

High awareness, high risk? A paradoxical examination of cyber fraud victimisation patterns among older victims

Suman Kumar and Mamta Patel

Abstract

Purpose – This study aims to examine the cybercrime awareness among older victims of cyber fraud, emphasising the paradox of high awareness coexisting with vulnerability.

Design/methodology/approach – The data used for this study are based on the experience of 98 older individuals who were victims of cyber fraud. The data were collected with the help of a structured interview schedule and a Cybercrime Awareness Scale, using a purposive sampling method.

Findings – This study revealed a paradoxical relationship between awareness and victimisation. Cybercrime awareness among older victims is widespread yet unevenly distributed across socio-demographic profiles. The strongest predictors of awareness are education, nativity and religion, but none of these factors provides guaranteed protection against cyber fraud victimisation.

Practical implications – The study's findings suggest that we need programs focused on behaviour that move beyond not just sharing information, instead offering training that builds emotional and cognitive resilience among older adults.

Originality/value – This research provides new insights that the persistence of victimisation among highly aware individuals demonstrates that cybersecurity is not just a technical issue but also a matter of how we think (cognition) and behave (behaviour) online.

Keywords Cybercrime awareness, Cyber fraud, Older victims, Digital literacy, Behavioural vulnerability

Paper type Research paper

Suman Kumar and Mamta Patel are both based at the Department of Criminology and Forensic Science, Dr Hari Singh Gour University, Sagar, India.

Introduction

Ageing population and digital vulnerability

The ageing population is growing rapidly worldwide, causing a major transformation in digital participation and vulnerability. According to the International Telecommunication Union, older people are the fastest-growing group of internet users ([Ageing in a Digital World – from Vulnerable to Valuable, 2021](#)). However, they often struggle with the skills and the necessary knowledge needed to stay safe online ([Carlson, 2006](#)). As people get older, they face age-related challenges, such as vision and hearing loss ([Dixon et al., 2022](#)), feelings of social isolation ([Strupczewski, 2024](#)), limited experience with digital technologies ([Chen et al., 2024](#)), loneliness, emotional vulnerability, cognitive impairment and mental capacity ([Dote Pardo, 2026](#); [Fenge and Lee, 2018](#); [Lee et al., 2017](#)) all of which make them vulnerable towards online spaces. Other factors include poverty, minority status, rapid expansion of fintech services and complex family dynamics ([Dote Pardo, 2026](#); [Lee et al., 2017](#)). Digital initiatives have helped many older adults gain access to technology, and they have also inadvertently opened new doors for scammers, fraudsters and cyber threats ([Kumar and Patel, 2025](#)).

Received 14 November 2025
Revised 18 February 2026
24 February 2026
Accepted 28 February 2026

Conflict of interest: The authors declare that the authors have no conflicts of interest.

Older individuals often experience the “Digital divide,” which extends beyond mere access challenges to the internet or devices (Mubarak and Suomi, 2022; Van Deursen and Helsper, 2015). It also incorporates self-doubt and uncertainty when they are trying to navigate digital spaces (Pehlivanoglu *et al.*, 2024) and find it challenging to keep up with fast-changing digital tools (Li *et al.*, 2024). These vulnerabilities are further stretched through factors such as fear of missing out and trust in authority (Shang *et al.*, 2022), which fraudsters exploit. Previous studies have shown that the use of information and communication technologies (ICT) has increased among older adults compared to their younger counterparts, but remains low (Jena and Paltasingh, 2025). They are more likely to fall victim to cybercrime due to difficulties such as recognising deception or verifying content authenticity (Chen *et al.*, 2025). The use of ICT among older people is positively influenced by digital literacy, infrastructure differences, accessibility, awareness and training, education, financial support, social support and perceived ease and utility of the internet system; on the other hand, it is negatively associated with tech-phobia, privacy concerns, chronic illness, cognitive functioning, age and living environment (Jena and Paltasingh, 2025). As a result, digital vulnerability among the ageing population not only creates personal risks but also social challenges.

Challenges in translating cyber awareness into safe online behaviour

Public and private organisations have introduced various campaigns to improve users’ understanding of online safety amid growing cyber risks. These programmes generally emphasise teaching people how to spot common scams, create or use strong passwords and follow basic safety practices online (Prümmer *et al.*, 2024). Being aware does not always lead to behavioural changes. Even when they are familiar with security measures that make them stay safe online, they may fail to respond consistently because they feel overwhelmed, find the steps too complicated, act out of forgetfulness or overconfidence (Herley, 2009; Stanton *et al.*, 2016). Numerous awareness campaigns adopt a one size fits for all approach that neglects specific needs and challenges, such as sensory, cognitive and socio-emotional causes of older users’ (Shang *et al.*, 2022). The studies also revealed a gap between the knowledge users currently have and the knowledge they need to make effective decisions about their online privacy (McDonald and Cranor, 2008, 2010). These programmes often focus on pre-emptive education – helping individuals to avoid potential threats – but provide limited guidance or support for those who have already been victimised. This knowledge-action gap highlights the need for more adaptive, context-sensitive and post-incident interventions tailored to the realities of vulnerable groups.

