Journal of Artificial Intelligence and Autonomous Intelligence Received 02-04-2025; Accepted 12-06-2025; Published 19-06-2025

Assessing Cybersecurity Vigilance Among End Users of AI Based Social Media Apps

Aakanksha aakanksha.1@rajguru.du.ac.in
Department of Computer Science,
Shaheed Rajguru College of Applied Sciences for Women,
University of Delhi, Delhi, India.

Apeksha Deore apekshadeore7202@gmail.com
Department of Electronics,
Shaheed Rajguru College of Applied Sciences for Women,
University of Delhi, Delhi, India.

Veenu Bhasin veenu.bhasin@pgdav.du.ac.in
Department of Computer Science,
P.G.D.A.V. College,
University of Delhi, Delhi, India.

Corresponding Author: Veenu Bhasin

Abstract

As India rapidly advances in its digital transformation, maintaining strong cybersecurity measures and implementing AI responsibly have become top priorities. The increasing reliance on digital public infrastructure, cloud computing, and AI-driven governance has exposed the country to significant risks, including cyberthreats and data breaches. While policy measures such as Digital Personal Data Protection Act 2023, forensic analysis of electronic evidence, and initiatives like Cyber Surakshit Bharat have enhanced digital security, challenges persist.To protect India's growing digital landscape, it is essential to strengthen cybersecurity frameworks, address AI-related risks, ensure strict regulatory compliance and enhance cybersecutity vigilance amongst the end users. This paper gauges the vulnerabilities of end users and their vigilance while using social media apps through a survey. As digital engagement increases, so does the risk of exposure to threats such as data breaches, cyber bullying, misinformation, and online fraud. The study underscores the growing necessity for individuals to develop digital vigilance and awareness.

Keywords: Artificial intelligence, Cybersecurity, Vigilance.

1. INTRODUCTION

With India's rapid adoption of digital technologies, Artificial Intelligence (AI) has emerged as critical area requiring vigilance and proactive governance in cyber security. The growing usage of

Citation: Veenu Bhasin, et al. Assessing Cybersecurity Vigilance Among End Users of AI Based Social Media Apps. Journal of Artificial Intelligence and Autonomous Intelligence. Research. 2025;2(2):17.
Pages:246-263

AI-based social media apps for mundane tasks have raised concerns about the privacy and security of users in the digital world. There has been an exponential increase in cyberattacks like spams and digital arrest, in recent times. To address cybersecurity challenges, initiatives like Cyber Surakshit Bharat [1], focus on strengthening cybersecurity awareness among government officials, while AI capacity-building programs aim to ensure responsible deployment of AI in governance. Government of India has developed the Indian Cyber Crime Coordination Centre (I4C)[1], to increase the coordination of law enforcement agencies (LEAs) in tackling cybercrimes. This initiative facilitates a structured framework for efficient addressing of digital threats. Moreover, the National Cyber Crime Reporting Portal [2], has been introduced where citizens can directly report cybercrimes. These reports are automatically forwarded to the relevant law enforcement agencies as per their location, for prompt legal action. These measures highlight the government's dedication to strengthening cybersecurity and encouraging public participation in cybercrime prevention. To combat financial fraud effectively, the Government of India has introduced the Citizen Financial Cyber Fraud Reporting and Management System [2]. This organized and systematic approach provides the instant reporting of financial fraud cases and helps prevent the unauthorized transfer of funds by fraudsters. These Government policies are promising if they are implemented efficiently at the grassroots level. A dedicated toll-free helpline, '1930', has been established to help victims file cyber fraud complaints, ensuring a quick and efficient response. Despite all the above policies and government initiatives to ensure cybersecurity for end users, there are growing incidents of cyberattacks. Therefore, in addition to all such measures, the vigilance of end users is the key to secure cyber system. Cybersecurity vigilance among end users of AI-based social media applications is crucial due to the increasing prevalence of cyber threats and the integration of AI in these platforms. To assess cybersecurity vigilance, it is essential to understand the technological factors as well as user behavior including awareness.

AI plays a significant role in enhancing cybersecurity measures through threat detection, incident response, and security analytics [3–6]. In addition, AI tools are used to automate cybersecurity tasks, allowing professionals to focus on strategic aspects [7]. This includes tasks such as intrusion detection, spam and phishing detection, and malware analysis [8].

Despite the use of AI to provide cyber security and prevent fraud, challenges persist. AI-based cybersecurity systems face challenges such as trust, accountability, privacy, bias, and financial costs [8]. These challenges need to be addressed to improve user acceptance and effectiveness. Social engineering attacks and scams are prevalent on social media platforms, exploiting users' trust and leading to data breaches and financial losses [9]. Therefore, user behavior and vigilance remain a critical factor. Studies show that users often do not act on their privacy concerns, highlighting a gap between awareness and behaviour [10]. Furthermore, cyber protection behavior significantly influences self-disclosure on social networking sites. Educating users through cybersecurity training programs can mitigate risks associated with self-disclosure [11]. To increase awareness, authors in [6], suggest that personalized training and education can significantly reduce repeat offenses of cyber violence. Gamification and phishing testing are effective strategies to enhance cybersecurity awareness among users [12]. Continuous support through chatbots integrated with social networking can provide immediate advice and recommendation, improving user vigilance against cyber threats [13]. This paper tries to get insights on various aspects of cybersecurity, AI applications, and user behaviour on social media.The aim is to assess the vigilance of the users in securing their data and information and hence contributing towards a more secure and resilient digital ecosystem. Further, the survey aims to find out the vulnerabilities in cybersecurity and usage of AI tools.

