

Social Media Privacy & Data Leaks: Risks, User Behavior, and Cybersecurity Awareness Among Students

Lipika Rajanandini Sahu¹, Vishal Kumar. R², Rohan S Nair³, Aathish Karkera⁴

¹Assistant Professor, CS & IT, Jain Deemed to be University, Karnataka, India

²Student, BCA Cybersecurity, Jain Deemed to be University, Karnataka, India

³Student, BCA Cybersecurity, Jain Deemed to be University, Karnataka, India

⁴Student, BCA Cybersecurity, Jain Deemed to be University, Karnataka, India

Abstract - Social media platforms have become an essential part of everyday communication, allowing billions of users to connect, share information, and interact online. Platforms such as Facebook, Instagram, TikTok, and X have made it easier for people to exchange ideas, build communities, and access information instantly. However, along with these advantages, social media has also introduced serious concerns related to user privacy and data security. Many users unknowingly share personal information such as their location, daily activities, relationships, and contact details without fully understanding the risks associated with their digital footprint.

As the use of social media continues to grow, incidents of data leaks, identity theft, phishing attacks, and cyberstalking have also increased. In many cases, users are unaware of how their personal data is collected, stored, and analyzed by social media platforms, advertisers, and third-party applications. Oversharing personal details and not properly configuring privacy settings can significantly increase the chances of sensitive information being exposed or misused.

This study examines the relationship between social media usage, oversharing behaviour, and cybersecurity awareness among students. A mixed-methods research approach was used, combining survey responses and semi-structured interviews to understand how students interact with social media and how aware they are of privacy risks. The findings indicate that although many students are somewhat aware of privacy threats, a significant number still engage in risky online behaviours, such as sharing personal information publicly or ignoring basic security practices.

The results highlight a clear gap between users' awareness of privacy risks and their actual online behavior. The study suggests that improving digital literacy, promoting cybersecurity education, and encouraging responsible online practices can help reduce the risks associated with social media data exposure. Strengthening privacy awareness among students can play an important role in creating a safer and more secure digital environment.

Key Words: social media privacy, data leaks, cybersecurity awareness, digital footprint, oversharing, identity theft, phishing attacks, privacy settings, data

breaches, online security, personal data protection, cybercrime, information security, user behavior, data exploitation, cyberstalking, social engineering, privacy risks, digital literacy, online safety, data protection policies.

1. INTRODUCTION

Social media platforms such as Facebook, Instagram, TikTok, and X (formerly Twitter) have become a central part of modern digital communication. These platforms allow users to interact, share information, and build online communities instantly. With billions of active users worldwide, social media has significantly transformed how people communicate, access information, and express their opinions. Students and young adults are among the most active users of these platforms, often relying on them for social interaction, collaboration, and entertainment.

Despite the benefits of connectivity and information sharing, social media platforms also introduce serious concerns related to privacy and data security. Users frequently share personal information such as photos, locations, daily activities, and opinions without fully understanding how this information may be collected, stored, and used by third parties. These activities create digital footprints that can reveal sensitive personal details about individuals. When combined with weak privacy settings and limited cybersecurity awareness, this information can be exploited by cybercriminals, advertisers, or other organizations.

Several well-known incidents have demonstrated the potential consequences of social media data misuse. For example, the Cambridge Analytica scandal revealed how personal data from millions of Facebook users was collected and used for political profiling and targeted advertising without proper consent. Similar data breaches and privacy violations continue to occur, exposing large amounts of user data and raising concerns about how social media companies manage and protect personal information.

Students are particularly vulnerable to these privacy risks because of their high levels of social media engagement and tendency to share personal content online. Oversharing personal details, accepting unknown friend requests, and ignoring privacy settings are common behaviors that can increase exposure to cyber threats such as phishing attacks,

identity theft, and cyberstalking. Although many users claim to be concerned about privacy, their actual online behavior often does not reflect safe cybersecurity practices.

This study aims to examine privacy risks associated with social media usage, focusing on oversharing behavior, digital footprints, and cybersecurity awareness among students. By analyzing user behavior and existing research on social media privacy, this paper seeks to identify key vulnerabilities and highlight the gap between privacy awareness and real-world practices. Understanding these factors is important for developing effective strategies that promote safer online behavior and strengthen data privacy protection in the digital environment.

2. LITERATURE REVIEW

Previous research has explored various aspects of social media privacy, including oversharing behavior, digital footprints, large-scale data breaches, and cybersecurity awareness among users. With the rapid growth of social media platforms, researchers have increasingly focused on understanding how personal information shared online can expose individuals to privacy risks and cyber threats.