Research gap: awareness among actual victims

Despite the proliferation of studies on cybersecurity awareness and digital literacy, relatively few studies have examined awareness among individuals who have been victimised. Much of the existing literature focuses on hypothetical or preventive contexts-sampling the general population about their knowledge of online risks- rather than analysing how victims perceive and respond to threats in real time (Karagiannopoulos *et al.*, 2021; Kumar and Patel, 2025).

Digital inclusion policies have expanded online participation across social and economic groups, and the problem of digital inequality has become more complex. Differences in education, income, and the urban-rural divide background may influence both awareness and exposure to risk (Jena and Paltasingh, 2025). However, little empirical research has systematically examined how these demographic factors relate to cybercrime awareness among actual victims, particularly among older adults. Therefore, this study seeks to bridge the gap through analysing cybercrime awareness among older victims of cyber fraud, focusing on how awareness varies across social dimensions and why it fails to ensure

protection. This research also aims to contribute to the development of victim-centred prevention strategies that extend beyond awareness alone.

Literature review

Cybercrime risks in later life

Scholars challenge the assumption that older adults are inherently more vulnerable as consumers in digital contexts. [Berg \(2015\)](#) demonstrates that despite the age-related challenges, older adults make fewer wrong market decisions compared to their younger groups. Moreover, they show more environmentally conscious consumption patterns regardless of their age, economic awareness, time constraints and limited calculating skills. In contrast, evidence suggests that for older people, when experiencing cybercrime, the results are often more severe. [Havers \(2025\)](#) reveals that older adults are more likely to face severe cyber incidents and less likely to report less serious offences. This underreporting stems from feelings of shame, lack of awareness and prior negative experiences with law enforcement agencies. Similarly, [Havers et al. \(2024\)](#) identify additional deterrents, such as the fear of judgment, perceived futility of reporting and lack of social support. [Burton et al. \(2022\)](#) further reveal a more complex relationship of factors, such as social isolation, cognitive and physical limitations, mental health challenges, accumulated wealth, limited cybersecurity skills, societal perceptions and the nature of fraudulent content, heightened their exposure to financial cybercrime.

Research on digital exclusion provides further insights into the structural root of this vulnerability. [Pérez-Escolar and Canet \(2023\)](#) identified older adults as digitally vulnerable groups, constrained by barriers related to access, digital literacy and system usability. Similarly, [Tsatsou \(2022\)](#) outlines overlapping forms of exclusion – limited access, inadequate institutional support systems and low digital competence – collectively reinforce marginalisation in the digital sphere. [Tsatsou \(2022\)](#) argues that such exclusion is not shaped by a single factor, but rather by the combination of socio-economic, cultural and structural inequalities. [Li \(2024\)](#) extends this argument, demonstrating that in urban settings, older individuals with limited digital access and literacy are more susceptible to financial exploitation. Furthermore, [Sakariassen \(2025\)](#) notes that older adults are often compelled to use digital services, but they often lack the necessary skills, confidence and resources – such as affordable devices, stable internet access and practical guidance – to do so safely. [White et al. \(2017\)](#) reveal that gist reasoning increases with age and protects against risky behaviour, while *verbatim* reasoning predicts greater risk-taking.

Further complicating this landscape, [Chattopadhyay and Singh \(2024\)](#) observe that even after experiencing cyber victimisation, some older adults persist in risky online behaviours, highlighting the gaps in awareness and behavioural adaptation. [Tripathi \(2019\)](#) identifies institutional failings, including insufficient responsiveness from banks and police, a lack of data protection and privacy safeguards and the absence of proximal family support, which collectively hinder effective redress and exacerbate vulnerability to cybercrime.

The structural and psychological dimensions of digital exclusion are also well-documented. [Adamczyk and Betlej \(2021\)](#) attribute digital marginalisation among older adults due to limited access to digital infrastructure, poor quality of life, health issues, lack of motivation and low psychological readiness. On a similar note, [Phiayura et al. \(2025\)](#) underscore the compounded barriers arising from inadequate digital infrastructure, technological complexity and socio-cultural constraints – including low digital literacy, psychological and cognitive limitations and poor cybersecurity awareness – that collectively heighten vulnerability to digital risks. [Gupta \(2025\)](#) further adds that a lack of preparedness not only increases stress but also diminishes their perceived quality of life. [Culén & Van Der Velden \(2013\)](#) further argue that digital vulnerability among older adults is a design issue:

technological systems frequently neglect physical, cognitive and social dimensions of ageing, thereby reinforcing exclusion and amplifying susceptibility to cyber threats.

