International Journal of Advance and Innovative Research
Volume 13, Issue 2: April - June 2026
ISSN 2394 - 7780

SOCIAL MEDIA PRIVACY AWARENESS AND CYBERSECURITY PRACTICES AMONG YOUTH

Mr. Arvind Kumar[1], Mr. Amit Punia[2] and Prof. (Dr.) Gaurav Aggarwal[3]
[1]B.Tech. CSE, Faculty of Engineering & Technology, Jagannath University, Delhi NCR, Bahadurgarh
[2]Assistant Professor, Faculty of Engineering & Technology, Jagannath University, Delhi NCR, Bahadurgarh
[3]Dean and HOD, Faculty of Engineering & Technology, Jagannath University, Delhi NCR, Bahadurgarh

ABSTRACT:
Social media platforms such as Instagram, WhatsApp, Facebook, and Snapchat will continue to play a significant role in communication, education, and entertainment among youth. However, increasing digital engagement will also heighten concerns related to cybersecurity, identity theft, cyberbullying, and data misuse. This study will assess the level of social media privacy awareness among youth and evaluate their online privacy practices, cybersecurity knowledge, and perceptions of digital safety. Data will be collected from 50 respondents through a structured online questionnaire and analyzed using statistical tools such as percentage, mean, median, and mode. The findings will indicate that Instagram will remain the most preferred social media platform among participants. Most respondents will demonstrate awareness of privacy settings and the use of two factor authentication, while a considerable proportion will understand how applications utilize personal data. Despite this awareness, risky online behaviors, such as accepting friend requests from strangers and clicking on unknown links, will continue to be prevalent. Some participants will also report experiencing cyber related issues, including hacking and fake accounts. The study will conclude that although youth will exhibit a moderate to high level of awareness regarding cybersecurity and privacy protection, gaps in understanding data usage and persistent risky behaviors will necessitate enhanced digital literacy and cybersecurity education to promote responsible social media usage and strengthen online safety.

Keywords: *Social Media Privacy, Cybersecurity Awareness, Digital Privacy, Youth Behavior, Online Safety, Data Protection, Social Media Usage, Cyber Risks*

INTRODUCTION

In the modern era, social media has woven itself into the fabric of daily existence, particularly for the younger generation. Platforms like Instagram, Snapchat, Facebook, and WhatsApp serve as more than just communication tools; they are essential hubs for entertainment, information exchange, professional networking, and the curation of personal identity. As digital technology continues its rapid advancement, young people find themselves increasingly reliant on these digital spaces for their social lives and information gathering. This shift has fundamentally rewritten the rules of communication, behavioral habits, and how youth engage with the world around them.[1] These platforms function through intricate algorithms and data driven systems designed to monitor user activity, individual tastes, and social connections. This harvested data typically fuels targeted marketing, content suggestions, and platform finetuning. While these capabilities can make for a more tailored user experience, they simultaneously trigger significant alarms regarding personal data privacy and the security of sensitive information. A vast number of users remain in the dark about how their private details are gathered, stored, or distributed to outside entities, which heightens the danger of data exploitation and security failures.[2]. A further pressing issue is the widespread lack of knowledge among young people concerning privacy configurations and digital safety protocols. It is common for users to broadcast sensitive data such as private photographs, real time locations, and personal views without a full grasp of the associated hazards. This trend fuels problems like identity theft, digital harassment, and the unauthorized hijacking of personal data. Furthermore, once data enters the online sphere, it transforms into a permanent digital record, creating a situation where controlling or erasing that information in the future becomes nearly impossible.[3]

CONCEPT OF PRIVACY IN THE DIGITAL WORLD

Digital privacy represents an individual's power to oversee how their personal details are gathered, utilized, archived, and moved across the web. In today's hyperconnected environment, every digital footprint whether browsing a site, using a mobile tool, or interacting on a social feed leaves a trail of data. This information can range from basic identifiers like names and addresses to more complex data like search histories, buying habits, and psychological profiles. Consequently, the notion of privacy has moved beyond physical walls and into the boundless virtual landscape.[4] Privacy in this realm is deeply tied to technical concepts like data encryption, identity verification, and access management. These digital shields are intended to lock away user information from prying eyes Yet, even with these tools, risks remain high due to sloppy security habits, a lack of user education, and inconsistent protection standards across different platforms. Frequent violations manifest as massive data leaks, hacking incidents, and the illicit sharing of user archives. It is vital to recognize that

