Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Cybersecurity Vulnerabilities and Fraud Mitigation Strategies Among Senior Citizens

An Analytical Study of Threat Patterns, Risk Factors and a Layered Protection Framework

Vaishnavi Punalkar
Assistant Professor,
Suryadatta College of Management Information
Research & Technology (SCMIRT), Pune, India

Sourabh Kulkarni
Research Student, MSc. Computer Science
Suryadutta College of Management Information
Research & Technology (SCMIRT), Pune, India

Abstract - The expansion of digital banking, mobile payments, messaging platforms and online public services has created new opportunities for older adults, while also exposing them to increasingly organised forms of cyber-enabled fraud. This paper develops an analytical account of the threats affecting senior citizens and proposes a practical, layered framework for prevention and response. It synthesises published research, law-enforcement reporting and policy material discussed in the supplied review paper. The analysis distinguishes the reasons older adults may be targeted from the factors that can make a particular person susceptible, and examines impersonation, technical-support fraud, investment scams, romance fraud, family-emergency deception, phishing and recovery scams. Particular attention is given to India, including digital-arrest schemes, the 1930 cyber-fraud helpline and the National Cyber Crime Reporting Portal. The study uses a desk-based, thematic research design and does not claim to have collected primary survey or experimental data. Its proposed framework combines accessible education, family and community support, financial-institution safeguards, telecom and platform controls, rapid reporting, and victim-centred legal assistance. The analysis indicates that effective protection cannot depend on individual vigilance alone. It requires systems that make verification easier, interrupt suspicious payments, support early disclosure and preserve the autonomy of older users. The paper concludes with implementation priorities and a research agenda for evaluating interventions in the Indian context.

KEYWORDS: Senior citizens, cybercrime, elder fraud, social engineering, digital arrest, phishing, financial exploitation, digital literacy, fraud prevention, India.

I. INTRODUCTION

Digital services now support routine activities such as receiving pensions, paying bills, managing bank accounts, purchasing medicines and communicating with family. These services can improve independence and reduce the need to travel. However, they also create points of contact through which criminals can impersonate trusted organisations, manipulate users and move money quickly. Older adults are not a uniform or inherently vulnerable group; many use digital services confidently. Risk emerges from the interaction of individual circumstances, scam design, service usability and the speed of financial systems.

The supplied review reports a sharp increase in losses recorded by the United States Federal Bureau of Investigation Internet Crime Complaint Center (FBI IC3) among people aged 60 and above, reaching approximately USD 7.7 billion in 2025. It also describes the scale of digital-arrest fraud in India, where government statements reported losses of around Rs. 3,000 crore. These are reported figures rather than complete measures of incidence, because many victims do not make formal complaints (FBI IC3, 2026; Drishti IAS, 2025).

This paper reframes the review findings as a research-oriented analysis: it identifies the interacting sources of risk, evaluates mitigation options by layer, and sets out a framework that can be tested in future field research.

II. RESEARCH PROBLEM AND RATIONALE

Research on fraud against older adults is distributed across criminology, psychology, gerontology, human-computer interaction, banking regulation and law enforcement. Each field contributes a partial explanation. Crime statistics describe complaints and financial losses; behavioural studies examine persuasion and decision-making; usability research investigates security practices; and regulatory guidance recommends institutional controls. When these perspectives are considered separately, prevention may be

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

reduced to a narrow message such as ‘do not click suspicious links’. Such advice does not adequately address scams in which a victim is persuaded to make a payment voluntarily.

A central distinction is between unauthorised transactions and authorised payments induced by deception. In the first case, a criminal accesses an account or payment credential without permission. In the second, the customer personally approves a transfer because a caller or online contact has created a false emergency, investment opportunity or official investigation. Authentication systems can help prevent account takeover, but they may not identify a payment that the customer believes to be legitimate. This gap makes behavioural safeguards and transaction-level intervention important.

The research problem addressed here is therefore: how can a coordinated, accessible and autonomy-preserving set of measures reduce cyber-enabled fraud against senior citizens, particularly in India, where digital payments and smartphone use are expanding?

A. Research Questions

- RQ1: Which scam patterns most frequently expose older adults to financial and personal harm?
- RQ2: How do cognitive, psychosocial, technological and situational factors interact with scam tactics?
- RQ3: Which individual, family, financial, platform and policy interventions have the clearest support in the reviewed evidence?
- RQ4: How can these interventions be adapted to Indian languages, payment practices and reporting mechanisms?
- RQ5: What indicators should be used to evaluate whether a layered protection framework is effective?

B. Significance of the Study

The study is relevant to older users, families, banks, payment providers, telecom operators, digital platforms, community organisations and public authorities. It treats fraud prevention as a shared responsibility and seeks to avoid victim-blaming. It also highlights the need to protect digital inclusion: excluding older adults from online services may reduce immediate exposure but can undermine independence and access to essential services.

