ISSN: 2348-473X
Peer Reviewed & Refereed Journal (IF: 6.74)
Journal Website: www.nrjss.in

NAVIGATING THE DIGITAL AGE: DIGITAL LITERACY, FEAR OF SCAMS, AND SELF-PROTECTION MEASURES AMONG SENIOR CITIZENS

Nireekshan Singh Gowgi S K

Assistant Professor
Department of Social Work, Government First Grade College, Bettampady, Puttur, Dakshina Kannada

ABSTRACT

In the present age, reliance on technology has become a vital part of daily living. The introduction and use of technology in almost every field has significantly simplified life's complexities. At the same time, the inability to use technology effectively can make individuals socially disadvantaged. Hence, the necessity for people to make use of technology for their own benefit has grown stronger than ever. Computers, internet access, and smartphones have now become inseparable elements of people's lives across all social groups.

However, certain sections of the population continue to remain behind in this process of technological adaptation. Among them, the most affected are rural communities, the illiterate and grassroots-level groups. Within these, senior citizens are considered the most vulnerable. They often struggle to cope with the fast-paced changes brought about by technology and find it challenging to keep up. In their efforts to adapt, senior citizens attempt to learn basic computer literacy, internet usage, smartphone handling, and entrepreneurial activities using various applications. While this has simplified their daily lives and strengthened their bond with younger generations, challenges persist.

Despite its advantages, technology also carries risks. Daily news reports often highlight incidents of its misuse, where fraudsters exploit vulnerable groups. Senior citizens, owing to their limited digital literacy, frequently become the easiest targets of such online scams.

This research aimed to study 101 senior citizens, focusing on their digital literacy, fear of online scams, and the preventive measures they adopt to safeguard themselves. Data collection was carried out using an interview schedule, and the gathered responses were analysed systematically.

The findings reflect senior citizens' perceptions and their confidence levels regarding online scams. The processed data have been presented using suitable tables for better understanding.

Keywords: Online Scams, Senior Citizens, Fear, Confidence, Technology, and Awareness.

INTRODUCTION

The pace of technological progress today is vastly different from that of three decades ago. The entry of computers into people's lives has led to remarkable transformations across multiple dimensions of human activity. The influence of computers and the internet has touched every sector of society, but today's digital environment cannot be attributed to computers alone. Continuous advancements in research and its applications to daily life have resulted in the digitization of nearly all aspects of human existence.

At present, even basic records such as hospital data on births and deaths are stored digitally. From young school children to elderly citizens, almost every service connected to their lives is now accessible through smartphones. In today's internet-driven world, individuals no longer need to physically visit offices for services. Applications, information, and availing facilities can all be managed through mobile devices.

The tendency to preserve essential information in digital form has grown significantly, offering quick and low-cost access to services at any time and place. Yet, while digital storage offers convenience, it also brings risks. Misuse and leakage of such information have given rise to multiple forms of cybercrimes. Fraudsters often exploit vulnerable groups such as children, women, the technologically inexperienced, the illiterate, and especially senior citizens. Even those senior citizens who are educated but only moderately familiar with technology fall prey to such schemes.

Senior citizens' susceptibility to online fraud arises from factors like over-trusting others, poor understanding of digital systems, or the desire to make easy investments/money. Socially, the problem is compounded by the increasing isolation of senior citizens from the mainstream. This feeling of neglect pushes them to seek adaptation to smartphones and internet-based platforms, often relying on family and community support. It becomes the responsibility of society to build awareness, instil confidence, and shield them from online scams. In this regard, government initiatives play a vital role, particularly through awareness campaigns in newspapers, television, and social media platforms.

Among the common techniques used by fraudsters to target senior citizens are phishing, tech support scams, lottery/gift scams, fake investment and pension schemes, online shopping scams, romance and friendship scams, charity fraud, KYC/banking update frauds, digital arrest, part-time job scams, and health product frauds. These represent only a fraction of the evolving strategies, as criminals continuously innovate new methods despite on-going awareness campaigns.

