Omniscient
(An International Multidisciplinary Peer Reviewed Journal)
Vol 4 Issue 1 Jan-Mar 2026 EISSN: 2583-7575

# Understanding Silence: A Sociological Exploration of the Challenges Faced by Elderly Cybercrime Victims in Approaching Formal Reporting Channels in India

**Rupak Verma*[1] & Reema Gill[2]**
[1]Research scholar, Department of Sociology, Central University of Haryana
[2]Associate Professor, Department of Sociology, Central University of Haryana
*Corresponding Author: vermarupak20@gmail.com
Available at https://omniscientmjprujournal.com
DOI: https://doi.org/10.5281/zenodo.20353621

## ABSTRACT
The Indian society is digitizing at a rapid pace. This development has resulted in new opportunities for senior citizens to utilize technology but, at the same time, has also exposed them to severe cybercrime threats. This paper examines the socio-cultural barriers that prevent senior Indians from coming forward to report their experiences of victimization due to hacking. Previous studies have already pointed out the knowledge gaps, decreased intentions to report, inefficiencies in the reporting system, and vulnerabilities intersecting with digital literacy, gender, and socio-economic factors. We have discovered that senior citizens are struggling to navigate digital environments because of insufficient awareness about online cyber threats and risky online practices, which are further worsened by the hindrances created by institutions to make complaint filing easier. The significance of this paper is threefold: it belongs to the growing literature on digital gerontology and the victimology of cybercrime by highlighting an impediment in the Indian socio-cultural setting. The findings suggest that the need for immediate action to safeguard this vulnerable group in a rapidly digitizing environment is imperative.

**Keywords**: Cybercrime, Reporting, Vulnerability, Elderly, Victimization.

## INTRODUCTION
People live, talk, and do business in very different ways now that the digital change has happened. India's digital infrastructure is growing as one of the fastest, and well over 700 million people use the internet there. Technology has become a part of daily life in a way that has never been seen before (Kumar & Patel, 2021). This digital shift is meant to make it easier to connect and obtain services, but it has made life more dangerous, especially for older people who use these spaces with varying levels of knowledge and skill with technology.

"Older adults," in this case, refers to those who are 60 years of age and over. This group is expected to grow in India, and by 2050, approximately 20% of the population will fall under this category. Tripathi et al. (2019) made this prediction. This cohort is a group that is prone to threats like phishing scams, financial fraud, identity theft, and also social engineering attacks due to increasing application of technology for self-service needs related to banking, healthcare, connecting, and entertainment.

Although cybercrime often targets older people, the great majority of cybercrime incidents go unreported (Button et al., 2009). One of the most important issues is the lack of reporting of cybercrime incidents, which is particularly evident in India because the infrastructure that deals with the problem is not complete and is underdeveloped, and there could be cultural issues that

Received: 04-02-2026 Revised: 11-04-2026 Accepted:23-04-2026 Published:23-05-2026

impede reporting. It is important to determine why older people do not report the hacking incident in order to ensure that the right measures are being taken to improve the support services for victims.

This paper seeks to use the sociological approach to examine the relationship between the individual, the social, and the structural in the reporting of cybercrime against older people in India. This study critically discusses the recent empirical studies and theories that identify the processes that shape the creation of digital vulnerability. Moreover, the study seeks to identify the necessary steps to promote the concept of digital justice for older people in society. These steps include the need to promote educational initiatives, legal protection, and the development of supportive networks that specifically address the unique challenges faced by older people in the digital landscape.

Research has largely focused on the technical mechanisms of cybercrime or the cognitive declines associated with aging that lead to victimization. Nonetheless, there is a severe shortage of research examining the sociological barriers through an intersectional lens, particularly focusing on how gender, social class, and the cultural environment of India influence silence. This paper attempts to fill this void by shifting focus from personal responsibility to structural examination within the Indian reporting system.

## RESEARCH OBJECTIVES

1. To identify the socio-cultural factors (stigma, shame, and self-identity) that prevent elderly Indians from reporting cybercrime.
2. To analyze the structural and institutional barriers within the Indian cybercrime reporting infrastructure.
3. To investigate how intersectional factors, such as gender and the urban-rural divide, compound digital vulnerability.
4. To propose evidence-based policy recommendations for enhancing digital justice and victim support.

## THEORETICAL FRAMEWORK: UNDERSTANDING DIGITAL VULNERABILITY THROUGH A SOCIOLOGICAL LENS

### The Social Construction of Digital Vulnerability

However, cyber vulnerability is not entirely a technological construct. It is a social construct that is related to the intersectionality of age, class, gender, education level, and digital capital. In terms of the concept of capital as proposed by Bourdieu, the concept of older adults' cyber vulnerability can be seen as a lack of digital capital, which is the knowledge and skills needed to safely and successfully navigate the online world (Ragnedda & Muschert, 2013).

