IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

Role of Social Media Platforms like Instagram, Facebook, and WhatsApp in Increasing Cyber Security Risks among College Students.

Dr. Parag Vasantrao Pimplapure
Associate Professor and HoD, Department of Commerce
Doshi Vakil Arts College and G.C.U.B. Science & Commerce College, Goregaon-Raigad.

Abstract: *Social media platforms such as Instagram, Facebook, and WhatsApp have become an important part of daily life for college students. These platforms allow users to communicate, share information, and stay connected with friends and family. However, the increasing use of social networking applications has also increased the risk of cyber security threats. Many students share personal information, photos, and opinions online without fully understanding the possible risks. This can make them vulnerable to cyber attacks such as phishing, hacking, identity theft, cyberbullying, and online scams.*

The main purpose of this study is to analyze how the use of Instagram, Facebook, and WhatsApp influences cyber security risks among college students. The research also aims to identify the most common types of cyber threats faced by students on these platforms and evaluate their level of cyber security awareness. In addition, the study examines how online behavior and privacy settings affect students' vulnerability to cyber attacks.

The study uses a questionnaire survey to collect data from college students who actively use social networking applications. Based on the findings, the research suggests preventive measures such as increasing cyber security awareness, improving digital literacy, and encouraging safe online practices to reduce cyber security risks among college students.

Keywords: Social Media Usage, Cyber Security Risks, College Students, Cyber Security Awareness

1. Introduction

In today's digital world, social media has become an important part of everyday life. Platforms such as Instagram, Facebook, and WhatsApp are widely used by people of all age groups, especially college students. These applications allow users to communicate instantly, share photos and videos, exchange ideas, and stay connected with friends and family. Many students also use social media for educational purposes, such as sharing study materials, discussing assignments, and participating in online groups.

The popularity of social networking applications has increased rapidly over the past few years due to the availability of smartphones and internet access. Social media platforms provide many benefits, including easy communication, quick access to information, and opportunities for social interaction. However, along with these benefits, the use of social media has also created several cyber security challenges.

Cyber security refers to the protection of digital information and online systems from unauthorized access, attacks, or damage. As more people use social media platforms, the risk of cyber threats has also increased. College students are among the most active users of social networking applications, which makes them more exposed to cyber risks. Many students share personal information, photos, location details, and opinions on social media without being fully aware of the possible dangers.

DOI: 10.48175/IJARSCT-33147

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, April 2026 Impact Factor: 8.2

There are many types of cyber threats that can occur on social media platforms. Some of the most common threats include phishing attacks, hacking, identity theft, cyberbullying, and online scams. Phishing attacks are attempts by cybercriminals to trick users into revealing sensitive information such as passwords or bank details. Cyberbullying involves using digital platforms to harass or threaten others. Identity theft occurs when someone uses another person's personal information for fraudulent activities. These threats can affect students' privacy, security, and mental well-being.

Another important issue is the lack of cyber security awareness among many social media users. Some students may not know how to use privacy settings properly or how to recognize suspicious links and messages. Weak passwords, accepting friend requests from unknown people, and sharing too much personal information online can increase the risk of cyber attacks. Therefore, it is important for students to understand safe online practices and take steps to protect their digital identity.

This research focuses on studying the relationship between social media usage and cyber security risks among college students. The study analyses how the use of Instagram, Facebook, and WhatsApp influences students' exposure to cyber threats. It also aims to identify the most common types of cyber security risks faced by students and evaluate their level of awareness regarding cyber security practices.

Furthermore, the research examines how online behaviour and privacy settings affect students' vulnerability to cyber-attacks. Based on the findings, the study suggests effective preventive measures that can help reduce cyber security risks associated with social media usage. The results of this research may help students, educators, and institutions understand the importance of cyber security awareness and encourage safer use of social networking platforms.

Objectives

- To analyze how the usage of Instagram, Facebook, and WhatsApp influences cyber security risks among college students.
- To identify the most common types of cyber threats faced by college students on social media platforms.
- To evaluate the level of cyber security awareness among college students while using social networking applications.
- To examine the impact of online behavior and privacy settings on students' vulnerability to cyber attacks.
- To recommend effective preventive measures to minimize cyber security risks associated with social media usage among college students.

Hypothesis

H_0: There is no significant relationship between the usage of social media platforms and cyber security risks among college students.

H_1: There is a significant relationship between the usage of social media platforms and cyber security risks among college students.

H_2: College students frequently experience various cyber threats such as phishing, hacking, cyberbullying, and identity theft while using social media platforms.