2. LITERATURE REVIEW

The rapid growth of India's digital infrastructure and governance has been supported by extensive research and policy frameworks. Studies on cybersecurity, such as those conducted under the Cyber Surakshit Bharat initiative, emphasize the importance of building robust digital defense mechanisms against evolving threats. Training programs for Chief Information Security Officers (CISOs) and IT officials highlight the need for continuous skill development to combat cyber risks effectively. Existing literature on digital public infrastructure underscores the role of platforms like Aadhaar, UPI, and DigiLocker [14], in driving financial inclusion and secure identity management. India's Digital Public Infrastructure (DPI) has revolutionized digital innovation by merging public investment with private sector-driven advancements.Widely used platforms such as Aadhaar, UPI, and DigiLocker provide the foundational framework, while private enterprises develop specialized applications. Research on the impact of the GI Cloud (MeghRaj) [15],initiative demonstrates how cloud services improve the efficiency of e-governance applications, ensuring scalability and resilience. The expansion of India's data center ecosystem, particularly through the National Informatics Centre (NIC) and National Data Centre (NDC) [16], projects, has been documented in reports analyzing the growing demand for cloud storage and AI applications. India has secured a major milestone in cybersecurity by attaining Tier 1 status in the Global Cybersecurity Index (GCI) 2024 [17], which is released by the International Telecommunication Union 12(ITU) India's cybersecurity success is the result of proactive government initiatives catering to enhance cyber resilience, strengthening cybercrime laws, and implementing sturdy security standards at multifaceted levels. Currently, India's legal institutions are well-equipped to tackle cyber threats and its digital infrastructure. Moreover, Sectoral Computer Incident Response Teams (CSIRTs) [17], facilitates location-based technical assistance with incident reporting, thereby enhancing cybersecurity .

The Department of Telecommunications (DoT) continues to drive the nation's cybersecurity initiatives, ensuring a safe and resilient digital future on the international stage [18]. The Digital Personal Data Protection Act, 2023 (DPDP'23) emphasizes individuals' rights to protect their personal data by integrating key data protection principles as follows:

- Obtaining consent for the lawful and transparent processing of data,
- restricting the use of user data to specific purposes only,
- minimizing data collection to essential levels,
- ensuring accuracy and timely updates,
- limiting storage only for necessary periods,
- implementing strong security measures, and
- upholding accountability through penalties for breaches and data adjudication.

Researchers stated that role of AI in cybersecurity can act as a double-edged sword [19]. AI, with the ability to process large data, helps detecting threats and responding to cyber attacks in real time. The same ability of AI is exploited by cybercriminals in breaching security. As mentioned in the research study [20], the shortage of skilled cybersecurity professionals poses significant risks to corporations, national security, law enforcement, and the intelligence community. In many cases,

attackers exploited vulnerabilities in IT infrastructures, taking advantage of security system flaws, configuration errors, and unpatched software to breach both government and private networks.

Education and vigilance play an indispensable role in India's cybersecurity strategy. Despite all the policies and security standards, user awareness and vigilance is so crucial that there is a growing emphasis on awareness campaigns and behavioral change initiatives to improve cyber security among end users. These campaigns aim to educate users about potential threats and encourage safer online behaviors [21]. The authors emphasized the importance of user behavior, including knowledge, attitudes, and skills, and found it crucial to understand and improve cyber security practices.

The studies by [22, 23] show that there is a difference in the level of awareness and vigilance between users. Some users are highly aware and cautious regarding AI-driven phishing attacks and other cyber security threats, others lack the necessary knowledge and skills to effectively identify and mitigate these threats.

AI technologies can be used in cyber security to automate threat detection and response, making it easier to identify and mitigate cyber threats on social media platforms. AI can be used to analyse large datasets to detect patterns and anomalies indicative of cyber-attacks [24–26]. Further, the tools such as certificate transparency monitoring can enhance user confidence and empower them to take proactive measures against phishing by alerting users to potential threats [22]. The increased use of chatbots and intelligent agents in almost every website and app can provide continuous support, helping users stay informed about the latest threats. Users can be trained and educated on best practices in cybersecurity [13, 27]. A research study by [28], suggests the substantial role of AI in enhancing cybersecurity and breaching privacy due to the integration of AI in social media. AI bots can emulate humans online, such as playing games, clicking links automatically, and buying, selling, reselling, or blocking best-seller seats for concerts or items on shopping sites. Users are concerned about data breaches, identity theft, and the misuse of personal information. AI-based cybersecurity measures should ensure transparency and adhere to ethical and regulatory frameworks to provide fairness and user data protection [29, 30].

AI can also be used to enhance cybersecurity vigilance. The users can be trained by engaging them in interactive tools like gamification and help them utilize these tools to simulate real-world threats using AI-generated scenarios [27]. The users can be taught the privacy management features. AI-driven phishing detection tools can empower them to enhance their cybersecurity vigilance [22, 29]. To adopt safer online practices, recommender systems can analyse user behaviour and provide personalized recommendations to help users. These recommender systems can identify users who may need additional support or training [13, 21].

In summary, enhancing cybersecurity vigilance among end users of AI-based social media apps requires a multifaceted approach that includes user education, AI-driven threat detection, and adherence to ethical standards. By addressing both technological and human factors, it is possible to create a safer and more secure online environment.

3. METHODOLOGY

This paper aims to measure the level of cybersecurity awareness among users of AI-based social media apps. By identifying common cybersecurity threats faced by users on these platforms, we try to evaluate the effectiveness of current user practices and platform safeguards. Through this paper, we suggest strategies to improve user vigilance and safety through the usage of best practices in the cyber world. The study in this paper tries to answer the following research questions:
RQ1: What is the general level of cybersecurity awareness among users of AI-based social media platforms?
RQ2: What types of cybersecurity risks are most prevalent on these platforms?
RQ3: How do users perceive the privacy and security features of these apps?
RQ4: What practices do users adopt to secure their accounts and data?
RQ5: Do these social media platforms protecting users privacy and secure their personal data?
RQ6: Are the users aware of their data protection rights?

Design and Tools: To answer the above research questions, a comprehensive survey was conducted. The survey was done using a questionnaire. The questionnaire was designed using Google Form to include a total of 23 questions that helped in assessing cybersecurity vigilance, usage behaviours, perception, and expectations. Most of the questions were closed-ended and 4 point Likert scale was used to answer the questions. The quesionare does not include questions that can be considered as Personal Sensitive Information (PSI). The only personal data collected was 'Age Group' the participant belongs to.

Sample: The sample data was collected from a group of 314 participants using convenience sampling. The participants were informed about the research objectives and their involvement in the survey was completely voluntary and anonymous.The data was collected from diverse demographic groups using Whatsapp and email.

