Social Media Scams: Consumer Vulnerability and Prevention Strategies

Author Ms.K.Keerthana

II.M.Com(CS)

Department of Corporate Secretaryship PSG College of Arts & Science

Coimbatore-641014.

e-mail: keerthana7010660610@gmail.com

Co-Author Dr.S.Jeyalakshmi Associate Professor

Department of Corporate Secretaryship PSG College of Arts &amp Science;

Coimbatore-641014.

e-mail: jeyapsgphd@gmail.com

ABSTRACT

This study gives a comprehensive evaluation of social media frauds, focusing on their impact, underlying issues, and prospective options for reform. By reviewing relevant literature and empirical data, the research finds major elements leading to the rise and impact of these frauds on social media users. The results highlight the need for continued efforts to address the changing nature of online threats and point to important knowledge gaps. Although the study achieves its goals and offers insightful information, it also admits its limits with regard to demographic factors like age, gender, and occupation. These limitations emphasize the value of more comprehensive, multidisciplinary, and long-term methods in further studies. Beyond scholarly debate, the study's implications are useful for professionals, decision-makers, and interested parties in improving digital safety and thwarting cybercrime. All things considered, this study establishes the foundation for upcoming developments in our knowledge of and defense against social media fraud.

Keywords: Social Media Scams, Online Fraud, Scam Prevention, User Awareness, Social Media Platforms

INTRODUCTION

Social media scams have become a significant issue in the online community. With billions of users, scammers take use of the massive audience on social media platforms like Facebook, Instagram, Twitter, LinkedIn, and TikTok to defraud individuals and businesses of money, commit identity theft, or accomplish other malicious objectives. These frauds include phishing attempts, romantic scams, financial fraud, and phony giveaways. Scammers use social engineering, psychological manipulation, and phony profiles to trick victims into parting with money, clicking on dangerous links, or disclosing personal information. Artificial intelligence (AI) and deepfake technologies have advanced scam tactics, making it harder to distinguish between legitimate and fraudulent activity.

STATEMENT OF THE PROBLEM

The rapid growth of social media has created new opportunities for scammers to target consumers, exploiting their vulnerabilities and causing financial and emotional harm. Despite efforts to combat these scams, consumers continue to fall victim to phishing, fake news, online harassment, romance scams, and other types of social media scams.

OBJECTIVES

1. To examine the prevalence and common types of scams on social media platforms.
2. To analyze consumer awareness and susceptibility to social media scams.
3. To explore the role of fake accounts, phishing, and influencer fraud in deceiving consumers.
4. To assess the financial and psychological impact of social media scams on consumers.
5. To recommend effective prevention strategies for consumers and social media platforms.

RESEARCH METHODLOGY

This study employs a descriptive research design to explore the types of scams on social media and the factors influencing consumer vulnerability. The research focuses on digital consumer behavior, awareness, and preventive strategies. Data was collected using both primary and secondary methods. Primary data was obtained through a structured questionnaire distributed to social media users, while secondary data was sourced from academic journals, reports, and published articles. A sample size of 105 respondents was selected to evaluate awareness and susceptibility to social media scams. The data was analyzed using percentage analysis, T-test, One-Way ANOVA, and Chi-square test to draw meaningful insights.

REVIEW OF LITERATURE

Winifred R Poster (2022)

This special issue builds on interdisciplinary discussions within science and technology studies (STS) and expands research on the underside, illicit, and irregular forms of digital behaviour. With a focus on how scams, fakes, and frauds are embedded in the digital economy, we examine the institutions that shape online scams, the labor involved in performing and/or navigating them, and the role of platforms in hosting them. Deception is a ubiquitous feature of the online marketplace, from phone calls from phony tech support workers at Microsoft to fraudulent emails requesting payment of advance fees and phony job postings on employment platforms.

İlke Yurtseven, Selami Bagriyanik, Serkan Ayvaz (2021)

This paper studied about the widespread use of social media for online socialization, bad actors can now utilize these platforms to reach enormous audiences with their destructive content, including spam, hate speech, and even phishing. Detection is a critical step in stopping these operations. Therefore, this study's primary objective is to review the state-of-the-art in dangerous content detection and the role that AI algorithms play in efficiently identifying spam and frauds on social media.

