International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Online Payment Scams on Social Media Marketplaces : A Growing Threat

Christina Puyam, Harshithananda. R, Olumide Joshep and Adlin Jebakumari
Department of Computer Science and Information Technology
Jain (deemed-to-be) University, Bangalore, India

***Abstract* – Social marketplaces have become incredibly popular places for informal buying and selling, but their naturally trust-based structure has also raised the risk of online payment scams. The study examines how users experience these scams, the frequency of reports, and what has prevented victims from seeking help. Most people have faced scams and report them infrequently, and there is substantial confusion over how to report incidents of scams. Psychological barriers, confusing guidelines set forth by the platforms, and a lack of trust in authorities further reduce reporting. The findings stress the need for easier reporting mechanisms and better means of awareness.**

Recommendations are provided to better protect users and improve digital marketplace safety.

Keywords: Scam, Social Media, Online, Money, Fraud, Digital Safety

I. INTRODUCTION

Instagram, Facebook Marketplace, and WhatsApp have grown to be quite popular trading platforms where users buy and sell products easily. Since it's not a regulated e-commerce system, social media transactions rely heavily on personal communication and building trust between two unknown parties, that is, customers like me and you, and non-verified sellers who can be commoners like us. This opens up wide avenues for scammers to exploit users through fake listings, advance payment frauds, QR code manipulations, and impersonation. They can show many offers, which are tempting for social media users to buy their products.
The product can be real or may not exist.

With more and more users being exposed to this type of scam, few report these events due to confusion, mistrust, or a belief that little will come of it. These unreported cases create a vicious cycle where sites struggle to take action, victims stay uninformed, and scam methods continue to proliferate. This lacks the awareness of the scam by that scammer to other users who use the same platform without knowledge of the scam that the non-verified sellers are doing on the social media platform. Many of the users don't report the scam and are ashamed because they were scammed, and many think there is no use in reporting the scam, as they won't be refunded or profit from anything.

This paper explores these challenges through a user survey, examining scam exposure, reporting behaviour, barriers to action, and perceptions of safety. It develops recommendations for platforms, policymakers, and digital safety. It develops recommendations for platforms, policymakers, and digital safety advocates for improving trust in platforms and reducing the incidence of scams. Also, to get more awareness of these scams among social media users and help reduce scams, as many people are not aware of these social media scams going around them, spreading awareness can help reduce these social media scams. If social media starts taking action and adding some feature to report and actually lodge cases for social media market scams, it'll be helpful, and all of this comes only when the people who are getting scammed share their experience of which account they got scammed from. Scams occur, and very little is known to explain why victims do not report their scams from the social media marketplaces.

II. LITERATURE REVIEW

Different studies have focused on online fraud, trust, and security in digital platforms. However, most works have focused on how scams operate or how users fall victim to them afterwards. Fatima (2021) identified a taxonomy of risks in social commerce by explaining both system-level and user-level vulnerabilities. This study does not explore what happens after a scam has taken place or how the victims respond. Mokhberi et al. (2024) also studied trust and safety on Facebook Marketplace by showing how privacy and risk influence user decisions without analysing the reporting behaviour of scam victims.

Other research concentrates on impersonation, stolen accounts, and the conversion rates of scams. For instance, Beluri et al. (2024) have shown how easily users fall for giveaway scams. These works describe the mechanisms of scams but do not examine why victims seldom report incidents of fraud. Regional studies like that of Abdullah et al. (2025) indicate high fraud prevalence in regions like Malaysia, but do not discuss the psychological or procedural barriers that impede reporting. It all talks about what is potentially causing the scam and not about what people should do after getting scammed. To reduce the risk of getting scammed, user awareness about the scam is important, and no paper that we have come across has spoken about the scam.
Similarly, studies related to trust in extended payment systems, crypto fraud using fake profiles, and mobile-money scams have focused heavily on attack patterns and user risk but have not

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

covered post-scam responses. Even policy-oriented papers and consumer protection guidelines identify experience on social media marketplaces. This presents a clear research gap. Little is currently known about the reasons, be they lack of trust, unclear procedures, fear, or confusion, which stop victims from reporting such incidents. The current study addressed this gap by directly surveying users in pursuit of the personal, practical, and platform-related barriers to reporting behaviour.

III. METHODOLOGY

An online Google survey was designed and shared to understand the reporting behaviour of victims of social media marketplace scams. The purpose was to get honest, firsthand insights in a format that guaranteed anonymity and comfort. As scams can be personal or embarrassing to discuss for a few people, an online questionnaire was a suitable method for gathering responses without pressure, so we prepared a questionnaire in Google Forms and got a few genuine responses, which we used to analyse.

63 valid responses were obtained for the questionnaire. The questionnaire comprised multiple-choice questions, rating scale questions (1 to **5),**

and a few open-ended questions. These items were designed to measure five important areas we needed to analyse: (1) exposure to scams, (2) reporting behaviour,
(3) reasons for not reporting, (4) trust in platforms and authorities, and (5) familiarity with reporting tools. Basic information about usage habits was also collected from the Google Form.
Data analysis was done using simple descriptive methods. Percentages were used to observe trends, and common themes from open-ended responses were grouped manually. Because the study focuses on user perception rather than technical measurements, it offers qualitative redress mechanisms but provides little insight into how often victims use them.

A consistent pattern throughout the literature is that while much is known about how results show the experiences and opinions of everyday users of social media marketplaces and may also provide insight into some of the barriers that are not well examined by prior research.