Data Analysis: Sampled data was analysed using descriptive statistics. The methodology used some key variables to study and analyse the vulnerability and vigilance of the users. These variables were assessed using the appropriate questions in the questionnaire like user knowledge of AI functionalities in apps, awareness of phishing, deepfakes, and social engineering attacks, use of privacy settings, MFA, password hygiene and frequency of encountering suspicious content or links.

4. RESULTS AND DISCUSSION

Despite the presence of stringent laws and governance assistance, people are exposed to the vulnerabilities such as online scams, fraudulent attempt to steal personal data, etc. The gap is due to the significant lacuna of the vigilance among the people regarding multiple parameters which is being analysed by conducting a research survey through questionnaire. To assess the awareness among the citizens, this survey was conducted through Google form which seeks responses of users on different parameters related to AI in various different fields. In order to have an overall broader perspective this survey collected data across various geographical regions of India in the domain of academics and research, with focus on young users. Responses collected were from users across

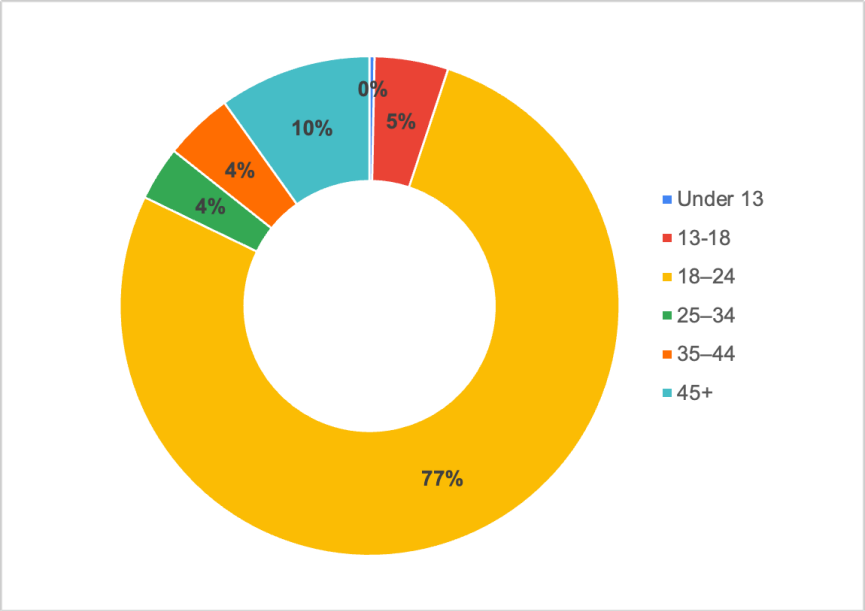


Figure 1: Percentage of Respondents Across Age Groups

various age groups. We received 314 responses. The three-fourth of the respondents (77%) are in the age group 18-24 and rest of the respondents are in other age groups. FIGURE 1 gives the percentage of the respondents across different age-groups.

4.1 Social Media Applications and Financial Transaction Applications - Usage Pattern

As depicted in FIGURE 2, the most preferable social media applications are WhatsApp and Instagram. It showcases that exposure to vulnerabilities via these apps is certainly more and hence judicious use of it should be done. As the users use it most of the times therefore it becomes essential to make users more vigilant about the security risks associated with these applications.

Other social media applications that are used by more than half of the respondents include Linkedin, Telegram and Truecaller apart from the delivery apps Blinkit, Zomato and Amazon. According to Slava Gomzin [31], Telegram, although claims that its ”way more secure” than WhatsApp, is not End-to-End Encrypted, uses proprietary protocols (which are not audited as standards ones), thus making it vulnerable and prone to leakage of information. Truecaller asks for the permission to access all the information in contact list of a user before the user can start using the services provided by Truecaller [32]. This leads to the privacy breach of the user and his/her contacts making them vulnerable to social media bullying and spams. All the delivery apps (like Blinkit, Zomato and Amazon) keep personal information (like, DOB, location, phone number etc.) about users, apart from their preferences and financial transactions. This adds to the financial and personal data vulnerabilities.

FIGURE 3 shows the most commonly used online payment apps are Google Pay, Paytm and PhonePe. These should have strong passwords. Additionally, enabling two-factor authentication (2FA) and

