Article

Not peer-reviewed version

Digital Deception: Online Fraud Targeting the Elderly – Patterns, Mechanisms, and Policy Responses

Wendy Carter *

Posted Date: 13 May 2025

doi: 10.20944/preprints202505.0928.v1

Keywords: online fraud; elderly users; phishing; digital literacy; cybercrime; scam prevention; human-computer interaction

 doi:10.20944/preprints202505.0928.v1

Article

Digital Deception: Online Fraud Targeting the Elderly – Patterns, Mechanisms, and Policy Responses

Wendy Carter

Independent Researcher, Australia; wendycarter8866@gmail.com

Abstract: Older adults are increasingly targeted by sophisticated online scams, exploiting cognitive vulnerabilities, digital illiteracy, and social isolation. This paper offers a comprehensive overview of the phenomenon of online fraud against the elderly, drawing on interdisciplinary research from computer science, psychology, and cyber policy. We identify common scam typologies—such as phishing, romance fraud, and tech support scams—and analyze the underlying mechanisms that make older users particularly susceptible. Drawing on empirical studies and real-world case reports, the paper also explores detection and prevention strategies, with emphasis on algorithmic fraud detection, interface design for cognitive accessibility, and the role of digital literacy education. We argue for a proactive cybersecurity framework that integrates machine learning tools, user-centered design, and targeted public policy to reduce the incidence and impact of cyber fraud on older populations.

Keywords: online fraud; elderly users; phishing; digital literacy; cybercrime; scam prevention; human-computer interaction

Introduction

The rapid digitalization of society has created a paradox for elderly users: while the internet offers opportunities for connection, healthcare access, and financial management, it also exposes them to significant cyber risks. Among the most pressing of these risks is online fraud. Older adults—typically defined in cybercrime literature as individuals aged 60 and above—are increasingly targeted by internet scams that exploit cognitive aging, technological unfamiliarity, and socio-emotional vulnerabilities (Choi et al., 2020; Cross, 2016).

The global scale of this problem is evident. In the United States alone, the FBI's Internet Crime Complaint Center (IC3) reported that in 2022, victims over the age of 60 lost over $3.1 billion to cyber-enabled fraud, marking a 74% increase from 2021 (FBI IC3, 2023). This trend is mirrored globally, with elderly victims often suffering not only financial loss but also psychological distress, social withdrawal, and diminished trust in digital services (Button et al., 2009; Lichtenberg et al., 2016).

Scholars in computer science have highlighted the increasing technical sophistication of scams, including the use of deepfakes, spoofed websites, and AI-generated phishing messages (Canham et al., 2021). From a psychological standpoint, research shows that age-related cognitive changes—such as declines in working memory, processing speed, and executive function—may reduce older adults' ability to recognize deception cues (James et al., 2014). Furthermore, social isolation and desire for human contact make elderly users more likely to respond to scams involving emotional manipulation, such as romance or grandparent scams (Pak & Shadel, 2011).

Despite the severity of the problem, research on online fraud targeting the elderly remains fragmented across disciplines. This paper seeks to integrate findings from cybercrime research, human-computer interaction (HCI), and aging studies in order to: (1) categorize the primary types of online fraud targeting older adults; (2) identify the cognitive, social, and technical mechanisms that

 doi:10.20944/preprints202505.0928.v1

increase susceptibility; and (3) review existing and emerging prevention strategies, with a focus on technology design and policy frameworks.

In doing so, we aim to inform researchers, policymakers, and technology designers about the unique needs of aging digital users and to propose actionable interventions that reduce their risk of victimization in an increasingly connected world.

Literature Review

1. Technological Dimensions: How Online Scams Exploit System Vulnerabilities

Online fraud is a dynamic field of cybercrime that evolves alongside technological advancement. From simple email phishing to complex multi-layered social engineering attacks, the arsenal available to cybercriminals continues to expand. For elderly users, who often lack up-to-date digital literacy, this creates an asymmetric battlefield (Hunsaker & Hargittai, 2018).

Phishing remains one of the most prevalent threats. These scams involve the use of deceptive emails, websites, or messages to trick users into revealing personal data, login credentials, or financial information (Abawajy, 2014). Older users are particularly vulnerable due to outdated browsers, poor password hygiene, and a lower likelihood of using multi-factor authentication (DeLiema, 2018). Additionally, the rise of AI-generated content—such as realistic deepfake audio and text—has further blurred the line between legitimate and fraudulent communication (Floridi et al., 2020).