Several studies have highlighted the dangers of oversharing personal information on social media platforms. Users often share photos, location information, personal opinions, and daily activities without fully considering the long-term consequences of these actions. Such behaviors create digital footprints that remain accessible online for long periods of time. Research has shown that cybercriminals can use these publicly available details to conduct social engineering attacks, identity theft, and phishing campaigns. Oversharing also increases the risk of cyberstalking and unauthorized access to personal accounts.

Another important area of research focuses on the predictive capabilities of social media data. Studies have demonstrated that digital traces such as likes, posts, and online interactions can reveal sensitive information about individuals. For example, previous research has shown that social media activity can be used to predict personality traits, political preferences, and behavioral patterns. These predictive capabilities raise ethical concerns about how organizations collect and analyze personal data without users fully understanding how their information is being used.

Real-world data breach incidents have also played a significant role in highlighting the privacy risks associated with social media platforms. One of the most widely discussed examples is the Cambridge Analytica scandal, where personal data from millions of Facebook users was collected and used for political profiling and targeted advertising. Similar incidents have demonstrated how weak data protection policies and third-party applications can expose large amounts of user data to unauthorized access. These events have increased public awareness about the

importance of data privacy and responsible data management.

Research on cybersecurity awareness further indicates that many social media users lack sufficient knowledge about online privacy risks and protective practices. Students and young users, despite being frequent users of digital platforms, often demonstrate limited awareness of privacy settings, strong password practices, and other security measures. Studies suggest that improving digital literacy and cybersecurity education can significantly reduce the likelihood of users becoming victims of cybercrime.

Although existing studies provide valuable insights into social media privacy risks, there is still limited research that focuses specifically on students' behaviors and awareness levels regarding data privacy and cybersecurity practices. Understanding how students interact with social media platforms and how they manage their personal information online is essential for developing effective strategies to improve digital safety and reduce the risks associated with data leaks.

3. METHODOLOGY

This study investigates social media privacy risks, oversharing behavior, and cybersecurity awareness among students. A mixed-methods research approach was adopted in order to obtain both quantitative and qualitative insights. The methodology combines survey-based data collection with semi-structured interviews to better understand how students use social media and how aware they are of potential privacy threats. Using both methods allows the study to capture statistical trends while also exploring the reasons behind user behavior.

The quantitative component of the study was conducted using an online survey distributed to university students. The survey was designed to measure several aspects of social media usage, including privacy awareness, frequency of information sharing, and adoption of cybersecurity practices. The questionnaire consisted of multiple sections covering demographic information, social media usage patterns, privacy concerns, oversharing behavior, and security practices such as the use of strong passwords and two-factor authentication. Responses were collected using a five-point Likert scale to evaluate participants' level of agreement with statements related to privacy risks and cybersecurity awareness.

Participants in the study consisted primarily of undergraduate and graduate students between the ages of 18 and 25. This group was selected because students represent one of the most active demographics on social media platforms and are therefore more exposed to privacy risks and data leakage issues. The survey was distributed through online platforms and university communication channels to reach a diverse group of participants. A total of several

hundred responses were collected and filtered to ensure completeness and reliability.

In addition to the survey, semi-structured interviews were conducted with a smaller group of participants selected from the survey respondents. These interviews allowed researchers to explore participants' attitudes, motivations, and experiences related to social media privacy in greater detail. Interview questions focused on topics such as reasons for sharing personal information online, awareness of data breaches, and perceptions of privacy risks associated with social media platforms.

The collected data were analyzed using both quantitative and qualitative methods. Survey responses were examined using descriptive statistics to identify patterns in privacy awareness, oversharing behavior, and cybersecurity practices. Correlation analysis was also used to examine relationships between variables such as social media usage frequency and the likelihood of oversharing personal information. Qualitative interview responses were analyzed using thematic analysis to identify recurring patterns and key themes related to privacy awareness and online behavior.

By combining survey data with interview insights, this methodology provides a comprehensive understanding of how students interact with social media platforms and how their behavior may expose them to privacy risks. The findings from this approach help identify gaps between users' awareness of privacy threats and their actual online practices, which can inform future strategies for improving cybersecurity education and digital literacy.