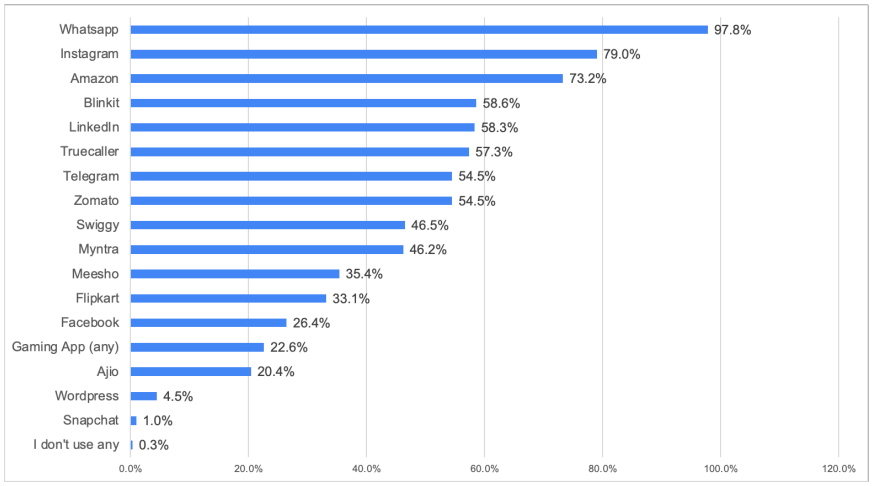


Figure 2: Usage of Social Media Apps

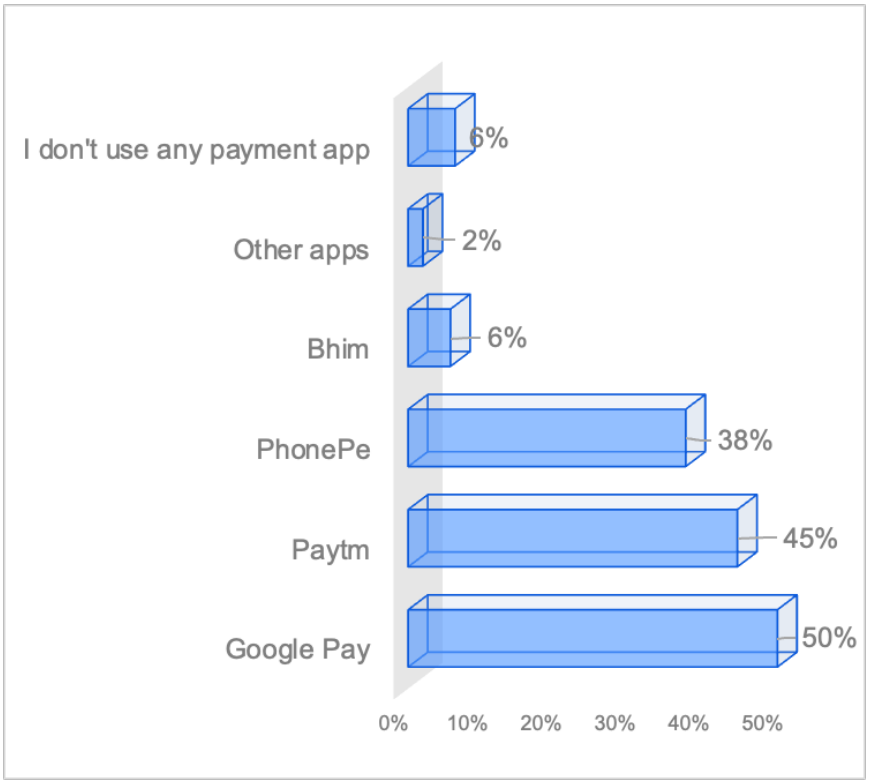


Figure 3: Usage of Financial Transaction Apps

avoiding public Wi-Fi can further enhance security. Users should also regularly update apps and be cautious of phishing attempts.

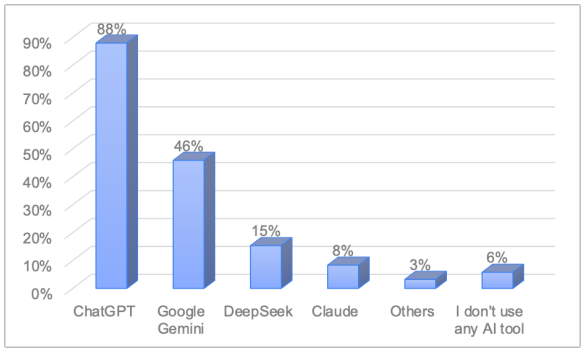


Figure 4: Usage of AI tools

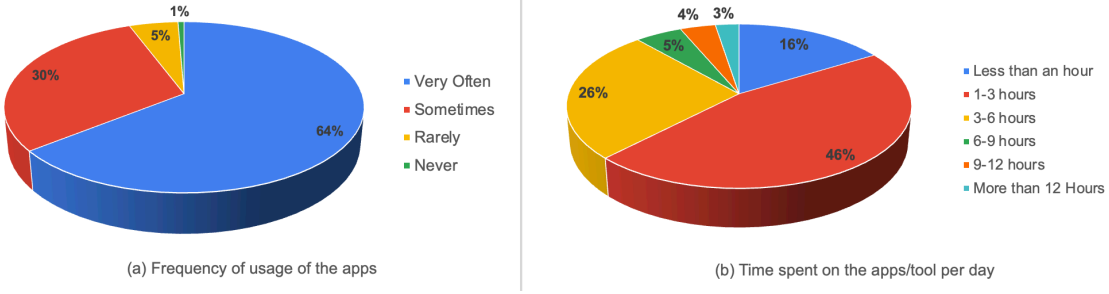


Figure 5: Usage of apps

ChatGPT is one of the most preferable AI tools used by people as depicted in FIGURE 4, with 88% of the respondents claiming to use this tool. As the most widely used tool, ChatGPT represents the largest potential cybersecurity exposure like Users entering sensitive or regulated data into the tool. Lack of awareness about data retention policies poses another threat. OpenAI states inputs may be used to improve models unless API or ”chat history off” settings are used. The users should be aware of the mere fact that not all information shared by ChatGPT is authentic, its retrieved from certain fixed databases. Google Gemini is the second most used AI tool. Being part of Google’s services, it may inherit risks involving data sharing (across linked accounts Gmail, Drive, etc.) and the data mining under Google’s own data mining policies. DeepSeek, being used by 15% being relatively new and not so popular have lack of transparency about data hosting or security posture, which could be a concern.

As illustrated in FIGURE 5, 64% percent of people often use these tools and apps, confirming the extent of exposure by the users is the new normal. A large chunk of the respondents, i.e. 84%, use the social media apps and AI tools for more than an hour daily. The time spent on social media apps and gaming apps represents exposure to vulnerabilities in cyberspace, particularly youth and kids.

