

Determinants of Social Media Cybercrime Victimization Among Young Adults: The Role of Awareness and Security Practices

Veena A¹, Rajee Johnson²

¹ Postgraduate, Garden City University, Bangalore, India.

² Assistant Professor, Garden City University, Bangalore, India

Abstract: The use of social media has become increasingly central to contemporary understanding and forms part of a communicational shift predominantly associated with individuals ages 18 - 30 years. Yet the popularity of the internet has also led to an increase in cybercrime showing a significant rise in cybercrimes like phishing, hacking, impersonation, cyberbullying or intimidation online and identity theft or stealing someone else's personal information online for illegal activity. We focus on the deterrent power of security features and user awareness against social media cybercrime across different adult age groups. This study was carried out among 400 social media users aged 18 years and above. Stratified random sampling was used to select subjects based on their social media usage patterns. Questionnaires, online surveys, focus group discussions, and interviews were used as data collection instruments to gather information on the real-life experiences, perceptions, and reporting behaviors related to cybercrime exposure, preventive practices, and awareness among different age groups. Youth tend to have better knowledge of technical security features, while the older group shows lower levels of security awareness and utilization. Though the respondents have encountered various cybercrimes, the reporting levels are low across all age groups due to lack of trust in the platforms, consequences of reporting, and lack of knowledge regarding reporting mechanisms. This study emphasizes the need to promote age-targeted digital literacy programs, robust access control mechanisms, and enforcement of online security laws. The study provides significant insights to policymakers and cybersecurity experts to devise effective strategies to prevent cybercrime among different age groups of adults.

Key Words: Social Media Cybercrime, User Awareness, Security Features, Digital Literacy and Age-Based Differences

1. INTRODUCTION:

Social media has significantly transformed human interactions by providing platforms for communication, entertainment, business, and activism. With billions of active users worldwide, platforms such as Facebook, Twitter, Instagram, LinkedIn, TikTok, and Snapchat have changed the way individuals and organizations connect. However, this rapid digital expansion

has also led to the rise of various forms of cybercrime (McAlaney & Benson, 2019; Jain & Ghoshal, 2021). Cybercrime is not a new phenomenon. As technology continues to evolve, cybercriminals adapt by developing new methods to exploit digital platforms (Smith, 2020). The widespread use of social media has introduced additional risks, including identity theft, phishing scams, cyberstalking, and online harassment (Chua & Banerjee, 2015; Europol, 2022). This shift from traditional cyber threats to advanced social media crimes highlights the urgent need for stronger cybersecurity measures and greater user awareness (National Cyber Security Centre, 2021).

Social media crimes appear in several forms. Phishing scams are among the most common, where fraudulent messages trick users into revealing sensitive information such as passwords and banking details (Chua & Banerjee, 2015). Identity theft is another serious issue, where criminals steal personal information to impersonate individuals and commit fraud (Canadian Anti-Fraud Centre, 2021). Cyberbullying and online harassment have also become widespread, often causing serious emotional harm to victims (Golladay & Holt, 2020). In addition, financial fraud and scams, including fake investment schemes and online shopping fraud, continue to threaten users (Alazab & Broadhurst, 2016). Victims of social media crimes frequently experience psychological distress. Cyberbullying, harassment, and online blackmail can lead to anxiety, depression, and, in extreme cases, suicidal thoughts (Cross, 2015; Whitty & Buchanan, 2012). Along with emotional harm, these crimes can also result in significant financial losses for both individuals and businesses. Fraudulent schemes, ransomware attacks, and online scams have caused billions of dollars in damages globally (Internet Crime Complaint Center, 2022). Many high-profile cases demonstrate the seriousness of social media crimes. By analyzing these cases, researchers can

identify patterns and develop effective preventive measures (Button et al., 2007). Governments, financial institutions, and social media platforms are working to reduce these threats through stronger security strategies.

Major platforms have introduced several security measures to combat cybercrime. Two-factor authentication (2FA) improves account security, while content moderation helps detect and remove harmful material. Artificial intelligence is also being used to identify suspicious activities, detect fake accounts, and prevent fraud (Trend Micro, 2023). User verification systems help reduce identity theft and impersonation (Duggan & Smith, 2016). Despite these efforts, cybercriminals continue to adapt, making continuous improvements in cybersecurity essential. The future of social media crimes presents new challenges. AI-driven scams, deepfake impersonations, and misinformation campaigns are becoming increasingly sophisticated (Rusch, 2022). Addressing these threats requires cooperation between social media companies, law enforcement agencies, policymakers, and users to build a safer and more secure digital environment

2. METHODOLOGY

In this study, This research seeks to identify the psychological and economic impacts of social media crimes and Reporting ratio through a survey method. A mix of statistical data (quantitative analysis) and individual experiences (qualitative analysis) was employed to better comprehend the victimization.