Academic research in this area remains limited, yet findings underline the growing threat. The COVID-19 pandemic accelerated dependence on digital services, making senior citizens more vulnerable. Studies such as **Zukry et al**. (2024) emphasize awareness initiatives and stricter regulation; **Saifuddin et al**. (2024) identify risks such as cognitive decline, social isolation, low digital skills, and financial vulnerability; while **Kemp** and **Perez** (2023) stress the psychological and health consequences of scams.

Further contributions include **Chattopadhyay** and **Singh** (2024), who call for stronger legal protections in India, and **Sudra** (2023), who warns against new forms of fraud including crypto-currency scams. Other research highlights the importance of emotional support (**Li et al**., 2022; **Ebner et al**., 2018) and simpler complaint mechanisms (**Pacheco**, 2024).

Overall, literature reveals that online scams against senior citizens are a **multidimensional issue** involving technological, psychological, and policy aspects. A layered response is required - combining digital awareness, age-friendly online platforms, AI-powered fraud detection, stricter legal systems, and stronger family and community support.

RESEARCH METHODOLOGY

Scope of the Study

This research seeks to examine the fear of online scams among senior citizens and their struggles in safely navigating digital platforms. By exploring their experiences, awareness, and levels of caution, the study aims to highlight gaps in knowledge and areas needing intervention. While previous digital inclusion initiatives have focused mainly on accessibility and adaptability, this study attempts to explore how fear of scam/s, protective behaviour, and self-confidence interact with senior citizens' online activities such as payments, messaging, and transactions.

Specific Objectives

1. Explore senior citizens' understanding of digital literacy dimensions relevant to safe use,
2. Analyse online/mobile scam exposure, awareness, and perceived vulnerability,
3. Assess confidence levels in using digital or online platform,
4. Understanding the level of fear of being scammed via digital/online platforms, and
5. Explore self-protective measures senior citizens currently use.

Area of Study

The study was conducted among 101 senior citizens residing in Puttur, Sullia, and Kadaba taluks of Dakshina Kannada district, Karnataka, India. The participants were individuals who used computers or smartphones with internet access for online transactions and related activities. Data collection was carried out through an interview schedule. To meet the specific objectives, the researcher adopted a **descriptive research design**.

Tool Used

Based on a review of related studies and the objectives of this research, an interview schedule with 35 questions/statements was designed. The tool was pre-tested with 10 randomly chosen respondents, after which necessary revisions were made before finalization. The finalized schedule consisted of two major parts:

- **Part I:** Five items collecting basic socio-demographic details such as age, gender, education, and related information.
- **Part II:** Thirty items covering aspects linked to digital literacy, awareness, attitudes, and experiences regarding online fraud.

Ethical Consideration

The aims of the study were explained to all participants before data collection, and their consent was obtained. Participants had the freedom to withdraw at any point. Confidentiality was maintained throughout, with no disclosure of identities. The data collected were used strictly for academic and research purposes. Sensitive personal credentials were not gathered, and the rights of respondents were safeguarded at every stage.

Limitations of the Study

The findings of the research are based on data from senior citizens living in selected rural and urban areas, with variations influenced by education level and extent of digital exposure. Therefore, the interpretations and conclusions can only be generalized to the specific study area and population under consideration.

Results and Discussion

Age: Out of the total respondents, 50 (49.50%) belonged to the age group of 60-64 years; 25 (24.75%) were in the 65-69 age range; 20 (19.80%) belong to 70-74 years; and 06 (5.94%) were above 74 years of age.

Gender: Among the participants, 56 (55.45%) were male, while 45 (44.55%) were female.

Education: The educational background of respondents showed that 25 (24.75%) had no formal education, 32 (32.67%) had completed primary schooling, 15 (14.85%) had studied up to high school, and 28 (27.72%) had attained graduation or higher levels of education.

