Global Journal of Sociology and Anthropology
Vol. 14 (1), pp. 001-005, December, 2025
ISSN: 2756-3456

Full Length Research Paper

Financial Cyber-Fraud Tactics Targeting Elderly Victims in Delhi: A Secondary Data Based Sociological Study

Rupak Verma
Research Scholar, Department of Sociology
Central University of Haryana
Vermarupak20@gmail.com

Accepted 17th November 2025
Author retains the copyrights of this article

Abstract: - *The rapid growth of digital financial services has undoubtedly made everyday transactions more convenient and accessible. But this growth has also made older people more likely to fall for cyber-related financial scams. Adopting a sociological perspective, this study explores the nature and impact of financial cyber fraud targeting senior citizens in Delhi, drawing upon empirical research, government records, and policy analyses. The findings reveal that social engineering remains the most common method used to commit such frauds, alongside phishing, vishing, SIM-swap attacks, QR code manipulation, and UPI-based scams. Beyond limited levels of digital literacy, the study identifies age-related factors such as trust, social isolation, and structural inequalities embedded within India's rapid digitization process as key contributors to seniors' vulnerability to cyber fraud. The research also highlights significant underreporting of these crimes in Delhi, which can be largely attributed to inconsistent institutional responses and limited awareness of existing reporting mechanisms. Importantly, the consequences of cyber fraud extend well beyond financial loss, leading to reduced digital participation, diminished autonomy, and considerable psychological distress among older victims.*

The study concludes that age-sensitive interventions are essential to ensure the safe and equitable participation of senior citizens in India's evolving digital financial ecosystem. Such interventions should include inclusive technology design, targeted digital and financial literacy programs, regulatory reforms, and accessible as well as responsive reporting and redressal mechanisms.

Keywords: - *cyber-fraud, victims, financial, digital literacy, social vulnerability.*

Introduction: - More financial services are being done online, which has made banking easier to get to and more handy. But this also has rendered older Indians more vulnerable to new risks. Digital payment solutions have been more abundant in cities: mobile wallets, the Unified Payments Interface, and internet banking. At the same time, financial cybercrime has become a major social issue today. Maini and Sindhi (2025) refer to the indications that older persons are getting targeted more than they should. Delhi happens to be an interesting area where cyber-fraud methods and social weaknesses among older people can be said to intersect. This is because it is the capital of India and one of the main places where digital money is becoming popular.

In this regard, the research closes a gaping gap in city-specific empirical work by using a sociological framework to evaluate secondary data about financial cyber fraud tactics that target elderly victims in Delhi. Financial cyber-fraud encompasses various technologically mediated deception techniques-phishing, vishing or voice phishing, SIM-swap attacks, manipulating QR codes, and spoofing caller ID. These techniques lever on both psychological and technological weaknesses: for example, social engineering techniques designed to break down defenses based on appeals to authority, urgency, and trust. Cyber-fraud targeting the elderly is still underreported in national statistics across India. However offenses against the elderly were kept as a separate category by the National Crime Records Bureau since 2014, with subsequent reports citing rising numbers.

Sociologically speaking, it is not possible to reduce the vulnerability of older populations to cyberfraud to individual-level characteristics; it can only be contextualized within larger institutional and psychosocial factors. Beyond justifying targeting seniors through a cultural framework, ageism, systematic stereotyping and discrimination against older adults, facilitates the portrayal of elderly victims by criminals as being "ideal" targets with financial resources but low levels of digital literacy. Research has documented that low digital literacy, high deference to authority people, social isolation, and loneliness all increase the risk of fraud (Saifuddin et al., 2024). Loneliness, for instance, is empirically linked with increased exposure to scams with a reported odd ratio of 1.06, while urban residential patterns indicate that city-specific social dynamics determine victimization risks (Saifuddin et al., 2024). These findings raise the importance of investigating financial cyberfraud as a sociological issue related to age-based power dynamics, digital inequalities, and urban social structures.

Literature Review and Theoretical Framework

Criminological Perspectives on Elder Financial Exploitation

Financial exploitation of the elderly represents a category within criminology that involves an opportunity structure, an accountable predator, and a vulnerable target. While the classical streams of sociological theories, such as routine activity theory and social learning models, are applicable frameworks for understanding the crime pattern, the literature on elder cyber-fraud in India has been based on criminological and legal aspects rather than an empirical test of particular sociological theories (Srivastava 2023).

The internet world presents what may be regarded as new "routine activities" in which the growing online existence of older persons for financial transactions, coupled with declining capable guardianship due to a lack of computer literacy, creates opportunities for motivated cybercriminals. Cyber-enabled financial crimes differ from traditional elder abuse in the secrecy and size of digital fraud operations, allowing offenses to target multiple victims simultaneously beyond regional boundaries.