H_3: The level of cyber security awareness among college students significantly affects their ability to protect themselves from cyber threats on social networking applications.

H_4: Online behaviour of college students, such as sharing personal information and interacting with unknown users, significantly increases their vulnerability to cyber-attacks.

H_5: Privacy settings and security practices on social media platforms significantly influence the level of cyber security risk faced by college students.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

20 Research Methodology

This study adopts a descriptive research design to examine the influence of social media usage on cyber security risks among college students.

Both primary and secondary data are used in the study. Primary data is collected through share a Google form link to college students. Secondary data is gathered from academic journals, research articles, books, and credible online sources related to cyber security and social media usage.

A sample of 86 college students is selected using the convenience sampling technique. The collected data is analyzed using percentage analysis and simple statistical tools, and the results are presented through tables.

Statistical Analysis

Table 1: Social Media Platforms Used by Students

Platform Used	Frequency	Percentage
WhatsApp	41	47.67%
Instagram & WhatsApp	26	30.23%
Instagram	14	16.28%
Instagram, Facebook & WhatsApp	4	4.65%
Facebook & WhatsApp	1	1.16%
Total	**86**	**100%**

Table 2: Time Spent on Social Media

Time Spent Per Day	Frequency	Percentage
1–3 hours	52	60.47%
Less than 1 hour	27	31.40%
3–5 hours	5	5.81%
More than 5 hours	2	2.33%
Total	**86**	**100%**

The data shows that WhatsApp (47.67%) is the most frequently used social media platform, followed by Instagram and WhatsApp combined (30.23%). Facebook usage is relatively low among college students.

Additionally, 60.47% of students spend 1–3 hours daily on social media, indicating high engagement with these platforms.

The high usage rate and extended time spent online increase students' exposure to potential cyber security threats, particularly on interactive platforms like Instagram and WhatsApp.

Table 3: Experience of Cyber Threats

Response	Frequency	Percentage
No	58	67.44%
Yes	14	16.28%
Not Sure	14	16.28%
Total	**86**	**100%**

Table 4: Types of Cyber Threats Experienced

Type of Threat	Frequency	Percentage
Fake profile / Impersonation	5	5.81%
Hacking	5	5.81%
Online fraud/scam	2	2.33%
Phishing	2	2.33%
Multiple threats	4	4.66%

DOI: 10.48175/IJARSCT-33147

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

Table 5: Platform Where Threat Occurred

Platform	Frequency	Percentage
Instagram	16	18.60%
WhatsApp	11	12.79%
Facebook	2	2.33%
Other	6	6.98%
Not Applicable	51	59.30%

Although the majority of students (67.44%) reported not experiencing cyber threats, 16.28% confirmed experiencing cyber attacks, while another 16.28% were unsure. Among the threats reported: Fake profiles and impersonation, Hacking, Online scams, Phishing attacks Instagram recorded the highest number of cyber threat incidents (18.60%), followed by WhatsApp (12.79%). This suggests that visually interactive platforms with large public networks may present higher cyber security risks.

Table 6: Cyber Security Awareness Level

Awareness Level	Frequency	Percentage
Moderately aware	24	27.91%
Highly aware	21	24.42%
Not aware	21	24.42%
Slightly aware	20	23.26%
Total	**86**	**100%**

Table 7: Awareness of Two-Factor Authentication (2FA)

Response	Frequency	Percentage
No	40	46.51%
Yes and use it	27	31.40%
Yes but don't use it	11	12.79%
Heard but don’t understand	8	9.30%

Table 8: Participation in Cyber Security Awareness Programs

Response	Frequency	Percentage
No	62	72.09%
Yes	24	27.91%

The findings show that cyber security awareness among students is moderate but inconsistent.

Nearly 48% of respondents reported either low awareness or no awareness of cyber security risks. Additionally, 46.51% of students are not aware of two-factor authentication, an important security feature.

Furthermore, 72.09% of students have never attended a cyber security awareness program, which explains the moderate awareness levels.

Table 9: Privacy Settings of Social Media Accounts

Privacy Setting	Frequency	Percentage
Completely private	54	62.79%
Public	17	19.77%
Partially private	10	11.63%
Not sure	5	5.81%

Table 10: Accepting Requests from Unknown People

Response	Frequency	Percentage
Never	56	65.12%
Rarely	17	19.77%
Sometimes	10	11.63%
Always	3	3.49%

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

Table 11: Sharing Personal Information on Social Media

Response	Frequency	Percentage
Never	77	89.53%
Rarely	6	6.98%
Occasionally	2	2.33%
Frequently	1	1.16%

Table 12: Clicking Unknown Links

Response	Frequency	Percentage
Never	65	75.58%
Rarely	9	10.47%
Sometimes	8	9.30%
Yes	4	4.65%

Most students demonstrate relatively safe online behavior. 62.79% maintain completely private social media accounts, which helps reduce exposure to cyber threats.