Device Usage: A majority, 76 (75.24%), relied on smartphones for daily activities such as payments, purchases, and online transactions, while 25 (24.75%) used computers for these purposes.

Table - 01

Internet Usage

Sl. No.	Responses	Respondents
1	Rarely	33 (32.67%)
2	Once in a week	08 (7.92%)
3	Daily	60 (59.40%)

Table - 02

Knowledge about online scams/fraud

Sl. No.	Responses	Respondents
1	Yes	72 (71.28%)
2	No	29 (28.71%)

Table - 03

Source of knowledge about online scams/fraud

Sl. No.	Responses	Respondents
1	Friends	35 (34.65%)
2	TV/Newspaper	28 (27.72%)
3	Social Media	09 (8.91%)
4	Never heard of it	29 (28.71%)

Table - 04

Verification of online link

Sl. No.	Responses	Respondents
1	Always verify	17 (16.83%)
2	Sometimes verify	42 (41.58%)
3	Never verify	42 (41.58%)

Table - 05

Loss of money

Sl. No.	Responses	Respondents
1	Yes	09 (8.91%)
2	No	92 (91.08%)

Table - 06

Felt constant fear of being targeted/scammed through online

Sl. No.	Responses	Respondents
1	Yes	63 (62.37%)
2	No	38 (37.62%)

Table - 07

Protective measures

Sl. No.	Responses	Respondents
1	Yes	48 (47.52%)
2	No	53 (52.47%)

Table - 08

Trust level

Sl. No.	Responses	Respondents
1	Completely	06 (5.94%)
2	Sometimes	35 (34.65%)
3	Never	67 (66.33%)

Table - 09

Clicked on suspicious online link

Sl. No.	Responses	Respondents
1	Yes	24 (23.76%)
2	No	77 (76.23%)

Table - 10

Believing big online discounts

Sl. No.	Responses	Respondents
1	Yes	11 (10.89%)
2	No	90 (87.10%)

Table - 11

Shared bank details with stranger/s

Sl. No.	Responses	Respondents
1	Yes	10 (9.90%)
2	No	91 (90.09%)

Table - 12

Digital confidence

Sl. No.	Responses	Respondents
1	Yes	43 42.57%)
2	No	58 (57.42%)

Table - 13

Confidence level (on a 0-10 points scale where '0' refers to 'No confidence')

Sl. No.	Responses	Respondents
1	0	26 (25.74%)
2	1	--
3	2	9 (891%)
4	3	2 (1.98%)
5	4	3 (2.97%)
6	5	21 (20.79%)
7	6	2 (1.98%)
8	7	5 (4.95%)
9	8	11(10.89%)
10	9	2 (1.98%)
11	10	14 (13.86%)

Table - 14

Willingness to learn about online safety

Sl. No.	Responses	Respondents
1	Yes	60 (59.40%)
2	No	41 (40.59%)

Table - 15

Greatest fear

Sl. No.	Responses	Respondents
1	Losing money in online scam	53 (52.47%)
2	Sharing of personal information	20 (19.80%)
3	Accidently clicking on harmful link	16 (15.84%)
4	I do not have any fear	12 (11.88%)

Table - 16

Methods of verifying online links

SL. No.	Responses	Respondents
1	I Check if I Know the sender	35 (34.65%)
2	I ask family or friends for advice	38 (37.62%)

3	I trust my instincts & ignore anything suspicious	12 (11.88%)
4	I usually believe message unless proven fake	02 (1.98%)
5	No opinion	14 (13.86%)

Table - 17

Types of online message/s that make senior citizens feel unsafe

SL. No.	Responses	Respondents
1	Message asking for bank details	59 (58.41%)
2	Calls saying, I won a lottery or prize	10 (9.90%)
3	Unknown number asking for personal information	16 (15.84%)
4	None, I do not feel unsafe	04 (3.96%)
5	No opinion	12 (11.88%)