Digital Divide and Age-Related Vulnerability

The so-called digital divide is understood here as unequal access and competence in information and communication technology, forming the backdrop of elderly people's vulnerability to cyber fraud. Scholars have identified time and again that elderly people in India have lower levels of digital literacy compared to younger groups, given the limited exposure to technology during their formative years and a lower chance of learning skills (Tripathi et al., 2019). This literacy gap manifests itself not only in technical skill inadequacies but also in a lack of understanding about cybersecurity issues and strategies adopted to perpetrate fraud.

Changes in cognition with getting older have the effect of making you more vulnerable, but they are very individual indeed. Some studies say this could change the way older people make decisions and assess risks, as well as their sensitivity to persuasion. Such features call for caution so that ageist stereotypes are avoided (Tripathi et al., 2019). From a sociological point of view, the salient factor is how social and technological systems fail to adapt to the different cognitive profiles of senior users, rather than how individuals' cognitive skills decline.

Social Isolation and Trust Dynamics

Another critical factor affecting elderly people's vulnerability to financial cyberfraud is social characteristics. Social isolation, a well-documented concern among India's urban elderly, is likely to increase dependency on digital communication channels for social connectivity at the cost of protective social networks that can help detect fraud (Tripathi et al., 2019). In this regard, information gaps used by fraudsters arise from a lack of regular interactions with family or community members who are more digitally literate.

Another sociological aspect of vulnerability involves trust patterns in elderly individuals. Studies have shown that older adults may have a higher default level of trust in figures of authority, institutional representatives, and individuals perceived as helpful or familial. (Maini & Sindhi, 2025) Trust is adaptive across most social contexts but becomes maladaptive when cybercriminals use social engineering to make it seem as though the bank, a government agency, or even one's family member is in trouble.

Methodology

The study analyzes secondary data. This research aimed to find trends in financial cyberfraud that particularly targeted the senior population in India, specifically Delhi where possible. Sources included scientific studies in disciplines of sociology, criminology, and cybersecurity, and information provided by law enforcement and financial regulatory authorities. The analytic approach was a thematic synthesis of qualitative and quantitative evidence that identifies common fraud tactics, vulnerability factors, impacts, and prevention strategies documented across multiple sources. Limitations of this approach include the fact that reliance on published sources alone may underrepresent the actual victimization due to underreporting and can be limited in the number of Delhi-specific quantitative datasets in the peer-reviewed literature. Despite such disadvantages, secondary analysis has its merit in surfacing established patterns and evidence-based insights for understanding elderly financial cyber-fraud victimization.

Findings: Fraud Tactics and Operational Mechanisms

Prevalent Fraud Methods

A review of the literature currently available clearly indicates a taxonomy of financial cyber-fraud strategies perpetrated on elderly victims in India. One of the popular attack vectors reported by different studies is phishing operations that use fake websites and deceiving messages to obtain banking passwords and personal information (Maini & Sindhi, 2025). Many of these attacks pose as official banking portals or government services, through which fraudsters take advantage of the inability of senior customers to make proper differentiation between genuine and fake digital communications.

Vishing is voice phishing, and it has worked particularly well against senior groups. Attackers in these scams call victims while pretending to be government officials, bank executives, or police officers. In such incidents, the arguments of urgency and authority are used by the caller to convince victims to disclose account credentials, authorize transactions, or reveal one-time passwords. Their style is consistent with the fact that elderly people are more comfortable with phone conversations than with computer interfaces, which adds to increasing the effectiveness of these voice-based attacks.

SIM switching is another sophisticated mode of attack that gives the attacker an opportunity to get cloned SIMs of victims' cell numbers for intercepting OTPs and thereby taking control over accounts. This makes victims vulnerable even when they have not disclosed their credentials because it circumvents the authentication procedures meant for enhancing online transactions security (Maini & Sindhi, 2025).

The rise in QR code frauds and those committed on the Unified Payments Interface shows flexibility in this peculiarly Indian digital payment environment. Fraudsters either generate fake QR codes, disguise receipts of payments, or use social engineering to get victims to approve a transfer through UPI systems. While the ability to transact on UPI is handy in applications in which it is useful, it can also allow for fast fraudulent transfers before the victim realizes the fraud (Maini & Sindhi, 2025).

The investment and Ponzi schemes targeting the elderly promise vast returns on investment in fake prospects. These frauds take advantage of elders' need for financial security in retirement and may involve long-term relationship development prior to money solicitation, thus making identification difficult (Maini & Sindhi, 2025).

