Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STRATEGIES FOR PROTECTING SENIOR CITIZENS AGAINST ONLINE BANKING FRAUD AND SCAMS: A SYSTEMATIC LITERATURE REVIEW

MUHAMMAD AMIRRUL ALHAFIZ BIN MOHD ZUKRY[1], MUHAMMAD NUR AQMAL BIN KHATIMAN[2], PROF. TS. RUSLI BIN HAJI ABDULLAH[3]

[1] Student, Universiti Putra Malaysia, Department of Computer Science, Serdang, Malaysia

[2]Student. Universiti Putra Malaysia, Department of Computer Science, Serdang, Malaysia

[3]Professor. Universiti Putra Malaysia, Department of Software Engineering and Information Systems, Serdang, Malaysia

E-mail: [1]gs67390@student.upm.edu.my, [2]gs67393@student.upm.edu.my, [3]rusli@upm.edu.my

ABSTRACT

This systematic literature review examines the need for strong strategies to protect seniors from online banking fraud and scams. The demographic's increased use of digital banking platforms due to the COVID-19 epidemic has increased their cyber risk. This study identifies and evaluates multifaceted strategies to improve digital literacy, create user-friendly digital banking interfaces, enact and enforce strict regulatory frameworks, and encourage senior citizens to use electronic banking post-COVID-19. Digital literacy empowers seniors by helping them navigate online banking platforms securely and spot scams. This requires operational proficiency, cybersecurity knowledge, and threat identification and response. Online banking platforms must be user-friendly. For seniors with various digital skills and physical limitations, straightforward and easy-to-use interfaces can reduce the risk of fraud. This comprises simplifying transaction processes, providing clear instructions, and providing customized support. Seniors using online banking need regulatory frameworks to protect their financial interests and privacy. This evaluation assesses the effectiveness of current fraud and scam laws and practices and the need for improvements to address senior folks' special vulnerabilities. It shows how technology and law interact, emphasizing that regulatory authorities must adapt to digital changes to ensure comprehensive protection. Seniors have adopted e-banking due to the COVID-19 epidemic, which forced a move to digital platforms for many daily activities, including banking. Seniors face a variety of online hazards, yet this transition offers convenience and accessibility. Trust-building, education, and support services are crucial to helping this generation adopt e-banking, according to the analysis. According to this analysis, older folks need a multi-pronged cybersecurity approach that includes technological, educational, and regulatory components to improve their online banking experience and safeguard them from fraud and scams.

Keywords: *Online Banking Security, Elderly Fraud Protection, Digital Literacy for Seniors, Cybersecurity Measures, User Interface Design, Regulatory Policies, E-Banking Adoption*

1. INTRODUCTION

The advent of the digital age has revolutionized the way financial transactions are conducted, with online banking emerging as a cornerstone of modern financial management. This digital transformation, while offering unprecedented convenience and efficiency, has also ushered in a new era of cybersecurity threats, particularly affecting the most vulnerable segments of society, such as senior citizens. Defined broadly as individuals aged 50 and above, this demographic group often faces unique challenges in the digital realm, including varied levels of education, digital literacy, and IT proficiency. These factors not only heighten their susceptibility to online banking fraud and scams but also underscore the pressing need for tailored protective measures.

The urgency to address these vulnerabilities has been further amplified by the COVID-19 pandemic, which necessitated a swift and widespread transition to digital platforms for a myriad of daily activities, including banking. This shift, while necessary, exposed senior citizens to a broader spectrum of cyber threats, from phishing scams to sophisticated fraud schemes, highlighting the critical gaps in current cybersecurity measures and digital literacy programs.

Against this backdrop, our systematic literature review seeks to unearth effective methods to bolster the online banking security of senior citizens, thereby mitigating the risks associated with online fraud and scams. The review is predicated on the hypothesis that enhancing digital literacy, refining online banking interfaces to be more user-friendly, strengthening regulatory frameworks, and supporting the adoption of e-banking in the post-pandemic era can collectively forge a more secure digital banking environment for senior citizens.

This exploration is guided by a series of research questions (RQs) aimed at dissecting the multifaceted nature of online banking security for senior citizens. Central to our inquiry is the investigation of the specific needs and vulnerabilities of this demographic, the effectiveness of existing cybersecurity measures, and the potential for new strategies and interventions. Through a meticulous review of literature published between 2015 and 2023, this study endeavours to synthesize evidence-based recommendations, drawing from a broad spectrum of research focusing on cybersecurity, digital literacy, and anti-fraud measures tailored to the elderly.

