IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"The Rise Of Social Media-Driven Stock Market Investment Scams: Analysing Financial Fraud In The Age Of Social Media"

Kale Santosh Subhash , Sandhya M. ** , Toge Ashwini Uddhav***,Toge Kiran***

*Assistant Professor, Shikshan Maharshi Guruvarya R.G. Shinde Mahavidyalaya Paranda Dist: Dharashiv, Maharastra

** Assistant Professor, Government First Grade College Kaup Udupi, Karnataka

***Research Scholar

ABSTRACT:

Social media has become a powerful tool for communication and information sharing in the age of technology, particularly when it comes to stock market investment. But this development has also opened the door for a rise in investment frauds driven by social media. This study explores how scammers use social media's reach, confidentiality, and speed to share information in order to commit financial frauds.

This study analyses prominent scam techniques, such as pump-and-dump schemes, fake recommendations, fraudulent investment platforms, phishing, false promises of high returns, and misrepresenting recognized financial institutions. Using a mixed-methods approach that includes **case study analysis** of reported scams in India and **social media group interaction analysis**, the study finds common scammer tactics include phishing, Ponzi schemes, and urgency-based manipulation. The findings highlights warning signs and psychological manipulation techniques used to lure victims, emphasizing the need for awareness and enhanced regulatory efforts to protect investors.

KEYWORD: Social Media, Stock Market, Investment Scams, Investor Awareness, Investor Protection,Financial Fraud, Cyber security, Fraud Detection Technique, Financial Regulation.

INTRODUCTION:

Social media has made it easier for people to invest in the stock market, but it has also created new opportunities for scams. These scams use social media's reach and anonymity to trick people into investing in fake or risky opportunities. This can lead to big financial losses for the victims. Scammers use a variety of tactics to cheat investors. These include creating fake profiles, spreading false information, and promising high returns. It can be hard to spot these scams because they often look legitimate.

These scams are a big problem because they can hurt people's finances and trust in the financial system. It's also hard for regulators to keep up with the scammers because social media is constantly changing. There are a few things that can be done to make social media investing safer. This includes better laws, more education for the public, and new tools to find scams. By working together, social media companies, financial institutions, and regulators can make it harder for scammers to steal people's money.

Scammers use social media ads to promote fake financial investments, often impersonating legitimate companies like Legal & General. They create convincing but fraudulent ads that promise guaranteed high returns, directing victims to fake websites that look credible at first glance. Scammers may contact victims via messages, emails, or calls, posing as real company employees and using fake documents to support their claims. Victims are lured into transferring money, believing they are making legitimate investments.

For stock investment they promise through their platform like real platform use current company names registration number. Use Methods and Tactics of buy Upper Circuit stock, Discounted price for Subscribe IPO, IPO Subscription, Block Dealing, Institutional Account, Primary market deal for investment through their Fake platform.

REVIEW OF LITERATURE:

The rise of social media-driven stock market investment scams is a growing concern, with various studies highlighting the use of social media in perpetrating financial fraud. Mirtaheri (2019) and Renault (2017) both identify the prevalence of pump-and-dump schemes, where false hype is spread to artificially inflate the value of a stock or crypto currency. Dong (2016, 2018) further demonstrate the leading effect of social media in detecting fraudulent behavior, with the latter proposing a framework that leverages unstructured data from financial social media platforms to assess the risk of corporate fraud. These studies collectively underscore the need for enhanced monitoring and regulation of social media platforms to combat the spread of financial fraud.

Social media has become a breeding ground for stock market manipulation and investment scams, with fraudsters using platforms to inflate stock prices through pump-and-dump schemes (Renault, 2017). This is particularly concerning for students, who are more susceptible to falling for these scams due to their reliance on social media for information (Ramli, 2023). The situation is further exacerbated by the use of cyber-attacks to disseminate false information, leading to significant market fluctuations (Mantere, 2013). These findings underscore the need for increased vigilance and regulation in the use of social media for stock market activities.

Research has identified several red flags in social media group communication, including unsolicited messages and offers, promises of guaranteed profits, pressure and urgency, emotional manipulation, requests for personal and financial information, and suspicious links and apps (Tsikerdekis, 2014; Briscoe, 2014; Williams, 2017; Kogan, 2021). These red flags are often used in online deception for illicit financial gain and reputation damage (Tsikerdekis, 2014). They can be detected through linguistic cues to deception, with machine learning classifiers achieving high accuracy in identifying them (Briscoe, 2014). The risks associated with these red flags are categorized into five risk categories, emphasizing the need for effective risk management (Williams, 2017). Furthermore, the manipulation of financial news on social media can have significant indirect consequences, such as reduced trading activity and price volatility (Kogan, 2021).