Social Engineering as Enabling Mechanism

Across all fraud tactics, social engineering psychological manipulation to influence victims' behavior functions as the critical enabling mechanism (Maini & Sindhi, 2025). Perpetrators employ several psychological tactics particularly effective against elderly populations:

1. Authority appeals: They are impersonating officials from banks, law enforcement, or government agencies to leverage respect for institutional authority.
2. Urgency creation: The individual claims that there are immediate threats to bank accounts, legal troubles, or family emergencies that require rapid action without consultation.
3. Trust exploitation: The process involves building rapport through prolonged interaction or impersonating trusted entities.
4. Complexity exploitation: They are using technical jargon and complicated procedures to confuse victims and discourage questioning.

These social engineering tactics transform technical vulnerabilities into successful fraud by exploiting psychological and social factors rather than solely technological weaknesses.

Sociological Vulnerability Factors

Digital Literacy Gaps

The fact that many seniors don't know how to use technology makes them more vulnerable, and this is the issue that is talked about the most. Research has shown over and over that older Indians are less aware of safety and less skilled with technology than younger Indians (Tripathi et al., 2019). This plays out in a variety of ways, including a general difficulty with digital interfaces, a general misunderstanding of how authentication processes work, an inability to detect fraudulent messages, and unfamiliarity with privacy settings and security measures.

Digital literacy deficit is thus a result of institutional inequities in technological education, not a failure at the level of the individual. Current senior populations in India entered adulthood before extensive digitalization kicked in, with very little official and unofficial training in digital skills. The educational programs and financial service interfaces developed predominantly for younger digitally native populations fail to meet the learning and engagement needs of the senior users (Tripathi et al., 2019).

Trust Patterns and Social Isolation

Sociological research has pointed out a few trust patterns in elderly subjects that make them more susceptible to such attacks. For example, older citizens may have greater baseline trust than others in the authorities and representatives of institutions because this degree of trust was well-earned in contexts of the past (Maini & Sindhi, 2025). Such trust is then exploited by cybercriminals through impersonation, knowing full well that older targets are less likely to question or verify any claim made by a purported authority.

Social isolation increases vulnerability through a variety of methods. For instance, socially isolated elderly persons may not have regular interaction with family members or peers who can alert them about fraudulent activities or recognize questionable messages. Loneliness can make people more receptive to unsolicited contact, even from strangers, which may lead to relationship-based fraud. In addition, socially isolated older persons may have fewer opportunities to learn about new fraud strategies via informal social networks (Tripathi et al., 2019).

Institutional and Structural Factors

An older individual's vulnerability in respect of online financial fraud depends on both personal and systemic factors. India's financial services have rapidly transitioned to digital; however, the development of interfaces suitable for older adults, educational tools, and support networks has not kept pace. The banking and payment system may be hard to use for older people since it is built to work well for younger customers.

Uncoordinated institutional responses to cybercrime further create vulnerability. Even today, financial institutions, law enforcement, and government agencies are not working in coordination with each other, and effective mechanisms for detecting and reporting the problems are few (Maini & Sindhi, 2021). For instance, the reporting processes involve such a level of digital literacy and perseverance that the already victimized seniors lack.

Statistical Trends and Scale of Victimization

National Patterns

The National Crime Records Bureau's introduction in 2014 of special reporting categories for crimes against the elderly was a crucial improvement in the recording of elder abuse. There has been an uptick in reported victimization in recent years, as indicated by the number of incidents with older victims that have been reported. Increases should be viewed with caution when interpreting these numbers, as this could be due not only to increased victimization but also to improved reporting practices.

According to Maini & Sindhi (2025), the underreporting of financial cybercrime against senior citizens remains a bone of contention for researchers. This is in respect to the fact that the victim may fail to report due to embarrassment, not knowing that crimes have been committed, not thinking it will work, or finding the reporting process too difficult to understand. As a result, official statistics probably reflect just a fraction of the actual victimization, which makes an accurate scale assessment very difficult.

Delhi Context and Data Limitations

While national trends provided a background, the peer-reviewed literature contained, quite surprisingly, very little quantitative data on senior financial cyber-fraud victimization in Delhi. Qualitative research in other Indian cities such as Mumbai by Tripathi et al. (2019) and case studies from states such as Chhattisgarh remain the only sources of this information, and the reviewed literature does not, even now, report accurate, and quantitatively based estimates of the prevalence for Delhi. The policy formulation and resource allocation in the capital region remain particularly and seriously hindered due to this gap in data.

This gap in the case of Delhi also reflects some more general problems in the collection of cybercrime data across India, such as fragmented reporting systems, jurisdictional problems with digital crimes, and a general lack of funding for research into victimization surveys. This is where future research and policy development needs to be focused.