As we embark on this systematic review, it is imperative to acknowledge the evolving nature of online banking and cybersecurity threats. The dynamic interplay between technological advancements and emerging fraud tactics necessitates a proactive and adaptive approach to safeguarding senior citizens. By consolidating current knowledge and identifying gaps in the literature, this review aims to contribute to the ongoing discourse on enhancing the resilience of senior citizens against online banking fraud and scams, ultimately fostering a safer and more inclusive digital financial ecosystem.

The increasing reliance on online banking among senior citizens, coupled with their heightened vulnerability to cyber threats, underscores the necessity of a comprehensive and multifaceted strategy to protect this demographic. Through this systematic literature review, we seek to illuminate the pathways towards achieving this goal, advocating for a collaborative effort that spans educational initiatives, technological innovations, regulatory reforms, and community support systems.

2. BACKGROUND

2.1 Online Banking Fraud

The term "online banking fraud" has been defined and discussed in various studies. Carminati et al. introduced the concept of BankSealer, a decision support system for analyzing online banking fraud. They described it as a general framework for online banking fraud and anomaly detection that synthesizes relevant information for each user and transaction [1]. Furthermore, Woods & Walter highlighted that online banking fraud is often categorized separately in surveys, even though it can result from various modes of attack such as malware, fraudulent emails, or other forms of cyber threats [2].

Additionally, online banking fraud encompasses unauthorized and deceitful activities aimed at users of digital banking platforms, with the intention of illicitly acquiring funds or sensitive information [3]. These fraudulent activities range from phishing—wherein individuals are duped into disclosing banking credentials on counterfeit websites or emails—to identity theft and malware attacks that covertly gather banking data [4]. The evolving nature of these threats poses a significant challenge to cybersecurity measures, necessitating continuous adaptation and enhancement of protective strategies.

Moreover, Mustafa & Jeffrey defined fraud as intentional and dishonest actions practiced acquiring unjustifiable benefits, emphasizing the deceptive nature of fraudulent activities [5]. Additionally, Wang et al. discussed the focus of monitoring the risk in banks, including fraud of debit cards, credit cards, and online banking, indicating the broad scope of fraud within the banking sector [6]. Furthermore, Singh et al. developed an approach using hidden Markov models for credit card fraud detection, highlighting the specific application of fraud detection techniques in the context of credit card transactions [7].

Existing literature provides diverse perspectives on the definition of online banking fraud, ranging from general frameworks for fraud detection to specific applications in credit card fraud detection. These definitions and discussions contribute to a comprehensive understanding of the concept of online banking fraud and the various forms it can take. Figure 1 shows several types of cybercrime in banking sectors.

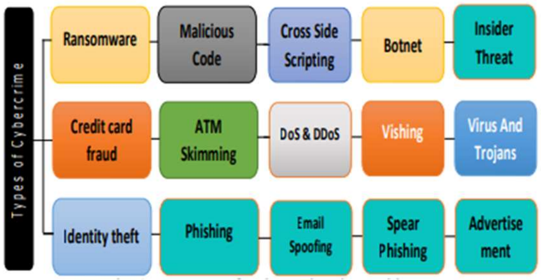

Figure 1: Types of Cybercrime Activities in Banking Sector

2.2 Senior Citizens

The term "senior citizens" refers to individuals aged 50 and above, a demographic characterized by its diversity in digital literacy, educational backgrounds, and technological exposure [8]. This group faces unique digital barriers, including physical limitations like reduced vision and motor skills, cognitive changes, and psychological apprehensions towards technology, which amplify their susceptibility to online banking fraud [9]. Recognizing the heterogeneity within this age group is pivotal for tailoring cybersecurity education and interventions.

The term "senior citizens" has been defined and discussed in various studies. Issac et al. defined senior citizens as Indian citizens aged 60 years or more [10]. Similarly, Rengamani et al. mentioned that senior citizens represent a substantial percentage of the population around the world and most of them need health care [11]. Additionally, Thamutharam et al. specified that in their study, senior citizens referred to individuals aged 65 and above [12]. Moreover, Fithri et al. also referred to senior citizens as individuals aged 65 and above [13]. In conclusion, the literature provides diverse perspectives on the definition of "senior citizens," with the common age threshold being 60 or 65 years and above.