III. OBJECTIVES

- To classify major cyber-enabled fraud patterns affecting senior citizens.
- To organise vulnerability factors without treating age as a sufficient explanation.
- To examine psychological mechanisms used in social-engineering attacks.
- To analyse the Indian digital-arrest context and existing reporting channels.
- To assess the relative evidence supporting prevention and response measures.
- To propose a layered framework and practical evaluation indicators.

IV. RESEARCH METHODOLOGY

A. Research Design

The paper adopts a desk-based analytical research design grounded in a narrative review and thematic synthesis. It uses the supplied review paper as its principal source map and follows the themes, terminology and research concerns developed there. The accompanying sample paper was used only as a guide for organisation and presentation, not as a source of subject-matter claims. No interviews, questionnaires, experiments or field observations were conducted for this document.

B. Source Categories

The reviewed material falls into four broad categories: (1) official and law-enforcement reporting, including FBI IC3 and Indian cybercrime institutions; (2) peer-reviewed research in psychology, gerontology, criminology and usable security; (3) regulatory and policy documents concerning financial exploitation and customer safeguards; and (4) reputable news and policy reporting used in the review to describe recent Indian cases and digital-arrest developments. Foundational work is retained where it provides concepts that remain useful, such as persuasion principles and fraud taxonomies.

C. Thematic Analysis Procedure

The source material was organised under recurring themes: scale and trends, targeting and susceptibility, cognitive and psychosocial factors, digital skills and usability, scam typologies, emerging technologies, Indian institutional context, consequences, mitigation and research gaps. The themes were then compared to identify where multiple sources converge and where claims remain preliminary. Mitigation evidence is described qualitatively as strong, moderate or emerging, consistent with the approach used in the supplied review. These labels are indicative rather than the result of a formal systematic-review grading instrument.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

D. Evidence Interpretation

Complaint statistics are treated as reported cases and reported losses, not as a complete estimate of all fraud. Cross-country comparisons are made cautiously because reporting systems and definitions differ. Recent Indian digital-arrest figures are presented as figures reported by authorities or secondary sources, not as independently audited estimates. Findings from laboratory phishing tasks are not assumed to predict every real-world incident.

E. Ethical and Methodological Boundaries

The paper does not diagnose cognitive impairment, infer that all older adults share the same risk profile, or suggest that relatives should take control of a person's finances. The proposed framework emphasises informed choice, proportional safeguards and confidentiality. Since this is a secondary-source study, its conclusions are analytical and should be tested through representative Indian field research before being treated as measured intervention effects.

V. CONCEPTUAL BACKGROUND

A. Cyber-Enabled Fraud and Social Engineering

Cyber-enabled fraud uses digital communication, accounts, platforms or payment infrastructure to deceive a person for financial or other gain. Social engineering is the manipulation of human judgement through trust, fear, urgency, authority, affection or apparent reciprocity. Unlike malware-based attacks, social engineering can succeed even when a device and account are technically secure, because the victim is persuaded to perform the requested action.

B. Targeting Versus Susceptibility

Targeting describes why offenders select a person or group; susceptibility describes why a particular interaction succeeds. Older adults may be targeted because some hold retirement savings or are reachable through telephone and messaging channels. Susceptibility varies widely and can be influenced by isolation, bereavement, digital confidence, interface design, financial habits and the credibility of the scam narrative. Ross et al. (2014) caution against the broad claim that older adults are inherently more gullible than younger people.

VI. THREAT LANDSCAPE AND REPORTED TRENDS

The supplied review summarises FBI IC3 figures for people aged 60 and above. The figures show a rise in both complaint volume and reported losses between 2022 and 2025. They illustrate the scale of reported harm, although they should not be interpreted as a population prevalence rate.

Year	Complaints (approx.)	Reported losses	Approx. annual loss change
2022	88,000	USD 3.1 billion	—
2023	101,000	USD 3.4 billion	+10%
2024	147,000	USD 4.9 billion	+43%
2025	201,000	USD 7.7 billion	+59%

Table 1. Reported FBI IC3 complaints and losses among victims aged 60 and above. Values are rounded as presented in the supplied review; see FBI IC3 annual reports (2023–2026).

The review notes that investment fraud accounted for a substantial portion of reported losses in 2025, with technical-support and confidence or romance scams also prominent. Cryptocurrency-related complaints and losses were especially significant. It also describes the use of cryptocurrency kiosks and AI-assisted impersonation, including cloned voices in family-emergency narratives (HousingWire, 2026; AARP, 2026).

The figures must be interpreted carefully. First, reporting is voluntary, so embarrassment, uncertainty or fear may keep incidents out of official records. Second, agencies may use different categories and reporting procedures. Third, a rise in reported losses may reflect changes in the number of incidents, the average amount lost, awareness of reporting channels or a combination of these factors. The safest conclusion is that reported losses have grown sharply and that older victims can experience severe individual financial consequences.