STATEMENT OF PROBLEM:

Social media has changed how people invest in the stock market, making it easier and more accessible. However, this convenience has led to an increase in investment scams. Scammers use the wide reach, anonymity, and fast information spread on social media to trick people into losing money. They create fake investment platforms, get people to share personal information, and make false promises of high returns.

The results are severe. People lose a lot of money and face financial ruin. They also experience stress, and anxiety, and lose trust in the financial system. These scams also damage confidence in real investment opportunities, hurting the overall market. Regulators find it hard to catch and punish scammers because of the constantly changing nature of social media and the anonymity it provides.

To solve this problem, we need to strengthen laws, run public awareness campaigns, and develop better tools to detect scams. Social media companies, financial institutions, and regulators must work together. This includes better monitoring, educating the public about scams, and creating technology to find and stop fraud.

By studying these scams and their effects, we can protect investors and keep the financial system trustworthy. This research will look at these scams, finds common scammer tactics, and suggest ways to prevent these financial crimes highlighting warning signs and psychological manipulation techniques used to lure victims, emphasizing the need for awareness and enhanced regulatory efforts to protect investors

RESEARCH METHODOLOGY:

This study employs a mixed-methods approach Qualitative data used. **Case studies** of reported scams are analyzed to identify common tactics like fake investment platforms and phishing. **Social media group analysis** examines interactions to uncover trust-building, urgency creation, and manipulation techniques. Qualitative data from case studies and social media groups is examined through content and narrative analysis.

This study uses a mixed-methods approach, combining **case study analysis** and **social media group interaction** analysis to explore tactics used in social media-driven stock market scams. Fourteen registered scam cases in India were analysed to identify common techniques, including pump-and-dump schemes, phishing, Ponzi schemes, and impersonation of financial institutions and interactions in 20 public and private social media groups were examined to uncover manipulation tactics, such as urgency creation and trust-building.

Content and Narrative Analyses were applied to identify recurring patterns and psychological strategies, which revealed common warning signs like unsolicited messages, guaranteed profits, and limited-time offers. While the data focuses on accessible cases and public social media interactions, it offers valuable insights into scam detection and investor protection.

THE OBJECTIVE OF THE STUDY: The primary objective of this study is to analyse the mechanisms through which social media facilitates stock market investment scams. The study aims to:

1. Identify and analyse the common tactics used by scammers on social media platforms.
2. Highlight warning signs and psychological manipulation methods.

DATA ANALYSIS AND INTERPRETATION: Data was analysed in two different ways 1) Analysis of case Study 2) Analysis of Social Media Group

1) ANALYSIS OF CASE STUDY: After analysing 14 case studies some Common Methods and Tactics used by Scammers are as follows:

- ***Fake Investment Platforms*:** Fraudsters create convincing, professional-looking websites and apps that mimic legitimate financial institutions. They build fancy websites and apps that look like real investment places. They might even copy real companies' names to make them seem more believable.
- ***Tricking You Out of Information*:** Scammers often use social engineering techniques, such as phishing emails and messages, to gain the trust of victims Scammers pretend to be important financial people to gain your trust. They might use emails, calls, or messages to get your personal info. Phishing: Fake emails or messages that seem real try to get you to enter info on fake websites. Vishing: Phone calls where someone pretends to be a financial advisor to get your info or money.
- ***Promising Crazy Returns:*** They'll promise you way more money than you could normally make to get you to invest. They attract victims by promising unrealistic returns on investments, often much higher than what is available through genuine investment channels
- ***Ponzi Schemes:*** They pay early investors with money from later investors, making it seem profitable until it runs out.
- ***Spreading Lies on Social Media:*** They use social media and messaging apps to reach a lot of people quickly and cheaply. They'll share links to their fake investment platforms.
- ***Pretending to Be Someone Else*:** Scammers act like real banks, financial advisors, or investment companies. They use official-looking documents to trick you.
- ***Pressuring You to Invest:*** They'll call you out of the blue with "exclusive" investment offers. This creates a fake sense of urgency so you don't do your research before investing.
- ***Making You Pay Upfront*:** They'll promise big returns if you give them money first. Once you pay, they disappear with your cash.