The current research turned to technological and interdisciplinary approaches to address these challenges. Karagiannopoulos *et al.* (2021) argue that older people have specific resource requirements for cybercrime awareness, reinforcing the need for more tailored prevention and reporting mechanisms. They advocate for educational initiatives on cyber-risks and prevention initiatives co-designed with the intended recipients at the grassroots level.

Methodology

In a study, 425 victims were contacted, of whom 98 were older people; the responses of those older victims were used in this research. The samples were collected with the help of a structured interview schedule and the modified Cybercrime Awareness Scale (CCAS-RS), which was developed by Dr S. Rajasekar and approved by the National Psychological Corporation, Agra, India, consisting of 36 items, 21 positive and 15 negative, scale initially recorded the responses from Strongly Agree to Strongly disagree, which is changed as “Strongly Agree, Agree, Undecided, Don’t Know, Disagree, Strongly Disagree”. The adapted version’s reliability was assessed using Cronbach’s alpha, which shows high reliability ($\alpha > 0.80$). Construct validity was examined through Exploratory Factor Analysis using Principal Component Analysis with Varimax Rotation. The Kaiser–Meyer–Olkin measure of sampling adequacy was 0.952, and Bartlett’s Test of Sphericity was statistically significant ($p = 0.000$), accounting for 63.28% of total variance, following a purposive sampling method. The data were from the two cyber police stations (Ranchi and Jamshedpur) of the state of Jharkhand, India. The data includes all victims from the registered cases of 2018–2023, as well as those who visited the cyber police station Ranchi between September 2023 and December 2023; these are those victims whose cases were not registered with the Cyber Police Station (CID), Ranchi.

Victims were first contacted with the help of the police stations where their cases were registered, and a meeting place was decided upon. The meeting place was either the police station, the victim’s home, or a suitable location for the victim to meet.

Result

The majority of the sample consists of the male population, accounting for 87.76% (86 out of 98), and is heavily concentrated in the “high awareness” and “very high awareness” categories, accounting for 88.37% (76 out of 86). In contrast, the female population accounted for 12.24% (12 out of 98) and the awareness level concentration in the “high awareness” and “very high awareness” is 75% (9 out of 12), which is approximately 13% less than the male population.

Across all age groups, “very high awareness” is consistent. Victims aged 60–66 ($n=49$) showed the highest number of individuals with “*Very High Awareness*” (69.4%, 34 out of 49), followed by those aged 67–73 (63.9%, 23 out of 36). The age group 74–80 ($n=12$) also demonstrated high awareness, with 66.7% having “very high awareness”. The oldest age group (above 80) included only one individual, who also fell within the “very high awareness” category. Lower levels of awareness were rare among all age groups. Only the 67–73 age group showed a case with “very low/no awareness” ($n=1$), and both the 60–66 and 67–73 age groups showed a “low awareness” ($n=1$ each).

“Very high awareness” (67.3%, $n=66$) is evident among victims with higher academic qualifications. Specifically, 63.6% (35 out of 55) of graduates and 86.2% (25 out of 29) of post-graduates fall into the “very high awareness” category. Conversely, lower levels of awareness are predominantly found among victims with lower educational qualifications. All four victims in the high school category were distributed across “moderate/average” and

“very high” categories. The “low” and “moderate/average” awareness primarily comprises victims with an intermediate education or a graduate degree. It is noteworthy that “very low” and “low” awareness categories are absent among victims with a high school or PhD education, and are nearly absent among post-graduates.

The income data shows a clear pattern of “very high awareness” across all income brackets, with 67.3% (66 out of 98) of the sample comprising it. This is true across all income brackets above 100,001, where 100% of victims reported “very high awareness”. However, awareness levels are more dispersed within the “no income” group. Only 50% (6 out of 12) reported “very high awareness”, while 33.3% (4 out of 12) reported “high awareness”, 8.3% (1 out of 12) each reported “moderate/average awareness” and “very low/no awareness”. The “very low” and “low” awareness categories were only present in the “no income” and “less than 50,000” group. The “moderate/average” awareness was primarily composed of victims earning “less than 50,000” and “between 50,000 and 100,000”.