2.1 Survey Design

A guided questionnaire was designed with a blend of multiple-choice and open-ended questions, It concentrated on salient areas such as: Demographics (gender, age, frequency of usage of social media), kinds of crimes faced (identity theft, phishing, cyberbullying, fraud), psychological effect (stress, anxiety, depression), financial effect (amount of money lost, recovery) and preventive steps taken (awareness, security settings).

2.2. Data Collection

Online surveys were used through platforms such as Google Forms, social media, and email, People of various backgrounds were invited to ensure a wide range of data, The responses were gathered over a time period to obtain real-time data.

2.3. Data Analysis

Numerical data (Quantitative Analysis)

Percentages and statistics were employed in measuring the level of crime frequency, levels of emotional distress, and losses, Charts and graphs were prepared to easily present findings. Comparisons between groups of different ages, genders, and platforms were made if necessary. Open-ended answers were examined in order to determine typical experiences and emotional responses, Themes that were recurring included fear, embarrassment, issues regarding trust, or financial hardship.

2.4. Aim

The primary aim of this research is to investigate the prevalence, impact, and reporting patterns of social media scams across different age groups. Through a survey-based approach, the study seeks to identify which age group is most vulnerable, understand the psychological and financial consequences of these scams, and assess the level of awareness and action taken by victims. This research ultimately aims to support the development of more effective preventive strategies and awareness programs to reduce the risk of online scams.

2.5. Objective

To analyze the age-wise distribution of individuals affected by social media scams. To assess the reporting behavior of scam victims across different age groups. To compare the psychological and financial impact experienced by victims. To identify the age group most vulnerable to social media scams. To recommend preventive measures and awareness strategies based on the findings.

2.6 Ethical Considerations

Informed consent was given by all participants prior to recording their responses. Confidentiality was ensured by avoiding the collection of personal identifiers such as names and contact information. The data were only utilized for research purposes and kept safe.

2.7. Materials Required:

Survey Responses, statistical tools / Software and reference literature

After collecting the questionnaire responses, the data were organized and entered into the Statistical Package for the Social Sciences (SPSS) for analysis. SPSS was used to process and analyze the collected data through descriptive statistical techniques such as frequencies, percentages, and tables. This helped to summarize respondents' demographic information, social media usage patterns, and awareness of social media crimes. The use of SPSS allowed the researcher to interpret the data accurately and present the results in a clear and systematic manner.

2.8. Analysis

Analysis focused on following Data :

Age group analysis of Social media scam victimization 'A Survey based study', the gap in reporting social media crimes ' Survey based analysis and the cost of Social media Scams : Analysing Financial and Psychological Impacts on Victims

3. RESULT AND DISCUSSION

Age group from 18 to 26:

In a survey conducted among 100 participants, a striking 68% shared that they had experienced some form of scam on social media. This number shows that social media scams are not rare or isolated—they are becoming a common part of users' online experience.

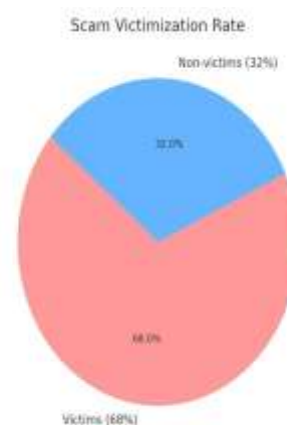


Fig 1.1 Victims of the scams ratio

However, despite such a high rate of victimization, only 15 out of the 100 participants reported the scam to either the platform or any legal body. This low reporting rate suggests that most victims choose to remain silent. This reveals a major gap between being affected and seeking help—people are falling victim, but very few are taking action afterward.



Fig 1.2 Reporting Ratio of the Victims

When it came to the type of damage caused by these scams, an interesting pattern emerged. While some victims reported financial losses, the bigger issue for most was the emotional and mental stress they went through. Many shared that the incident left them feeling anxious, scared to use social media again, or ashamed that they were tricked. Some even avoided online communication afterward because they no longer felt safe or confident.

This shows that for many people, the psychological impact of being scammed is more painful than the money lost.

