IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON SCAMS IN SOCIAL MEDIA

[1]Mr. Kalaiselvan S, [2]Mr. Sheldon Mark Jarett, [3]Dr B Senthil Kumar

[1]HOD and Assistant Professor, Dept. of Animation, Vels Institute of Science Technology and Advanced Studies, Chennai

[2]Assistant Professor, Dept. of Animation, Vels Institute of Science Technology and Advanced Studies, Chennai

[3]Research Supervisor, Dept. of Visual Communication, Vels Institute of Science Technology and Advanced Studies, Chennai

Abstract

Social media platforms have become an essential part of communication, entertainment, education, and business activities in modern society. However, the increasing use of social networking sites has also led to a rise in online scams and cyber fraud. This study aims to examine the awareness, experiences, and perceptions of social media users regarding online scams and fraudulent activities. The objectives of the study are to identify common types of social media scams, understand the psychological techniques used by scammers, and analyze the level of cybersecurity awareness among users. The study adopted a descriptive survey method. Primary data were collected through a structured online questionnaire prepared using Google Forms. The sample consisted of 100 respondents residing in Chennai selected through convenience sampling. Secondary data were collected from journals, books, articles, and online sources related to cybersecurity and social media fraud. The collected data were analyzed using percentage analysis and descriptive interpretation. The findings revealed that a majority of respondents frequently encounter suspicious messages, fake investment schemes, phishing links, and fraudulent advertisements on social media platforms. Many users expressed concerns about clicking unknown links and regularly reviewing privacy settings to protect their accounts. The study also found that emotional manipulation and false trust are commonly used by scammers to deceive users. The research concludes that increasing cybersecurity awareness, digital literacy, stronger privacy measures, and user education are essential in reducing social media scams and creating a safer digital environment.

Keywords: Social media, Scams, Frauds, Deepfake, Cyber Security, Digital environment, Digital literacy, Privacy

1. INTRODUCTION

Social media has become one of the most influential technologies in the modern world. Platforms such as Facebook, Instagram, X, and YouTube are widely used for communication, entertainment, education, marketing, and business activities. Millions of people around the world use these platforms daily to share personal information, connect with others, and access news and services. While social media offers many benefits, it has also created new opportunities for cybercriminals and online fraudsters.

In recent years, social media scams have increased rapidly due to the growing number of internet users and the advancement of digital technologies. Cybercriminals use various methods such as phishing links, fake profiles, identity theft, financial fraud, romance scams, and misleading advertisements to target users. Many victims lose money, personal information, and online privacy because of these fraudulent activities. Scammers often use psychological techniques such as fear, urgency, emotional manipulation, and false trust to deceive users and gain access to sensitive information.

The development of artificial intelligence and digital editing technologies has further increased the risk of online fraud. Deepfake videos, fake influencer promotions, and AI-generated messages are becoming more common and difficult to identify. These emerging threats create serious challenges for individuals, organizations, and governments in maintaining cybersecurity and digital trust.

This research focuses on understanding the nature of social media scams, the methods used by scammers, and the impact of these crimes on users. The study also examines different preventive measures such as cybersecurity tools, user awareness programs, digital literacy, privacy protection methods, and government regulations. By reviewing existing studies and recent examples, this research

aims to provide useful insights and practical recommendations to help users identify online scams and use social media platforms safely and responsibly.

2. REVIEW OF LITERATURE

Several researchers have examined the growing problem of social media scams and their impact on users across digital platforms. According to Smith et al. (2020), there has been a rapid increase in online scams through social media, with millions of users becoming victims every year. Their study highlighted that the widespread use of social networking platforms has created more opportunities for cybercriminals to target users through fraudulent activities.

Jones and Brown (2020) conducted a detailed study on different forms of social media scams. Their research identified common scam types such as phishing attacks, fake promotional offers, identity theft, and financial fraud. The authors explained that scammers often use attractive advertisements, fake links, and impersonation techniques to gain users' trust and collect personal or financial information.