2.3 Digital Literacy

Digital literacy signifies the competency to use digital devices, platforms, and the Internet safely and effectively. It includes basic operational skills, such as navigating web browsers and using smartphones, as well as advanced knowledge like understanding online privacy settings and identifying secure websites [8]. For senior citizens, digital literacy extends beyond mere technological usage to encompass a critical awareness of the digital landscape, essential for safeguarding against frauds and scams.

Digital literacy is a multifaceted concept that has been examined in various studies, each offering unique insights into its definition and implications. For instance, Alexander et al. Μαρτζούκου et al. identified three different digital literacies: universal literacy, creative literacy, and literacy across disciplines, emphasizing critical stances towards digital technologies, technical skills of digital content production, and diffusion of digital literacy across educational curricula [14]. Futurelab, an independent research organization, defined digital literacy as the capacity to create and share information efficiently in several formats, along with the ability to understand how and when to use digital tools [15]. Furthermore, Sparks et al. defined digital literacy as the ability to access new knowledge using digital tools, apply it to solve issues, perform information transactions, and use digital technology efficiently and safely [16]. Additionally, Çetindamar & Abedin emphasized the changing definitions of digital literacy and proposed the competencies required for digital literacy today [17]. These diverse perspectives contribute to a comprehensive understanding of digital literacy, encompassing critical thinking, technical skills, and efficient use of digital tools.

2.4 Cybersecurity Measures

These measures encompass strategies, tools, and practices designed to protect individual and organizational digital systems from cyber threats. For seniors, this includes personal security practices such as the use of strong passwords and two-factor authentication, as well as broader institutional cybersecurity efforts by financial entities and regulatory agencies to thwart fraudulent activities [3]. The dynamic between technological advancements and emerging fraud tactics necessitates a proactive and adaptive security stance to ensure the integrity and safety of online banking platforms.

The definitions provided draw on a range of empirical studies and theoretical analyses, including on the impact of internet scam victimization and online privacy concerns [3], on the relationship between digital literacy and life satisfaction among elderly Koreans [8], and Gupta (2008) on the privacy and security concerns of senior citizens online [4]. These citations offer a foundational understanding of the terms and concepts at play, highlighting the multidimensional challenges and considerations in safeguarding senior citizens in the digital banking ecosystem.

3. METHODOLOGY

The methodology for this systematic literature review is designed to meticulously identify, evaluate, and synthesize all relevant research concerning the safeguarding of senior citizens in online banking environments. This approach ensures that the review is comprehensive, transparent, and replicable, adhering to the principles of systematic literature review processes.

3.1 Research Questions

The research questions addressed by this study are:

RQ1: "What methods are effective in safeguarding senior citizens in online banking from fraud and scam activities?"

RQ2: "How do demographic factors (such as age, education level, and IT proficiency) influence the effectiveness of different safeguarding methods for senior citizens in online banking?"

RQ3: "What role do financial institutions and technology providers play in enhancing the online banking security of senior citizens, and how can their efforts be optimized?"

3.2 Search Strategy

A systematic search strategy was employed to identify studies published from January 2017 to December 2023. This timeframe ensures that the review captures the most recent advancements and trends in cybersecurity, digital literacy, and online banking technologies. Databases searched include IEEE Xplore, Scopus, and Google Scholar.

3.2.1 Search keywords

The searching process of the related literatures are conducted using a combination of keywords related to the index terms such as:

- “technique"
- "senior citizens"
- "financial fraud"
- "security measures"
- “financial fraud”

3.2.2 Selected databases

After defining several keywords that will be used to search related literature, we decided to conduct the search using relevant databases. Table 1 shows the list of selected databases that will be used for this purpose.

Table 1: Selected Databases for Finding Articles.

Database	URL
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
Scopus	https://www.scopus.com/home.uri
Google Scholar	https://scholar.google.com
ResearchGate	https://www.researchgate.net
Springer	https://www.springer.com/gp
ScienceDirect	https://www.sciencedirect.com
MDPI	https://www.mdpi.com
SemanticScholar	https://www.semanticscholar.org

3.3 Inclusion and Exclusion Criteria

Following are the criteria that we have agreed to have in making decision whether to include or exclude the studies that are found in the databases mentioned in previous section. Generally, our work excluded studies that did not specifically address senior citizens not accessible in full text. Table 2 shows the inclusion and exclusion methods based on the specific criterions.

Table 2: Criteria of Including and Excluding Existing Literature.

Criteria	Inclusion	Exclusion
Were published in peer-reviewed journals or conference proceedings.	/	X
Focused on online banking fraud prevention measures applicable to senior citizens.	/	X
Included empirical data or theoretical analyses.	/	X
Did not specifically address senior citizens.	X	/
Were published before 2017.	X	/
Did not accessible in full text.	X	/
Review article and systematic literature review article.	X	/

Table 3: The Study Framework for Meta-Analysis and Systematic Review.