Studies on the digital divide have acknowledged that access to technology is only the first level of inequality because it fails to consider other inequalities in terms of the ability to effectively capitalize on technology among different demographic groups. Greater disparities arise in such areas as digital skills, especially critical evaluation skills and the ability to identify and manage online risks (van Deursen & van Dijk, 2014). These differences for older adults are further heightened by cohort effects of having matured in an era where digital technologies were limited and by age-related changes that may impact information processing and decision making in digital spaces.

### Routine Activities Theory and Cyber Victimization

RAT was first conceptualized by Cohen and Felson (1979) to explain the dynamics of conventional crime but has since been adapted to explain cybercrime victimization. According to the theory, a crime occurs when there is an intersection of three components: a motivated offender, a suitable target, and the absence of effective guardianship. In cyberspace, older adults may present suitable targets due to perceived wealth, limited levels of technological expertise, and naturally trusting personalities (Cross, 2016).

Research from India supports the fact that due to increased exposure of the elderly population to digital platforms for conducting financial transactions and participating in social media, the risks of cyber victimization have significantly increased (Tripathi et al., 2019). Greater exposure and reduced guardianship-that is, knowledge of using digital technologies-make it easier for people to be victimized. To develop strategies to prevent such incidents, one needs to understand how they occur. That means the way one uses the Internet would bring down the risks.

### The Sociology of Reporting: Silence and Disclosure

The decision to report a crime is a social process influenced by various factors, including shame, stigma, perceived authority legitimacy, expected response, and social support systems. For victims of cybercrime who are older, additional barriers include generational attitudes towards seeking assistance, concerns about blame or being judged as incompetent and fears of losing independence if family members consider them incapable of handling their affairs (Goudriaan et al., 2006).

From a symbolic interactionist perspective, the meanings that elderly victims give to their victimization-whether they see themselves as deserving victims worthy of help or as careless individuals who should have been more careful-significantly influence reporting behavior. Disclosing cyber victimization within cultural contexts that correlate age with wisdom and capability may result in challenges to self-identity and social status; therefore, there are strong disincentives to reporting it.

## METHODOLOGY

The current research is based on a qualitative synthesis framework that will critically review both theoretical concepts and empirical evidence available today. Such a methodology allows us to incorporate various sources into our analysis in order to understand fully the problem of cyber-victimization among the elderly population.

### Research Design

The research uses thematic synthesis of secondary sources that have been extracted from peer-reviewed journal papers, institutional documents, which include reports of HelpAge India, and relevant case studies from the years 2019 to 2025.

### Inclusion Criteria

The studies chosen for this review were selected by the application of the following criteria:

(a) Elderly Indians, aged 60 above,

(b) Cyber victimization, specifically hacking and online scams,

(c) Reporting patterns with respect to cybercrimes.

### Data Analysis

Thematic analysis was done to ensure that all patterns recurring in the data could be identified. The results obtained were categorized according to the three main dimensions namely (a) personal/cognitive barriers, (b) social/cultural barriers, and (c) structural/ institutional barriers.

## FINDINGS

### Recognition Gaps: The Invisible Crime

Older people normally do not report cases of cybercrime since they are not aware that it has happened to them. Cybercrimes normally involve sophisticated techniques of social engineering that make it very difficult to tell the real from the imaginary encounters (Kumar & Patel, 2025), and as a result, older people may end up thinking they are having real encounters rather than being victims of cybercrime. This is different from conventional crime since it leaves physical evidence behind. The study reveals that older people are not aware of the existence of cybercrime and thus do not even know they have been defrauded or that what has happened to them is a crime that needs to be reported.

There are a variety of reasons for this delay in acknowledgment. Firstly, the elderly know very little about basic cyber threats or how a hacker works. Without this knowledge framework, the elderly may think that the fake messages are genuine mistakes, misunderstandings, or bad business deals, but not planned criminal acts. Secondly, the reality is that many cybercrimes are just very complicated from a technical point of view, which makes it difficult for non-experts to know if someone is trying to harm them or not.

Some risky pre-fraud trends were also discovered among Indians, and these are reflective of poor threat detection capabilities. To exemplify this, Kumar and Patel (2025) showed that 18.4% of senior victims of cyber fraud have already shared their contact information online, and 51% have already engaged in activities that led to their victimization, like reacting to unsolicited messages and clicking on suspicious links and the like. These trends reveal that older individuals lack the critical thinking skills necessary to detect potential threats online.

Cyber threats are in continuous evolution, and that is one more factor that increases the recognition gap. Even the computer-savvy may not be able to recognize new fraud because scammers invent increasingly sophisticated methods to carry out their work. For elderly people who do not use digital technology very much, keeping up with new risks presents an enormous problem.