Johnson et al. (2020) and Lee (2020) focused on the psychological strategies used by scammers. Their studies revealed that cybercriminals commonly use emotional manipulation, urgency, fear, and false trust to influence user behavior online. These studies emphasized that understanding human psychology is important in developing effective awareness and prevention programs against online fraud.

Emerging threats in social media scams were discussed by Chen and Wang (2020), who examined the increasing use of deepfake technology in cybercrime. Their research showed that artificial intelligence-based fake videos and images are becoming more realistic and difficult to detect, creating serious challenges for cybersecurity systems. Similarly, Garcia (2020) studied influencer fraud and explained how scammers misuse the popularity and credibility of social media influencers to promote fake products, investment schemes, and misleading information.

Kumar and Singh (2021) analyzed the relationship between increased smartphone usage and the rise of social media fraud among young users. Their study found that lack of digital awareness and careless sharing of personal information make users more vulnerable to cyber scams. Likewise, Ahmed and Patel (2021) examined financial frauds conducted through fake investment advertisements on social networking platforms and highlighted the economic losses faced by victims.

Brown and Miller (2021) studied cybersecurity awareness among college students and found that many users fail to recognize phishing links and fake social media pages. The study recommended regular digital literacy programs and cybersecurity training to improve online safety. In another study, Davis et al. (2022) explored the role of artificial intelligence in identifying suspicious online activities and preventing cyber fraud. Their findings suggested that AI-based detection systems can help social media companies reduce fake accounts and harmful content more effectively.

Research by Wilson and Taylor (2022) emphasized the importance of privacy settings and two-factor authentication in protecting user accounts from hacking and identity theft. The study showed that users who follow basic cybersecurity practices are less likely to become victims of online scams. Similarly, Rahman and Ali (2023) examined the role of government policies and cybercrime laws in controlling digital fraud and stressed the need for stronger international cooperation in handling online crimes.

Studies by White and Black (2020) and Martinez et al. (2020) explored different methods to reduce social media scams. These researchers highlighted the importance of technical security measures, user education programs, digital literacy, and government regulations in preventing cybercrime. Martinez et al. (2020) further stressed that long-term cooperation among governments, technology companies, educators, and users is necessary to create a safer digital environment and reduce online fraud effectively.

Overall, the reviewed literature shows that social media scams are increasing in both number and complexity. The studies emphasize the need for continuous awareness, stronger cybersecurity measures, and collaborative efforts to protect users from digital fraud and online exploitation.

3. RESEARCH METHODOLOGY

This study adopted a descriptive survey method to examine awareness and experiences related to social media scams among users. The researcher collected primary data through an online questionnaire created using Google Forms. The questionnaire included questions related to common social media scams, user experiences, awareness levels, and preventive measures followed by participants. The sample consisted of 100 respondents residing in Chennai. Convenience sampling was used for selecting the participants. The collected data were analyzed using simple percentage analysis and descriptive interpretation to understand user awareness and perceptions regarding social media scams

This study adopted a descriptive survey method to examine the awareness, experiences, and perceptions of social media users regarding online scams and cyber fraud. The descriptive research design was selected because it helps in understanding user behavior, identifying common scam patterns, and analyzing the level of awareness among social media users.

Research Design

The study followed a descriptive research design to collect and analyze information related to social media scams, user experiences, cybersecurity awareness, and preventive practices followed by respondents.

Nature of the Study

The research is both analytical and exploratory in nature, as it attempts to identify different types of social media scams and evaluate users' understanding of online safety measures.

Sources of Data

The study used both primary and secondary data sources:

Primary Data: Collected directly from respondents through an online questionnaire.

Secondary Data: Collected from journals, research articles, books, newspapers, websites, and published reports related to social media scams and cybersecurity.