Similarly, 65.12% never accept friend requests from unknown individuals, and 89.53% never share personal information publicly.

However, some risky behaviors remain: 18.60% rarely or never update passwords, 24.42% occasionally click unknown links, Some students accept unknown requests

These behaviors increase vulnerability to cyber attacks such as phishing and account hacking.

Table 13: Most Effective Preventive Measures

Preventive Measure	Frequency	Percentage
Strong passwords	29	33.72%
Cyber security education	21	24.42%
Regular privacy checks	17	19.77%
Two-factor authentication	14	16.28%
Limit personal information sharing	5	5.81%

Table 14: Support for Cyber Security Training Programs

Response	Frequency	Percentage
Agree	45	52.33%
Strongly Agree	23	26.74%
Neutral	16	18.60%
Disagree	1	1.16%
Strongly Disagree	1	1.16%

The analysis indicates that strong passwords (33.72%) and cyber security education (24.42%) are perceived as the most effective preventive measures.

Additionally, 79.07% of respondents either agree or strongly agree that cyber security training programs should be introduced in colleges. This highlights the strong need for institutional awareness initiatives.

Hypothesis Mapping (Source : Data Collected through Google form**)**

1. Usage of social media and Risk (H_0 & H_1)

Result: The analysis shows no significant relationship between the number of hours spent on social media and the likelihood of experiencing a cyber threat (p = 0.4282$).

Conclusion: Increasing the time spent on social media does not automatically translate to a higher risk of cyber threats in this specific group of college students.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

2. Prevalence of Cyber Threats (H_2)

Findings: Among the students who reported experiencing threats, the most common types were:

Hacking: 10 cases

Fake profiles/Impersonation: 9 cases

Online fraud/scam: 5 cases

Phishing: 2 cases

Conclusion: H_2 is Supported. Students frequently encounter a variety of threats while using social networking platforms.

3. Awareness and Ability to Protect (H_3)

Findings: While awareness level did not show a direct impact on whether a student *experienced* a threat ($p = 0.5986$), it had a highly significant impact on their security behavior:

Awareness vs. Password updates: $p = 0.0000$

Awareness vs. Two-Factor Authentication (2FA) usage: $p = 0.0025$

Conclusion: H_3 is Supported. Students with higher awareness are significantly more likely to adopt protective measures.

4. Online Behavior and Vulnerability (H_4)

Findings: Specific online behaviors were strongly linked to cyber security incidents:

Accepting unknown requests: Showed a very significant relationship with experiencing threats ($p = 0.0020$).

Clicking unknown links: Also showed a significant relationship ($p = 0.0279$).

Conclusion: H_4 is Supported. Risky behaviors like interacting with strangers and clicking suspicious links significantly increase a student's vulnerability.

5. Privacy Settings and Security Practices (H_5)

Findings: Interestingly, the analysis did not find a significant statistical difference in threat experience between students with "Private" vs "Public" accounts ($p = 0.8044$) or those who update passwords vs those who don't ($p = 0.2177$).

Conclusion: H_5 is Not Supported in this dataset. This suggests that even with privacy settings, other factors (like behavior or sophisticated attacks) may still lead to cyber risks.

3. Conclusion

This research study aimed to analyze the cyber security risks associated with the use of social networking platforms among college students, specifically focusing on Instagram, Facebook, and WhatsApp.

The study also examined the types of cyber threats faced by students, evaluated their level of cyber security awareness, assessed the impact of online behavior and privacy settings on vulnerability to cyber-attacks, and suggested preventive measures to reduce cyber security risks.

The findings of the study reveal that social media platforms have become an integral part of students' daily lives. Among the respondents, WhatsApp and Instagram emerged as the most frequently used platforms, while Facebook usage was relatively low.

A majority of the students reported spending one to three hours daily on social media applications, indicating a high level of engagement with digital communication platforms. Such frequent use increases the likelihood of exposure to cyber threats.

The study identified several types of cyber threats experienced by students, including fake profiles, hacking, phishing attacks, and online scams. Among these, fake profiles and hacking incidents were the most common threats reported by respondents. The analysis also indicated that Instagram was the platform where the highest number of cyber threats occurred, followed by WhatsApp. These findings highlight the potential risks associated with highly interactive social media environments where users frequently communicate with unknown individuals.