ANALYSIS AND INTERPRETATION

PERCENTAGE ANALYSIS

Have you ever reported a social media scams to the social media platforms or authorities

	Factor	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	56	53.3	53.3	53.3
	No	49	46.7	46.7	100.0
	Total	105	100.0	100.0	

INTERPRETATION

From the above table we can understand that 53.3% of the people have reported the social media scams to the social media platforms or authorities and 46.7% of the people have not reported the social media scams to the social media platforms or authorities.

T TEST

Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
How concerned are you about the potential impact of social media scams on your personal life and financial security	Male	44	3.0455	1.11969	.16880
	Female	61	3.2951	.97201	.12445

INTERPRETATION

It is inferred from the above table that the respondents who are Female(3.2951) have high mean score how concerned about the potential impact of social media scams on their personal life and financial security and the respondents who are Male(3.0455) have low mean scorehow concerned about the potential impact of social media scams on their personal life and financial security .From the table, the significance value of the T test is 0.304, which is greater than 0.05. Since the p-value exceeds the standard significance level of 0.05, we accept the null hypothesis (Ho) and reject the alternative hypothesis (H1). This implies that there is no significant difference between gender and how concerned about the potential impact of social media scams on their personal life and financial security.

ANOVA

How aware are you of social media scams

Factor	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	59.426	4	14.856	15.036	.000
Within Groups	98.803	100	.988		
Total	158.229	104			

INTERPRETATION

From the above table, the significance value of the anova test is 0.000, which is less than 0.05. Since the p-value is less than the standard significance level of 0.05, we reject the null hypothesis (H0) and accept the alternative hypothesis (H1). This implies that there is significant difference between age groups and awareness in social media scams.

CHI SQUARE

		What are the common warning signs of a social media scam				Total
	Factor	Suspicious links/Fake website	Unverified accounts	Too-good-to-be-true offers	Urgent requests for Money/Personal information	
Age	Below 18	6	1	0	0	7
	18-30	41	6	7	4	58
	31-40	20	2	2	0	24
	41-50	6	1	0	0	7
	51or older	8	1	0	0	9
Total		81	11	9	4	105

Chi-Square Tests

Factor	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.072[a]	12	.853
Likelihood Ratio	10.438	12	.578
Linear-by-Linear Association	2.300	1	.129
N of Valid Cases	105		

INTERPRETATION

From the table, the significance value of the chi-square test is 0.853, which is greater than 0.05. Since the p-value exceeds the standard significance level of 0.05, we accept the null hypothesis (Ho) and reject the alternative hypothesis (H1).

This implies that there is no significant difference between age group and the common warning signs of a social media scam

FINDINGS

PERCENTAGE ANALYSIS

- The majority of the respondents are from the age group of 18-30 (i.e., 55.2%)
- The majority of the respondents are female (i.e.,58.1%).
- The majority of the respondents are from Master's Degree(i.e.,41%).
- The majority of the respondents are College Student(i.e.,65.7%).
- The majority of the respondents have heard about social media scams (i.e.,91.4%).
- The majority of the respondents have fallen victim to a social media scams(i.e.,73.3%).
- The majority of the respondents have lost their money or information theft (i.e.,56.2%).
- The majority of the respondents have reported the social media scams to the social media platforms or authorities (i.e.,53.3%).
- The majority of the respondents have not use two-factor authentication (2FA) for their social media accounts(i.e.,56.2%).
- The majority of the respondents use different passwords for different social media accounts(i.e.,53.3%).
- The majority of the respondents have not received education or training on how to avoid social media scams(i.e.,67.6%).

T TEST

- This implies that there is no significant difference between gender and how effective the people think social media platforms are in preventing scams.
- This implies that there is no significant difference between gender and how concerned about the potential impact of social media scams on their personal life and financial security.