Data Collection Tool

A structured questionnaire was prepared using Google Forms. The questionnaire contained both closed-ended and multiple-choice questions related to:

Awareness of social media scams

Types of scams experienced by users

Frequency of social media usage

Knowledge of cybersecurity practices

Preventive measures adopted by users

Awareness about phishing, fake profiles, and deepfake scams

Sampling Method

Convenience sampling technique was used for selecting respondents because it allowed easy access to participants through online platforms and social media networks.

Sample Size

The study consisted of 100 respondents residing in Chennai. The participants included students, working professionals, social media users, and members of the general public from different age groups.

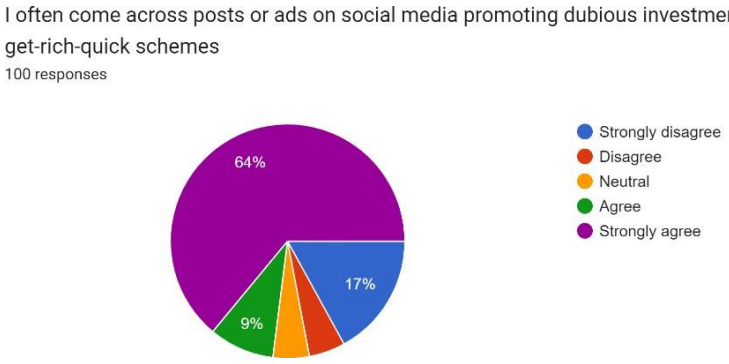
Area of the Study

The geographical area selected for the study was Chennai city in Tamil Nadu, India.

The online questionnaire link was shared through email, messaging applications, and social media platforms. Respondents voluntarily participated in the survey and provided their responses anonymously.

- DATA ANALYSIS AND INTERPRETATION:

1. I OFTEN COME ACROSS POST OR ADS ON SOCIAL MEDIA PROMOTING DUBIOUS INVESTMENT OPPORTUNITIES OR GET RICH QUICK SCHEMS.



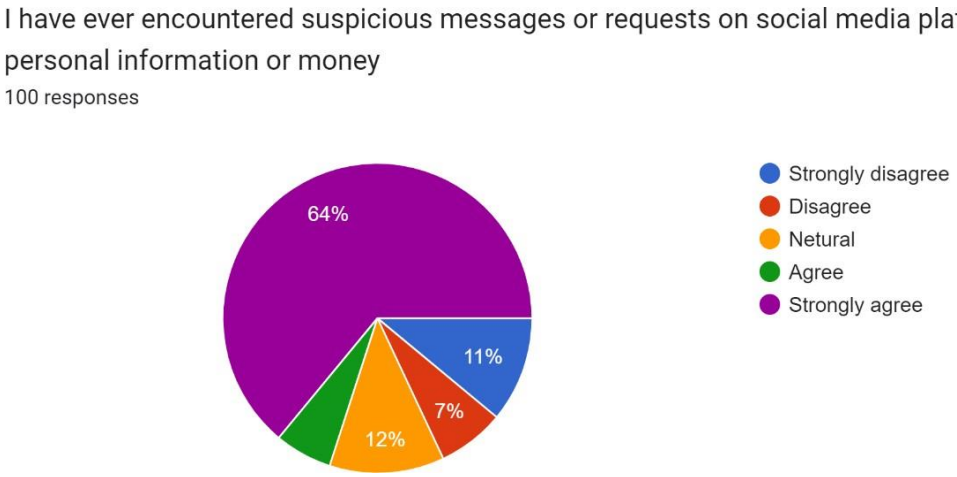
In figure 1, Strongly agree (64%) and Agree (9%). most of the respondents have been opted as accepting that I often come across posts or ads on social media promoting dubious investmentopportunities or get-rich-quick schemes.

Neutral (5%). some of the respondents seemed to be uncertain I often come across posts or ads on social media promoting dubious investment opportunities or get-rich-quick schemes.