- ***Red Flags Identified:*** Red flags identified in case studies include promises of guaranteed high returns with low risk, unsolicited messages from unknown contacts, and pressure tactics such as limited-time offers or urgency to invest. Scammers often request money transfers to personal accounts or through unofficial channels and use deep fake videos and images of reputed individuals to lend credibility

2) ANALYSIS OF SOCIAL MEDIA GROUP: After analysing 20 Social Media Group communication show several Common Methods and Tactics use commonly associated with investment scams scammer Building Trust and Familiarity, Creating a Sense of Urgency, Promising High Returns, Manipulating and Guilt, Encouraging Larger Investments, Leveraging Authority Figures, Addressing Concerns and Offering Help. Follows are the Details:

- ***Greeting and Politeness:*** The scammer consistently uses polite greetings and refers to the victim in a friendly manner, such as "Good morning," "Good evening," "I hope you had a pleasant weekend. "And using terms like "dear" and "darling" to build rapport and trust.
- ***Persistent Contact:*** Frequent check-ins and updates to maintain constant communication and keep the victim engaged.
- ***Limited-Time Opportunities:*** Repeatedly emphasizes urgent trading opportunities, e.g., "….. will lead everyone to trade " and "The opportunity to make money won't always be there.". Emphasizes urgency and limited-time offers, e.g., "Do you need to reserve operations for you?" and "tomorrow there will be a 78% discount rate OTC, buy to make 22% profit."
- ***Pressure to Act Quickly:*** The scammer pressures the victim to convert funds and participate in trades quickly to not miss out.
- ***High-Profit Projections:*** The scammer promises high returns with specific figures, such as such as "an expected return of 15%-30%" daily and "800% profit in three months." which are typically unrealistic and designed to entice the victim.
- ***Fear of Missing Out (FOMO):*** Statements like "I hope you don't miss your next chance to make money" and "You will be eliminated" create a fear of missing out on lucrative opportunities.
- ***Guilt and Criticism:*** The scammer criticizes the victim's hesitance, saying things like "Give you the opportunity to make money you won't make money" and "I don't understand what you're thinking."
- ***Gradual Increase in Investment Requests:*** Initially discusses smaller amounts and gradually pressures the victim to invest more significant sums
- ***Funds and Profit Management***: The scammer claims to follow the "EG plan" to make the investment strategy sound legitimate and professional.
- ***Use of Authorised person name***: Refers to an authoritative figure Name leading the trading group, which adds a false sense of legitimacy and expertise to the scam.
- ***Solution-Oriented Approach***: When the victim expresses concerns, the scammer provides solutions, such as "Please contact the account manager" and "If you buy stocks as they suggested, you will make a profit of 20%."

- ***Key Red Flags Identified:*** Red flags identified in Social Media Group communication include Unsolicited Messages and Offers, Promises of Guaranteed Profits, Pressure and Urgency, and Emotional Manipulation, Requests for Personal and Financial Information ,Suspicious Links and Apps.The following are details:
  - Initial unsolicited messages about trading opportunities and rewards.
  - Messages from an unknown contact offer high returns with minimal effort.
  - Initiating contact without prior engagement, e.g., “welcome to the …….. Group.”
  - Unrealistic promises of consistent and high returns in a short period. Unrealistic guarantees, e.g., “Wealth Doubling Plan” and “expected return rate of 30%.”
  - Statements claiming 100 percent winning percentage and other too-good-to-be-true claims.
  - Consistent pressure to make quick decisions and invest more funds. Consistent urgency to act quickly without proper research, e.g., “buy to make 20% profit.”
  - Creating a sense of urgency and fear of missing out on high profits.
  - Asking about the amount of money available for investment
  - Using guilt and fear tactics to manipulate the victim into complying with demands.
  - Persistent messaging despite the victim's hesitations and refusals.
  - Directing to download potentially harmful software, e.g., “download the APP first.”

FINDING:

The study reveals that social media-driven investment scams are increasingly prevalent, with scammers using sophisticated techniques to deceive investors. Key tactics include creating fake investment platforms, phishing for personal information, and making unrealistic promises of high returns to lure victims. Social engineering is heavily utilized, with scammers building trust through friendly communication, leveraging authority figures, and creating urgency with limited-time offers. Psychological manipulation, such as guilt-tripping hesitant investors and instilling fear of missing out (FOMO), is common, encouraging impulsive decisions.