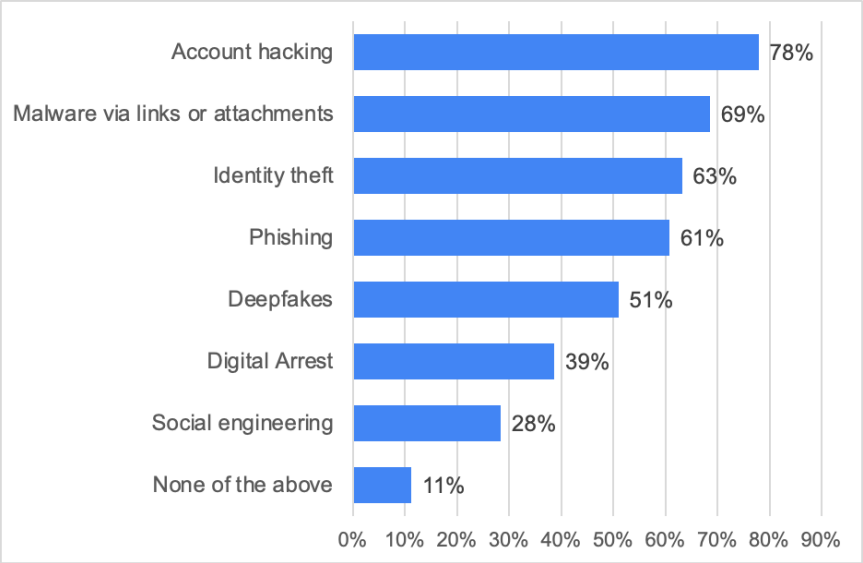


Figure 6: Familiarity of respondents with various cyber security threats

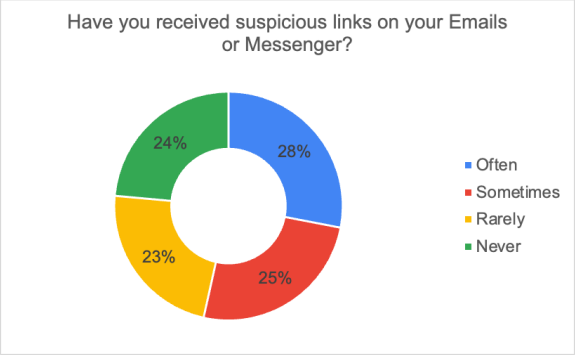


Figure 7: Suspicious Links

4.2 Awareness and Encounter with Threats

As is evident from the FIGURE 6, more than 60% of the respondent are aware of cyber threats like Account hacking, Malware, Identity theft and Phishing. Only 11% responded with being unaware about any of these threats. These 11% are most vulnerable as they don't even know that there can exist threats like that , and they will not be vigilant. Around 40% are even aware of Digital arrest, which is good as that is one threat which people fall prey to very easily.

As depicted in FIGURE 7, 76% percent of people had received and are aware of suspicious links on email or Messenger. The rest 24% percent never received any such suspicious links, this might be pointing to they being unaware of links being shared with malicious intent. This represents the vigilance inculcation required in order to not get trapped by clicking and redirected to fraudulent spaces on the internet.

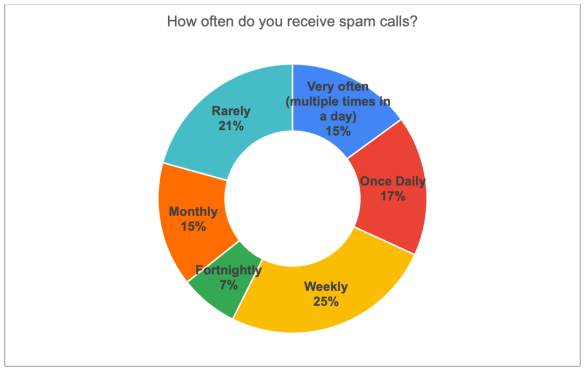


Figure 8: Frequency of receiving spam calls

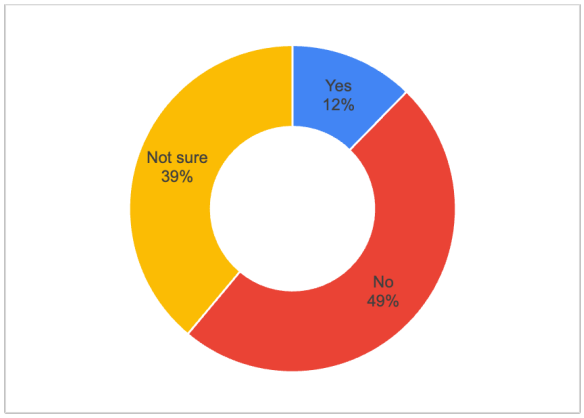


Figure 9: Trust on AI systems to protect your privacy and personal data on social media

Spam Calls are another common issue. 57% receive spam calls at least weekly (FIGURE 8). This indicates widespread exposure to phone-based threats like Robocalls, Phishing and Scam attempts (tech support, bank impersonation, etc.). High spam call rates signal phone numbers exposed which might result through breaches or public listings or inadequate mobile security policies. Bombardment of spam calls may result in letting their guard down and making them vulnerable to scams. 43% respondents receive spam calls less than weekly and are less targeted or better protected, but still experience interruptions.

To the survey question ”Do you trust AI systems to protect your privacy and personal data on social media?”, only 12% have responded affirmatively (FIGURE 9). This subset becomes vulnerable to data misuse, profiling, or algorithmic manipulation because of may be being less cautious. The survey showed a strong skepticism about how AI is protect their personal data on social media. The 39% respondents which are ”not sure” suggest uncertain and uninformed about how AI interacts with data privacy, making them arguably the most vulnerable.

The survey showed that most of the respondents have not encountered any of scam or threat. As per FIGURE 10, 89% people have never faced any issue on uploading personal photographs on social media platforms. As depicted in FIGURE 11 (a), 83% have never been trapped in a fraud or scam online and only 9% have been scammed. The perturbing section is the 8% of respondents, who are