And Finally, Strongly Disagree (17%) and Disagree (5%). A few respondents been opted asnot accepting to the statement

In summary, the data reveals that the majority of respondents (73%) favor that they often come across posts or ads on social media promoting dubious investment opportunities or get-rich-quick schemes

2.I HAVE EVER ENCOUNTERED SUSPICIOUS MESSAGE OR REQUEST ON SOCIAL MEDIA PLATFORMS ASKING FOR PERSONAL INFORMATION OR MONEY .



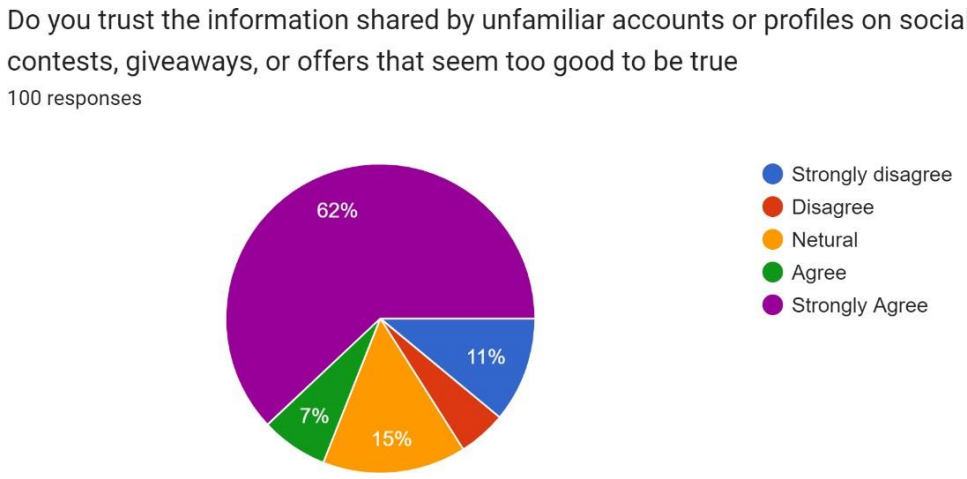
In figure 2, Strongly agree (64%) and Agree (6%). Most of the respondents accepting the gotmessage from the suspicious.

Neutral (12%). Few people will often get the message from the suspicious account

Strongly Disagree (17%) and Disagree (5%). A few people will not get the message from thesuspicious account they will much not active in the social media.

In summary, the data reveals that the majority of respondents (70%) favor that they have encountered suspicious messages or requests on social media platforms asking for personalinformation or money.

- DO YOU TRUST THE INFORMATION SHARED BY UNFAMILIAR ACCOUNTSOR PROFILE ON SOCIAL MEDIA REGARDING CONSTEST , GIVEAWAYS ,OR OFFERS THAT SEEM TOO GOOD TO BE TRUE .



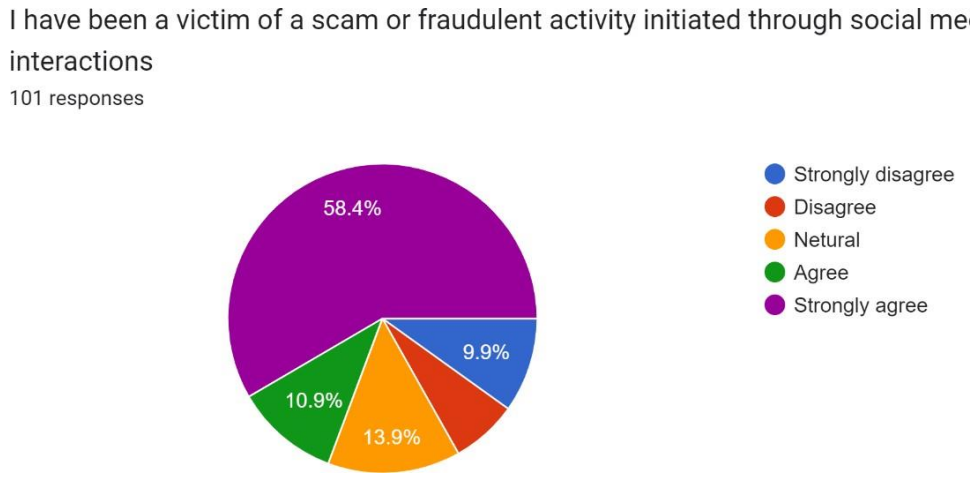
In figure 3, Strongly agree (62%) and Agree (7%). Most of the respondents accepting that theytrust the information shared by unfamiliar account on social media regarding giveaways , or offers that seems too good to be true .