Key red flags include unsolicited communication, guaranteed profits with low risk, high-pressure tactics, and requests for sensitive information. The study emphasizes the need for increased awareness and stronger regulations to address these scams. By educating the public on recognizing warning signs and implementing stricter oversight of social media investment ads, potential scams can be more effectively identified and prevented.

The findings underscore that collaboration between social media platforms, financial institutions, and regulatory agencies is crucial to combat this issue. Such measures will not only help safeguard individual investors but also maintain public trust in financial markets amidst the evolving digital landscape.

CONCLUSIONS:

This research analyse how scammers operate to manipulate and defraud individuals through social media and messaging platforms. It is essential to remain vigilant, and sceptical of unsolicited investment offers, and avoid sharing personal or financial information with unknown contacts. If you suspect fraudulent activity, report it to the relevant authorities and the platform involved.

The analysis reveals a classic investment scam using trust-building, high returns, urgency, and manipulation to lure victims. The scammer's persistence and attempts to discredit legitimate advice, coupled with the push towards using dubious platforms, highlight significant red flags.

RECOMMENDATIONS: following are the recommendation divided in Investors, Regulator, Social media Platform

1. Recommendations for Investors:

- *Avoid Engagement:* Refrain from responding to unsolicited investment offers, which are often scams.
- *Verify Investment Sources:* Independently verify the legitimacy of any investment offers and individuals promoting them.
- *Educate Yourself:* Regularly update your knowledge on common scam tactics and ways to protect yourself.
- *Report Suspicious Activity*: Immediately report suspicious offers, messages, or profiles to the platform used and relevant authorities.

2. Recommendations for Regulators:

- *Enhance Monitoring: Increase monitoring of social media platforms to detect fraudulent activities and scam profiles.*
- *Strengthen Regulations: Develop and enforce stricter policies targeting social media-based financial scams.*
- *Public Awareness Campaigns: Run campaigns to educate the public on identifying scams and avoiding investment fraud.*
- *Encourage Reporting Channels: Simplify reporting processes for individuals to report suspected scams easily.*

3. Recommendations for Social Media Platforms:

- *Strengthen Verification: Implement more robust verification processes for accounts promoting financial services or investments.*
- *Deploy Scam Detection Tools: Use AI and machine learning to identify and block scam-related content and profiles.*
- *Increase Transparency: Educate users on spotting fake profiles and scams, providing clear warnings on investment risks.*
- *Collaborate with Regulators: Work with regulatory bodies to develop unified strategies for scam prevention and quick response to reported cases.*

REFERENCES:

1. National Institute of Securities Markets. (n.d.). Beware of investment scams. NISM
2. Times of India. (2024). A resident of Kolkata lost Rs 20 lakh in an online investment. Times of India
3. Indian Express. (2024). Mumbai stock market investment scam on WhatsApp. Indian Express
4. Hindustan Times. (2024). How fraudsters pull off stock market investment scams: A step-by-step guide from Mumbai police. Hindustan Times
5. Forbes. (2024). Financial scams in India. Forbes
6. India Today. (2024). Bengaluru businessman loses Rs 5.2 crore to cyber crooks in stock market scam. India Today
7. Times of India. (2024). Get rich quick schemes? Times of India
8. The Hindu. (2024). T.N. Cyber Crime issues advisory on new investment scam. The Hindu
9. Economic Times. (2024). WhatsApp investing scams: Red flags to watch out for. Economic Times
10. NDTV. (2024). Common financial frauds in India: How to stay safe. NDTV
11. Indian Express. (2024). 'Epidemic' of online share trading frauds: In 2 months, 110 people in Pune lose Rs 18 crore. Indian Express
12. Deccan Herald. (2024). Bengaluru realtor falls for Rs 1.30 crore 'JP Morgan' investment scam. [Deccan Herald](https://www.deccanherald.com/india/karnataka/bengaluru/bengaluru-realtor-falls
13. News18. (2024). "Alarming Surge in Stock Market Investment Scams: Social Media Accounts Under Scanner." News18
14. Economic Times. (2024). "Stock Market Fraud via WhatsApp, Facebook, Telegram: Two Investors Lost Over Rs 3 Crore. How to Identify Scam and Protect Yourself." Economic Times.
15. Times of India. (2023, December 2). Digital pandemic: 266 stock market investment scams in 4 months. The Times of India.
16. Dong, J. (2016). "The Role of Social Media in Financial Fraud Detection." Journal of Financial Crime, 23(4), 123-139.
17. Dong, J. (2018). "A Framework for Detecting Corporate Fraud Using Social Media Data." International Journal of Accounting Information Systems, 29, 45-60.
18. Mirtaheri, S. (2019). "Social Media and Stock Market Scams: The Case of Pump-and-Dump Schemes." Financial Markets and Portfolio Management, 33(2), 201-219.
19. Renault, T. (2017). "The Impact of Social Media on Financial Markets: Evidence from Pump-and-Dump Schemes." Review of Finance, 21(3), 1029-1065.
20. Mantere, M. (2013). "Cyberattacks and the Dissemination of False Information in Financial Markets." Journal of Cybersecurity and Information Systems, 5(2), 150-165.
21. Ramli, R. (2023). "Susceptibility of Students to Social Media-Driven Investment Scams." Journal of Financial Education, 39(1), 58-72.
22. Briscoe, E. (2014). "Linguistic Cues to Deception and Their Use in Machine Learning Classifiers." Journal of Computational Linguistics, 40(4), 759-772.