ISSN 2394 - 7780

privacy isn't merely about keeping secrets; it is fundamentally about agency the freedom to decide what parts of oneself are visible and who is allowed to see them. As our private lives become inseparable from digital platforms, the necessity of understanding and defending digital boundaries becomes paramount.[5] digital privacy has immense economic weight. Personal data is a high value commodity for corporations, enabling them to refine their marketing and services. However, when this data is used without permission or oversight, it opens the door to identity fraud, financial scams, and blanket surveillance. Finally, digital privacy involves a watchful eye on how governments handle personal records. While data collection is often justified by national security or crime fighting, the absence of strict transparency and regulation can lead to the erosion of fundamental civil rights.[6]

Meaning and Importance of Social Media

Social media is defined as the digital landscape where individuals interact to create, distribute, and swap information or ideas within virtual networks. Major platforms managed by entities such as the Office of Communications and Marketing include Facebook, X (formerly Twitter), Instagram, LinkedIn, and YouTube. In the contemporary world, social media is indispensable. it keeps the global community linked, allowing for the free flow of ideas and opinions in what should be a protected environment. It also serves as a powerful engine for building brands, supporting social movements, and staying current with global news.

Key characteristics of social media include:

Interactive Technology: It utilizes digital tools to allow the instant sharing of text, images, and videos.

User Generated Content: The heart of these platforms is the content created by users, which invites engagement through likes, shares, and public discourse.

Global Reach: Currently, over 4.7 billion individuals worldwide utilize social media services.

Community and Conflict: While it is praised for building global communities, it is also criticized for being a conduit for misinformation and toxic speech.

Commercial Influence: It has become a cornerstone of modern corporate marketing strategies.

Dominant Platforms: The global market is currently led by giants such as Facebook, YouTube, WhatsApp, Instagram, and WeChat.[7]

The Growth of Social Media and Data Sharing

The explosion of social media over the last ten years has fundamentally altered how people communicate, particularly among the youth. Platforms have transitioned from simple chat rooms into massive digital ecosystems that dictate social norms and information flow. This expansion is powered by the near universal access to smartphones and highspeed web connections, leading to a cycle of constant engagement and data creation.

Data Generation in Social Media Platforms

Data creation in the digital space happens through both intentional and hidden interactions. While users "actively" share things like posts and messages, platforms "passively" harvest data in the background. This includes tracking how long you look at a post, your physical location, the specific hardware you use, and your network of friends. Merging these two types of data allows companies to build "shadow profiles" that predict a user's future behavior and secret preferences.

User Behavior and Data Sharing Practices

Sharing habits among the young are often driven by deep seated social and psychological needs. The craving for social approval, peer connection, and a strong online "brand" pushes users to post personal details frequently. Often, this happens without a clear understanding of the privacy tradeoffs. Features like disappearing "stories" and live broadcasts have accelerated the speed and volume of this sharing, making it harder for users to pause and reflect on the risks.

Role of Algorithms and Data Utilization

Social networks rely on complex machine learning models to sift through user data. These algorithms study behavior

to tailor specific feeds and ads to each person. While this makes the app more addictive and personalized, it creates a "black box" where users don't know how their data is being stored or which third party brokers are buying it.

ISSN 2394 - 7780

Digital Footprint and Long-Term Impact
A primary danger of social media is the creation of a "permanent record" or digital footprint. Anything put online can be archived, screenshotted, or sold, making total deletion nearly impossible. This data persistence can shadow a user for decades, potentially hurting their reputation, blocking job prospects, or compromising their physical safety. Therefore, understanding that "the internet is forever" is a core requirement for modern digital life.[8]

Importance of Privacy Awareness Among Youth
In the current era, being "privacy literate" is a vital part of being a responsible digital citizen. Because young people are the most active demographic online, they are also the most exposed. Building awareness is the only way to transform from a passive victim of data harvesting into an empowered user.[9]

Role of Privacy Awareness in Reducing Cyber Threats
Knowledge is the best defense against cybercrime. Youth who lack adequate training in data protection are highly vulnerable to cyber threats such as identity theft, phishing attacks, and digital stalking. For identity theft, phishing scams, and digital stalking. Malicious actors use social media as a hunting ground to find personal identifiers. By mastering privacy settings and using advanced security tools, users can effectively lock their digital doors against these predators.[10]

Understanding the Impact of Digital Footprint
Young users often post in the "heat of the moment." Privacy awareness teaches them that every digital action contributes to a lasting profile. Understanding that a post today could impact a university application or a job interview five years from now promotes a culture of mindfulness and careful decision making before hitting the "post" button.[11]

Awareness of Data Collection and User Consent
Social media thrives on a data for service trade. Privacy awareness helps users read between the lines of long, confusing legal documents. It allows them to understand what they are actually "signing away" when they click "accept" and empowers them to demand more transparency from the corporations they use.[12]

Contribution to Cybersecurity and Safe
Practices Even the best security software can't stop a user from making a mistake. Awareness ensures that youth adopt "hygiene" habits like using two factor authentication and unique passwords. These small steps are often more effective at stopping data breaches than the most expensive antivirus programs.