The marital details reveal that the sample is overwhelmingly composed of married victims (89.8%, 88 out of 98), who account for 93.9% (62 out of 66) of the sample within the “very high awareness” category. This means that 70.5% (62 out of 88) of all married victims in the sample reported a “very high” level of cybercrime awareness. In contrast, the non-married groups (widows and widowers) show a markedly different pattern. The widow group ($n=7$) has a more distributed awareness profile; 28.6% (2 out of 7) victims are in the “very high awareness” category. In total, 66.7% (2 out of 3) of the widowers have “very high awareness”, and 33.3% (1 out of 3) remain in the “moderate/average” level of awareness. Notably, all the lowest awareness levels (“very low/no awareness” and “low awareness”) are within the married groups, underscoring that within a highly aware group, vulnerable subgroups exist.

There is a pronounced and stark disparity in awareness levels between rural and urban victims. The data is heavily skewed toward urban victims, who constitute 93.9% (92 out of 98) of the sample. Urban group is the primary contributor in the “very high awareness” category, where out of 66 victims, 95% (65 out of 66) individuals are from the urban group. In contrast, the rural group (6.1%, 6 out of 98) has significantly lower strength than the urban group. In the rural group, 16.7% (1 out of 6) individuals are in the category of “very high awareness”. The awareness level in the rural group (83.3%; 5 out of 6) primarily falls within the “low”, “moderate/average”, and “high” awareness categories.

Religiously, the sample predominantly comprises individuals who identify as Hindu (87.8%, $n=86$). Overall, 67.3% (66 out of 98) reported “very high awareness”. This pattern is heavily influenced by the Hindu group, which accounts for 62 of these 66 victims, meaning that 72.1% (62 out of 86) of Hindu victims have a “very high” level of awareness. The patterns observed in other religious groups are different; Christians showed a mixed pattern, i.e. 57.1% (4 out of 7) in the “very high awareness” and 14.3% (1 out of 7) in the “low awareness”, Muslims reported “moderate/average” (2 out of 4) and “high” awareness (2 out of 4). It is significant to note that all the lowest awareness levels (“very low/no awareness” and “low awareness”) are observed within the Hindu and Christian groups.

Overall, across all demographic variables, the awareness level is high among older victims of cyber fraud, as shown in [Table 1](#). 86.7% of the sample comprises a high level of awareness (19.4% ‘high awareness and 67.3% “very high awareness”). 10.2% of the victims showed a “moderate/Average” level of awareness. On the other hand, very few victims showed a low level of awareness, comprising 3% (1% “very low/no awareness” and 2% “low awareness”) of the total sample.

A series of Kruskal–Wallis tests is performed to examine differences in awareness levels across socio-demographic variables (see [Table 2](#)). Educational qualification $H(4) = 18.185$,

Table 1 Cybercrime awareness among victims of cyber fraud

Level of awareness	Frequency	%
Very low/No awareness	1	1.0
Low awareness	2	2.0
Moderate/average awareness	10	10.2
High awareness	19	19.4
Very high awareness	66	67.3

Source(s): Created by the authors

Table 2 Kruskal–Wallis test results of significant demographic variables and cybercrime awareness

Variable	H	df	p	Mean ranks	Significant pairs (Bonferroni-adjusted)
Educational qualification	18.185	4	0.001	HS:22.75, Int:26.00, Grad:48.62, PG:58.88, PhD:65.50	High School – Post Graduation ($p = 0.040$) Intermediate – Post Graduation ($p = 0.009$)
Nativity	8.817	1	0.003	Rural:21.83, Urban:51.30	Rural – Urban ($p = 0.003$)
Religion	11.076	3	0.011	Hindu:51.97, Christian:42.29, Muslim:15.75, Sikhs:23.00	Muslim – Hindu ($p = 0.016$)

Note(s): $n = 98$. H = Kruskal–Wallis test statistic. HS = High School, Int = Intermediate, Grad = Graduation, PG = Post Graduation

Source(s): Created by the authors

$p = 0.001$; Nativity $H(1) = 8.817$, $p = 0.003$ and religion $H(3) = 11.076$, $p = 0.011$ showed a significant effect on awareness. The mean ranks of educational qualifications show that awareness increases with educational level, from high school (mean rank = 22.75) to PhD (mean rank = 65.50). Similarly, urban victims (mean rank = 51.30) showed substantially higher awareness levels compared to rural victims (mean rank = 21.83). Further, the religious background of the victims showed that Hindu victims (mean rank = 51.97) have higher awareness levels, followed by Christians (mean rank = 42.29), Sikhs (mean rank = 23.00) and Muslims (mean rank = 15.75). No statistically significant differences in awareness level are found for gender ($p = 0.051$), marital status ($p = 0.093$), monthly income ($p = 0.351$), age ($p = 0.539$), occupation ($p = 0.408$), family structure ($p = 0.209$) and community ($p = 0.426$).

Discussion

This research examines the cybercrime awareness among the older victims of cyber fraud. Aimed to identify the extent of awareness, socio-demographic correlates and the paradoxical coexistence of high awareness and victimisation. Previous research heavily concentrated on and emphasised education and awareness to prevent cyber fraud. However, our results show a paradoxical relationship. From the results, it is evident that older victims showed a high level of awareness (86.7%; high and very high), despite the fact that cyber fraud remains prevalent.