### Thresholds of Disclosure and Internalized Ageing

Recent studies have identified that older adults, in particular those aged 75 years and over, are most likely to become crime victims again and thus lose more money overall compared to the younger ones (Button et al., 2009). Very disturbing results were yielded by this study. In situations when hackers manage to successfully target the older adult, then they place their names on "sucker lists" shared among other cybercrime fraudsters.

Repeated victimization begets a vicious cycle. First, a victim may lose faith in the use of digital technologies and, worse, in his own judgment. This could lead either to a complete halt of all digital activities-digital exclusion-or to further vulnerability as victims desperately attempt to recuperate their money through new schemes promising to do so. A 2025 study by Kumar and Patel showed that older people who had previously been scammed were later targeted by "recovery scams" promising to recover the money on their behalf for an upfront fee.
Not reporting the first victimization makes this cycle worse in that it prohibits police from noticing trends, warning future victims, and stopping criminal activities. Being a victim repeatedly can also

be very traumatic and provide major detriments to your mental and physical health: social isolation, anxiety, depression-which puts you at an even more vulnerable state.

**Structural Barriers and Institutional Barriers**

Personal factors combine with large structural barriers in making it difficult for older persons in India to report cybercrime. Legal and regulatory mechanisms to combat cybercrime are still insufficient because the law is full of gaps, institutions cannot do enough, and mechanisms for victim support are inadequate (Chattopadhyay & Singh, 2024).

The Indian Cyber Crime Reporting Portal is a giant leap in terms of ease in reporting cybercrime, and it also had some flaws in terms of further proceedings, language, and ease of access for elders. The absurdity of a victim of cybercrime needing to be tech-savvy in order to report their victimization stems from their lack of knowledge about how to report their victimization.

In addition, police agencies are not trained to deal with both elder abuse and cyber victimization. Such a response could lead to victim-blaming and victim-minimizing, failing to address the vulnerability of the victim.

As reported by the study, police might simply not care for elderly victims because, instead of serious crimes that should be investigated, they think losses among the elderly are due to their carelessness.

Another major issue is the inadequacy of organized services aimed at supporting victims. In India, there are no organized mechanisms to extend financial counseling, psychological support, or assistance in criminal court matters to elderly victims. Whereas some countries have established special teams in order to address issues relating to fraud committed against the elderly. The absence of such support mechanisms decreases the possibility that a victim will report the incident and encourages him to deal with the after-effects himself.

**Intersectional Vulnerabilities: Gender and Geography**

It is not possible to comprehend how elderly people become victims of cybercrime and struggle to report crimes against them without considering structural injustices and the Intersectionality of their social identities. The level of exposure to cyber threats and access to methods of redress vary based on factors like gender, socioeconomic standing, caste, and whether or not a person resides in an urban or rural setting.

It is for this reason that the elderly women of India, being women and also older, are particularly vulnerable. Thumboo and Mukherjee's study illustrates how older women, compared to older men, are less likely to access the internet, be digitally literate, or use technology on their own. Lifelong patterns of inequality, including less schooling, less participation in the labor force, and cultural norms that perceive technology as a male domain, make women more likely to be excluded from the digital world.

Problems for older women victims of hacking continue when they actually try to report it. Patriarchal families might have difficulty making such financial decisions and filing complaints. Additionally, the gender-based expectations of shame and family honor might make it very challenging to talk about being a victim of financial loss or online exchanges which family members may consider inappropriate.

Socio-economic status also has a big effect on how much cybercrime is reported and how vulnerable people are. Rich older adults may be more likely to fall for clever financial scams that target wealthy people, but they also have more resources to help them function better and can

easily get legal help. On the other hand, older adults from lower-income families may come across fraud involving small-value transactions or those dealing with government benefits. Still, they do not have the money or social capital required to file formal complaints or address the system.

Another form of inequality is the difference between cities and rural places. While older people in cities generally face fewer problems in accessing the digital tools and infrastructure to report cybercrime, those in rural areas have more barriers, including slow internet connections, low levels of digital literacy, language barriers (as most resources for reporting cybercrimes are available in either Hindi or English), and distance from law enforcement agencies that can entertain cybercrime complaints.

## DISCUSSION

The results from this research suggest that the "silence" observed among the elderly victims of cybercrimes in India is neither an act of omission nor a simple construct. Rather, it is a socio-constructed concept formed by the interaction of culture, structure, and institutions. In this regard, this section attempts to interpret these results using a sociological perspective.