Steps	***Description***
Research Question Formulation	Main RQ: Effective methods in safeguarding seniors in online banking from frauds and scams.
	Additional RQs cover demographic factors' influence and the role of financial institutions and technology providers.
Search Strategy	Systematic search from Jan 2017 to Dec 2023 in selected databases. Keywords related to online banking security, elderly fraud protection, etc.
Inclusion and Exclusion Criteria	Included: Peer-reviewed journals & conference proceedings, focus on online banking fraud prevention for seniors, empirical or theoretical analysis, English language.
	Excluded: Non-senior focused, pre-2017 and inaccessible full texts.
Quality Assessment	Clarity of Objectives: Whether the study clearly defined its research goals and hypotheses. Methodological Rigor: The appropriateness of the study design and methodology for addressing the research objectives. Sample Size and Selection: The size and selection process of the study population, considering the relevance to the senior citizen demographic. Data Analysis: The appropriateness and rigor of the data analysis methods. Bias and Limitations: The study's discussion of potential biases and limitations and how they were addressed.
Data Collection	Summarizing key study information (authors, publication year, methodology, findings, recommendations).
Data Analysis	Thematic synthesis approach for data analysis to identify themes and assess safeguarding methods' effectiveness.
Reporting	Systematic reporting of findings, addressing each research question. Highlights evidence-based strategies, implications for policy, and suggestions for future research.

3.4 Quality Assessment

A checklist was developed based on established criteria to assess the quality of the included studies. This checklist will evaluate:

- **Clarity of Objectives**: Whether the study clearly defined its research goals and hypotheses.
- **Methodological Rigor**: The appropriateness of the study design and methodology for addressing the research objectives.
- **Sample Size and Selection**: The size and selection process of the study population, considering the relevance to the senior citizen demographic.
- **Data Analysis**: The appropriateness and rigour of the data analysis methods.
- **Bias and Limitations**: The study discussed potential biases and limitations and how they were addressed.

3.5 Data Collection

Data extraction involved summarizing key information from each study, including the author(s), year of publication, research methodology, key findings, and recommendations related to the safeguarding of senior citizens in online banking. This process was conducted independently by two reviewers to ensure accuracy and completeness, with discrepancies resolved through discussion or consultation with a third reviewer.

3.6 Data Analysis

A thematic synthesis approach was used to analyze the extracted data, allowing for the identification of common themes and patterns across the studies. This approach facilitated the comparison of different safeguarding methods, the assessment of their effectiveness, and the exploration of the roles of various stakeholders in enhancing online banking security for senior citizens.

3.7 Reporting

The findings are reported systematically, addressing each research question in turn. The report synthesizes evidence-based strategies and interventions identified in the literature, highlighting their implications for policy, practice, and future research. This structured reporting ensures that the review provides actionable insights for enhancing the safety and security of senior citizens in online banking environments.

By following this detailed methodology, the systematic literature review aims to contribute significantly to the body of knowledge on protecting senior citizens from online banking fraud and scams. It offers a foundation for developing targeted interventions, guiding policy formulation, and suggesting directions for future research in this critical area of cybersecurity and elder care. Based on the above five steps of our research methodology, Table 3 provides the framework for it.

4. RESULT

This section summarizes the results of the study.

4.1 Search Results

Table 4 shows the results of the search procedure. From that procedure, we identified 50 unique studies that are related to our review topic.

Table 4: Number of Articles Found in Selected Databases.

Database	Number of articles found
IEEE Xplore	4
Scopus	1
Google Scholar	7
ResearchGate	16
Springer	2
ScienceDirect	12
MDPI	1
SemanticScholar	7
Total	**50**

4.2 Study Characteristics

This systematic literature review meticulously examined 50 scholarly papers, employing a stringent inclusion and exclusion criterion, specifically targeting individuals over the age of 50, who are perceived as particularly susceptible to the phenomena under investigation. The primary aim was to uncover and articulate the existent research gaps within these selected studies, particularly focusing on the outcomes pertinent to the specified age group. The analysis disclosed pronounced gaps, thereby delineating areas ripe for future scholarly inquiry. This endeavor not only underscores the critical need for enhanced protective measures for this demographic but also lays a foundational framework for subsequent research endeavors aimed at bolstering cybersecurity defenses for senior citizens, thereby contributing significantly to the broader discourse on cybersecurity and elder safety in the digital banking sector.