4. RESULTS & ANALYSIS

This section presents the findings obtained from the survey and interview data collected during the study. The analysis focuses on three major aspects: social media usage patterns, privacy awareness levels, and the adoption of cybersecurity practices among students. The results combine quantitative survey responses with qualitative insights gathered through interviews to better understand how students manage their personal information on social media platforms.

TABLE-I PARTICIPANT DEMOGRAPHICS

Category	Percentage
Female	52%
Male	45%
Non-binary	3%
Undergraduate Students	65%
Graduate Students	35%

Table I presents the demographic distribution of participants involved in the study. The majority of respondents were undergraduate students between the ages of 18 and 25. This group represents one of the most active populations on social media platforms and therefore provides valuable insights into user behavior and privacy awareness.

TABLE-II SOCIAL MEDIA PLATFORM USAGE

Platform	Percentage of Users
Instagram	72%
TikTok	68%
X (Twitter)	55%
Facebook	48%
Snapchat	41%

The survey results indicate that social media usage among students is very high. Instagram was the most frequently used platform among participants, followed closely by TikTok and X. The popularity of these platforms demonstrates how social media plays an important role in students' daily communication and online engagement.

TABLE-III PRIVACY AWARENESS LEVELS

Awareness Domain	Mean Score (1-5)	Agree/Strongly Agree
Concern about data leaks	3.8	68%
Awareness of digital footprints	4.0	75%
Knowledge of major data breaches	3.2	55%
Understanding of privacy settings	3.4	60%

Table III summarizes the privacy awareness levels of the participants. The results indicate that students generally demonstrate moderate awareness of privacy risks associated with social media usage. A majority of participants understand that digital footprints can reveal personal information. However, awareness of major data breach incidents and privacy protection measures remains relatively limited.

TABLE-IV OVERSHARING BEHAVIOR ON SOCIAL MEDIA

Activity	Percentage of Students
Sharing location information	62%
Posting personal photos publicly	58%
Sharing academic information	45%
Accepting unknown friend requests	39%

Oversharing behavior was also observed among many participants. As shown in Table IV, more than half of the respondents reported sharing location information and personal photos online without restricting visibility. These behaviors increase the likelihood of personal information being accessed by unauthorized individuals or cybercriminals.

TABLE-V ADOPTION OF CYBERSECURITY PRACTICES

Security Practice	Percentage of Students
Two-factor authentication	52%
Strong and unique passwords	48%
Restricting third-party app access	35%
Regularly updating privacy settings	42%

Table V presents the level of adoption of recommended cybersecurity practices among students. Although many participants expressed concern about data leaks and privacy risks, fewer students reported actively implementing protective measures. Only about half of the participants enabled two-factor authentication or used strong passwords, while even fewer restricted access to third-party applications.

Statistical analysis also revealed that the amount of time spent on social media platforms is related to the likelihood of oversharing personal information. Students who reported spending more hours on social media were more likely to share personal details publicly. In contrast, participants with higher levels of privacy awareness demonstrated slightly lower levels of risky online behavior.

Insights from the interviews further supported these findings. Many participants stated that although they understand the potential risks of social media data exposure, they often prioritize convenience and social engagement over

privacy protection. Some students also reported that privacy settings on social media platforms can be confusing or difficult to manage, which discourages them from actively adjusting their security preferences.

Overall, the results highlight a significant gap between students' awareness of social media privacy risks and their actual online practices. While many users understand the potential dangers of oversharing and data leaks, inconsistent adoption of cybersecurity practices continues to expose personal information to potential misuse.

5. DISCUSSION

The findings of this study provide important insights into how students interact with social media platforms and how their behavior can expose them to privacy risks and data leaks. The results show that although many students are aware of the potential dangers associated with social media usage, this awareness does not always translate into safe online practices. This gap between knowledge and behavior highlights the complexity of user behavior in digital environments.

One of the most notable observations from the results is the high level of social media engagement among students. A large percentage of participants reported spending several hours each day on platforms such as Instagram, TikTok, and X. While these platforms provide opportunities for communication, collaboration, and entertainment, they also increase the chances of users sharing personal information without carefully considering the potential consequences. High levels of engagement can therefore increase exposure to privacy risks, particularly when users frequently post personal content.

The study also revealed that oversharing behavior remains common among students. Many participants reported sharing location information, personal photos, and daily activities without restricting access to their content. These behaviors create digital footprints that can be analyzed and exploited by cybercriminals, advertisers, or other third-party organizations. Similar findings have been reported in previous research, where oversharing on social media has been linked to increased risks of identity theft, phishing attacks, and cyberstalking.