Table - 18

Methods of ignoring suspicious calls

SL. No.	Responses	Respondents
1	I usually ignore unknown/suspicious calls	50 (49.50%)
2	Not ignored, I was unsure if it was real or fake	21 (20.79%)
3	Not ignored, I thought it was important	05 (4.95%)
4	No opinion	25 (24.75%)

Table - 19

Online scam and family support

SL. No.	Responses	Respondents
1	Yes, they teach me about online safety	37 (36.63%)
2	Sometimes, they warn me about scams	27 (26.73%)
3	No, I rely on my self	19 (18.81%)
4	I do not discuss online safety with family	18 (17.82%)

Table - 20

Online shopping and level of comfort

SL. No.	Responses	Respondents
1	Yes, but only from trusted websites	24 (23.76%)
2	No, I fear being Scammed	22 (21.78%)
3	I do not know how to shop online	23 (22.77%)
4	I prefer to buy things in store	32 (31.68%)

Table - 21

Common concerns about online security

SL. No.	Responses	Respondents
1	How to check if something is real or fake?	58 (57.42%)
2	Remembering passwords and security steps	13 (12.87%)
3	Knowing which apps are safe to use	06 (5.94%)
4	Nothing, I understand it well	11 (10.89%)
5	No opinion	15 (14.85%)

Table - 22

Methods of avoiding/ignoring suspicious link

SL. No.	Responses	Respondents
1	I usually ignore it	56 (55.44%)
2	I ask if it's real/safe	24 (23.76%)
3	I click to check what it is	08 (7.92%)
4	I forward it others	13 (12.87%)

Table - 23

Knowledge regarding kind of information scammers asks for

SL. No.	Responses	Respondents
1	Bank details and Password	45 (44.55%)
2	Personal details like name and age	16 (15.84%)
3	OTP & Security codes	19 (18.81%)
4	I do not know	21 (20.79%)

Table - 24

Anxiety/concern level (on a 0-10 points scale where ‘10’ refers to ‘High anxiety/concern’)

Sl. No.	Responses	Respondents
1	0	12 (11.88%)
2	1	08 (7.92%)
3	2	10 (9.90%)
4	3	08 (7.92%)
5	4	08 (7.92%)
6	5	14 (13.86%)
7	6	09 (8.91%)
8	7	04 (3.96%)
9	8	08 (7.92%)
10	9	03 (2.97%)
11	10	17 (16.83%)

The present study sought to examine senior citizens' digital literacy, experiences and perceptions of online/mobile scams, confidence in using online platforms, fear of being scammed, and the protective measures they adopt. The findings provide important insights into the ways senior citizens engage with digital platforms and the challenges they face in staying safe online.

Digital Usage and Awareness

The study shows that nearly half of the respondents (59.40%) (**Table - 01**) use the internet daily for payments, shopping, and other purposes. This indicates a notable level of digital adoption among senior citizens, reflecting India's broader movement toward digital transactions. However, the fact that nearly half still do not engage daily suggests that a digital divide persists.

Awareness of online scams is relatively high, with 71.28% (**Table - 02**) reporting knowledge of such frauds. Friends (34.65%) and traditional media such as television and newspapers (27.82%) were identified as the most common sources of information. Social media contributed less (8.91%), and a concerning 28.71% had never heard of scams at all (**Table - 03**). This highlights both the strengths and gaps in knowledge dissemination: while awareness exists, it is uneven, leaving some seniors highly vulnerable. Additionally, one-third (31.68%) still prefer offline shopping, reflecting hesitancy in adopting online commerce due to fears of fraud (**Table - 20**).

Risky Behaviours and Victimization

Despite awareness, many senior citizens engage in risky online practices. A significant proportion admitted to clicking on suspicious links (23.76%) or failing to verify online links (41.58%) (**Table - 09**). Alarmingly, 9.90% reported sharing bank details with strangers. Such behaviours create direct vulnerabilities to fraud and demonstrate that awareness does not always translate into safe practices (**Table - 11**).