A. Why Aggregate Losses Matter

Aggregate losses indicate the scale of the problem, but they do not capture the full impact on a person. A single loss may affect retirement security, access to healthcare, housing choices and family relationships. For someone with limited opportunity to rebuild

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

savings, a large transfer can have lasting consequences. Accordingly, prevention should be assessed not only by the number of incidents prevented but also by the severity of losses avoided and the quality of support provided after an incident.

B. Limits of Cross-National Comparison

The review refers to similar patterns in countries including the United Kingdom, Australia, Canada and Singapore. However, differences in legal definitions, reporting channels, age bands and financial systems make direct ranking unreliable. International evidence is most useful for identifying recurring scam mechanisms and policy approaches that may be adapted locally, rather than assuming that a measure will have identical effects in every jurisdiction.

VII. VULNERABILITY FACTORS AMONG SENIOR CITIZENS

The literature reviewed in the source paper groups risk factors into four connected clusters. These clusters are analytical categories rather than fixed traits. A person may experience one or more factors at a particular time, and the same factor may have little effect in a different situation.

Factor cluster	Examples described in the literature	Practical implication
Cognitive	Processing speed, working memory, evaluating deceptive cues under pressure; individual financial decision difficulties	Reduce time pressure; use clear verification steps and accessible prompts.
Psychosocial	Loneliness, bereavement, depression, trust, politeness norms and desire for connection	Build trusted support and make disclosure safe and non-judgemental.
Digital and technological	Uneven security skills, uncertainty about message verification, password-management difficulty and changing interfaces	Use simple defaults, guided setup and realistic practice.
Situational and structural	Accessible savings, living alone, frequent unsolicited contact, complex bank or government interfaces	Detect unusual transactions and improve service design and contact controls.

Table 2. Thematic synthesis of vulnerability factors, adapted from the studies discussed in the supplied review.

A. Cognitive and Decision-Making Factors

Some studies associate fraud victimisation with differences in selected cognitive measures, trust and financial decision-making capacity (Judges et al., 2017; Spreng et al., 2016). These findings do not mean that normal ageing inevitably produces poor judgement. Rather, a complex decision made under pressure may become more difficult when the caller controls the pace, supplies a large amount of information and discourages independent verification. A useful safeguard is to create a pause between the demand and the payment.

B. Psychosocial Factors

Fraud scripts often exploit ordinary human needs. A romance scam may build emotional intimacy over time; a family-emergency scam may activate concern for a relative; and a supposed official may use fear of punishment. Loneliness or bereavement can increase the value of a persuasive social connection, but these experiences do not make a person responsible for the offender's deception. Family and community support should therefore be offered respectfully, without ridicule or surveillance.

C. Digital Skills and Usability

Access to a smartphone does not necessarily imply confidence in identifying phishing, managing credentials or checking a sender's identity. Research on older adults' security practices shows that users often develop reasonable strategies from everyday experience, but those strategies may not match the risks of online systems (Frik et al., 2019). Technical warnings, complicated authentication and frequent interface changes can make safe behaviour harder to perform.

D. Situational Exposure

Risk also depends on how often a person receives unsolicited calls or messages, whether they live alone, the availability of a trusted person to consult, and whether a payment is unusually large or urgent. These circumstances are potentially modifiable by institutions through call screening, transaction alerts and clear escalation procedures.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

VIII. PSYCHOLOGICAL MECHANISMS USED BY SCAMMERS

Scammers rarely depend on technical deception alone. They create a story that narrows the victim's choices and makes immediate compliance appear safer than delay. Cialdini's (2009) persuasion principles provide a useful lens for understanding these tactics.

Persuasion mechanism	How it appears in a scam	Protective response
Authority	Caller claims to be police, bank staff or a government officer	End the call and independently contact the organisation using a verified number.
Scarcity and urgency	Victim is told that an account will be blocked or a relative is in danger	Treat deadlines and threats as reasons to pause, not to pay.
Liking and emotional connection	Fraudster builds friendship or romance before asking for money	Discuss unusual financial requests with a trusted person.
Reciprocity	Scammer offers help, a prize or an apparent favour before demanding payment	Do not treat a favour or promised reward as proof of legitimacy.
Social proof	Fake testimonials, endorsements or supposed investment success stories	Verify claims independently; do not rely on screenshots or online comments.
Commitment	Small initial steps lead to larger payments or disclosure	Stop when a request changes or becomes more demanding.

Table 3. Examples of persuasion mechanisms and corresponding interruption habits.

A. Fear and Authority

Digital-arrest narratives are a clear example of authority combined with fear and secrecy. A caller may claim that a parcel, bank account or identity document is linked to a serious offence. The victim may be instructed to remain on a video call, avoid contacting relatives and transfer funds for ‘verification’. The pressure is designed to prevent the person from checking whether the claim is real.

B. Urgency and Isolation

Urgency reduces the time available for reflection. Secrecy isolates the target from people who might challenge the story. A practical response must break both mechanisms: disconnect from the caller, contact a trusted person and verify through an independently obtained official channel. A real organisation should not require a customer to remain on an unsolicited call while transferring funds.