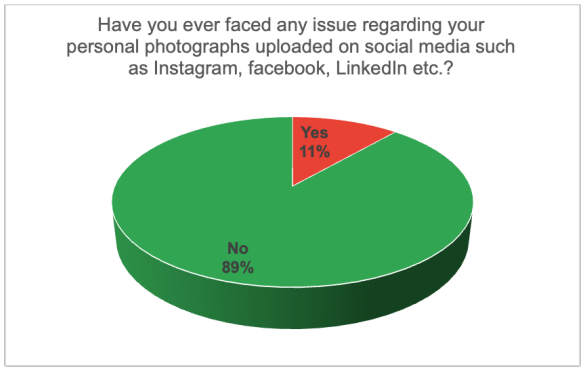


Figure 10: Personal Information Threats

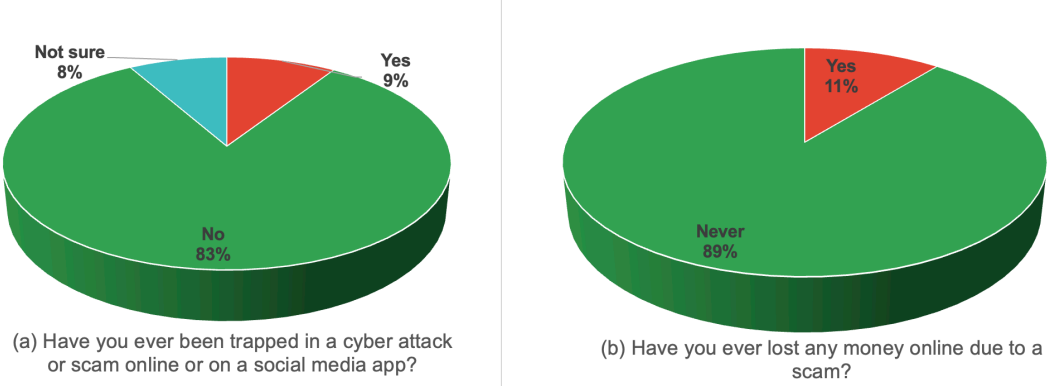


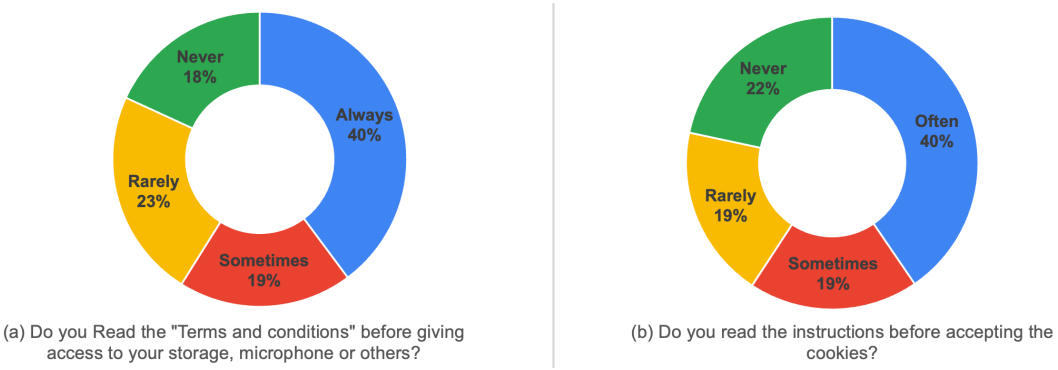
Figure 11: Scam exposure

not even sure if they had been scammed or not. FIGURE 11 (b) depicts that only 11% respondents have lost money in online scams. User vigilance is required while being online, so as to curb any threat in cyberspace to personal dignity and safety of person.

4.3 Awareness About Digital Personal Data Protection Act,2023 and Security Practices

The high percentage of respondents being aware about various threats and not having encountered scam, do not indicate high vigilance as is evident from FIGURE 12. Only 40% of the respondents always read the ”Terms and conditions” before giving access to the storage, microphone etc (FIGURE 12 (a)). Similarly, only 40% of the respondents often read the instructions before accepting the cookies (FIGURE 12 (b)). In both the cases, around 20% have never bothered to read, making them most vulnerable. The rest of the respondents although are somewhat alert but are still vulnerable in cyberspace.

FIGURE 13 adds another vulnerability aspect as only 43% respondents claim to read and adjust the ’Privacy and security settings’ of the apps.



(a) Do you Read the "Terms and conditions" before giving access to your storage, microphone or others?

(b) Do you read the instructions before accepting the cookies?

Figure 12: Vigilance for 'Terms and Conditions' and cookies

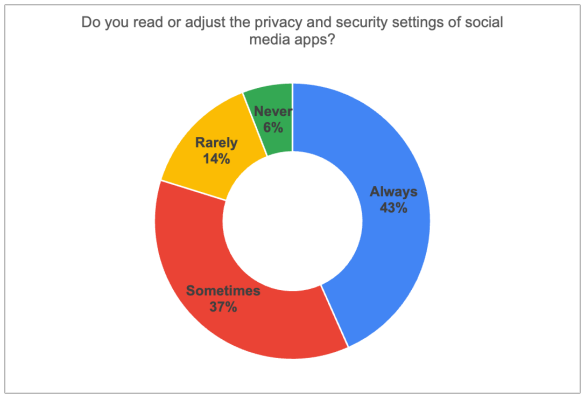


Figure 13: Adjusting privacy and security settings

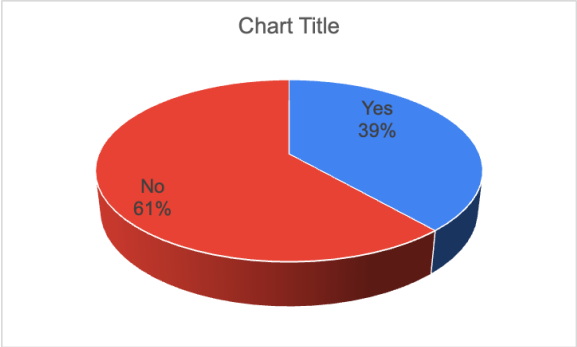


Figure 14: Awareness about The Digital Personal Data Protection Act, 2023

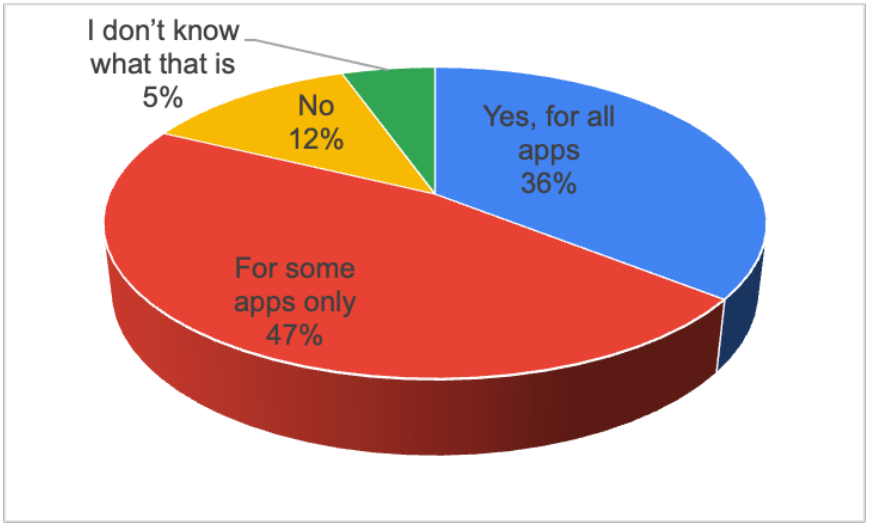


Figure 15: Usage of two-factor authentication or multi-factor authentication

As depicted in FIGURE 14, major chunk of the society (i.e. 61%) is unaware of DPDP'23. It is a matter of concern and needs to be catered at ground level.