Another growing threat is the tech support scam, where fraudsters impersonate IT professionals and deceive users into installing malware or giving remote access to their devices. This type of fraud preys on older adults' perceived lack of technical knowledge and their trust in institutional authority (Canham et al., 2021). Similarly, romance scams, often conducted over social media or dating platforms, use long-term psychological manipulation to extract large sums of money from emotionally vulnerable victims (Whitty & Buchanan, 2012).

Computer science research has also highlighted the critical role of poor interface design in enabling fraud. Complex navigation, ambiguous warning messages, and inconsistent security indicators can lead older users to make risky decisions (Redmiles et al., 2018). The field of Human-Computer Interaction (HCI) has called for inclusive design principles—such as large font sizes, clear security feedback, and step-by-step user flows—that take into account age-related declines in vision, cognition, and motor skills (Zhou et al., 2019).

Efforts to use machine learning and pattern recognition for fraud detection are promising but limited in their reach to end users. While backend systems at banks or tech platforms may detect anomalies in transaction patterns, these technologies are often invisible to the user and rely on post hoc intervention. As a result, preventative approaches—such as browser extensions that warn users in real time or interfaces that prompt for second opinions—are increasingly being researched as frontline defenses (Jain & Gupta, 2021).

2. Cognitive and Emotional Vulnerabilities in Older Adults

While online scams exploit external technological weaknesses, they also capitalize on internal vulnerabilities rooted in the aging process. Psychological and neurocognitive research indicates that older adults experience age-related declines in memory, processing speed, and executive function, all of which may impair their ability to identify fraudulent cues or assess risk accurately (Bayer, 2019; Reuter-Lorenz & Park, 2014; Spreng et al., 2016). These deficits can make them disproportionately susceptible to persuasive tactics used in fraudulent messages, particularly when the content is emotionally charged.

One well-documented phenomenon is the "positivity effect," in which older adults tend to focus more on emotionally positive information and show reduced attention to negative or threatening stimuli (Carstensen & Mikels, 2005). While this tendency can support emotional well-being, it may also hinder fraud detection—especially in scams that mask malicious intent behind friendly or flattering communication, such as romance frauds or fake investment schemes (James et al., 2014).

 doi:10.20944/preprints202505.0928.v1

Another important vulnerability is a decrease in skepticism toward social interactions. Research suggests that older individuals are more likely than younger adults to view strangers as trustworthy and less likely to question the motives behind requests for money or information (Castle et al., 2012). This is exacerbated by loneliness, bereavement, and shrinking social circles—conditions common in late adulthood—which may increase the emotional impact of scam communications (Shadel & Pak, 2007).

Cognitive load also plays a critical role. Fraudsters often use time pressure, complexity, or technical jargon to overwhelm potential victims. Older adults, who may process complex information more slowly, are more likely to fall prey when these tactics are combined with emotional appeals, such as urgent claims that a grandchild is in danger or that a bank account has been compromised (DeLiema, 2018).

Importantly, susceptibility to scams is not solely a function of cognitive decline or age. Studies have found that psychological traits such as low conscientiousness, high agreeableness, and financial risk tolerance can also predict victimization (Lichtenberg et al., 2016). Moreover, many victims report feeling shame or embarrassment after falling for a scam, which may delay help-seeking and increase the long-term psychological damage (Levine et al., 2021).

Thus, any effective intervention must address not only the technological frontiers of fraud but also the human dimensions—particularly those tied to the cognitive and emotional changes that accompany aging.

3. Sociocultural Contexts and Systemic Factors in Elderly Cyber Victimization

Beyond individual vulnerabilities and technological threats, online scams targeting older adults are embedded within broader sociocultural and systemic contexts. These contexts shape not only the frequency and form of victimization, but also the response by institutions, families, and the victims themselves.

One critical factor is the digital divide. Despite increasing internet use among seniors, older adults remain significantly less digitally literate compared to younger cohorts. In a comparative study across OECD countries, seniors were shown to have lower rates of smartphone usage, secure browsing habits, and awareness of digital threats (Friemel, 2016). In marginalized communities—such as low-income, rural, or ethnic minority populations—this divide is even more pronounced, resulting in compound vulnerability (van Deursen & Helsper, 2015).