C. Relationship-Based Manipulation

Romance and confidence scams may unfold over weeks or months. The offender establishes trust, then introduces an emergency, travel expense or investment opportunity. Whitty (2013, 2018) describes staged persuasion and psychological characteristics associated with romance-scam victimisation. Prevention should avoid simplistic warnings that dismiss online relationships; instead, it should focus on requests for money, secrecy, identity verification and pressure.

D. Behavioural Entry Points

Research on investment fraud suggests that the way a person responds to an unsolicited offer may be as important as general financial knowledge (DeLiema et al., 2020). This supports teaching an early-interruption habit: do not continue an unsolicited financial conversation; independently research the organisation; and never install remote-access software or transfer funds at the direction of an unknown caller.

IX. TYPOLOGY OF SCAMS AFFECTING OLDER ADULTS

The scam categories below are adapted from the fraud-taxonomy approach discussed by Beals et al. (2015) and the recent threat patterns summarised in the supplied review. The same incident may combine several categories.

Scam category	Typical narrative or technique	Common requested action
Government or law-enforcement impersonation	Victim is accused of a crime, parcel offence or tax issue; secrecy and immediate compliance are demanded	Transfer money to a ‘safe’ or verification account.
Technical/customer-support fraud	Pop-up or caller claims a device or account is compromised	Install remote-access software, disclose credentials or move funds.
Investment and cryptocurrency fraud	Fake adviser or platform displays apparent profits and blocks withdrawals	Make additional deposits or convert cash to cryptocurrency.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Romance and confidence fraud	Online relationship develops before an emergency or financial request	Send transfers, gift cards or cryptocurrency.
Family-emergency fraud	Caller imitates a relative or uses a cloned voice to describe urgent trouble	Send money quickly without checking with the relative.
Phishing, smishing and spoofing	Messages imitate banks, delivery firms, utilities or pension offices	Open a link, reveal login details or share an OTP.
Recovery fraud	A second offender claims to recover previously lost funds	Pay an advance fee or share more financial information.

Table 4. Common scam types, mechanisms and payment or access requests.

A. Authorised Payment Fraud

A particularly important distinction is whether the customer is tricked into approving a payment. In authorised payment fraud, the payment may pass normal authentication checks because the account holder has entered the details and approved it. This can make detection difficult for systems designed primarily to identify stolen credentials or unauthorised account access. Banks therefore need to consider behavioural signals and the context surrounding a transaction, while avoiding assumptions based only on a customer's age.

B. Repeat Victimisation and Recovery Scams

People who have already lost money may be contacted again by criminals claiming to be investigators, lawyers or recovery specialists. The promise of retrieving funds can be emotionally powerful. Victim lists may circulate among offenders, so post-incident support should include a warning about recovery fraud, guidance on securing accounts and a clear route for reporting further contact.

C. AI-Enabled Impersonation

Generative AI can improve the fluency and personalisation of scam messages. Voice cloning can make a family-emergency call sound familiar, while synthetic images or video may be used to promote fraudulent investments. As traditional cues become less reliable, verification should depend on a process rather than on how convincing a voice, image or message appears. A pre-agreed family code word and call-back to a known number are examples of process-based checks.

X. THE INDIAN CONTEXT: DIGITAL-ARREST FRAUD AND RESPONSE

India is a significant setting for this research because smartphone adoption and digital payments have expanded rapidly, while the population aged 60 and above is also growing. The UNFPA India Ageing Report 2023 estimates that older adults represented about 10.5 per cent of India's population in 2022 and projects a substantial increase by 2050. Digital inclusion can improve access to services, but it must be accompanied by usable security and accessible reporting.

A. Digital-Arrest Scam Pattern

In a digital-arrest scam, offenders impersonate police, customs, the Central Bureau of Investigation or another authority. They may claim that a parcel contains illegal goods or that a bank account is linked to money laundering. The victim is pressured to stay on a telephone or video call, keep the matter secret and transfer funds for supposed verification. The supplied review emphasises that ‘digital arrest’ is not a legal process through which an authority arrests a person by video call and demands payment.

The review reports that I4C recorded approximately Rs. 120.30 crore in digital-arrest losses between January and April 2024, and that a government statement to the Supreme Court in 2025 referred to losses of around Rs. 3,000 crore. These values are reproduced as reported in the review and should be checked against primary government records before formal policy use (PMF IAS, 2024; Drishti IAS, 2025).

B. Reporting and Institutional Mechanisms

The Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal and the 1930 helpline form important parts of the national response. Rapid reporting can allow banks and authorities to flag or freeze funds before they move through multiple accounts. The review highlights the need to make these channels familiar before an incident occurs, rather than expecting a distressed victim to discover them during a crisis.

C. Language and Trust

Awareness material should be available in regional languages and in formats that match how people communicate, including audio, video and in-person sessions. Terms such as phishing, OTP and two-factor authentication may be unfamiliar. Messages should

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

instead explain actions in everyday language: never share an OTP; do not install an app at the request of an unknown caller; disconnect and verify; and call 1930 promptly if money has been transferred.