Impacts of Victimization

Financial Consequences

One of the immediate and quantifiable consequences of becoming a cybercrime victim is monetary loss. In this case, it is particularly worse for older individuals because they lose all the money they have struggled to amass, pension funds, or retirement investments. When retired victims try to recover their money, they have fewer alternatives compared to younger victims whose resources can be replenished through continuous effort; thus, older victims are more vulnerable to long-term economic insecurity.

Further financial effects include the costs of restoring your identity, fixing your credit, and even paying lawyers' fees. There is also the chance of losing benefits or services if fraud hurts your credit score or account access. Low-income seniors find it hard to satisfy their wants when they lose even small amounts of money.

Psychological and Emotional Harms

Online fraud not only causes people to lose money but also has a very devastating consequence on the psychological well-being of elderly victims.

Researchers have found that victims of scams suffer from agony, shame, bitterness, and a loss of self-esteem (Tripathi et al., 2019). Those who have been victimized may feel guilty about self-blaming, which can lead them to doubt their decisions and capabilities. This can leave children feeling depressed or anxious and hurt their self-esteem.

Because fraud generally represents a rupture of trust, victims hurt even more due to the fewer chances of repairing trusting relationships. According to Tripathi et al. (2019), victims are less trusting in real messages and interactions, and may further seek social isolation to protect themselves.

Social and Behavioral Consequences

Victimization can affect how older adults engage in technology and social activities for a very long time. Studies have shown that those who have been victimized by fraud stop using digital financial services, shift to cash transactions, and may completely refrain from online activities. While this response is psychologically comforting, it inadvertently increases the chances of social and economic isolation as various basic services continue to shift towards digitalization (Tripathi et al., 2019).

After the incident of fraud, family relationships bear severe strain when family members voice dissatisfaction or feel critical of what the victim has done. Conversely, some older victims of cybercrime have become much less independent and rely more on their family to manage their finances. From the list of social effects provided above, it is evident that hacking causes considerably more significant effects other than just financial ones. Cybercrime has a big effect on the senior victim's ability to make their own decisions, fit in with their peers, and overall quality of life.

Conclusion

Online frauds related to finances committed at the expense of senior citizens in Delhi and everywhere in India are one of the serious social issues that, with advancing technology, aging of the population, and criminals adapting, continuously deteriorate. This secondary data study found some common types, like hacking, vishing, SIM swapping, and UPI-based fraud, which take advantage of the fact that the older people usually do not know how to use technology well, trust others easily, and live alone. There are more effects than just cash losses. The effects include mental pain and social isolation, which lower the quality of life and independence of older people.

We have to solve this problem by developing broad multistakeholder solutions that include new technologies, educational changes, new laws, and improved communications among institutions. Prevention attempts should be based on knowledge of the specific weaknesses and needs of the elderly, not on the assumption that everyone is good with technology. India is making the switch to digital systems, and both practical and moral reasons call for older people to be able to safely use digital banking systems.

References

HelpAge India. (2024). the intersection of age, gender, and technology: A study of cyber victimisation among older women in India. HelpAge India Research & Development Journal. https://www.helpageindia.org/wp-content/uploads/2025/07/HelpAge-India-Research-Development-Journal-October-2024.pdf#page=35

Maini, R. N., & Sindhi, V. K. (2025). Digital banking fraud in India: Typologies, victim behaviour, and AI-enabled risk governance in a global context. International Journal for Multidisciplinary Research, 7(5). https://doi.org/10.36948/ijfmr.2025.v07i05.55593

Saifuddin, N. F., Musa, B., Zakaria, N. S., Ismail, R., Hasan, N. A., & Razali, F. M. (2024). Scams issues among elderly: A conceptual paper. International Journal of Academic Research in Business and Social Sciences, 14(10), 3268–3283. https://doi.org/10.6007/ijarbss/v14-i10/23268

Soffer, H. (2022). Old age and the potential for web fraud: An in-depth analysis (SSRN Scholarly Paper No. 4602538). https://doi.org/10.2139/ssrn.4602538

Srivastava, A. (2023). Cybercrime and senior citizens in IndiaA comparative study of legal frameworks within cyberspace globally. Chanakya National Law University Journal of Law and Public Affairs, 21(2). https://doi.org/10.55662/cylr.2023.2102

Tripathi, K., Robertson, S., & Cooper, C. (2019). A brief report on older people's experience of cybercrime victimization in Mumbai, India. Journal of Elder Abuse & Neglect, 31(4-5), 378-384. https://doi.org/10.1080/08946566.2019.1674231