4.3 Quality of The Studies

The quality assessment of the studies incorporated into this review was conducted with a high degree of rigor, focusing on research published within the last five years to ensure relevance to current digital banking risks faced by senior citizens. This period was chosen to reflect the latest developments and challenges in cybersecurity. Each study was subjected to multiple rounds of reviews to scrutinize methodological soundness, sample adequacy, statistical robustness, and clarity in reporting outcomes. This thorough evaluation process revealed a range of research qualities, highlighting the necessity of discerning appraisal to identify the most reliable and impactful studies. This iterative process ensured that our analysis was both comprehensive and up to date, reflecting the latest insights and methodologies in the field. As part of ensuring the selected studies are among the high-quality studies, we will thoroughly ensure that the selected studies are providing correct or relevant insights for the research questions determined for this subject. All insight for each research question will include a proper citation.

5. RESULT

In this section, we discuss the answer to our research questions.

5.1 What methods are effective in safeguarding senior citizens in online banking from fraud and scam activities?

The comprehensive analysis of literature indicates that the most effective methods for safeguarding senior citizens in online banking include a combination of educational programs focused on digital literacy, the development of user-friendly digital interfaces, regulatory reforms aimed at protecting vulnerable users, and the provision of robust support systems for e-banking adoption.

Digital literacy programs significantly enhance the ability of senior citizens to identify and avoid online banking fraud. Social engagement through digital means also plays a crucial role in improving the life satisfaction and cybersecurity awareness of the elderly. Lee et al., found that smartphone use motives, social capital, and digital literacy are positively correlated with life satisfaction among elderly Koreans [8]. This suggests that digital literacy not only aids in fraud prevention but also contributes to broader well-being. Kim et al., highlighted the effect of digital literacy on life satisfaction, focusing on its impact on reducing depression and enhancing social participation among the elderly [9]. These findings emphasize the dual benefits of digital literacy programs in combating online fraud and improving overall quality of life. The key findings revolve around the effectiveness of the proposed ensemble method in enhancing accuracy, robustness, and adaptability of fraud detection systems, rather than directly relating to digital literacy or social engagement aspects. Focus on developing a robust fraud detection system for financial transactions. Moreover, social engagement plays a role in spreading awareness about online fraud and sharing best practices within communities, further reinforcing the defensive measures against such threats. Thus, while the paper concentrates on a deep learning approach to detect fraud, the underlying need for digital literacy and social engagement emerges as foundational elements in creating a comprehensive ecosystem where technical and human-centric strategies coalesce to combat online banking fraud effectively [18].

The necessity of user-friendly UI/UX design in mobile and online banking applications for senior citizens is critical. Simplified transaction processes, clear instructions, and responsive support systems significantly reduce the risk of fraud. Ubam et al., conducted a case study in Sarawak, Malaysia, focusing on the UI/UX analysis & design of mobile banking apps for senior citizens [19]. The study underscores the importance of involving seniors in the design process to create interfaces that address their specific needs.

There are significant concerns regarding the current regulatory frameworks' ability to protect senior citizens from digital fraud. Calls for stronger regulatory measures are common, focusing on the need for stringent data protection laws and mandatory security standards for financial institutions. Murthy et al., discussed the exploitation of senior citizens' fears and vulnerabilities, advocating for regulatory changes to prevent digital frauds [20]. Gupta, B. (2008) examined online privacy and security concerns of senior citizens, emphasizing the importance of empirical studies to guide policy adjustments [4]. These findings underscore the urgency for a comprehensive review and overhaul of the existing cybersecurity policy and regulatory framework to address these deficiencies. Akinbowale et al., enhanced legislation, improved policy alignment and implementation, specific laws to empower investigation and prosecution, and the development of standardized risk management protocols are recommended [21]. Additionally, the findings advocate for increased supervision and monitoring, better coordination and government support, and the nurturing of technical cybersecurity expertise to effectively mitigate cyberfraud within the South African banking industry.

The COVID-19 pandemic has significantly influenced the adoption of e-banking among senior citizens. Trust-building measures, education, and technical support are crucial for encouraging this demographic to embrace e-banking. Jena et al., explored the factors impacting senior citizens' adoption of e-banking post-COVID-19 pandemic, finding that a positive attitude towards technology and clear communication about security measures are essential [22].

5.2 How do demographic factors (such as age, education level, and IT proficiency) influence the effectiveness of different safeguarding methods for senior citizens in online banking?