D. Institutional Coordination

A fraud may involve a spoofed telephone number, a messaging account, a mule bank account and a payment platform. No single institution sees the entire chain. The Indian response therefore requires timely information-sharing, consistent escalation routes and cross-border cooperation. Public communication should also avoid creating panic or implying that every unknown call is criminal; the objective is to teach verification habits that can be used calmly and repeatedly.

XI. CONSEQUENCES OF FRAUD VICTIMISATION

Financial loss is the most visible outcome, but it is not the only one. Research discussed in the supplied review identifies stress, depression, loss of confidence, relationship difficulties and, in severe cases, suicidal thoughts among fraud victims (Button et al., 2014). The impact may be especially serious for people who depend on fixed retirement income or who have limited time to rebuild savings.

A. Financial and Practical Effects

A large loss can reduce the funds available for healthcare, housing, daily living and support for dependants. Victims may borrow from relatives or sell assets. Even when some money is recovered, the process can involve repeated calls, documentation, uncertainty and time away from ordinary activities. The loss may also undermine confidence in digital banking and public services.

B. Psychological and Social Effects

Shame and self-blame can prevent victims from telling family members or reporting the incident. Some fear that relatives will regard them as incapable of managing their own affairs. A blaming response can deepen isolation and make a second scam more likely to succeed. A supportive response should focus on the offender's conduct, immediate safety and practical next steps rather than asking why the victim believed the story.

C. Autonomy and Protection

Families may respond by taking over an older person's finances or discouraging all use of digital devices. Although intended as protection, blanket restrictions can reduce independence and social connection. The more balanced approach is protection without paternalism: offer a trusted contact, transaction alerts, shared verification routines and optional payment safeguards while keeping the account holder involved in decisions.

D. Post-Incident Support Pathway

- Contact the bank or payment provider immediately and request that the transaction and beneficiary account be flagged.
- Report the financial cyber fraud through India's 1930 helpline and the National Cyber Crime Reporting Portal as quickly as possible.
- Preserve call logs, messages, payment references, screenshots and other relevant evidence.
- Secure affected accounts and devices; change compromised credentials and remove remote-access tools installed at a scammer's direction.
- Warn the victim about recovery scams and further contact from people promising guaranteed refunds.
- Provide emotional support and, where needed, counselling or legal assistance.

The sequence above is general guidance, not a guarantee that funds can be recovered. The chance of intervention may depend on how quickly the incident is reported, the payment route and whether funds remain traceable.

XII. MITIGATION STRATEGIES: A LAYERED MODEL

The evidence reviewed supports a defence-in-depth approach. Each layer addresses a different part of the fraud process, and no single layer is expected to stop every incident. The following sections translate the evidence into an integrated model.

A. Layer 1 — Education and Awareness

Education is most useful when it is specific, repeated and based on realistic scenarios. Burke et al. (2022) report that targeted educational interventions can reduce susceptibility in tested financial-fraud scenarios, while Scheibe et al. (2014) found that forewarning about persuasion tactics can help consumers resist deception. The supplied review notes that effects may be strongest immediately after instruction, which supports refresher sessions rather than a single awareness event.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

A concise set of memorable rules is preferable to a long technical checklist: (1) no legitimate authority will arrest a person over a video call and demand payment; (2) urgency plus secrecy is a warning sign; (3) never share an OTP or allow an unknown caller to control a device; and (4) hang up and independently verify. Training should include role-play of a threatening call, a fake investment offer and a family-emergency message.

B. Layer 2 — Family and Community Support

Families can establish code words for emergencies, agree that unusual money requests will be checked through a second channel, and enable transaction alerts with the older person's consent. Community organisations, resident groups, banks, pension offices and local police can host short sessions led by trained peer educators. A non-judgemental culture is essential: older adults should know they can report a mistake immediately without losing dignity or independence.

C. Layer 3 — Financial-Institution Safeguards

Banks and payment providers can identify unusual activity such as a large first-time transfer to a new beneficiary, several transfers in quick succession or a payment inconsistent with a customer's established pattern. Staff can ask calm, neutral questions when a customer appears to be under pressure or remains on a phone call while making a transaction. FinCEN (2022) provides guidance on indicators of elder financial exploitation, and FINRA (2017) describes safeguards such as trusted-contact arrangements and temporary holds in relevant circumstances.

Possible payment-friction measures include a cooling-off period for a high-value first payment to a new payee, a clear warning when a customer is on a call during a transfer, and customer-configurable transaction limits. These measures should be proportionate, transparent and accessible, with a route for legitimate urgent payments. Independent evaluation is needed before their effectiveness can be stated conclusively.