Female victims reported being 13% less aware compared to the male victims, in line with findings that reveal females have less exposure to digital technologies (Bansal and Choudhary, 2024; Borda et al., 2022). On a different note, results also demonstrate that men are more likely to be victimised and more likely to report. This may be due to socio-cultural barriers women face in society to accessing technology. In terms of age, the awareness level across each group is high, still not guaranteed protection from cyber fraud, in line with findings of Karagiannopoulos et al. (2021) revealing that awareness alone is not immune to fraud. There are factors such as psychological barriers and social isolation that may undermine decision-making, producing “informed vulnerability”.

The individual with higher educational attainment shows a higher level of awareness, which replicates the findings of previous studies, in which it is demonstrated that higher educational attainment or digital exposure can help to achieve digital literacy (Jain and Pamu, 2023; Jena and Paltasingh, 2025). However, in the case of older individuals, educational attainment failed to protect against cyber fraud. With higher educational attainment, individuals may develop confidence in using digital technologies, but may miss subtle cues of deception or underestimate the estimated risk (Karagiannopoulos *et al.*, 2021). This suggests that cognitive ability does not necessarily translate into behavioural caution, highlighting the need for targeted awareness programmes that address not only digital competence but also psychological and behavioural vulnerabilities.

Awareness was high across all income groups, particularly among those with a monthly income above ₹100,001. This aligns with the findings of Arvind *et al.* (2025) and Bakshi and Bhattacharyya (2021), which revealed that social and economic status shape digital engagement and the risk of exposure to victimization. Nevertheless, economic status shapes digital access and literacy, but it also creates opportunities for exploitation. Therefore, digital inclusion without behavioural discipline can heighten vulnerability.

Married victims have the highest level of awareness. However, the findings of Arvind *et al.* (2025) and Morrison *et al.* (2021) suggest that a stable family environment alone cannot reduce vulnerability. Within a marital relationship, shared trust and joint decision-making may foster complacency, particularly in financial management. Conversely, widowed victims exhibited lower and more variable awareness, possibly due to less experience with technology and reduced social support factors. Nuclear family victims overall demonstrated a relatively higher level of awareness.

Gupta (2025) and Nair and Lalmohan (2020) revealed the digital divide continues to disadvantage the rural population. Similar observations were made in our results, where urban victims reported a high level of awareness. Nonetheless, urban awareness is also linked to high victimisation rates, a phenomenon where increased online engagement raises both literacy and risk (Arvind *et al.*, 2025). Urban victims may encounter more complex scams that exploit psychological and emotional manipulation rather than informational deficits. The victims who identify as Hindu demonstrated a higher level of awareness compared to other religious groups. This pattern points towards wider social inequalities in access to education and technology. It is likely that religion itself is not a direct cause of these differences, but the educational and social context in which victims live.

The Kruskal–Wallis tests confirm the consistent relationship of education, nativity and religion with awareness, whereas variables such as age, income, occupation, marital status and family structure are non-significant. Gupta (2025) argued that awareness depends more on the cognitive and experiential engagement with digital environments rather than demographic categories. Across all results, a consistent pattern of high awareness and high victimisation coexistence is observed, termed the “paradox of informed exposure”. For the victims, who are from a rural background and with less education, vulnerability comes from the lack of knowledge, whereas for the victims who are from an urban background, stems from greater visibility and overconfidence in navigating digital space or systems. These findings suggest that awareness provides protection, but not sufficient, and it must be translated into behavioural resilience that offers a true protective factor against digital risks.

Implications for policy and practice

The findings suggest that among older adults, awareness alone is insufficient to protect against and counter cyber fraud victimisation. Effective preventive strategies should

therefore target both aspects of vulnerability: how they think about online risks (cognitive) and how they act when they face them (behavioural):

- For educated and urban residents, interventions should focus on behavioural reinforcement, critical verification habits and resistance to emotional manipulation.
- For rural and less educated individuals, programs must emphasise basic digital literacy, language-accessible training and community-based awareness.
- Family- and community-based targeted interventions can help to strengthen collective vigilance, using peer networks to enhance safety behaviours.
- A multisector collaboration approach among different elements of society can help to translate awareness into practical digital resilience rather than passive knowledge.
- A culture-sensitive practical awareness campaign should be implemented, and must emphasise that older adults, who have special needs and require care.