Social isolation is another powerful contributor. Older adults living alone or in residential care are more likely to engage with strangers online, including scammers, in an attempt to satisfy emotional needs. These interactions are often prolonged, with victims forming what they believe to be genuine relationships, particularly in romance scams (Whitty & Buchanan, 2012). The normalization of online relationships and the stigma associated with victimization may further suppress reporting and exacerbate long-term damage.

Cultural attitudes toward aging and technology also play a role. In some societies, aging is associated with helplessness or irrelevance in digital spaces. This perception can lead to underinvestment in targeted digital literacy programs and in age-sensitive cybercrime prevention strategies (Marston et al., 2019). Moreover, elderly victims are frequently met with dismissive attitudes—by law enforcement, banks, and even family members—who may perceive them as careless or cognitively impaired rather than as targets of sophisticated criminal activity (Cross, 2016).

Institutional responses have often lagged behind the evolving landscape of elder-targeted cybercrime. While financial institutions and social platforms have introduced some safeguards, these are rarely designed with older users in mind. Furthermore, legal frameworks in many countries lack specific statutes that address online elder fraud as a distinct form of exploitation, resulting in fragmented enforcement and weak penalties for offenders (Leukfeldt et al., 2019).

A growing body of research calls for a shift from reactive to proactive approaches. This includes the integration of digital safety training into senior community centers, the development of culturally

 doi:10.20944/preprints202505.0928.v1

competent intervention models, and coordinated strategies across sectors—health, law enforcement, technology, and aging services—to support both prevention and recovery (Moschis, 2017).

Policy Responses and Technological Interventions

Efforts to combat online fraud against the elderly must operate on multiple fronts—technical, institutional, and societal. Because the risks arise from an intersection of cognitive aging, systemic exclusion, and technological asymmetry, no single solution is sufficient. Effective interventions must be designed with both the human and technological user in mind, combining real-time prevention, post-fraud support, and proactive policy design.

1. Age-Inclusive Technology Design

At the core of technical prevention is the design of digital interfaces that minimize cognitive burden and promote clarity in security decisions. User interface (UI) and user experience (UX) principles must reflect age-related cognitive and sensory changes. Studies in Human-Computer Interaction (HCI) advocate for larger clickable areas, simplified navigation, high-contrast displays, and consistent warning signals (Zhou et al., 2019). Security alerts should be context-aware and adaptive, distinguishing between novice and expert users and offering layered explanations for risk-related prompts (Redmiles et al., 2018).

In parallel, browser extensions and AI-driven agents that detect scam behavior—such as suspicious URLs, deepfake speech, or unusual transaction patterns—can provide real-time support. However, these tools should be designed with transparency and explainability to foster trust among older users. Systems that integrate voice guidance or screen readers should be prioritized, particularly for seniors with visual impairments.

2. Digital Literacy and Empowerment

Prevention must also operate through education. Government agencies, local authorities, and non-profits should invest in age-specific digital literacy programs that go beyond basic usage and include modules on privacy, fraud detection, and response protocols. Evidence shows that targeted, hands-on digital safety workshops—especially those delivered in community centers or intergenerational settings—can significantly reduce vulnerability among older adults (Choi et al., 2020).

Moreover, peer-led learning has been shown to be effective. Older adults may feel more comfortable receiving technology training from age-similar individuals, reducing stigma and increasing confidence. These programs should be culturally sensitive and multilingual where necessary, addressing the specific needs of marginalized subgroups such as immigrants, rural seniors, and those with limited formal education.

3. Legal and Institutional Reforms

Legal systems in many countries lack dedicated provisions for prosecuting cybercrimes against seniors. Laws addressing elder abuse typically focus on physical or financial abuse by known individuals, not anonymous actors across digital platforms. There is growing advocacy for a legal recognition of "digital elder fraud" as a distinct offense category, with associated investigative protocols and victim protections (Leukfeldt et al., 2019).