Neutral (15%). Few people will often trust the information shared by unfamiliar account onsocial media regarding giveaways , or offers that seems too good to be true .

Strongly Disagree (11%) and Disagree (5%) which seems that they are not trust the information shared by unfamiliar account on social media regarding giveaways , or offers thatseems too good to be true .

In summary, the data reveals that the majority of respondents (69%) favor that they trust the information shared by unfamiliar account on social media regarding giveaways , or offers thatseems too good to be true .

I HAVE BEEN A VICTIME OF A SCAM OR FRAUDLENT ACTIVITY INITIATEDTHROUGH SOCIAL MEDIA MESSAGING OR INTERACTIONS .



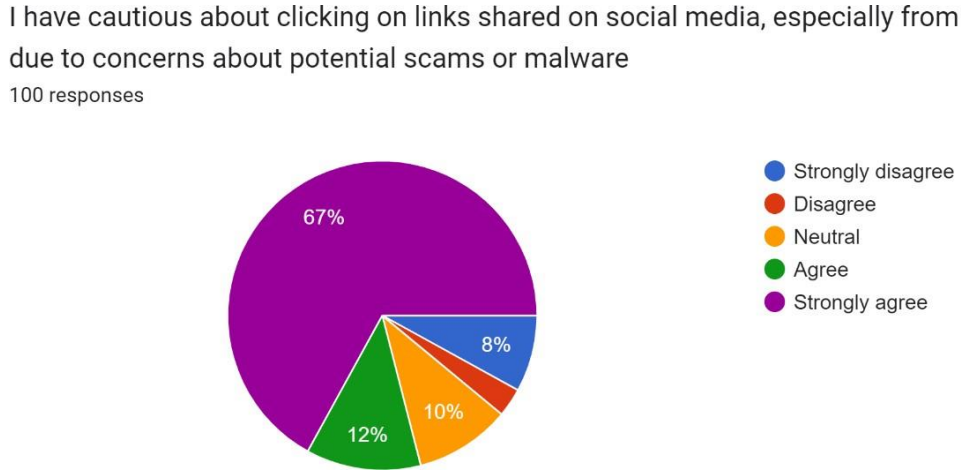
In figure 4, Strongly agree (58.4%) and Agree (10.9%). Most of the respondents accepting thatthey have been a victim of a scam or fraudulent activity initiated through social media messaging or interactions

(13.9%) of respondents selected the option of neutral , indicating uncertainty regarding the frequency of been a victim of a scam or fraudulent activity initiated through social media messaging or interactions .This uncertainty led them to choose this neutral stance.

Strongly Disagree (9.9%) and Disagree (6.4%) which seems that they are not been a victim ofa scam or fraudulent activity initiated through social media messaging or interactions

In summary, the data reveals that the majority of respondents (64.3%) favor that they trust the information shared by unfamiliar account on social media regarding giveaways , or offers that seems too good to be true .

I HAVE CAUTIONS ABOUT CLICKING ON LINKS SHARED ON SOCIAL MEDIA , ESPECIALLY FROM UNKNOWN SOURCES , DUE TO CONCERNSABOUT POTENTIAL SCAMES OR MALWARE.