Multi-factor authentication is a security mechanism that enhances login security beyond user name and password. The multi-factor authentication requires two or more distinct authentication factors. The two-factor authentication is a subset of multi-factor authentication. As in FIGURE 15, majority of the respondents (82.1%) use two-factor or multi-factor authentication either for all or some apps. This shows strong general awareness and adoption, although the Partial Adoption is More Common**.** The largest group (46.5%) use MFA on some apps only, possibly indicating that it's seen as necessary for sensitive services (like banking or email) only, but not applied universally. 12.4% do not use MFA and 5.4% are unaware of what MFA is. These groups may present potential security risks and may benefit from awareness campaigns or support in setup.

As depicted in FIGURE 16, status downloader application is not used by majority of the respondents (i.e. 86%), this reduces the vulnerabilities, as it minimizes threat to the internal storage of the device and cloud data.

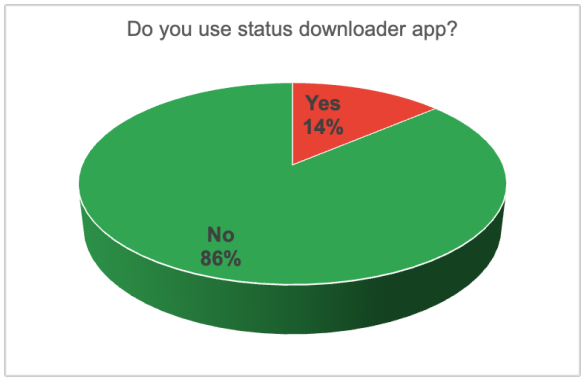


Figure 16: Status Downloader app usage

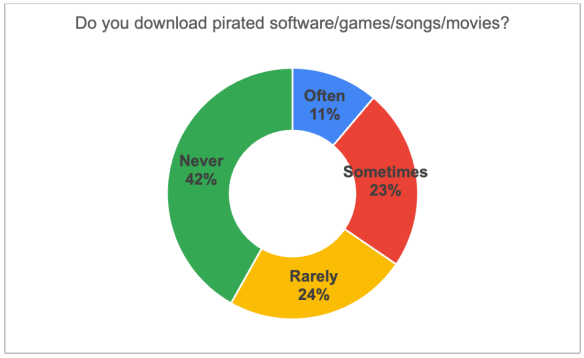


Figure 17: Data from pirated sites

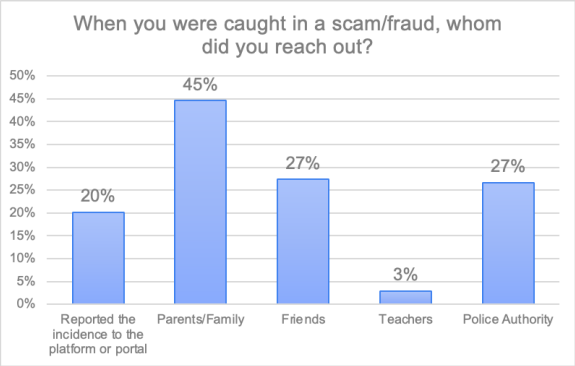


Figure 18: Reporting Scam

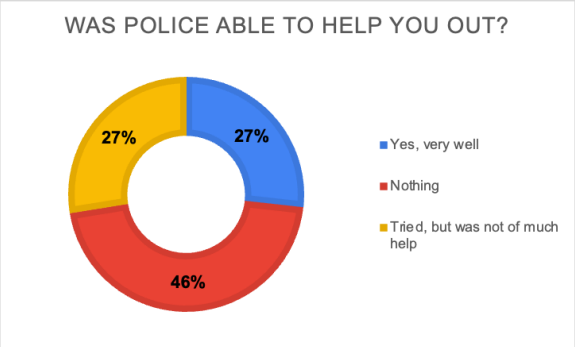


Figure 19: Opinion on Police

In response to ”Do you download pirated software/games/songs/movies?” (FIGURE 17), 58% admitted to pirating at least rarely, suggesting a widespread but varied level of engagement in digital piracy. Only 11.2% do it often, thus implying that habitual piracy is a minority behavior. Claim of the majority of the respondents (42%) that they never engage in piracy is reassuring, showing their strong ethical or legal stance or fear of legal consequences or malware. The fact that a large portion fall into “sometimes” and “rarely” shows many engage in piracy selectively. The use of pirated content being an ethical and legal issue, also makes them vulnerable. Many users may not realize pirated content can expose them to malware or security vulnerabilities.

4.4 Reporting of Frauds

FIGURE 18 shows that 45% people prefer sharing the vulnerability of being caught in fraud to parents/family and 27% with friends. Only 27% reported to police authority and among them 73% affirmed that police was not able to help them (FIGURE 19). Only 27% people confirmed that police was able to help them. This showcase poor public opinion on administration’s Assistance. The government should establish the faith of masses by adequately executing the policies to the same and leverage vigilance among the masses.

5. CONCLUSION

Assessing cybersecurity vigilance among end users of AI-based social media apps involves understanding the role of AI in cybersecurity, user behaviour, challenges faced by AI systems, and effective intervention strategies. Educating users and providing continuous support are essential to awareness and action, thereby enhancing overall cybersecurity vigilance. The results of this study show that users have low to moderate awareness of AI-driven risks. It was observed that most of the users are not bothered about the settings and normally rely on default settings. Most of the users have limited or no understanding of deepfakes or AI-generated scams and are using the AI apps and tools randomly without being aware of the repercussions. Younger users may be more tech-savvy but not necessarily more vigilant. This study emphasizes the need for enhanced in-app cybersecurity training. The app developers should clearly mention the AI use in user interactions and their impact. To further enhance the vigilance, security platforms should have partnerships with cybersecurity educators. Lastly, AI-driven alerts can help users to identify any suspicious activities during their usage of these online social media apps. In short, this study emphasizes the importance of bridging the gap between advanced AI integration and user cybersecurity awareness to ensure safer digital experiences. This research delves into the relationship between the time individuals spend on various online platforms and their susceptibility to cyber vulnerabilities. It was observed that on an average, users are using these apps for many hours on daily basis. This increases their vulnerability for cyber-attacks and data leakage. As per the analysis done in the survey, it was found that with the growing usage of AI-based social media apps for mundane tasks have raised concerns about the privacy and security of users in the digital world. It is evident that the users need to be more vigilant and cautious while using these apps and putting their confidential data in the public domain. By fostering a proactive approach to cybersecurity, users can better identify potential threats, safeguard their personal information, and respond effectively to the ever-evolving challenges of cyberspace. Strengthening digital literacy and responsible online behavior is crucial in ensuring a safer and more secure digital environment. This paper emphasizes the need for judicious and secure use of social media apps robust security mechanisms, ethical AI governance, and resilient digital policies to safeguard India's technological progress.