ONE WAY ANOVA

- This implies that there is significant difference between age groups and awareness in social media scams.
- This implies that there is significant difference between age groups and Fake reviews and endorsements from influencers.
- This implies that there is significant difference between age groups and some influencers buy fake followers, likes and comments.

- This implies that there is significant difference between age groups and some of them have personally bought a product based on an influencer's promotion and felt deceived.
- This implies that there is significant difference between age groups and Influencers exaggerate product benefits to mislead consumers.
- This implies that there is significant difference between age groups and Influencers frequently promote products they don't actually use.
- This implies that there is significant difference between age groups and Influencers often prioritize making money over being honest with their audience.

CHI SQUARE

- This implies that there is significant difference between age group and those received education or training on how to avoid social media scams.
- This implies that there is no significant difference between age group and who do you believe should be responsible for preventing influencer fraud.
- This implies that there is no significant difference between age group and the scam result in any financial loss or information theft.
- This implies that there is no significant difference between age group and how often do you update your passwords.
- This implies that there is no significant difference between age group and steps social media companies should take to reduce scams.
- This implies that there is no significant difference between age group and advice they give to someone to help them avoid social media scams.
- This implies that there is significant difference between age group and those who received education or training on how to avoid social media scams.
- This implies that there is no significant difference between age group and those who heard of social media scams.
- This implies that there is significant difference between age group and the social media platforms they actively use.
- This implies that there is no significant difference between age group and the reason they primarily use social media for.
- This implies that there is no significant difference between age group and those who fallen victim to a social media scams.
- This implies that there is no significant difference between age group and the scam result in financial loss or information theft.
- This implies that there is no significant difference between age group and how did they find out about the scam.

- This implies that there is significant difference between age group and who they think is most likely to perpetrate social media scams.
- This implies that there is no significant difference between age group and the common warning signs of a social media scam.
- This implies that there is significant difference between age group and those who reported a social media scams to the social media platforms or authorities.
- This implies that there is significant difference between age group and those who use two-factor authentication (2FA) for their social media accounts.
- This implies that there is significant difference between age group and who use different passwords for different social media accounts.
- This implies that there is significant difference between age group and who believe should be responsible for preventing influencer fraud.

SUGGESTION

- Expand Research – Increase sample size and explore additional influencing factors.
- Real-World Application – Implement findings and collaborate with industry experts.
- Technology Use – Leverage AI and automation for scam detection.
- Policy Enhancement – Strengthen regulations based on research insights.
- Awareness & Training – Conduct workshops and campaigns to educate users.

CONCLUSION

This study provides valuable insights into social media scams, their impact, and the factors influencing consumer vulnerability. The findings highlight the growing sophistication of scams and emphasize the need for enhanced awareness and preventive measures. While the research successfully meets its objectives, limitations such as demographic factors suggest the need for broader future studies. The study’s implications extend beyond academia, offering practical benefits for policymakers, professionals, and stakeholders. Continued research, technological advancements, and policy interventions will be essential in mitigating social media scams and improving digital security.

BIBLIOGRAPHY

1) Patel, P., Kannoorpatti, K., Shanmugam, B., Azam, S., &amp; Yeo, K. C. (2017, January). A theoretical review of social media usage by cyber-criminals. In 2017 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

2) Mouncey, E., &amp; Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. Journal of Economic Criminology, 7, 100125.

3) Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., &amp; Gualtieri, G. (2020). Online romance scams: relational dynamics and psychological characteristics of the victims and scammers. A scoping review. Clinical practice and epidemiology in mental health: CP &amp; EMH, 16, 24.

4) Li, X., Rahmati, A., &amp; Nikiforakis, N. (2024, February). Like, comment, get scammed: Characterizing comment scams on media platforms. In Proceedings Network and Distributed System Security Symposium

5) Damilola, O., Emmanuel, A., &amp; Ngoc, P. B. (2023). Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention. In Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria.

6) Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Ver Steeg, G., &amp; Galstyan, A. (2021). Identifying and analyzing cryptocurrency manipulations in social media. IEEE Transactions on Computational Social Systems, 8(3), 607-617.