Chi-square tests of independence were used to test the three hypotheses, supplemented by Spearman's rank correlation because several variables were ordinal. Analysis was conducted using Python with pandas and scipy.

5. Results and Discussion

1) Demographic characteristics of the sample (N=102)

Demographic Variable	Category	N	Percentage
Gender	Female	55	53.9
Gender	Male	47	46.1
Age	27–29	59	57.8
Age	21–23	9	8.8
Age	24–26	9	8.8
Age	18–20	7	6.9
Age	Not stated	18	17.6
Study level	Postgraduate	42	41.2
Study level	3rd Year	25	24.5
Study level	Other/Professional	21	20.6
Study level	2nd Year	10	9.8
Study level	1st Year	4	3.9

Table 1: Demographic profile of the research sample (N=102).

The sample consisted of 55 females (53.9%) and 47 males (46.1%). The largest age group was 27–29 years (57.8%). Postgraduate students formed the largest study-level group (41.2%), followed by third-year students (24.5%) and other/professional courses (20.6%).

2) Social Media Usage Patterns

WhatsApp (89.2%), Instagram (83.3%), and YouTube (75.5%) were the most-used platforms, followed by Facebook (47.1%) and Snapchat (6.9%).

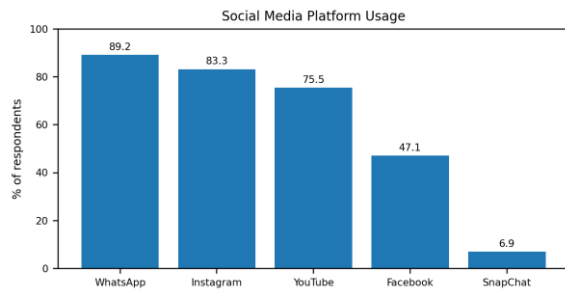


Figure 1: Percentage of respondents using each social-media platform.

Half of the sample (50.0%) spent 1–3 hours per day on social media, while 33.3% spent 3–5 hours and 6.9% spent more than five hours.

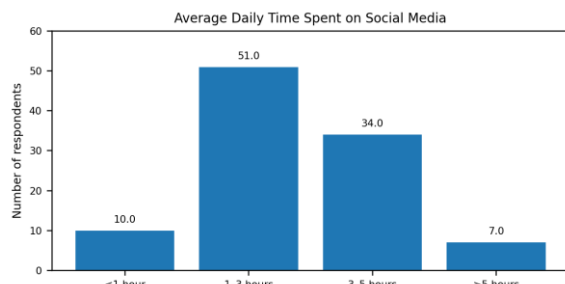


Figure 2: Average daily time spent on social media.

3) Cybersecurity Awareness

Among 98 valid responses, 52.9% agreed and 11.8% strongly agreed that they knew how to use privacy settings, giving 64.7% positive responses. A further 27.5% were neutral and 4.0% disagreed or strongly disagreed.

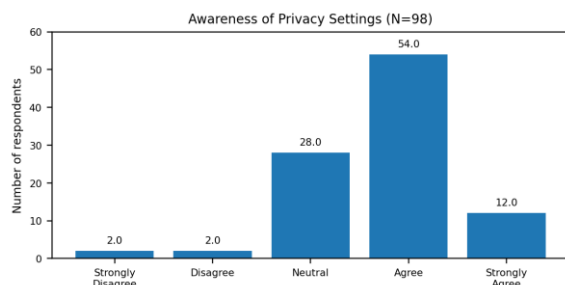


Figure 3: Self-reported awareness of privacy settings (N=98).

In the phishing knowledge check, 81.4% correctly identified the definition of phishing, while 18.6% selected incorrect options.

4) Risky Online Behaviour and Experiences

A total of 25.5% of respondents reported at least one adverse cybersecurity experience. Specifically, 16.7% had received a message or email requesting personal data or a password, 5.9% had an account hacked or compromised, and 2.0% had shared a password with someone else. Nine respondents (8.8%) reported cyberbullying or online harassment; among these, 55.6% did not report the incident.

5) Academic and Health Impact

Agreement was highest for the statement that social media reduces study time (57.8%), followed by sleep disruption or physical discomfort (48.0%) and anxiety when unable to access social media (22.5%).

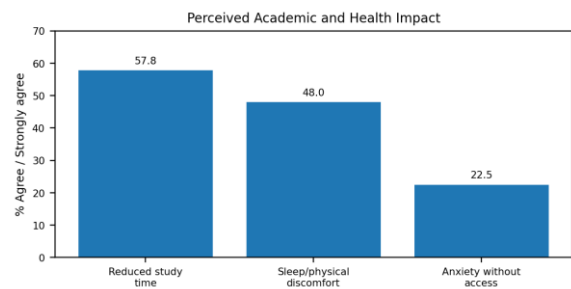


Figure 4: Percentage agreeing with academic and health impact statements.