Demographic factors such as age, education level, and IT proficiency significantly influence the effectiveness of online banking safeguarding methods for senior citizens. Older adults may experience difficulties in navigating complex security protocols due to varying degrees of familiarity with technology. Higher education levels typically correlate with a better understanding of potential cyber threats and the measures needed to counteract them. Consequently, designing protection strategies for seniors requires a nuanced understanding of these demographic variables to ensure that the safeguards are both effective and user-friendly for the intended audience.

According to Robinson & Edwards, they describe a framework for automatic scam-baiting, in which scammers are randomly assigned to different reply to strategies, which engage them in conversation automatically [23]. While originally designed as a means of testing antifraud countermeasures, this framework provides a means for direct behavioral experimentation on email-based fraudsters. By carefully designing reply to strategies and comparing their performance to control measures, we can use fraudster engagement with different reply to strategies as a means of testing hypotheses about what fraudsters find attractive in conversations with their 'victims'.

Without knowing the several types of cyber-attacks citizens also getting effected by the phishing activities [24]. It is commonly recognized that phishing is an affordable and hassle-free approach to harm the target because of awareness factors for the seniors. Mostly, sending malware to other computers via regular emails from reputable sources and giving hackers access to them. With the rise of services such as Dropbox, Office 365, Salesforce and other services, hackers are strengthening their capabilities with a variety of annoying attacks.

To assert the fact that demographic factors do have influences on the effectiveness of different safeguarding methods for senior citizens in online banking, Mortimer et al., conducted a cross-cultural study on m-banking adoption and found that data analysis revealed factors influencing adoption [25]. Similarly, Ngo et al., highlighted that cybercriminals target senior citizens due to their lower technological savviness, higher assets, and trust, suggesting the need for broader categories of cybercrime victimization [26]. Brands & Wilsem and Cook et al., also found empirical support for the relationship between perceived online risk and fear of economic cybercrime, indicating the influence of fear on online activities [27] [28]. Additionally, Habili et al., identified demographic variables such as age, education level, and income as influential in people's propensity to use online banking services [29].

Moreover, Chakraborty et al., demonstrated that perceptions of severity of a hacking incident are significant drivers of perceived online shopping risk for both older and younger adults, indicating the impact of perceived risk on online behavior [30]. Furthermore, Barroso et al., highlighted that online tasks requiring more digital experience are more efficiently exploited by those with a higher level of education, emphasizing the influence of education on digital activities [31]. Additionally, Saqib found that prior experience with computers and technology, along with attitudes towards computers, influence both attitude and behavior towards online banking, indicating the influence of technology proficiency and attitudes [32].

Furthermore, Chaudhry et al., suggested shifting the use of personal checks to less costly methods such as online banking due to technological evolution, indicating the influence of technological advancements on payment methods [33]. Additionally, Heller et al., explored housing policies and the influence of demography, highlighting the relevance of demographic factors in policy considerations [34]. Moreover, Jena identified significant predictors such as performance expectancy, effort expectancy, perceived risk, self-efficacy, perceived trust, and anxiety in older users' intention to use e-banking post-COVID-19, indicating the influence of various factors on e-banking adoption [35].

In conclusion, the studies provide comprehensive insights into the influence of demographic factors on the effectiveness of safeguarding methods for senior citizens in online banking. The findings underscore the significance of age, education level, IT proficiency, and perceived risk in shaping online banking behaviors and attitudes among senior citizens.

5.3 What role do financial institutions and technology providers play in enhancing the online banking security of senior citizens, and how can their efforts be optimized?

Financial institutions and technology providers are pivotal in enhancing online banking security for senior citizens. Their roles include developing secure and user-friendly banking platforms, offering tailored digital literacy training, and ensuring robust customer support. Optimization of their efforts can be achieved through ongoing collaboration with senior advocacy groups, cybersecurity experts, and regulatory bodies to ensure the evolving needs and vulnerabilities of senior citizens are adequately addressed and protected against.

The role of financial institutions and technology providers in enhancing the online banking security of senior citizens and optimizing their efforts has been extensively explored in the literature. Arcand et al., extended their research beyond mobile adoption to address customer engagement with financial institutions and issues relating to relationship quality [36]. This highlights the long-term impact of customer relationships on the security efforts of financial institutions. Additionally, Hua et al., emphasized the critical role of financial service providers (FSPs) in financing small and medium-sized enterprises, indicating the broader impact of financial institutions on the economy [37]. Furthermore, Manzano et al. identified key drivers of internet banking services use, emphasizing the importance of risk in online financial services. This underscores the significance of risk management in the security efforts of financial institutions [38].