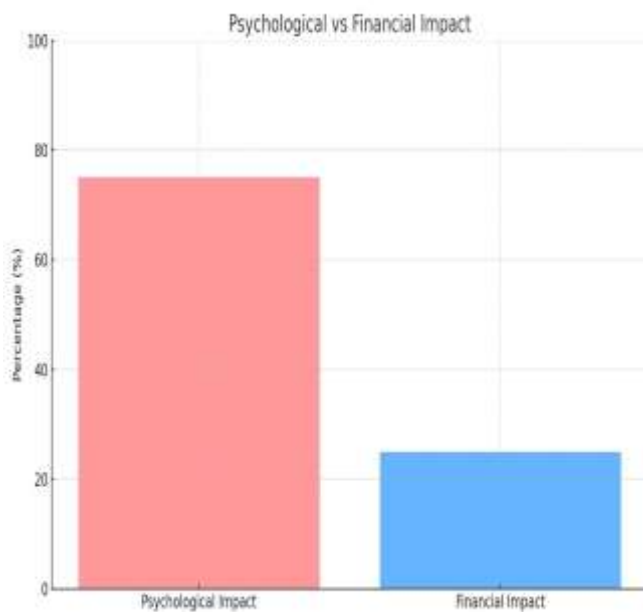


Fig 1.3 Impact comparison of people affected Psychologically and Financially Age group from (27- 32)

In our survey, individuals aged 27 to 33 were found to be the most affected by social media scams. Out of 100 total respondents, 34 people from this age group reported being scammed.

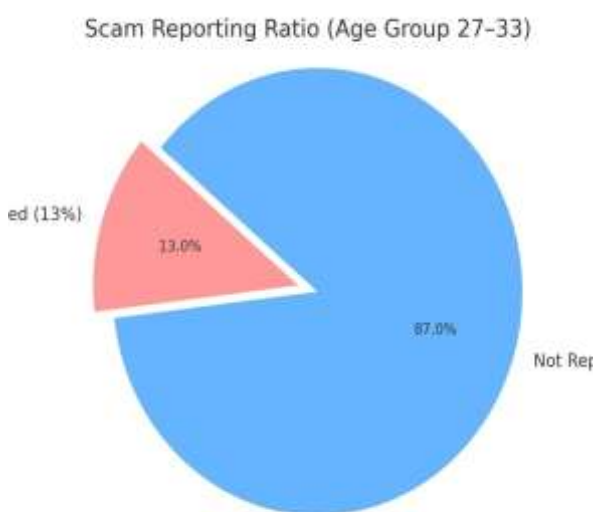


Fig 1.4 Scam Reporting Ratio of the Victims (27-33)

What's concerning is that out of the 34 victims, only 13 actually reported the scam. This means a majority

chose not to come forward. This shows a gap in awareness and possibly a lack of trust in victims.

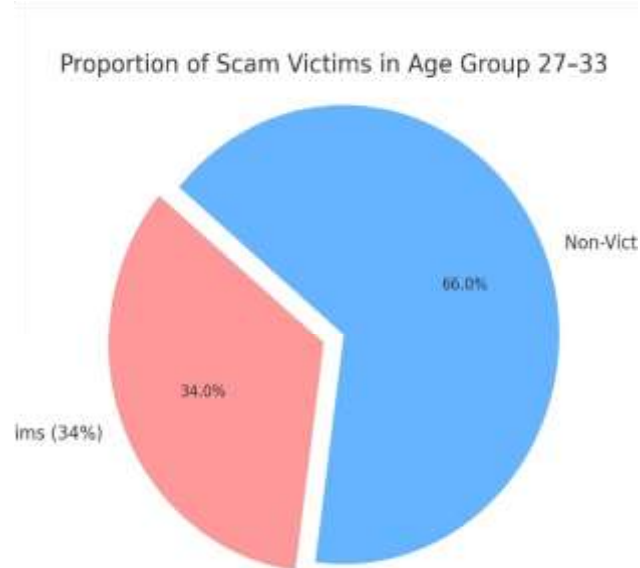


Fig 1.5 Impact comparison of people affected Psychologically and Financially (27-33)

When asked about the effects of the scams, many participants described both financial loss and emotional distress. However, the emotional or psychological impact stood out more. Victims mentioned feeling anxious, stressed, or even depressed. While financial losses did occur, many participants said the emotional toll lasted longer. The feeling of being tricked or taken advantage of stayed with them.

Overall, this age group faces both financial and emotional harm from social media scams, with psychological impact being more severe. This highlights the need for better education on digital safety, emotional support for victims, and easier ways to report and deal with such crimes.