IV. FINDINGS

These are a few findings we have from the survey we conducted through Google Forms. As mentioned earlier, we tried to cover a few important areas, which are discussed below:

A. High Exposure but Low Reporting: More than a third of 36.1% of the respondents personally experienced a scam, while 52.4% were not sure, thereby inferring that suspicious activities are a common feature. However, only 38.1% of those experiencing scams reported the same. The major reasons for not reporting were primarily not knowing how to report (47.6%) and, secondly, reporting would not lead to any real action (20.6%).

B. Major Barriers to Reporting:

Users face barriers both on the emotional and practical sides. Many believe reporting is ineffective, while others are unsure about the right steps. On top of all, distrust is a strong factor: only 36.5% believe social media platforms could take action, and only 34.8% believe authorities are capable of dealing well with online scam cases. Users also worry about long procedures for reporting and the possibility of sharing personal details.

C. Unclear and Inconsistent Reporting Systems:

The experience in reporting is different across all the various platforms. About 31.7% find it easy, while 23.8% find it very difficult. Most users, or 73%, do not clearly understand how to report a scam, and the driven approach was appropriate. Support Others:
Only 25.4% of the respondents had witnessed or heard about successful recoveries following reporting.
Nevertheless, many users are willing to support others: 42.9% report having assisted someone who was
scammed, reflecting high community concern. Another 20.6% would like to help but do not know how; so many were not aware of how to handle the situation, and even though they wanted to help, they were not aware of the procedure for how to exactly report these social media scams.

E. Platform Use Habits:

Instagram accounts for 42.9%, followed by Facebook Marketplace with 23.8%. Almost half of the respondents said that they transact "rarely", which may reduce their familiarity with safety tools and reporting features. The platform the user is using is also a really important thing, as there are many social media platforms, and main thing we want is awareness in people, even a layman as every individual works really hard to live life and scam can make them feel bad or embarrassed, so we had a question asking which platform is used by most individuals and according to the responses, the highest was instagram then Facebook and other social media applications, which have market/business accounts in the respective applications, can be used by non-verified persons, which is one of the main causes. We also had a question in short-answer form asking for suggestions to have more awareness and to improve the system in such a way that these scams are reduced, for which many of them suggested a button to report scams in particular and many more suggestions, which are really good.
These findings help to get a better solution for the lack of awareness among people and will help reduce social media

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

market scams. While social media marketplaces provide convenience and reach for both buyers and sellers, they are also the platform they use most often. Such inconsistency creates confusion and directly contributes to the low reporting rates. This is the exact reason user awareness is required for social media market scams.

Low Success Rates, yet Willing to

highly susceptible to online payment fraud due to the limited security measures in place, insufficient awareness among users, and poor regulatory structures. Victims often have problems identifying credible sellers, and when

scammed, they seldom recover their money because of anonymity and cross-border challenges. Despite

With growing cases, there is a scarcity of research that focuses on the upsurge of payment-related scams in

Social media marketplaces, their methods, and prevention strategies. This gap highlights the urgent need for

The evolving nature of these scams is under examination to find measures to reduce risks. So the survey helped us to analyse a few things by getting responses from different age groups and different education levels. Helping us get an insight into many different experiences by other individuals. An understanding of the challenges users face provides directions for designing safer, more trustworthy online marketplaces.

ACKNOWLEDGMENT

The authors would like to express their profound gratitude to their mentor, Adlin Jebakumari, for her invaluable guidance, insightful feedback, and unwavering support throughout the course of this research. Her expertise, patience, and thoughtful suggestions were instrumental in shaping the direction of this study and enhancing its overall quality.

The authors also sincerely appreciate her continuous encouragement and motivation, which greatly contributed to overcoming challenges during the research process. Her mentorship has not only enriched this work but has also provided the authors with a deeper understanding of research methodologies and academic writing.

The successful completion of this study would not have been possible without her dedicated guidance and support.

REFERENCES

[1] Arumugam, N., Shanthi, A., & Dharinee, S. (2021). A study on online shopping scams and user risk behaviour. *International Journal of Social Science Research*, 10(1), 22–31.

[2] Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimisation. *Criminology, 46(1),* 189–220.

[3] Whitty, M. T. (2017). Do you choose to tell? The reporting of romance scam victims to the police. *Victims & Offenders*, 12(2), 212–231.

[4] Cross, C., Richards, K., & Smith, R. (2016). *The reporting experiences and support needs of victims of online fraud*. Australian Institute of Criminology.

[5] Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online fraud victims: Reporting, self-blame and support. *Security Journal*, 27(1), 36–54. https://doi.org/10.1057/sj.2012.11

[6] Modic, D., & Anderson, R. (2015). Reading this may harm your computer: The psychology of malware warnings. *Journal of Cybersecurity*, 1(1), 81–98.

[7] Whitty, M. T. (2019). The scammers' persuasive techniques model: Development of a model for online dating scams. *Journal of Cybersecurity*, 5(1), 1–9.

[8] Mokhberi, A., Keil, M., & Bansal, G. (2024). Trust, privacy, and safety factors influencing buyer decisions on Facebook Marketplace. *Journal of Information Systems Research*, 35(2), 142–159.

[9] Liu, E., Chen, X., & Xu, T. (2024). Measuring conversion rates of giveaway scams on social platforms. *Proceedings of the ACM Web Conference*, 1221–1232.

[10] Abdullah, N. A., Karim, K., & Nasir, F. (2025). Online fraud through social media in Malaysia: Trends and challenges. *Asian Journal of Cybersecurity Studies*, 3(1), 44–59.

[11] Beluri, M., Rani, T., & Naresh, P. (2024). Dynamics of buy-and-sell of social media accounts and scam enablement. *Computers & Security*, 134, 103–218.

[12] Zhang, H., & Kim, S. (2025). Trust in extended payment services on social networking sites. *Journal of Retailing and Consumer Services*, 79, 104–145

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026