Conclusion

This study revealed a paradoxical relationship between awareness and victimisation. The study highlights that cybercrime awareness among older victims is widespread yet unevenly distributed across socio-demographic profiles. The strongest predictors of awareness are education, nativity, and religion, but none of these factors provide guaranteed protection against cyber fraud victimisation. The persistence of victimisation among highly aware older individuals indicates that cybersecurity is not only a technological issue but also a matter of how we think and behave online. Bridging this gap, this study suggests and calls for a multidimensional, context-sensitive approach that combines awareness, emotional confidence and practical support. In this way, older people not only learn and understand online risks but also feel capable, empowered and secure when using technology in their everyday lives. The research also suggests that future studies should include older adults, who have special needs and require care.

Acknowledgements

The authors are thankful to the Cyber Police Station, Ranchi (CID), and the Cyber Police Station, Jamshedpur, officers and staff for their support. Suman Kumar is thankful to the Ministry of Social Justice & Empowerment, Government of India, New Delhi, India, for providing a Senior Research Fellowship.

Ethics statement

This research has obtained ethical approval from the Institutional Ethics Committee of Dr. Harisingh Gour Vishwavidyalaya (A Central University), Sagar, Madhya Pradesh, India, with approval number DHSGV/IEC/2025/06.

Funding

No funding received for this research.

References

Adamczyk, M. and Betlej, A. (2021), "Social determinants of digital exclusion in an ageing society. The case of Poland", *Entrepreneurship and Sustainability Issues*, Vol. 8 No. 3, pp. 122-135, doi: [10.9770/jesi.2021.8.4\(37\)](https://doi.org/10.9770/jesi.2021.8.4(37)).

Ageing in a Digital World – from Vulnerable to Valuable (2021), “International telecommunication union”.

Arvind, L., Gautam, V. and Maheshwari, V. (2025), *Understanding Senior Citizens' Experience with Online Fraud: A Survey Based Assessment*, Safer Internet India.

Bakshi, T. and Bhattacharyya, A. (2021), “Socially Distanced or Socially Connected? Well-being through ICT Usage among the Indian Elderly during COVID-19”, *Millennial Asia*, Vol. 12 No. 2, pp. 190-208, doi: [10.1177/0976399621989910](https://doi.org/10.1177/0976399621989910).

Bansal, N. and Choudhary, H. (2024), “Growing old in the digital era: a qualitative study of internet use and outcomes among urban Indian older adults”, *Working with Older People*, Vol. 28 No. 4, pp. 317-335, doi: [10.1108/WWOP-08-2023-0032](https://doi.org/10.1108/WWOP-08-2023-0032).

Berg, L. (2015), “Consumer vulnerability: are older people more vulnerable as consumers than others?”, *International Journal of Consumer Studies*, Vol. 39 No. 4, pp. 284-293, doi: [10.1111/ijcs.12182](https://doi.org/10.1111/ijcs.12182).

Borda, M., Grishchenko, N. and Kowalczyk-Rólczyńska, P. (2022), “Impact of digital inequality on the COVID-19 pandemic: evidence from European Union countries”, *Sustainability*, Vol. 14 No. 5, p. 2850, doi: [10.3390/su14052850](https://doi.org/10.3390/su14052850).

Burton, A., Cooper, C., Dar, A., Mathews, L. and Tripathi, K. (2022), “Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: a realist review”, *Experimental Gerontology*, Vol. 159, p. 111678, doi: [10.1016/j.exger.2021.111678](https://doi.org/10.1016/j.exger.2021.111678).

Carlson, E.L. (2006), “Phishing for elderly victims: as the elderly migrate to the internet fraudulent schemes targeting them follow”, *Elder LJ*, Vol. 14 No. 2, p. 423.

Chattopadhyay, S. and Singh, M. (2024), “Cyber-Crimes against elderly people in India-Search for defence mechanism to counter”, *NUJS J. Regul. Stud*, Vol. 9 No. 3, p. 38.

Chen, H., He, M., Xu, X. and Atkin, D. (2025), “Examining older adults' vulnerability to online health scams: insights from routine activity theory”, *Frontiers in Public Health*, Vol. 13, p. 1585851, doi: [10.3389/fpubh.2025.1585851](https://doi.org/10.3389/fpubh.2025.1585851).

Chen, L., Jia, J., Xiao, M., Wu, C. and Zhang, L. (2024), “A study on the influence of digital literacy on elderly user's intention to identify social media false information”, *The Electronic Library*, Vol. 42 No. 5, pp. 701-721, doi: [10.1108/EL-10-2023-0257](https://doi.org/10.1108/EL-10-2023-0257).

Culén, A.L. and Van Der Velden, M. (2013), “The digital life of vulnerable users: Designing with children, patients, and elderly”, in Aanestad, M. and Bratteteig, T. (Eds), *Nordic Contributions in is Research*, Springer Berlin Heidelberg, Berlin, Heidelberg, Vol. 156, pp. 53-71, doi: [10.1007/978-3-642-39832-2_4](https://doi.org/10.1007/978-3-642-39832-2_4).