Financial institutions play a critical role in both detection and recovery. Many banks have developed AI systems that detect anomalies in spending patterns, but few of these are tailored to the behaviors of elderly users. Creating opt-in "digital guardianship" mechanisms—where trusted family members or advisors receive notifications of large or unusual transactions—could offer an additional layer of oversight while respecting privacy (Lichtenberg et al., 2016).

Government agencies should also maintain centralized reporting systems and public awareness campaigns. Public service announcements, social media content, and official warnings should be

 doi:10.20944/preprints202505.0928.v1

distributed in formats accessible to older populations, including printed materials, radio, and television.

4. Psychological and Social Support for Victims

The psychological consequences of falling victim to online scams are often underestimated. Older adults frequently report feelings of shame, fear of losing autonomy, and reluctance to inform their families or authorities (Levine et al., 2021). Victim support services should thus include not only financial counseling and fraud recovery guidance, but also trauma-informed psychological care.

Social reintegration programs can help rebuild trust in technology and social engagement, reducing the isolation that often follows such experiences. Support groups—both online and offline—may provide therapeutic environments where older victims can share experiences without judgment.

Discussion and Conclusion

The phenomenon of online fraud targeting older adults is emblematic of the broader challenges posed by an aging population navigating an increasingly digital world. This paper has sought to synthesize interdisciplinary perspectives—from computer science, cognitive psychology, and sociological studies—to present a holistic view of the problem, and to propose actionable solutions grounded in empirical evidence and human-centered design.

Our analysis has shown that elderly users are not passive victims of fraud, but rather active participants in digital systems that too often ignore their needs. Their susceptibility is shaped not simply by cognitive decline or technical naiveté, but by a complex interaction of emotional, social, and infrastructural factors. A scam message is not merely a phishing email; it is often a socially engineered artifact that exploits loneliness, trust, and the deep human need for connection.

Technological solutions alone are insufficient if they are not embedded in ecosystems that prioritize inclusivity and accessibility. Designing interfaces for the "average user" inherently marginalizes those outside of this demographic norm—particularly older adults, whose interaction patterns may differ significantly from younger, more tech-savvy individuals. Likewise, policy frameworks that fail to recognize elder-specific cybercrime as a distinct category overlook both the scale of the problem and its unique harm profiles.

There are several limitations to the current literature and practice. First, data on elder-targeted cybercrime is still fragmented and underreported, partly due to stigma and lack of centralized reporting mechanisms. Second, much of the research on fraud prevention remains reactive—focusing on after-the-fact interventions rather than structural prevention. Finally, there remains a need for more cross-cultural and intersectional analyses, especially in understanding how gender, socioeconomic status, and ethnicity mediate risk and response.

Looking forward, we argue that research and intervention must adopt an integrated, life-course perspective. This includes embedding digital safety education at multiple stages of adulthood, creating “digital transition” support programs for newly retired populations, and involving elderly stakeholders in the design of tools and policies intended to protect them. In parallel, investment in longitudinal data collection and interdisciplinary research consortia will help identify emerging threats and design preemptive strategies.

In sum, the digital safety of older adults is not merely a technological challenge—it is a societal imperative. As the global population continues to age, building systems that protect dignity, autonomy, and digital citizenship in later life must be at the forefront of cyber policy and design innovation.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237–248. https://doi.org/10.1080/0144929X.2013.798237

 doi:10.20944/preprints202505.0928.v1

Bayer, Y. M. (2019) Older Adults, Aggressive Marketing, and Unethical Behavior: A Sure Road to Financial Fraud?. Ethical Branding and Marketing: Cases and Lessons, 1-18.

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

Canham, S. L., Chang, J., Ferrari, M., Salas, A. S., & Lu, N. (2021). Cybercrime against older adults: What social workers need to know. *Journal of Gerontological Social Work*, 64(3), 280–294. https://doi.org/10.1080/01634372.2021.1884980

Carstensen, L. L., & Mikels, J. A. (2005). At the intersection of emotion and cognition: Aging and the positivity effect. *Current Directions in Psychological Science*, 14(3), 117–121. https://doi.org/10.1111/j.0963-7214.2005.00348.x

Castle, E., Eisenberger, N. I., Seeman, T. E., Moons, W. G., Boggero, I. A., Grinblatt, M. S., & Taylor, S. E. (2012). Neural and behavioral bases of age differences in perceptions of trust. *Proceedings of the National Academy of Sciences*, 109(51), 20848–20852. https://doi.org/10.1073/pnas.1218518109

Choi, N. G., DiNitto, D. M., & Marti, C. N. (2020). Older adults who are victims of internet fraud: Prevalence, correlates, and implications. *Journal of Elder Abuse & Neglect*, 32(5), 431–448. https://doi.org/10.1080/08946566.2020.1803307

Cross, C. (2016). *Technology-facilitated fraud and older people: Challenges and opportunities for the criminal justice system*. Trends & Issues in Crime and Criminal Justice, No. 518. Australian Institute of Criminology.