In terms of victimization, 8.91% of respondents reported falling prey to scams, losing money, and subsequently filing complaints with cyber police (**Table - 05**). While the reporting behaviour is a positive sign, the fact that scams succeeded against these individuals underscores the effectiveness of scam tactics. Respondents commonly reported that scammers asked for bank details, passwords, or OTPs (44.55%) - methods well-documented in national cybercrime reports (**Table - 23**). Moreover, more than half (57.42%) expressed concern about not knowing how to distinguish between genuine and fake links or messages, which emerged as the most pressing issue regarding online security (**Table - 21**).

PSYCHOLOGICAL IMPACT: FEAR, ANXIETY, AND TRUST DEFICIT

The study reveals a deep psychological impact of online scams on senior citizens. A majority (62.37%) reported constant fear of being scammed (**Table - 06**), and 52.47% identified losing money as their greatest fear (**Table - 15**). On a 0-10 scale, 25.74% rated themselves as having zero confidence in online transactions (**Table - 13**), while 17.83% reported high levels of anxiety/concern (**Table - 24**).

This constant fear appears to have produced a trust deficit toward digital platforms. Nearly two-thirds (66.33%) stated that they "never trust online" (**Table - 08**) and 87.10% expressed disbelief in large online discounts. Such distrust, though protective in some respects, may also contribute to digital exclusion by discouraging seniors from participating in beneficial digital services such as e-governance, online banking, or telemedicine. Thus, fear acts both as a shield and a barrier, limiting digital empowerment (**Table - 10**).

PROTECTIVE MEASURES AND SUPPORT SYSTEMS

Despite fears, many seniors are adopting protective strategies. Nearly half (47.52%) reported taking safety precautions (**Table - 07**), with 49.50% ignoring unknown or suspicious calls (**Table - 18**) and 55.44% ignoring suspicious links. These measures suggest that senior citizens are actively trying to protect themselves within their limited knowledge (**Table - 22**).

Family and social networks also play an important role. Friends were the main source of scam awareness, and 36.63% reported that family members taught them safety tips (**Table - 19**). In verifying suspicious links, 37.62% relied on family or friends for advice (**Table - 16**). This underscores the importance of intergenerational support, where younger family members act as informal educators for older adults. Encouragingly, 59.40% expressed willingness to learn online safety measures, showing openness to structured interventions if offered in a senior-friendly format (**Table - 14**).

IMPLICATIONS FOR POLICY, PRACTICE, AND RESEARCH

The findings highlight the roles of government, non-governmental organizations, and academia in addressing the digital vulnerability of older adults. The absence of a senior citizen-specific digital safety policy has intensified the issue, calling for urgent action.

A major observation was the gap between **awareness** and **behaviours**. This suggests the need for exclusive online literacy programs tailored for senior citizens. Policies should go beyond awareness-raising to also build skills in identifying suspicious content. Government agencies, NGOs, and banks must collaborate to design strategies, such as deploying trained staff and creating dedicated helplines.

Banks, in particular, carry the responsibility to simplify services, strengthen fraud-prevention systems, and offer senior-friendly digital platforms. Cybercrime units should handle cases with empathy and resolve them quickly to minimize distress.

The involvement of families, especially younger generations, also plays a protective role. Together with government measures, such support can effectively shield older adults from cybercriminals.

Another finding was that **awareness alone does not ensure confidence**. Senior citizens' online activities remain influenced by underlying fears of scam. Thus, future research should focus on psycho-social aspects like confidence-building, stress reduction, and emotional support. Broader studies should also examine variations in rural-urban backgrounds, gender, and socioeconomic status to deepen understanding of vulnerabilities.