6) Support for Digital Safety Education

Support for integrating digital-safety education into the school or college curriculum was very high: 94.1% agreed, 3.9% were unsure, and 2.0% disagreed.

7) Hypothesis Testing

For H1, no significant association was found between usage level and self-reported privacy-setting awareness ($\chi^2=8.453$, $df=12$, $N=98$, $p=0.749$); Spearman's rho was -0.065 ($p=0.525$). H1 was therefore not rejected.

For H2, no significant relationship was found between daily usage time and grade bracket ($\chi^2=4.518$, $df=9$, $N=93$, $p=0.874$); Spearman's rho was 0.096 ($p=0.361$). H2 was not rejected.

For H3, a statistically significant relationship was found between age at first profile creation and phishing-identification ability ($\chi^2=10.502$, $df=3$, $N=102$, $p=0.015$); Spearman's rho was -0.260 ($p=0.008$). H3 was rejected. Phishing identification was highest among those who joined before age 13 (100%) and at 16–18 (96.6%), and lowest among those who joined after age 18 (68.8%).

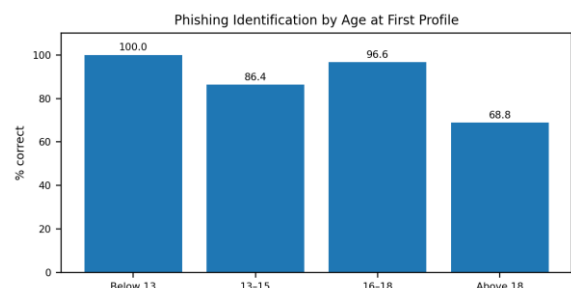


Figure 5: Phishing-identification accuracy by age at first profile creation.

6. Conclusion

This study examined social-media usage and cybersecurity awareness among college students in Kannur City. Respondents showed comparatively strong reported

awareness of privacy settings and a high ability to identify phishing, yet meaningful vulnerabilities remained: 25.5% had experienced an adverse cyber event and more than half of those reporting online harassment did not report the incident.

Usage level was not significantly related to security awareness or academic grades, whereas age at first profile creation was significantly related to phishing-identification accuracy. The findings suggest that usage alone does not determine cybersecurity awareness or academic outcomes. Instead, structured digital-safety education, targeted awareness campaigns, clear reporting mechanisms, and healthy social-media practices may help bridge the gap between awareness and protective action.

7.Future Scope

Future research should include larger and more demographically balanced samples, particularly younger traditional-age undergraduates, to improve generalisability. Further studies should restore the full five-item cybersecurity-awareness battery originally planned for the questionnaire and examine protective behaviours more directly. Longitudinal research could also determine whether digital-safety education produces sustained improvements in awareness, reporting behaviour, and safe online practices.

References

- [1] Uddin, M. K. et al. (2022). American Economic and Social Review.
- [2] Owusu-Acheaw, M. (2015). Social media usage and its impact on the academic performance of tertiary institution students.
- [3] Lenka, A. & Mishra, S. (2022). International Journal of Creative Research Thought (IJCRT).
- [4] Nawalagatti, A. V. (2022). International Journal Creative Research (IJCRT).
- [5] Alshwiah, A. & Alaulamie, L. (2022). Journal of Applied Research in Higher Education.
- [6] Borgohain, M. & Gohain, A. B. (2020). European Journal of Molecular & Clinical Medicine.
- [7] Haneefa, K. M., & Sumitha, E. (2011). Perception and Use of Social Networking Sites by the Students of Calicut University. DESIDOC Journal of Library & Information Technology, 31(4), 295–301.
- [8] Hunter, G. L. & Taylor, S. A. (2019). Journal of Consumer Marketing.
- [9] Mowafy, G. (2018). AUC Knowledge Fountain.
- [10] Talaue, G. M. et al. (2018). International Journal of Advanced Information Technology (IJAIT).
- [11] Oueder, M. & Abousaber, I. (2018). American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS).
- [12] Rajan, P. (2013). Study on social media usage and account security among college students.
- [13] Stefanescu, C. et al. (2018). Predictors of risky internet behaviour among adolescents.
- [14] Umar, T. I. & Idris, M. (2018). Social media usage and psychosocial behaviour among secondary school students.

Author Profile

Harsha Mohan is pursuing an MSc in Psychology at Jain (Deemed-to-be) University, Bengaluru. The present manuscript is based on the dissertation study examining cybersecurity awareness, social-media usage, cyber-risk experiences, and digital-safety education among college students.