Age 33 to 38 –

In the age group of 33 to 38, the survey revealed that 32 out of 100 participants had fallen victim to a social media scam. This indicates that nearly one-

third of the individuals in this age range are vulnerable to online fraud.

Reporting Ratio of Scam Victims (Age Group 33-38)

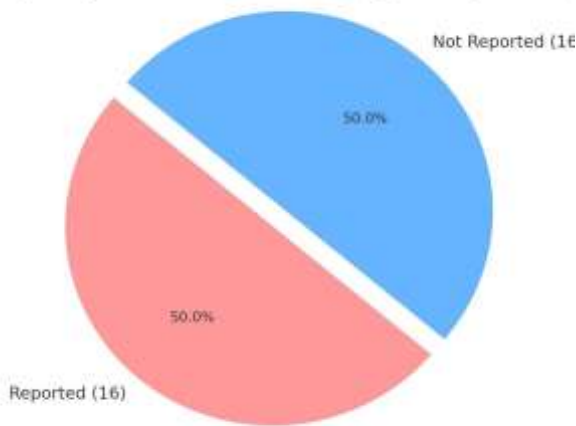


Fig 1.6 Reporting Ratio of the Victims for the Scams (33-39)

Among the 32 victims, exactly half—16 individuals—chose to report the scam to the relevant authorities or platforms. However, the fact that the other 16 did not report shows that barriers still exist, such as hesitation, lack of trust in the system, or uncertainty about how to proceed. When evaluating the type of impact, respondents from this age group described stronger psychological effects compared to financial losses. Many mentioned experiencing stress, anxiety, and a lingering fear of using online platforms.

This analysis highlights that for individuals aged 33 to 38, scams are not just a financial threat—they are deeply personal experiences that can leave lasting psychological effects. It underscores the importance of mental health support, digital literacy programs, and trust-building measures in online spaces for this age group.

Psychological vs Financial Impact (Age Group 33-38)

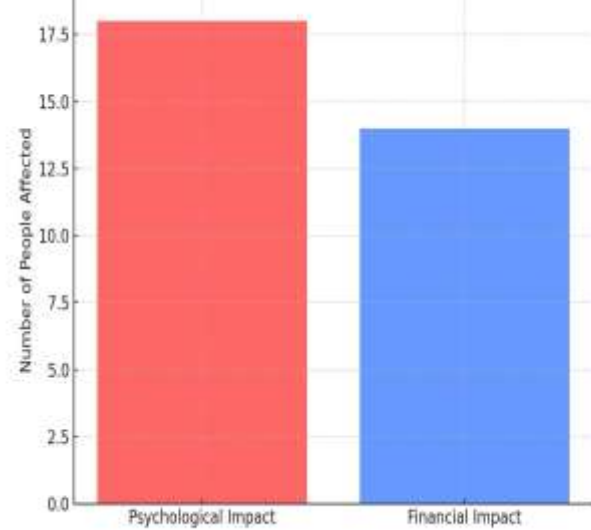


Fig 1.7 Impact comparison of people affected Psychologically and Financially (33-38)

Age group from 39 to 45, in the age group of 39 to 45, the data shows that out of 100 individuals surveyed, only 12 fell victim to social media scams. This indicates a lower incidence of online fraud compared to younger age groups.

Out of the 12 who were scammed, only 5 chose to report the incident to authorities or relevant platforms. This reveals a modest reporting rate, where less than half of the affected individuals took action.

Reporting Ratio of Scam Victims (Age Group 39-45)

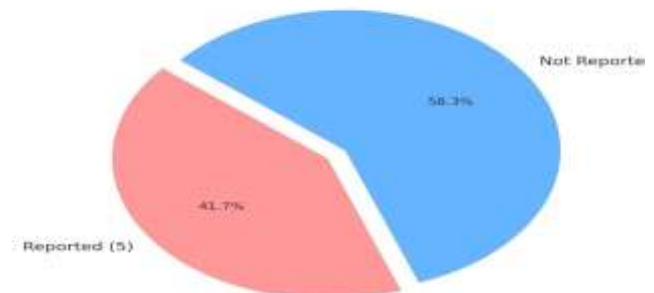


Fig 1.8 Reporting ratio of the victims for the Scams (39-45)

When examining the type of impact, the psychological toll was more pronounced than the financial loss. Many participants shared that the

emotional aftermath—such as embarrassment, anger, and loss of trust—was more distressing than the money lost.