Moreover, Purkait highlighted the major role of banks and financial institutions in online education and informing customers about security threats, indicating their proactive role in enhancing online banking security [39]. Mahmood et al., emphasized the influence of technological advancements on financial institutions, indicating the need for continuous optimization of security measures in line with technological changes [40]. Additionally, Jang & Kim emphasized the efforts of financial institutions in enhancing the usability of online security systems, highlighting the importance of user-friendly security measures for senior citizens [41]. This underscores the need for financial institutions to optimize security measures to cater to the needs of older users.

Furthermore, Rajaobelina et al. provided an in-depth examination of age-related links and presented relevant recommendations for financial institutions, emphasizing the need for tailored security measures for senior citizens [42]. Saroha & Laxmi highlighted the improvement of access to financial products for rural inhabitants through technical advancements, indicating the role of technology providers in enhancing financial inclusion and security [43]. Additionally, Bojang & Ceesay emphasized the critical elements of e-banking business, highlighting the strengthened online security of user financial information as a key focus for banks' e-banking strategy [44]. In conclusion, the literature provides comprehensive insights into the role of financial institutions and technology providers in enhancing online banking security for senior citizens. The findings underscore the proactive role of financial institutions in educating customers, the influence of technological advancements, and the need for tailored security measures to optimize online banking security for senior citizens. Figure 2 represents the effectiveness of literacy training or educational initiatives.

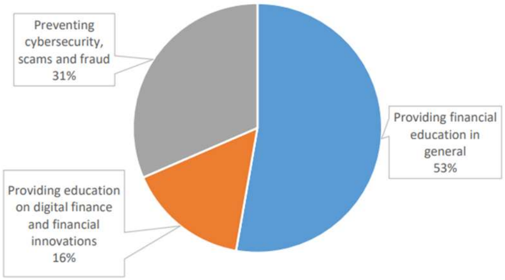

Figure 2: Effectiveness of Financial Education for Preventing Fraud

6. CONCLUSION

The synthesis of findings from the reviewed literature emphasizes the necessity of a multi-pronged approach to effectively safeguard senior citizens from online banking fraud and scams. This approach should integrate:

- Tailored Educational Programs: To enhance digital literacy among seniors, equipping them with the necessary skills and knowledge to navigate the digital banking landscape securely.
- Inclusive Design Principles: To ensure online banking platforms are accessible and user-friendly for seniors, reducing the risk of fraud.
- Robust Regulatory Support: To implement and enforce legal measures that provide strong protection against online fraud targeted at seniors.
- Comprehensive Support for E-Banking Adoption: To offer the necessary resources and support systems to help seniors transition to and navigate e-banking safely.

This review highlights the crucial role of collaboration among policymakers, financial institutions, technology developers, and community organizations in addressing the technological, educational, and legislative dimensions of cybersecurity for senior citizens. By fostering a safer and more inclusive online banking environment, stakeholders can significantly enhance the protection and confidence of senior citizens in digital financial services.

The findings of this review serve as a call to action for ongoing research, policy development, and practical implementations aimed at strengthening the defenses against online banking fraud for one of the most vulnerable segments of the population. As the digital financial landscape continues to evolve, it is imperative to continuously adapt and refine strategies to safeguard senior citizens, ensuring their security, confidence, and independence in the digital age.

REFERENCES:

[1] M. Carminati, R. Caron, F. Maggi, I. Epifani and S. Zanero, "BankSealer: An Online Banking Fraud Analysis and Decision Support System," in *IFIP Advances in Information and Communication Technology*, Marrakesh, 2014.

[2] D. W. Woods and L. Walter, "Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood," *IEEE European Symposium on Security and Privacy Wokrshops (EuroS&PW),* 2022.

[3] H. Chen, C. E. Beaudoin and T. Hong, "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors," *Computers in Human Behavior,* vol. 70, pp. 291-302, 2017.

[4] B. Gupta, "Online Privacy and Security Concerns of Senior Citizens: An Empirical StudyEmpirical Study," in *International Conference on Electronic Business (ICEB)*, Hawaii, 2008.

[5] I. Mustafa and E. O. Jeffrey, "Inside Abuse: A Threat to Banks' Stability," *The International Journal of Business & Management,* vol. 9, no. 7, pp. 339-348, 2021.