D. Layer 4 — Telecom and Platform Controls

Telecom operators can improve filtering of spoofed numbers and known scam traffic. Messaging and social platforms can detect coordinated impersonation accounts, fraudulent advertisements and suspicious links, then respond quickly to credible reports. Device makers can provide clear scam warnings, automatic security updates and controls that limit installation of remote-access applications. These interventions reduce exposure but cannot replace user verification and financial safeguards.

E. Layer 5 — Rapid Response, Law and Victim Support

A rapid reporting and fund-freezing pathway can reduce the time available for criminals to move money. Law-enforcement coordination is necessary when operations cross state or national borders. Victim support should include practical recovery guidance, counselling and protection from repeat targeting. A system that only records a complaint, without communicating next steps, may discourage future reporting.

XIII. PROPOSED INTEGRATED PROTECTION FRAMEWORK

Based on the themes in the reviewed literature, this paper proposes the Senior Citizen Cyber-Fraud Protection Framework (SCCPF). It is a conceptual framework, not a tested product or a claim of measured effectiveness. Its purpose is to coordinate prevention, detection, interruption and recovery around the needs and autonomy of older users.

Layer	Primary actors	Core functions	Suggested indicators
1. Contact prevention	Telecom operators, platforms	Filter spoofed calls; remove scam accounts and ads; flag suspicious links	Reported scam contacts; takedown response time
2. User and community readiness	Older users, families, NGOs, local bodies	Scenario training; code words; trusted contacts; multilingual guidance	Training reach; knowledge retention; confidence to report
3. Transaction protection	Banks, payment apps, regulators	Detect unusual payments; warnings; optional delays; staff escalation	High-risk transactions reviewed; intervention outcomes
4. Rapid incident response	Banks, I4C, police, cybercrime portal	Immediate reporting; beneficiary flagging; evidence preservation	Time from discovery to report; funds placed on hold
5. Recovery and accountability	Law enforcement, legal aid, counsellors	Investigation; victim support; repeat-scam prevention	Victim follow-up; support uptake; repeat victimisation

Table 5. Proposed five-layer Senior Citizen Cyber-Fraud Protection Framework.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

A. Operating Sequence

The framework begins before a scam occurs. Telecom and platform controls reduce the volume of malicious contact. Education and trusted relationships help the user recognise pressure tactics and verify unexpected requests. If a suspicious payment is attempted, the financial institution applies proportionate friction and escalates the case when appropriate. If money is transferred, the user or supporter reports immediately so that the bank and relevant authorities can attempt to interrupt the movement of funds. Finally, victim support and investigation address the consequences and reduce the risk of repeat victimisation.

B. Design Principles

- Autonomy: safeguards should support informed decisions, not automatically remove access from older customers.
- Usability: warnings and reporting instructions should use plain language, readable layouts and regional languages.
- Proportionality: friction should respond to risk signals and allow legitimate transactions through a clear process.
- Privacy: trusted-contact arrangements and transaction alerts should operate with informed consent.
- Coordination: institutions should share actionable information through lawful and secure channels.
- Accountability: interventions should be measured and independently evaluated.

C. Why a Layered Model Is Necessary

A scam can bypass any one defence. A call may pass telecom filters; the victim may know the warning signs but feel frightened; the bank may see a validly authenticated payment; and a report may arrive after funds have moved. Multiple independent opportunities to pause and verify make the overall system more resilient. This logic resembles defence-in-depth approaches used in safety and cybersecurity engineering.

XIV. EVALUATION PLAN AND RESEARCH PROPOSITIONS

The framework requires empirical testing before claims can be made about its effectiveness. A future study in India could use a mixed-method design involving older adults, family supporters, bank personnel and community educators. The following plan is proposed for subsequent research; it was not carried out for this paper.

A. Proposed Study Design

A multi-site study could recruit participants from urban, semi-urban and rural communities, with representation across age bands, gender, language preference and levels of digital experience. Researchers could first conduct a baseline survey of scam awareness, verification habits, previous exposure and confidence in reporting. Participants could then receive a scenario-based education session, with a follow-up assessment immediately after training and again after several months. Interviews with bank staff and community educators could identify practical barriers to adoption.

B. Proposed Evaluation Measures

Evaluation domain	Possible measure	Reason for inclusion
Knowledge	Correct identification of scam cues in short scenarios	Tests practical recognition rather than recall of technical terms.
Behavioural intention	Willingness to disconnect and verify before payment	Measures adoption of interruption habits.
Reporting readiness	Ability to identify 1930 and the reporting portal	Tests whether users know the first response step.
Institutional response	Time from alert to staff review or beneficiary flag	Assesses operational speed.
User experience	Perceived clarity, dignity, trust and ease of use	Checks for unintended barriers or paternalism.
Financial outcomes	Number and value of prevented or interrupted transfers	Provides outcome indicators where data access is lawful.

Table 6. Proposed indicators for future evaluation; no results are claimed in this paper.