Dixon, E., Anderson, J. and Lazar, A. (2022), “Understanding how sensory changes experienced by individuals with a range of Age-Related cognitive changes can affect technology use”, *ACM Transactions on Accessible Computing*, Vol. 15 No. 2, pp. 1-33, doi: [10.1145/3511906](https://doi.org/10.1145/3511906).

Dote Pardo, J.S. (2026), “Elder financial abuse and exploitation: a systematic review of vulnerabilities and protective factors”, *The Journal of Adult Protection*, pp. 1-13, doi: [10.1108/JAP-08-2025-0033](https://doi.org/10.1108/JAP-08-2025-0033).

Fenge, L.-A. and Lee, S. (2018), “Understanding the risks of financial scams as part of elder abuse prevention”, *The British Journal of Social Work*, Vol. 48 No. 4, pp. 906-923, doi: [10.1093/bjsw/bcy037](https://doi.org/10.1093/bjsw/bcy037).

Gupta, P. (2025), “Understanding cybersecurity awareness and perceptions among older adults in India”, *Scientific and Practical Cyber Security Journal*, Vol. 9 No. 3, pp. 149-159.

Havers, B. (2025), “Developing an intervention to protect older people from cybercrime”, PhD Thesis, UCL (University College London).

Havers, B., Tripathi, K., Burton, A., McManus, S. and Cooper, C. (2024), “Cybercrime victimisation among older adults: a probability sample survey in England and Wales”, *Plos One*, Vol. 19 No. 12, p. e0314380, doi: [10.1371/journal.pone.0314380](https://doi.org/10.1371/journal.pone.0314380).

Herley, C. (2009), “So long, and no thanks for the externalities: the rational rejection of security advice by users”, *Proceedings of the 2009 Workshop on New Security Paradigms Workshop, presented at the NSPW '09: 2009 New Security Paradigms Workshop*, ACM, Oxford United Kingdom, pp. 133-144, doi: [10.1145/1719030.1719050](https://doi.org/10.1145/1719030.1719050).

Jain, P. and Pamu, S. (2023), “Impacts of covid-19 on elderly and transitioning them to digital realm”, *HelpAge India-Research & Development Journal*, Vol. 26 No. 2, pp. 28-35.