CONCLUSION

Life shaped by technology is advancing rapidly, and keeping pace with this change has become a necessity. True progress can only be achieved when all segments of society -irrespective of age, gender, or economic background - participate equally in this digital transformation. To ensure inclusivity, the government has introduced several initiatives encouraging broader participation in the digital revolution. Consequently, a growing number of senior citizens are engaging in online activities and digital transactions.

While this development is positive, it also brings challenges. Older adults who are enthusiastic about using technology remain highly vulnerable to online scams due to limited awareness, the complexity of digital systems, or other related factors. Such risks affect not only their financial well-being but also their emotional state, social relationships, and physical health.

Therefore, it becomes the moral duty of every member of society to extend protection to senior citizens and prevent them from falling prey to online scams. Only then can the digital era truly be considered inclusive, safe, and empowering for all generations.

ACKNOWLEDGEMENTS

The author would like to express sincere gratitude to all those who contributed to the successful completion of this research. This study would not have been possible without the cooperation and support of the senior citizens of Puttur, Sullia, and Kadaba taluks, Dakshina Kannada, Karnataka, India, who generously provided the required data.

REFERENCES

1. Brancale, J. N., & Blomberg, T. G. (2024). Criminalizing abuse, neglect, and financial exploitation of older adults. *Laws*, *13*(4), 49. https://doi.org/10.3390/laws13040049
2. Chattopadhyay, S., & Singh, M. (2023). Cyber-crimes against elderly people in India – Search for defence mechanism to counter. *NUJS Journal of Regulatory Studies*, *9*(3), 39–52.
3. 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/gnx135
4. Dhivya, R., & Seethalakshmi, S. (2021). The survey on digital adaptation among senior citizens. *International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMSC)*, *1*(2), 36–45.
5. Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75*(3), 522–533. https://doi.org/10.1093/geronb/gby071
6. 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
7. Kemp, S., & Erades Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health*, *20*(7), 5404. https://doi.org/10.3390/ijerph20075404
8. Li, J. C. M., Wong, G. T. W., Manning, M., & Yeung, D. Y. (2022). Financial fraud against older people in Hong Kong: Assessing and predicting the fear and perceived risk of victimization. *International Journal of Environmental Research and Public Health*, *19*(3), 1233. https://doi.org/10.3390/ijerph19031233
9. Pacheco, E. (2024). Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors. *Journal of Digital Media & Interaction*, *7*(17), 107–126. https://doi.org/10.34624/jdmi.v7i17.31707
10. Parti, K. (2022). "Elder scam" risk profiles: Individual and situational factors of younger and older age groups' fraud victimization. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(3), 20–40. https://doi.org/10.52306/05030222KRSX1627
11. Saifuddin, N. F., Musa, B., Zakaria, N. S., Othman, N. F., Putera, A. D., Kunasekaran, P., Rosnon, M. R., Razak, M. A. A., & Ibrahim, R. (2024). Scams issues among elderly: A

conceptual paper. *International Journal of Academic Research in Business and Social Sciences*, *14*(10), 1624–1638. https://doi.org/10.6007/IJARBSS/v14-i10/21159

12. Sudra, R. (2023). AI in fraud detection for elderly people: Preventing scams against elderly people. *International Journal of Science and Research*, *12*(1), 1278–1286. https://doi.org/10.21275/SR231022120610
13. Teaster, P. B., Roberto, K. A., Savla, J., Du, C., Du, Z., Atkinson, E., Shealy, E. C., Beach, S., Charness, N., & Lichtenberg, P. A. (2022). Financial fraud of older adults during the early months of the COVID-19 pandemic. *The Gerontologist*, *63*(6), 984–992. https://doi.org/10.1093/geront/gnac077
14. Zukry, M. A. A. M., Khatiman, M. N. A. B. M., & Abdullah, R. B. H. (2024). Strategies for protecting senior citizens against online banking fraud and scams: A systematic literature review. *Journal of Theoretical and Applied Information Technology*, *102*(14), 5545–5556.