Another important finding of this study is the gap between privacy awareness and the adoption of cybersecurity practices. Although many students expressed concern about data leaks and privacy violations, fewer participants reported using security measures such as strong passwords, two-factor authentication, or restricted privacy settings. This indicates that awareness alone is not sufficient to ensure safe online behavior. Factors such as convenience, lack of technical knowledge, and the complexity of privacy settings may discourage users from actively protecting their personal data.

Social pressure and the desire for online engagement may also contribute to risky online behavior. Many students feel encouraged to share personal experiences, photos, and updates in order to maintain social connections or gain attention on social media platforms. Platform algorithms that reward engagement and visibility can further encourage users to share more personal information. As a result, users may prioritize social interaction over privacy protection.

The findings of this study also support previous research on digital footprints and predictive data analysis. Studies have shown that even small amounts of online activity, such as likes, posts, and comments, can reveal sensitive information about users, including personality traits, interests, and behavioral patterns. When combined with oversharing behavior, these digital traces can be used for targeted advertising, profiling, or other forms of data exploitation.

These findings highlight the need for stronger cybersecurity awareness and digital literacy programs, particularly for students who are among the most active users of social media. Educational institutions can play an important role in promoting responsible online behavior by incorporating cybersecurity education into academic programs. In addition, social media platforms should provide clearer privacy controls and more user-friendly security settings to help users better manage their personal information.

Overall, the discussion emphasizes that social media privacy risks are not only technical issues but also behavioral and social challenges. Addressing these risks requires a combination of user education, improved platform design, and stronger data protection policies. By improving awareness and encouraging safer online practices, it is possible to reduce the risks associated with data leaks and protect users in an increasingly digital society.

6. CONCLUSION

This study examined privacy risks associated with social media usage, focusing particularly on oversharing behavior and cybersecurity awareness among students. The results of the survey and interviews indicate that while students demonstrate a moderate level of awareness regarding social media privacy risks, many continue to engage in behaviors that may expose their personal information online. Activities such as sharing location data, posting personal content publicly, and neglecting privacy settings contribute to the creation of digital footprints that can be exploited by cybercriminals or third-party organizations.

The findings also reveal a clear gap between privacy awareness and the adoption of cybersecurity practices. Although many students expressed concern about data leaks and privacy violations, fewer participants reported consistently using protective measures such as strong passwords, two-factor authentication, and restricted privacy

settings. This suggests that awareness alone is not sufficient to ensure safe online behavior and that additional efforts are needed to encourage the practical application of cybersecurity knowledge.

Social media platforms continue to play an important role in communication, education, and entertainment for students. However, the design of these platforms often encourages frequent sharing of personal information, which may increase exposure to privacy risks. Without proper understanding of privacy controls and responsible online behavior, users may unknowingly contribute to the exposure of their own personal data.

Based on the findings of this study, improving digital literacy and cybersecurity education is essential for reducing the risks associated with social media usage. Educational institutions should incorporate privacy awareness and online safety training into academic programs to help students better understand how to protect their personal information. In addition, social media platforms should continue improving their privacy controls and security features to make them easier for users to understand and manage.

In conclusion, addressing social media privacy challenges requires a combined effort from users, educators, technology companies, and policymakers. By promoting responsible online behavior and strengthening cybersecurity awareness, it is possible to create safer digital environments where individuals can benefit from social media platforms without compromising their privacy and personal data.

REFERENCES

- [1] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," *Proceedings of the National Academy of Sciences*, vol. 110, no. 15, pp. 5802–5805, 2013.
- [2] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019.
- [3] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.
- [4] Federal Trade Commission, "Facebook, Inc. Cambridge Analytica data privacy investigation," *FTC Report*, Washington, DC, USA, 2019.
- [5] European Union, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union*, 2016.
- [6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *IEEE Symposium on Security and Privacy*, pp. 553–567, 2012.

[7] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019–2036, 2014.

[8] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY, USA: W. W. Norton & Company, 2015.

[9] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," *IEEE Symposium on Security and Privacy*, pp. 111–125, 2008.

[10] A. B. McDonald and L. F. Cranor, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 54–61, 2010.

[11] P. Wisniewski, H. Lipford, and D. Wilson, "Fighting for my space: Coping mechanisms for SNS boundary regulation," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 609–618, 2012.

[12] M. Madden, A. Lenhart, S. Cortesi, and U. Gasser, "Teens, social media, and privacy," *Pew Research Center*, Washington, DC, USA, 2013.