References

[1] https://i4c.mha.gov.in

[2] https://cybercrime.gov.in

[3] Taherdoost H. AI for Cyber Security and Cyber Security for AI: Complementary Role. In: Artificial Intelligence for Cyber Security and Industry 4.0. 1st Edition. CRC Press. 2025:1-23.

[4] Singh B, Kaunert C, Chandra S. Relishing Machine Learning Intelligence Combating Cyber Threats: Legal and Ethical Disquiets in Cyber Investigation at Global Scenario. In Navigating Cyber Threats and Cybersecurity in the Software Industry. IGI Global Scientific Publishing. 2025:129-150.

[5] Singh B. Appreciating Machine Learning Intelligence Combating Cyber Threats: Legal and Ethical Disquiets in Cyber Investigation at Global Scenario at the Age of Democracy. In Democracy and Democratization in the Age of AI. IGI Global Scientific Publishing. 2025: 259-284.

[6] Mengru C, Abd Rahman MR, Zahir MZ. Analysis of Managing Cyberviolence Based on Artificial Intelligence Technology. Edelweiss Appl Sci Technol. 2025;9:2341-2352.

[7] Gafni R, Levy Y. The Role of Artificial Intelligence (AI) in Improving Technical and Managerial Cybersecurity Tasks' Efficiency. Information & Computer Security. 2024;32:711-728.

[8] Alalwan JAA. Roles and Challenges of AI-Based Cybersecurity: A Case Study. Jordan J Bus Admin. 2022;18.

[9] Banire B, Al Thani D, Yang Y. Investigating the Experience of Social Engineering Victims: Exploratory and User Testing Study. Electron. 2021;10:2709.

[10] Vogler D, Meissner F. How Users Tweet About a Cyber Attack: An Explorative Study Using Machine Learning and Social Network Analysis. J Digit Media Policy. 2020;11:195-214.

[11] Khan NF, Ikram N, Murtaza H, Asadi MA. Social Media Users and Cybersecurity Awareness: Predicting Self-Disclosure Using a hybrid Artificial Intelligence Approach. Kybernetes. 2023;52:401-421.

[12] Tharayil SM, Sha'lan F, Alotaibi S, Almarhoun M, Hajjar A, et al. Enhancing Cyber Resilience Through AI-Driven Phishing Tests and Gamified Learning. In the International Conference on Artificial Intelligence and Smart Environment. Cham: Springer Nature. 2024;1353:146-157.

[13] Abdelhamid S, Mallari T, Aly M. Cybersecurity Awareness, Education, and Workplace Training Using Socially Enabled Intelligent Chatbots. In The learning ideas conference. Cham: Springer Nature. 2023:3-16.

[14] https://www.digitalindia.gov.in/digital-infrastructure/

[15] https://www.pib.gov.in/PressReleasePage.aspx/pib.gov.in/%20Pressreleaseshare.aspx?PRID=2082144

[16] https://www.nic.gov.in/#:~text=The%20National%20Data%20Centres%20form,and%20NDC%20Bhubaneshwar%

[17] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057035

[18] Kaul V, Enslin S, Gross SA. History of Artificial Intelligence in Medicine. Gastrointest Endosc. 2020;92:807-812.

[19] Taddeo M, McCutcheon T, Floridi L. Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword. Nat Mach Intell. 2019;1:557-560.

[20] Morovat K, Panda B. A Survey of Artificial Intelligence in Cybersecurity. In 2020 International conference on computational science and computational intelligence (CSCI). IEEE. 2020:109-115.

[21] van Steen T. Measuring Behavioural Cybersecurity: An Overview of Options. In International Conference on Human-Computer Interaction. Springer. 2023: 460-471.

[22] Soon JP, Chan RQ, Lee QH, Loke DE, Chun SL, et al. User Perceptions of Artificial Intelligence Powered Phishing Attacks on Facebook's Resilient Infrastructure. Int J Adv Appl Sci. 2024;13:878-886.

[23] Herath TB, Khanna P, Ahmed M. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. J Cybersecur Priv. 2022;2:1-18.

[24] Babulak E. AI Tools for Protecting and Preventing Sophisticated Cyber Attacks. IGI Global. 2023.

[25] Saranya V, Shree RS, Miriam JA, Muneera AN. Leveraging Artificial Intelligence for Cybersecurity: Implementation, Challenges, and Future Directions. In Machine Learning and Cryptographic Solutions for Data Protection and Network Security. 2024:29–43.

[26] Jabbarova K. AI and Cybersecurity-New Threats and Opportunities. J Res Adm. 2023;5:5955-5966.

[27] Pavlíček A. AI in Social Media: Harnessing Innovation Amid Ethical and Privacy Challenges. IDIMT-2024: Changes to ICT, Management, and Business Processes through AI. 2024.

[28] Zeadally S, Adi E, Baig Z, Khan IA. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access. 2020;8:23817-23837.

[29] Chung KC, Chen CH, Tsai HH, Chuang YH. Social Media Privacy Management Strategies: A SEM Analysis of User Privacy Behaviors. Comput Commun. 2021;174:122-130.

[30] Sahay RR, Sinha JK, Pandey S, Singh R, Balyan R, et al. Internet of Things and Artificial Intelligence Superseding in the Journey of Social Media. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN). IEEE. 2023:130-134.

[31] https://spectrum.ieee.org/telegram-security

[32] Dutta D, Agarwal S, Dash R, Sahoo B. A Detailed Analysis of Data Security Issues in Android Devices. In Intelligent Data Communication Technologies and Internet of Things: ICICI 2019. Springer International Publishing. 2019:410-417.