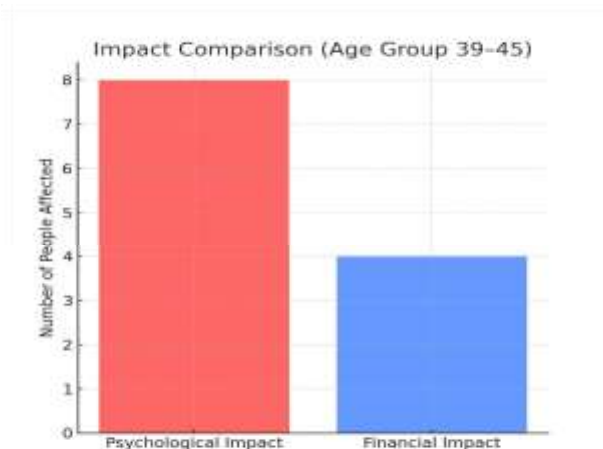


Fig 1.9 Impact comparison of people affected Psychologically and Financially (39-45)

Financial losses in this group were generally lower, possibly due to smaller transaction amounts or a quick realization of the scam before serious damage occurred. This suggests that while this age group may fall for scams less frequently, when it does happen, it leaves a lasting psychological impression.

4. CONCLUSION

This research provides a comprehensive overview of how social media scams affect individuals across various age groups, based on a survey of 100 participants. The study identified not only the prevalence of such scams but also offered valuable insights into how victims respond and cope with them. It became evident that scams are not limited to a specific age group, although certain age ranges are disproportionately affected.

The 18 to 26 age group was found to be the most vulnerable, with a high percentage of individuals having encountered scams. This vulnerability can be attributed to frequent engagement on social media platforms, a greater tendency to trust online content, and limited experience with cyber safety. Despite being the most affected, individuals in this group reported the lowest rate of filing complaints, indicating a lack of awareness or hesitancy in reporting due to embarrassment or fear of judgment.

In the 27 to 32 age group, the victim count was similarly high, with 34% of respondents falling prey to scams. This group showed a slightly improved reporting ratio, but the data still suggested that many individuals suffer in silence. Emotional impacts such as anxiety, guilt, and stress were prominent, with financial loss also being notable in some cases. The findings suggest that individuals in this age group may be lured by scam tactics involving job offers, loans, or investment opportunities, often linked to real-world financial pressures.

For the 33 to 38 age group, although the number of victims was slightly lower at 32%, they showed the highest likelihood of reporting the scam. This indicates a maturing awareness of cybercrime and a willingness to take action. Nevertheless, psychological consequences remained significant, pointing to a growing need for emotional support for victims alongside legal or financial solutions.

In contrast, the 39 to 45 age group displayed the lowest victimization rate, with only 12 individuals out of 100 reporting they had been scammed. This may be due to more cautious behavior or lower exposure to scam-prone online environments. Interestingly, despite the fewer cases, those who did fall victim experienced strong psychological impacts, reinforcing the idea that the emotional toll of scams is not solely dependent on age or frequency but also on the depth of trust breached.

Overall, the findings highlight three critical takeaways: first, the psychological effects of scams are generally more severe than the financial losses; second, many victims do not report the incidents, leading to under-representation in official statistics; and third, younger individuals are particularly at risk, making them a priority target for awareness campaigns. There is a clear need for improved cyber education, easily accessible reporting platforms, and supportive resources tailored for each age group. Empowering individuals to recognize scams and respond appropriately could greatly reduce the growing threat of digital fraud.

REFERENCE

1. Duggan, M., & Smith, A. (2016, January 14). The state of privacy in America. Pew Research Center. <https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/>
2. Chua, A. Y. K., & Banerjee, S. (2015). Understanding online scams: A literature review. Online Information

Review, 39(1), 42–59. <https://doi.org/10.1108/OIR-05-2014-0111/>

3. Whitty, M. T. (2013). The scam baiter: A new type of online vigilantism. *Deviant Behavior*, 34(1), 1–20. <https://doi.org/10.1080/01639625.2012.707502>
4. Button, M., Johnston, L., & Frimpong, K. (2007). Fighting fraud: The case for a national fraud strategy. *Criminal Justice Matters*, 68(1), 20–21. <https://doi.org/10.1080/09627250708553335>
5. McAlaney, J., & Benson, V. (2019). Cybersecurity and social media: Challenges and trends. In V. Benson & J. McAlaney (Eds.), *Cyber influence and cognitive threats* (pp. 123–136). Academic Press.
6. Internet Crime Complaint Center. (2022). Internet crime report 2021. Federal Bureau