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, 58(4), 706–718. https://doi.org/10.1093/geront/gnw209

FBI Internet Crime Complaint Center (IC3). (2023). *Elder Fraud Report 2022*. https://www.ic3.gov

Floridi, L., Cowls, J., Beltrametti, M., Chiarello, F., et al. (2020). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 30(1), 1–18. https://doi.org/10.1007/s11023-020-09517-8

Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, 18(2), 313–331. https://doi.org/10.1177/1461444814538648

Hunsaker, A., & Hargittai, E. (2018). A review of internet use among older adults. *New Media & Society*, 20(10), 3937–3954. https://doi.org/10.1177/1461444818787348

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, 26(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

Jain, S., & Gupta, A. (2021). Intelligent browser-based phishing detection using deep learning. *Journal of Information Security and Applications*, 59, 102857. https://doi.org/10.1016/j.jisa.2021.102857

Leukfeldt, R., Kleemans, E. R., & Stol, W. P. (2019). Cybercriminal networks and money mules: An exploratory analysis. *Trends in Organized Crime*, 22(1), 72–93. https://doi.org/10.1007/s12117-017-9316-x

Levine, K., McAuliffe, W., & Landa, K. (2021). Psychological consequences of cyber fraud victimization in older adults. *Journal of Aging & Mental Health*, 25(5), 931–942. https://doi.org/10.1080/13607863.2020.1727847

Lichtenberg, P. A., Stickney, L., & Paulson, D. (2016). Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist*, 39(1), 38–47. https://doi.org/10.1080/07317115.2015.1101632

Marston, H. R., Shore, L., & White, P. J. (2019). How older adults experience the digital divide: An exploratory study. *Gerontology & Geriatric Medicine*, 5, 1–9. https://doi.org/10.1177/2333721419850481

Moschis, G. P. (2017). Consumer behavior in later life: Current knowledge, issues, and new directions for research. *Psychology & Marketing*, 34(4), 384–396. https://doi.org/10.1002/mar.20994

Pak, K., & Shadel, D. (2011). *They're not just blowing smoke: Older adults and fraud victimization*. AARP Foundation.

Redmiles, E. M., Mazurek, M. L., & Dickerson, J. P. (2018). Dancing pigs or externalities? Measuring the rationality of security decisions. *Communications of the ACM*, 61(6), 62–70. https://doi.org/10.1145/3208034

Reuter-Lorenz, P. A., & Park, D. C. (2014). How does it STAC up? Revisiting the scaffolding theory of aging and cognition. *Neuropsychology Review*, 24(3), 355–370. https://doi.org/10.1007/s11065-014-9270-9

Shadel, D., & Pak, K. (2007). *They're not just blowing smoke: Older adults and fraud victimization*. AARP Foundation.

Spreng, R. N., Shoemaker, L., & Turner, G. R. (2016). Executive functions and neurocognitive aging. In D. T. Stuss & R. T. Knight (Eds.), *Principles of frontal lobe function* (2nd ed., pp. 530–550). Oxford University Press.

 doi:10.20944/preprints202505.0928.v1

van Deursen, A. J. A. M., & Helsper, E. J. (2015). A nuanced understanding of internet use and non-use among the elderly. *European Journal of Communication*, 30(2), 171–187. https://doi.org/10.1177/0267323115578059

Whitty, M. T., & Buchanan, T. (2012). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 18(3), 277–293. https://doi.org/10.1080/1068316X.2010.528288

Zhou, J., Rau, P. L. P., & Salvendy, G. (2019). Age-related differences in software usability and design preferences. *International Journal of Human–Computer Interaction*, 35(6), 483–495. https://doi.org/10.1080/10447318.2018.1464224