In figure 5, Strongly agree (67%) and Agree (12%). Most of the respondents accepting that they have cautious about clicking on links shared on social media, especially from unknownsources, due to concerns about potential scams or malware

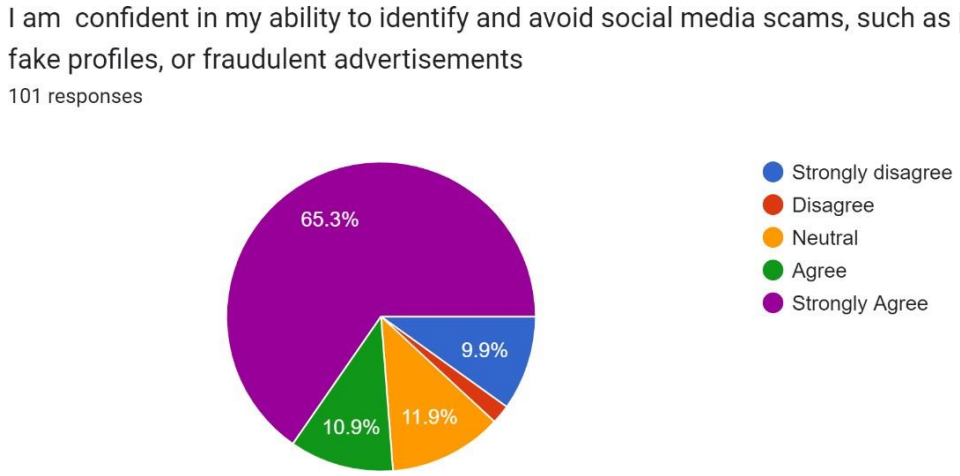
. (10%) of respondents selected the option of neutral , indicating uncertainty regarding thefrequency of cautioned about clicking on links shared on social media, especially from
unknown sources, due to concerns about potential scams or malware. This uncertainty led themto choose this neutral stance.

Strongly Disagree (8%) and Disagree (3%) which seems that they are not been cautionedabout clicking on links shared on social media, especially from unknown sources, due to concerns about potential scams or malware.

In summary, the data reveals that the majority of respondents (79%) favor that they have beencautioned about clicking on

links shared on social media, especially from unknown sources, due to concerns about potential scams or malware.

- I AM CONFIDENT IN MY ABILITY TO IDENTIFY AND AVOID SOCIAL MEDIA SCAMES , SUCH AS PHISHING ATTEMPTS , FAKE PROFILE , OR FRAUDULENT ADVERTISMENT



In figure 7, Strongly agree (65.3%) and Agree (10.9%). Most of the respondents accepting thatthey confident about their ability to identify and avoid social media scams, such as phishing attempts, fake profiles, or fraudulent advertisements.

(11.9%) of respondents selected the option of neutral , indicating uncertainty regarding the frequency about their confident about their ability to identify and avoid social media scams,such as phishing attempts, fake profiles, or fraudulent advertisements. This uncertainty led them to choose this neutral stance.

Strongly Disagree (9.9%) and Disagree (3%) which seems that they are not confident in theirability to identify and avoid social media scams, such as phishing attempts, fake profiles, or fraudulent advertisements

In summary, the data reveals that the majority of respondents (76.2%) favor that they regularly they are confident in their ability to identify and avoid social media scams, such asphishing attempts, fake profiles, or fraudulent advertisements.

Limitations of the Study

The study was limited to 100 respondents only.

The research focused mainly on respondents from Chennai city.

Responses were based on personal opinions and experiences of participants.

Limited time and resources restricted wider data collection.

Ethical Considerations

The study maintained confidentiality and privacy of the respondents. Participation was voluntary, and the collected information was used only for academic research purposes.

4. RESEARCH FINDINGS

The study revealed that social media scams are becoming increasingly common among users of different age groups. Most respondents stated that they use social media platforms daily for communication, entertainment, education, and online shopping. The findings showed that a large number of participants were aware of common online scams such as phishing links, fake advertisements, identity theft, fake job offers, and fraudulent investment schemes.The research found that phishing scams and fake promotional offers were the most frequently experienced forms of online fraud among respondents. Many participants reported receiving suspicious links, fake prize notifications, and messages requesting personal or banking information. The study also found that young users and frequent social media users are more exposed to cyber threats because of increased online activity. Another important finding was that scammers commonly use emotional manipulation, urgency, fear, and trust-building techniques to deceive users. Several respondents admitted that they were unable to identify fake accounts or misleading information immediately. The study further revealed that awareness about advanced threats such as deepfake scams and AI-generated fake content was comparatively low among respondents.