Building a Responsible Digital Environment
When a user values their own privacy, they are more likely to respect the privacy of their peers. This awareness fosters a more ethical digital culture, reducing the likelihood of "doxing," harassment, or the unauthorized sharing of someone else's private life.[13]

Role of Technology and Security Measures
Technology acts as both the threat and the solution in the digital world. As the mountains of data shared by youth grow taller, the engineering required to protect that data must become more advanced. These security layers are the only thing standing between a user's private life and global exposure.[14]

Encryption: This is the primary shield. Techniques like end-to-end encryption ensure that a message is scrambled at the moment it leaves a phone and only unscrambled when it reaches the correct recipient. To anyone in between, including the platform itself, the message appears as an unreadable format to unauthorized parties.[15]

Authentication: The days of simple passwords are over. Modern security relies on Multifactor Authentication (MFA), requiring a password plus a second "key" like a thumbprint or a code sent to a mobile device. This makes it nearly impossible for a hacker to get in, even if they know the password.[16]

Access Controls: Platforms provide "digital fences" in the form of privacy settings. These allow users to hide their profiles from strangers or restrict who can see their location.

AI and Machine Learning: Modern security uses AI to detect anomalous or suspicious behavior. If someone logs into your account from another country at 3 AM, these systems can automatically lock the account to prevent a breach before it even happens.[17]However, technology is only half the battle. Most breaches happen because of human error like using a weak password or clicking a bad link. Security is a partnership between smart code and smart users.[18]

ISSN 2394 - 7780

Cyber Risks Facing Today's Youth

While the internet is a doorway to knowledge, it is also an environment filled with potential risks and threats. The phrase "cyber pandemic" is often used to describe how quickly and dangerously online threats have spread.[19]

Cyberbullying: This is an ongoing crisis where digital tools are used to humiliate or terrorize others. This includes everything from toxic comments to the nonconsensual sharing of private images.[20]

Social Engineering: Predators often use "psychological hacking" to trick youth. By creating fake profiles and "grooming" victims, they can manipulate young people into revealing secrets or doing dangerous things.[21]

Phishing and Smishing: These are "fake" messages that look real. They often claim there is an emergency with an account to trick the user into typing their password into a fake website.[22]

Account Takeovers: Once a hacker gets in, they can ruin a person's reputation or steal their identity to commit crimes.[23]

Awareness and Protection Strategies for Youth

Because many young people haven't had formal training in digital safety, they are at higher risk. The following strategies are essential for staying safe:

Passphrases over Passwords: Instead of Dog123, use a long sentence like My Blue Cat Likes To Dance In The Rain!. Computers find these nearly impossible to crack.[24]

Multi Factor Authentication (MFA): Always turn this on. It is the single most important thing a person can do for their security.[25]

Password Managers: Use a digital vault to store your logins. This stops you from reusing the same password on every site.[26]

Developing a Skeptical Mindset: Messages that create urgency or appear unusual should be treated with caution, as they may indicate phishing attempts, it's probably a scam. Youth must learn to verify sources before trusting them.[27]

Privacy Hygiene: Regularly checking which apps have access to your camera, microphone, or location and turning off anything that isn't necessary.[28]

The Imperative for Research into Youth Social Media Privacy

The rapid pace of tech means we are often playing catchup. There is a critical need for research that looks at the "human side" of privacy. We need to understand why young people—who know about the risks—still choose to overshare. Current research is often too technical or too focused on behavior, but we need to see how they work together. We also need to test if the "safety tools" companies provide actually work or if they are just for show. As new threats like Deepfakes and AI profiling emerge, our research must evolve to protect the next generation.[29]

METHOD AND METHODOLOGY

1. **Research Method:** The present study was conducted using a quantitative research method to examine the level of social media privacy awareness among youth. A survey based approach was selected because it allows the researcher to collect information from a large number of participants in a systematic and organized manner. Quantitative research helps in understanding the awareness, attitudes, and behaviors of respondents through numerical data and statistical interpretation. The study mainly focused on analyzing how young users interact with social media platforms, their understanding of privacy settings, cybersecurity practices, and awareness regarding data protection. The research also examined the online behavior of youth and the risks they face while using digital platforms.
2. **Research Design:** A descriptive research design was used for this study. Descriptive research helps in presenting the current situation and understanding the characteristics, opinions, and awareness level of the participants regarding social media privacy.
3. **Area of Study:** The study was conducted among youth users of social media platforms. Participants included students and young individuals belonging mainly to the age group of 16–25 years. The respondents were active users of platforms such as Instagram, WhatsApp, Facebook, and Snapchat.
4. **Population of the Study:** The population of the study consisted of youth who actively use social media platforms. The total population selected for the research was 50 respondents. The respondents belonged to

ISSN 2394 - 7780

different age groups and included both male and female participants. Most participants were from the younger age category, particularly between 21–25 years, as this age group is highly engaged in social media usage.