C. Research Propositions

- P1: Scenario-based training will improve recognition of urgency, secrecy and impersonation cues compared with information-only guidance.
- P2: Repeated training and refresher prompts will retain practical verification behaviour better than a one-time session.
- P3: Optional payment friction combined with trained staff escalation will improve detection of suspicious authorised payments.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

- P4: Regional-language and audio-visual guidance will improve accessibility for users who are less comfortable with English-language interfaces.
- P5: Supportive, non-judgemental family and community responses will increase early disclosure and reporting intention.

D. Analysis Approach

Survey responses could be summarised using frequencies, percentages and group comparisons. Pre- and post-training scores could be analysed with suitable paired statistical tests if sample size and distributional assumptions permit. Interview material could be coded thematically to identify usability concerns, institutional barriers and unintended effects. Any report should disclose recruitment methods, sample size, missing data, intervention duration and limitations.

E. Safeguards for Participants

Researchers should avoid exposing participants to realistic threats without consent or adequate debriefing. Simulated scam messages should not collect real credentials or money. Participation must be voluntary, data should be minimised and protected, and any disclosure of an ongoing fraud should be handled through an approved referral protocol.

XV. SWOT-STYLE ASSESSMENT OF CURRENT MITIGATION

The following SWOT-style assessment is an analytical synthesis of the reviewed material. It is not a measured scorecard and should be read as a structured discussion of strengths, weaknesses, opportunities and threats.

Strengths	Weaknesses
• Growing public awareness of cyber fraud. • Existing reporting channels such as 1930 and the National Cyber Crime Reporting Portal. • Evidence that targeted education and forewarning can reduce susceptibility in studied scenarios. • Banks and telecom providers possess data that can help identify suspicious activity.	• Underreporting and fragmented data. • Uneven digital skills and language accessibility. • Authorised payments can appear legitimate to conventional controls. • Limited independent evaluation of some payment-friction and platform interventions.

Opportunities	Threats
• Regional-language and peer-led education. • Trusted-contact and customer-configurable safeguards. • Better coordination among banks, telecom firms and platforms. • AI-assisted detection and improved scam-account takedowns. • Independent Indian field studies and age-disaggregated data.	• AI-generated voices, images and personalised messages. • Cross-border criminal networks and mule accounts. • Rapid and difficult-to-reverse payment systems. • Repeat targeting through recovery scams. • Overly restrictive responses that undermine autonomy and digital inclusion.

Table 7. SWOT-style assessment of senior-citizen cyber-fraud mitigation.

A. Strengths and Opportunities

India has established reporting mechanisms and institutional structures that can form the basis of a coordinated response. Public education can be strengthened by moving from generic warnings to short, memorable scripts delivered through trusted local channels. Banks can use existing transaction-monitoring capabilities to identify unusual payment patterns, while platforms can reduce exposure by acting on impersonation and fraudulent advertisements.

B. Weaknesses and Threats

The largest weakness is the gap between a victim's experience and an institution's ability to respond quickly. A person may not know where to report, may feel ashamed, or may believe the caller's instruction to remain silent. At the same time, criminals adapt rapidly to new technology and payment methods. A defensive strategy that relies only on awareness or only on technical detection will remain incomplete.

C. Implementation Priorities

- Make the first reporting action visible in bank applications, branches and community awareness material.
- Train front-line staff to recognise coercion and ask neutral questions without stereotyping customers by age.
- Offer optional, understandable safeguards for first-time high-value transfers and new beneficiaries.
- Coordinate rapid takedown and account-flagging processes across relevant institutions.
- Provide clear post-incident support and explicit warnings about recovery scams.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

XVI. DISCUSSION

The analysis supports a shift from individual blame to shared responsibility. Fraudsters operate with prepared scripts, technical tools, access to personal information and the ability to move money across institutional boundaries. The victim is often required to make only one decision under intense pressure. It is therefore unrealistic to expect personal vigilance to serve as the sole defence. Systems should be designed to make safe decisions easier and harmful transfers harder to complete.

A second implication is that cybersecurity for older adults must extend beyond passwords and malware. Secure authentication remains important, but it does not prevent a customer from being persuaded to reveal an OTP, install remote-access software or authorise a transfer. Human-centred controls—clear prompts, trusted verification, transaction delays in appropriate circumstances and trained staff—address the point at which deception becomes a payment.

A third implication concerns dignity. Older adults should not be treated as a single risk category or deprived of digital access. The most appropriate safeguards are transparent, proportionate and chosen with the account holder. Family involvement can be valuable, but should be based on consent and a relationship of trust. This approach is consistent with the review's emphasis on supportive responses and the importance of autonomy.

A. Implications for Government and Regulators

Public authorities can support consistent reporting standards, multilingual awareness, faster inter-agency coordination and stronger cross-border investigation. Digital-inclusion programmes should include safety training as a core component. Regulators can encourage banks and payment providers to evaluate customer-protection measures and publish clear information about escalation and reimbursement processes.