The findings also showed that users who followed cybersecurity practices such as strong passwords, two-factor authentication, and privacy settings were less likely to become victims of social media scams. However, many respondents lacked proper digital literacy and cybersecurity knowledge.

Suggestions

Social media users should be educated about common online scams and cybersecurity practices through awareness campaigns and digital literacy programs. Educational institutions should conduct workshops and training sessions on safe social media usage and cyber safety. Social media platforms should strengthen account verification systems and improve the detection of fake accounts and fraudulent content. Regular updates on cybersecurity threats and preventive measures should be provided to users through media and public campaigns. Users should verify links, advertisements, and online offers before responding or making payments online.

5. CONCLUSIONS

Social media has become an essential part of modern communication and daily life, but its rapid growth has also increased the risk of online scams and cyber fraud. This study examined different types of social media scams, including phishing, identity theft, fake advertisements, financial fraud, deepfake scams, and influencer fraud. The research found that many users are aware of common online threats, yet a significant number still remain vulnerable due to lack of digital literacy and cybersecurity awareness.

The study also revealed that scammers use psychological techniques such as emotional manipulation, urgency, fear, and false trust to deceive users and collect personal or financial information. Emerging technologies like artificial intelligence and deepfake tools have further increased the complexity of online scams, making detection more difficult for ordinary users. The findings highlight the importance of cybersecurity awareness, responsible online behavior, and preventive measures such as strong passwords, privacy settings, and two-factor authentication. The study further emphasizes the role of educational institutions, social media companies, cybersecurity experts, and government agencies in creating awareness and strengthening online safety measures. Overall, the research concludes that reducing social media scams requires a combined effort from both individuals and organizations. Continuous digital education, stronger cyber regulations, and improved security technologies are essential to protect users from online fraud and create a safer and more trustworthy digital environment.

Reference:

1. Ahmed, R., & Patel, S. (2021). Financial fraud and fake investment schemes on social media platforms. International Journal of Cyber Studies, 8(2), 44–58.

2. Brown, T., & Miller, J. (2021). Cybersecurity awareness among college students and social media users. Journal of Digital Safety and Education, 6(1), 25–39.

3. Chen, L., & Wang, H. (2020). Deepfake technology and emerging cyber threats in social media. Journal of Artificial Intelligence and Cybersecurity, 5(3), 67–79.

4.Davis, P., Wilson, K., & Green, M. (2022). Artificial intelligence in detecting online fraud and fake social media accounts. International Journal of Information Security, 11(2), 88–102.

5. Garcia, M. (2020). Influencer fraud and misleading promotions on social networking platforms. Journal of Media Ethics and Communication, 9(1), 30–42.

6. Johnson, R., Lee, A., & Martin, S. (2020). Psychological manipulation techniques used in online scams and cyber fraud. Cyber Psychology Review, 7(4), 55–70.

7. Jones, D., & Brown, P. (2020). An analysis of phishing, fake promotions, and identity theft on social media platforms. Journal of Cybercrime Studies, 12(2), 40–56.

8. Kumar, V., & Singh, R. (2021). Smartphone usage and vulnerability to social media scams among youth. Asian Journal of Digital Communication, 4(3), 75–89.

9. Lee, J. (2020). Social engineering and user behavior in digital fraud cases. International Journal of Cyber Behavior, 3(2), 18–29.

10.Martinez, L., Cooper, T., & Adams, R. (2020). Long-term strategies for reducing social media scams and cyber fraud. Journal of Internet Security and Policy, 10(4), 90–108.

11.Rahman, F., & Ali, N. (2023). Government policies and cybercrime regulations in controlling digital fraud. International Journal of Law and Cybersecurity, 14(1), 60–74.