5. **Sampling Technique:** For the study, a convenience sampling method was used. Convenience sampling is a nonprobability sampling technique in which participants are selected based on their availability and willingness to participate in the survey. This method was chosen because it allowed easy access to respondents within a limited time period. It also helped in collecting responses quickly from active social media users.

6. **Sample Size:** The sample size of the study consisted of 50 respondents. The selected participants were sufficient to understand the general level of privacy awareness among youth and to analyze their social media behavior.

7. **Statistical Tools and Analysis :** The collected data was organized, classified, and analyzed using simple statistical methods. The following statistical tools were used in the study: Percentage Mean Median Mode.

RESULT

Table :1 Age Distribution

Age Group (Years)	No. of Population
10–15	**1**
16–20	**14**
21–25	**32**
26–30	**2**
31–35	**0**
36–40	**0**
41–45	**0**
46–50	**1**
Total	**50**

Statistical Measures

Mean = 22.09 years Median = 22.06 years Mode = 22.38 years

The above table presents the age distribution of the study participants. Most of the participants were between 21–25 years of age, accounting for 32 out of the total 50 participants. The next highest group was 16–20 years with 14 participants. Only a few participants belonged to the age groups 10– 15, 26–30, and 46–50 years, while no participants were found in the age groups between 31–45 years.

The average age of the participants was 22.09 years. The median and mode values were also close to the mean, showing that the participants were mainly concentrated

in the younger age group, especially in the early twenties. Table 02: Gender Distribution According to Age

Age Group (Years)	Male	Female
10–15	1	0
16–20	8	6
21–25	27	5
26–30	2	0
31–35	0	0
36–40	0	0
41–45	0	0
46–50	1	0
Total	39	11

Statistical Values Male

Mean Age: 22.80 years Median Age: 22.44 years Mode Age:

22.66 years Female

Mean Age: 20.97 years **Median Age:** 20.08 years **Mode Age:** 19.79 years

ISSN 2394 - 7780

The table shows the distribution of male and female participants across different age groups. Out of the total 50 participants, 39 were males and 11 were females.

Most of the male participants belonged to the 21–25 years age group, while the majority of female participants were found in the 16–20 and 21–25 years age groups.

Only a small number of participants were seen in the age groups above 25 years, and no participants were recorded between 31–45 years. The average age of male participants was slightly higher than that of female participants. The mean, median, and mode values for both groups indicate that most participants were concentrated in the younger age range, particularly in their early twenties.

Table 03: Which platforms do you use regularly ?

Response Category	Percentage	No. Of Population
Instagram	49.0%	25
WhatsApp	40.8%	20
others	6.1%	3
Facebook	2.1%	1
Snapchat	2.0%	1
Total	100%	50

Mean: Not applicable (Nominal Data) Median: Not applicable (Nominal Data) Mode: Instagram

Instagram is the most commonly used social media platform among the respondents, with 50% of users preferring it regularly. WhatsApp is the second most used platform at 40%. Facebook and Snapchat have very low usage compared to the other platforms. This indicates that youth mainly prefer visualcontent and messagingbased platforms over traditional social networking platforms.

How Many Social Media Accounts Do You Have?

Number of Accounts	Number of Responses	Percentage
1–2 Accounts	43	86%
3–4 Accounts	4	8%
5 or More Accounts	3	6%
Total	50	100

The majority of respondents (86%) maintain only 1–2 social media accounts. A smaller group of users have 3–4 accounts, while very few respondents manage more than five accounts. This shows that most users prefer limiting themselves to a small number of platforms rather than managing multiple accounts

Daily Usage Time of Social Media

Daily Usage Time	Number of Responses	Percentage
Less than 1 Hour	11	22%
1–5 Hours	28	56%
3–5 Hours	8	16%
More than 5 Hours	3	6%
Total	50	100%

Most respondents spend between 1–5 hours daily on social media platforms. Around 22% spend less than one hour per day, while a smaller percentage spends more than five hours daily. The data shows that social media has become a significant part of daily life for most young users.