In terms of cyber security awareness, the results suggest that the level of awareness among college students is moderate. While some students demonstrated a good understanding of basic cyber safety practices, many respondents

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, April 2026 Impact Factor: 8.2

lacked knowledge of advanced security features such as two-factor authentication (2FA). A large proportion of students were either unaware of this security feature or did not actively use it, which increases the risk of unauthorized access to social media accounts.

The research also examined the influence of online behavior and privacy settings on students' vulnerability to cyber attacks. The results indicate that many students maintain private accounts and avoid sharing personal information publicly, which reflects a certain level of caution and awareness regarding online safety. Additionally, most respondents reported that they rarely accept friend requests from unknown individuals and generally avoid clicking suspicious links.

However, some risky behaviors were also observed among a small group of respondents. These include infrequent password updates, occasional acceptance of unknown friend requests, and limited understanding of cyber security tools. Such behaviors can increase vulnerability to cyber attacks such as phishing, identity theft, and account hacking.

Another important finding of the study is that a large majority of students have not attended any cyber security awareness programs or training sessions. Despite this, most respondents strongly support the introduction of cyber security education in colleges and universities. Students also identified strong passwords, cyber security education, privacy management, and two-factor authentication as the most effective preventive measures to protect their online accounts.

Overall, the findings of this study highlight that while students have some awareness of online safety practices, there remains a significant need for structured cyber security education and awareness initiatives. Improving students' knowledge about cyber threats and promoting responsible online behavior can significantly reduce the risks associated with social media usage.

4. Recommendations

Based on the findings of the study, the following recommendations are proposed to enhance cyber security awareness and reduce cyber risks among college students:

1. Cyber Security Awareness Programs - Educational institutions should organize regular workshops, seminars, and awareness campaigns to educate students about cyber threats such as phishing, hacking, identity theft, and online scams.

2. Integration of Cyber Security in Academic Curriculum - Basic cyber security concepts should be included in the academic curriculum so that students gain formal knowledge about digital safety and secure online practices.

3. Encouraging the Use of Strong Passwords - Students should be encouraged to create strong and unique passwords for their social media accounts and update them periodically to prevent unauthorized access.

4. Promotion of Two-Factor Authentication (2FA) - Students should be informed about the importance of two-factor authentication and encouraged to activate this feature on their social media accounts to improve security.

5. Regular Review of Privacy Settings - Students should regularly check and update their social media privacy settings to ensure that personal information is visible only to trusted individuals.

6. Avoiding Unknown Links and Suspicious Messages - Students should be cautious about clicking on unknown links or downloading files from unfamiliar sources, as these may contain malware or phishing attempts.

7. Responsible Social Media Behavior - Students should avoid accepting friend requests from unknown individuals and should limit the sharing of sensitive personal information online.

8. Institutional Cyber Safety Policies - Colleges and universities should develop clear cyber safety policies and guidelines to promote responsible internet use among students.

9. Collaboration with Cyber Security Experts - Educational institutions should collaborate with cyber security professionals and organizations to conduct training sessions and awareness campaigns.

10. Establishment of Reporting Mechanisms - Institutions should establish support systems or help desks where students can report cyber incidents and receive guidance on protecting their digital accounts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, April 2026
Impact Factor: 8.2

Implementing these recommendations will help strengthen cyber security awareness among students and reduce the risks associated with social media usage.

BIBLIOGRAPHY

[1]. Godbole, N., & Belapure, S. (2011). *Cyber security: Understanding cyber crimes, computer forensics and legal perspectives*. Wiley India Pvt. Ltd.
[2]. Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI Global.
[3]. Sood, A. K., & Enbody, R. (2013). *Targeted cyber attacks: A superset of advanced persistent threats*. Syngress.
[4]. Chander, H., & Mehta, D. (2019). *Cyber laws and information technology*. PHI Learning Pvt. Ltd.
[5]. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.
[6]. Indian Computer Emergency Response Team. (2023). *Cyber security awareness and best practices*. https://www.cert-in.org.in
[7]. Ministry of Electronics and Information Technology. (2023). *Cyber security awareness initiatives in India*. https://www.meity.gov.in
[8]. National Cyber Crime Reporting Portal. (2024). *Cyber safety and cyber crime awareness*. https://cybercrime.gov.in
[9]. Reserve Bank of India. (2023). *Cyber security awareness for digital users*. https://www.rbi.org.in
[10]. Kaspersky India. (2024). *Cyber security tips and online safety guide*. https://www.kaspersky.co.in/resource-center