- Jena, B. and Paltasingh, T. (2025), "Digital literacy among older adults: a systematic review in Indian context", *Educational Gerontology*, Vol. 51 No. 4, pp. 371-386, doi: [10.1080/03601277.2024.2397428](https://doi.org/10.1080/03601277.2024.2397428).
- Karagiannopoulos, D., Kirby, D., Oftadeh-Moghadam, S. and Sugiura, D. (2021), "Cybercrime awareness and victimisation in individuals over 60 years: a portsmouth case study", *Computer Law & Security Review*, Vol. 43, p. 105615, doi: [10.1016/j.clsr.2021.105615](https://doi.org/10.1016/j.clsr.2021.105615).
- Kumar, S. and Patel, M. (2025), "Digital habits and cyber vulnerabilities among older victims of cyber fraud", *Working with Older People*, Vol. 29 No. 4, pp. 433-443, doi: [10.1108/WWOP-04-2025-0018](https://doi.org/10.1108/WWOP-04-2025-0018).
- Lee, S., Johnson, R., Fenge, L.-A. and Brown, K. (2017), "Safeguarding adults at risk of financial scamming", *Safeguarding Adults Under the Care Act 2014: Understanding Good Practice*, Jessica Kingsley Publishers, Vol. 240.
- Li, Y. (2024), "The impact of the old-age digital divide on household financial vulnerability", *Academic Journal of Business & Management*, Vol. 6 No. 5, doi: [10.25236/AJBM.2024.060518](https://doi.org/10.25236/AJBM.2024.060518).
- Li, Y., Liu, C., Sun, J., Zhang, J., Li, X. and Zhang, Z. (2024), "The digital divide and cognitive disparities among older adults: community-based cohort study in China", *Journal of Medical Internet Research*, Vol. 26, p. e59684, doi: [10.2196/59684](https://doi.org/10.2196/59684).
- McDonald, A.M. and Cranor, L.F. (2008), "The cost of reading privacy policies", *Isjlp*, Vol. 4, p. 543.
- McDonald, A.M. and Cranor, L.F. (2010), "Americans' attitudes about internet behavioral advertising practices", *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, presented at the CCS '10: 17th ACM Conference on Computer and Communications Security 2010, ACM, Chicago IL USA*, pp. 63-72, doi: [10.1145/1866919.1866929](https://doi.org/10.1145/1866919.1866929).
- Morrison, B., Coventry, L. and Briggs, P. (2021), "How do Older Adults feel about engaging with Cyber-Security?", *Human Behavior and Emerging Technologies*, Vol. 3 No. 5, pp. 1033-1049, doi: [10.1002/hbe2.291](https://doi.org/10.1002/hbe2.291).
- Mubarak, F. and Suomi, R. (2022), "Elderly forgotten? Digital exclusion in the information age and the rising grey digital divide", *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, Vol. 59, p. 469580221096272, doi: [10.1177/00469580221096272](https://doi.org/10.1177/00469580221096272).
- Nair, D.S. and Lalmohan, P. (2020), "Ageing in the digital age: an inquiry into the adoption of digital technologies among senior citizens", *Communication & Journalism Research*, Vol. 9 No. 2, pp. 1-18.
- Pehlivanoglu, D., Shoenfelt, A., Hakim, Z., Heemskerk, A., Zhen, J., Mosqueda, M., Wilson, R.C., et al. (2024), "Phishing vulnerability compounded by older age, apolipoprotein E e4 genotype, and lower cognition", *PNAS Nexus*, Vol. 3 No. 8, p. pgae296, doi: [10.1093/pnasnexus/pgae296](https://doi.org/10.1093/pnasnexus/pgae296).
- Pérez-Escolar, M. and Canet, F. (2023), "Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework", *Universal Access in the Information Society*, Vol. 22 No. 3, pp. 1059-1072, doi: [10.1007/s10209-022-00867-x](https://doi.org/10.1007/s10209-022-00867-x).
- Phiyura, P., Hassandoust, F. and Liew, A. (2025), "Digital safety and vulnerable groups: a systematic review of barriers, enablers, and Multi-Level interventions", *SSRN*, doi: [10.2139/ssrn.5414835](https://doi.org/10.2139/ssrn.5414835).
- Prümmer, J., Van Steen, T. and Van Den Berg, B. (2024), "A systematic review of current cybersecurity training methods", *Computers & Security*, Vol. 136, p. 103585, doi: [10.1016/j.cose.2023.103585](https://doi.org/10.1016/j.cose.2023.103585).
- Sakariassen, H. (2025), "Multidimensional digital vulnerability among older adults", *Nordicom Review*, Vol. 46 No. 2, pp. 137-160, doi: [10.2478/nor-2025-0012](https://doi.org/10.2478/nor-2025-0012).
- Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B. and Chi, M. (2022), "The psychology of the internet fraud victimization of older adults: a systematic review", *Frontiers in Psychology*, Vol. 13, p. 912242, doi: [10.3389/fpsyg.2022.912242](https://doi.org/10.3389/fpsyg.2022.912242).
- Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016), "Security fatigue", *IT Professional*, Vol. 18 No. 5, pp. 26-32, doi: [10.1109/MITP.2016.84](https://doi.org/10.1109/MITP.2016.84).
- Strupczewski, G. (2024), "Mitigating cyber risk in personal finance of the elderly. Insights into vulnerabilities, cyber hygiene and the role of personal cyber insurance", *Cybersecurity and Law, Akademia Sztuki Wojennej*, Vol. 11 No. 1, pp. 281-298.
- Tripathi, P.M. (2019), *Sociological Study of Cybercrime Causes and Control*, PhD, Chhatrapati Sahuji Maharaj University.

Tsatsou, P. (2022), "Vulnerable people's digital inclusion: intersectionality patterns and associated lessons", *Information, Communication & Society*, Vol. 25 No. 10, pp. 1475-1494, doi: [10.1080/1369118X.2021.1873402](https://doi.org/10.1080/1369118X.2021.1873402).

Van Deursen, A.J.A.M. and Helsper, E.J. (2015), "The third-level digital divide: who benefits most from being online?", *Communication and Information Technologies Annual*, pp. 29-52, doi: [10.1108/S2050-206020150000010002](https://doi.org/10.1108/S2050-206020150000010002).

White, C.M., Gummerum, M., Wood, S. and Hanoch, Y. (2017), "Internet safety and the silver surfer: the relationship between gist reasoning and adults' risky online behavior", *Journal of Behavioral Decision Making*, Vol. 30 No. 4, pp. 819-827, doi: [10.1002/bdm.2003](https://doi.org/10.1002/bdm.2003).

Further reading

Hart, T.A., Chaparro, B.S. and Halcomb, C.G. (2008), "Evaluating websites for older adults: adherence to 'senior-friendly' guidelines and end-user performance", *Behaviour & Information Technology*, Vol. 27 No. 3, pp. 191-199, doi: [10.1080/01449290600802031](https://doi.org/10.1080/01449290600802031).

Corresponding author

Suman Kumar can be contacted at: sumankr545@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgroupublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com