Purpose of Social Media Usage

Purpose	Number of Responses	Percentage
Communication	10	20%
Entertainment	24	48%
Education	13	26%
Business/Promotion	3	6%
Total	50	100%

ISSN 2394 - 7780

Entertainment is the primary reason for social media usage among respondents, accounting for 48% of responses. Educational use is also significant at 26%, followed by communication purposes. Only a small percentage of respondents use social media for business or promotional activities.

Awareness of Privacy Settings

Response	Number of Responses	Percentage
Yes	**48**	**96%**
No	**2**	**4%**
Total	**50**	**100%**

A large majority of respondents are aware of privacy settings available on social media platforms. This reflects a high level of digital literacy among youth. However, awareness does not always guarantee proper usage of privacy protection tools.

Do you use the same password everywhere?

Response Category	Percentage	No. of Respondents
No	82.0%	41
Yes	18.0%	9
Total	**100%**	**50**

The data indicates strong password hygiene among the group, with 82% of users stating they do not reuse the same password across different platforms. Conversely, 18% remain at high risk by using a single password for everything. This is a significant indicator of cybersecurity awareness within this demographic

REFERENCES (APA 7th Edition)

1. Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying, mental health, and youth safety. *Current Psychiatry Reports, 17*(10). https://doi.org/10.1007/s1192001506164
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465
3. Agosto, D. E., & Abbas, J. (2017). "Don't be dumb—that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society, 19*(3), 347–365. https://doi.org/10.1177/1461444815606121
4. Aichner, T., Grünfelder, M., Maurer, O., & Jegeni, D. (2021). Twentyfive years of social media: A review of social media applications and definitions from 1994 to 2019. *Cyberpsychology, Behavior, and Social Networking, 24*(4), 215–222. https://doi.org/10.1089/cyber.2020.0134
5. Barman, S., & Dakua, G. (2024). Studies on social media and its impact on youth: Exploring realworld consequences. *VIDYA A Journal of Gujarat University, 3*, 132–144. https://doi.org/10.47413/y9ty4d20
6. Bernhard, D., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of ComputerMediated Communication, 15*(1), 83–108. https://doi.org/10.1111/j.10836101.2009.01494.x
7. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP.2012.44
8. Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of ComputerMediated Communication, 13*(1), 210–230. https://doi.org/10.1111/j.10836101.2007.00393.x
9. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
10. Chou, H.L., & Chou, C. (2023). How teens negotiate privacy on social media proactively and reactively. *New Media & Society, 25*(6), 1290–1312. https://doi.org/10.1177/14614448211018797
11. Conti, M., Passarella, A., & Das, S. K. (2018). A survey on security and privacy issues of social networks. *IEEE Communications Surveys & Tutorials, 20*(1), 75–102. https://doi.org/10.1109/COMST.2017.2719798

12. Dar, S., & Nagrath, D. (2023). The impact that social media has had on today's generation of Indian youth: An analytical study. *MORFAI Journal, 3*(2), 166–176. https://doi.org/10.54443/morfai.v3i2.309
13. De Wolf, R. (2020). Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society, 22*(6), 1058–1075. https://doi.org/10.1177/1461444819876570
14. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638
15. Gholve, D. (2025). Data privacy while using social media platforms. *International Journal of Scientific Research in Modern Science and Technology, 4*, 27–33. https://doi.org/10.59828/ijsrmst.v4i10.385
16. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100. https://doi.org/10.1145/1290958.1290968
17. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and metaanalysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073–1137. https://doi.org/10.1037/a0035618
18. Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654. https://doi.org/10.1111/jcpp.12161
19. Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995
20. Nwaimo, C., Adegbola, A., & Adegbola, M. (2024). Datadriven strategies for enhancing user engagement in digital platforms. *International Journal of Management & Entrepreneurship Research, 6*(6), 1854–1868. https://doi.org/10.51594/ijmer.v6i6.1170
21. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299–1323. https://doi.org/10.1007/s1174702200845y
22. 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. https://doi.org/10.1177/0270467607311484
23. Vanderhoven, E., Schellens, T., Valcke, M., & Raes, A. (2014). How safe do teenagers behave on Facebook? An observational study. *PLOS ONE, 9*(8), e104036. https://doi.org/10.1371/journal.pone.0104036
24. Vickery, J. (2014). "I don't have anything to hide, but…": The challenges and negotiations of social and mobile media privacy for nondominant youth. *Information, Communication & Society, 18*(3). https://doi.org/10.1080/1369118X.2014.989251
25. Wash, R. (2010). Folk models of home computer security. *Proceedings of the Symposium on Usable Privacy and Security*. https://doi.org/10.1145/1837110.1837115