### The Symbolic Interactionism of Silence: Stigma and Identity

In symbolic interactionism terms, the act of reporting a crime involves performing one's social identity in public. In the case of the Indian socio-cultural environment, in which being older is equivalent to being wise and authoritative, having been a victim of a cybercrime and especially being duped by social engineering becomes an incredibly embarrassing experience. Our notions of recognition gap and threshold effect indicate that there is a cost-benefit evaluation performed by victims in relation to their social identity. Embarrassment and shame are not only matters of personal perception but reactions to a broader society-oriented perception of "ageism," according to which old people having problems with using technologies are perceived as cognitively diminished instead of being recognized as targets of advanced crime schemes. Therefore, choosing to stay silent allows victims to retain control of their own lives and avoid family intervention and limitations concerning their finances and technological access.

### Digital Capital and the Fallacy of "Up skilling"

However, current policy solutions in India seem more preoccupied with "upskilling" which is, in effect, putting the responsibility on the individual rather than on structural mechanisms. Based on the idea of digital capital discussed by Bourdieu, it can be argued that vulnerability is built into the system. It is important to understand that digital capital goes beyond mere skill; it refers to "habitus" – the intuition needed to function online safely (Ragnedda & Muschert, 2013).

However, this emphasis on education misses the point in terms of routine activities theory. Elderly people may become "suitable targets" due to their wealth, but the absence of effective "guardianship" in the digital environment means they will be easy to manipulate. In addition, the "sucker list" proves that repeat victimization is common among the elderly because once a person is singled out for manipulation, he or she will keep falling into a trap until there is institutional guardianship to prevent it.

### The "Dark Figure" of Crime and Policy Invisibility

One of the most significant consequences of under-reporting is the increasing size of the "dark figure of crime," which refers to the difference between real incidents of victimization and reported statistics. The absence of concrete statistics in this regard brings about something that can be termed as "policy invisibility." Due to the non-existent statistics regarding elderly victims of cyber-

crimes in India's Cyber Crime Reporting Portal, such victimization becomes an issue of least priority for the national government's cybersecurity policy-making. This, in turn, gives rise to a self-fulfilling prophecy because the lack of resources makes the entire process of reporting difficult and futile for the victim, leading to less reporting in the future.

## CONCLUSION

There are various reasons for the fact that the elderly population of India do not feel they are victims of cybercrime. These reasons vary from social aspects to structural issues and personal knowledge. This sociological research proves that the digital threat to the elderly population can be due to various reasons related to the age factor, the sociocultural context, and the failure of society as a whole rather than the incompetence of the elderly population to deal with technology.

A majority of the cases of cybercrime against the elderly population do not come into the hands of the authorities or the support system due to various reasons, including structural issues, a lower willingness to come forward with the issues, the repetition of the pattern of victimization, and the recognition of the issues. This unfortunate phenomenon affects the entire chain of the victimized population to the entire population of the society as a whole.

It implies that instead of concentrating on particular strategies to assist the elderly population to improve their ability to deal with technology, we have to improve the reporting of crimes, make the response to crimes smoother, and eliminate the problems to provide justice to all individuals. There are many digitally vulnerable groups, and a particular emphasis has to be placed on the elderly female population, the rural population, and the poor due to the compounded problems they are experiencing because of the weakness in two areas.

India is becoming more digital, and for the country to be socially inclusive and equitable, it is important that the elderly are able to use digital places confidently and safely. It is important that the rapid development of digital technologies should not lead to the marginalization or danger of vulnerable users. Instead, the rapid development of digital technologies presents an opportunity for the development of digital spaces that are safer, more inclusive, and more accessible for the elderly, especially those who may find it difficult to adjust to new technologies.

## REFERENCES

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: Literature review.

Chattopadhyay, S., & Singh, M. (2024). Cyber-Crimes against Elderly People in India-Search for Defence Mechanism to Counter. *NUJS J. Regul. Stud.*, *9*, 38.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187-204.

Goudriaan, H., Wittebrood, K., & Nieuwbeerta, P. (2006). Neighbourhood characteristics and reporting crime: Effects of social cohesion, confidence in police effectiveness and socio-economic disadvantage 1. *British journal of criminology*, *46*(4), 719-742.

Kumar, S., & Patel, M. (2025). Digital habits and cyber vulnerabilities among older victims of cyber fraud. *Working with Older People*, *29*(4), 433-443.

Ragnedda, M., & Muschert, G.W. (Eds.). (2013). the Digital Divide: The Internet and Social Inequality in International Perspective (1st ed.). Routledge.

Thumboo, S & Mukherjee, Dr. S (2024). The Intersection of Age, Gender, and Technology: A Study of Cyber Victimisation Among Older Women in India. *RESEARCH & DEVELOPMENT JOURNAL*, 34.

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), 437-447.

Van Deursen, A. J., & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New media & society*, *16*(3), 507-526.