B. Implications for Banks and Payment Providers

Financial institutions should combine transaction analytics with human review. A high-value payment to a new beneficiary is not proof of fraud, but it may justify a clear warning or a brief verification step, particularly when other risk signals are present. Staff training should focus on observable behaviour and transaction context rather than age alone. Trusted-contact arrangements should not transfer control of the account unless a separate lawful process applies.

C. Implications for Families and Communities

Families can normalise conversations about fraud before an incident occurs. A simple family protocol can specify that urgent requests for money will always be verified by calling back on a known number. Community groups can offer practical demonstrations using examples in local languages. The aim is to make asking for help routine rather than embarrassing.

XVII. LIMITATIONS OF THE STUDY

This paper is based on secondary sources and does not include original participant data. Complaint-based statistics undercount incidents and may not be directly comparable across agencies. Some recent figures in the supplied review are drawn from secondary reporting of official statements and should be verified against primary records before formal citation. Much of the Indian evidence on digital-arrest fraud is not available as a systematic, age-disaggregated dataset. Studies conducted in other countries or using laboratory simulations may not generalise fully to Indian older adults. Finally, the proposed framework and evaluation plan are conceptual and have not been tested as an integrated intervention.

XVIII. RECOMMENDATIONS

- Use repeated, scenario-based training in regional languages, focusing on urgency, secrecy, impersonation and independent verification.
- Promote immediate reporting through 1930 and the National Cyber Crime Reporting Portal, and make instructions visible in bank apps and branches.
- Offer proportionate, optional safeguards for unusual first-time payments, supported by staff trained to recognise coercion without stereotyping customers.
- Coordinate spoofed-number filtering, scam-account takedowns and lawful information-sharing among banks, telecom operators and digital platforms.
- Provide non-judgemental victim support, warn against recovery scams, and evaluate interventions using transparent outcome measures.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

XIX. CONCLUSION

Cyber-enabled fraud against senior citizens is a social, technological and financial problem. The reviewed evidence points to rising reported losses and serious impersonation schemes in India. Risk cannot be explained by age alone; it emerges from scam tactics, individual circumstances, uneven digital skills, service design and fast payment systems.

The proposed five-layer framework combines contact prevention, community readiness, transaction safeguards, rapid response and victim support. Protection should be shared across institutions while preserving older adults' autonomy. Its effectiveness in India must be tested through field studies.

Future research should develop age-disaggregated Indian data, test multilingual training and evaluate bank interventions, including responses to AI-generated impersonation. Safer digital inclusion depends on services that are easier to use safely and provide timely help when deception occurs.

XX. REFERENCES

[1] AARP. (2026). New FBI report: $20.9 billion lost to internet crimes in 2025, older adults hit hardest. https://www.aarp.org/money/scams-fraud/fbi-ftc-report-2025-losses
[2] Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. Stanford Center on Longevity and FINRA Investor Education Foundation.
[3] Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? Journal of Economic Behavior & Organization, 198, 250–266.
[4] Burnes, D., Henderson, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. American Journal of Public Health, 107(8), e13–e21.
[5] Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36–54.
[6] Cialdini, R. B. (2009). Influence: Science and practice (5th ed.). Pearson Education.
[7] Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud (Trends & Issues in Crime and Criminal Justice No. 518). Australian Institute of Criminology.
[8] DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. Journal of Consumer Research, 46(5), 904–914.
[9] Drishti IAS. (2025, December 3). SC directions on 'digital-arrest' scams. https://www.drishtiias.com/daily-updates/daily-news-analysis/sc-directions-on-digital-arrest-scams
[10] Ebner, N. C., et al. (2020). Uncovering susceptibility risk to online deception in aging. The Journals of Gerontology: Series B, 75(3), 522–533.
[11] FBI Internet Crime Complaint Center. (2023). 2022 Internet crime report. U.S. Department of Justice. https://www.ic3.gov
[12] FBI Internet Crime Complaint Center. (2024). 2023 Internet crime report. U.S. Department of Justice. https://www.ic3.gov
[13] FBI Internet Crime Complaint Center. (2025). 2024 Internet crime report. U.S. Department of Justice. https://www.ic3.gov
[14] FBI Internet Crime Complaint Center. (2026). 2025 Internet crime report. U.S. Department of Justice. https://www.ic3.gov
[15] Financial Crimes Enforcement Network. (2022). Advisory on elder financial exploitation (FIN-2022-A002). U.S. Department of the Treasury.
[16] Financial Industry Regulatory Authority. (2017). Regulatory Notice 17-11: FINRA adopts rules relating to financial exploitation of seniors. FINRA.
[17] Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., & Egelman, S. (2019). Privacy and security threat models and mitigation strategies of older adults. Proceedings of SOUPS 2019, 21–40.
[18] Grimes, G. M., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. Educational Gerontology, 36(3), 173–192.
[19] Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. First Monday, 7(4).
[20] HousingWire. (2026). FBI seniors cybercrime 2025. https://www.housingwire.com/articles/fbi-seniors-cybercrime-2025/

(This work is licensed under a Creative Commons Attribution 4.0 International License.)