23. Kogan, S. (2021). "The Impact of Manipulated Financial News on Social Media." Journal of Financial Markets, 24(2), 345-368.
24. Tsikerdekis, M. (2014). "Online Deception in Social Media for Financial Gain and Reputation Damage." Cyberpsychology, Behavior, and Social Networking, 17(3), 165-171.
25. Williams, L. (2017). "Risk Management of Social Media-Driven Financial Fraud." Journal of Financial Regulation and Compliance, 25(1), 112-127.
26. Legal & General. (2023). How to Avoid Investment Scams on Social Media. Legal & General
27. Kale Santosh Subhash,Toge Ashwini Uddhav,Dr B.N.Devkate, **"INVESTOR AWARENESS AND BEHAVIOR TOWARDS FINANCIAL ASSETS: A STUDY IN DHARASHIV DISTRICT (M.H)"**, International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.12, Issue 5, pp.i36-i51, May 2024, Available at :http://www.ijcrt.org/papers/IJCRT2405875.pdf
28. Kale, Santosh Subhash, Ankush G. Padale, and Ashwini Uddhav ,Toge. "Women Risk Fond Or Averse? A Study Of Women Investors Behaviour In Indian Stock Market."
29. Devkate, Balaji N., and Ashwini Uddhav Toge. "The Study Of Different Factors Which Affect Investment Decision Of Investors In Financial Asset."
30. Bhosle, P., and Santosh Kale. "The Study Of Factors That Affect Investment Of Individual In The Capital Market." *IRJMS-INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY* 4.4 (2018): 1-4.
31. Kale, Santosh, and Mohite Rajiv. "Study The Profile Of Salaried Investors Of Financial Assets With Special Reference To Osmanabad District." *DAMA International-International Science Journal* 7 (2020).
32. Kale, Santosh Subhash, and P. T. Bhosle. "A STUDY OF INDIVIDUAL INVESTORS PROFILE WITH SPECIAL REFERENCE TO MAHARASHTRA STATE."
33. Kale, Santosh Subhash. "A STUDY OF INVESTORS BEHAVIOUR IN CAPITAL MARKET OF MAHARASHTRA STATE." (2021).
34. Kale, Santosh, and Mohite Rajiv. "A Study Of Investors Attitude Towards A Unit Linked Insurance Plan (Ulip)." *CHINMAY PUBLICATION* (2014): 369-371.
35. Mirtaheri, S., et al. (2019). "Identifying and Characterizing Cryptocurrency Manipulation Schemes." Proceedings of the Web Conference 2019.
36. Dong, Y., Wang, X., & Zhang, P. (2018). "Combating Fraud in Financial Markets with Unstructured Data: A Text Mining Approach." Information Systems Frontiers, 20(5), 1027-1040.
37. Tsikerdekis, M., & Zeadally, S. (2014). "Online Deception in Social Media." Communications of the ACM, 57(9), 72-80.
38. Kogan, S., et al. (2021). "The Influence of Social Media on Financial Fraud: Evidence from Fake Investment Scams." Journal of Financial Markets, 54, 100579.
39. Briscoe, E., & Appling, D. S. (2014). "Early Detection of Social Media Financial Scams with Linguistic Cues." ACM Transactions on Management Information Systems, 5(3), 1-15.

40. Financial Conduct Authority (FCA). (2020). "Protecting Consumers from Investment Scams in a Digital Age."
41. Securities and Exchange Commission (SEC). (2022). "Investor Bulletin: Social Media and Investing – Avoiding Fraud."