[6] X. Wang, L. Zhang and Y. Liu, "Research and Design of a Rules Engine for Bank Anti-fraud Platform," in *Proceedings of the 2016 International Conference on Engineering Management*, Guangzhou, 2016.

[7] M. Singh, S. Kumar and T. Garg, "Credit Card Fraud Detection Using Hidden Markov Model," *International Journal of Engineering and Computer Science,* vol. 8, no. 11, pp. 24878-24882, 2019.

[8] J. H. Lee and S. M. Bae, "The Relationship between Smartphone Use Motives, social capital, digital literacy and life satisfaction," vol. 52, no. 12, pp. 2554-2562, 2023.

[9] J. S. Kim, H. S. Kim and K. Y. Lee, "The effect of digital literacy in the elderly on life satisfaction: Focusing on depression and social participation.," *ISG2024 Manuscript Handling System,* vol. 21, no. 2, 2022.

[10] A. Isaac, "Factors influencing the quality of life among senior citizens in Puducherry, India: A cross-sectional study," *Journal of Family Medicine and Primary Care,* vol. 10, no. 4, pp. 1670-1675, 2021.

[11] S. Rengamani, "A study on the quality of life among senior citizens residing in old age homes and in the community in Chennai, India," *Indian Journal of Community Medicine,* vol. 35, no. 4, pp. 523-527, 2010.

[12] S. Thamutharam, "Prevalence and factors associated with depression among senior citizens in rural Puducherry, India.," *Journal of Family Medicine and Primary Care,* vol. 10, no. 3, pp. 1089-1094, 2021.

[13] F. Fithri, "Factors affecting the quality of life of senior citizens in Yogyakarta, Indonesia," *Journal of Aging and Health,* vol. 32, no. 5, pp. 473-480, 2020.

[14] B. Alexander, A. Becker and M. Cummins, "Digital Literacy: An NMC Horizon Project Strategic Brief.," *The New Media Consortium,* 2020.

[15] V. Oudeweetering and J. Voogt, "Digital literacy for all: A systematic review of definitions and frameworks.," *Computers & Education,* vol. 122, pp. 107-121, 2018.

[16] D. Sparks, M. Honey and A. Hargreaves, "Digital Literacy: A Review of Research and Evidence.," *International Society for Technology in Education (ISTE).,* 2016.

[17] D. Cetindamar and B. Abedin, "Digital literacy and its components: A literature review from 2009 to 2019.," *Education and Information Technologies,* vol. 25, no. 5, pp. 4171-4209, 2020.

[18] L. S. Hasugian and Suharjito, "Fraud Detection for Online Interbank Transaction Using Deep Learning," *Syntax Literate : Jurnal Ilmiah Indonesia,* vol. 8, no. 6, 2023.

[19] E. Ubam, I. Hipiny and H. Ujir, "User Interface/User Experience (UI/UX) Analysis & Design of Mobile Banking App for Senior Citizens," in *2021 International Conference on Electrical Engineering and Informatics (ICEEI)*, Kuala Terengganu, 2021.

[20] N. Murthy and S. Gopalkrishnan, "Exploiting fear and vulnerabilities of senior citizens: are regulatory changes required to prevent digital frauds?," *Working with older people,* vol. 28, no. 1, 2024.

[21] O. E. Akinbowale, H. E. Klingelhofer, M. F. Zarihun and P. Mashigo, "Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry," *Heliyon,* vol. 10, no. 1, 2024.

[22] R. Jena, "Factors Impacting Senior Citizens' Adoption of E-Banking Post COVID-19 Pandemic: An Empirical Study from India," *J.Risk Financial Manag,* vol. 16, no. 9, p. 380, 2023.

[23] J. Robinson and M. Edwards, "Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments," *Secur J,* 2024.

[24] A. Q. Stanikzai and M. A. Shah, "Evaluation of Cyber Security Threats in Banking Systems," *IEEE Symposium Series on Computational Intelligence (SSCI),* 2021.

[25] G. Mortimer, L. Neale, S. Hasan and B. Dunphy, "Investigating the factors influencing the adoption of m-banking: a cross cultural study.," *The International Journal of Bank Marketing,* vol. 33, no. 4, pp. 545-570, 2015.

[26] F. Ngo, J. Lee and B. Duong, "Victimization in cyberspace: is it how long we spend online, what we do online, or what we post online?," *Criminal Justice Review,* vol. 45, no. 4, pp. 430-451, 2020.

[27] J. Brands and J. Wilsem, "Connected and fearful? exploring fear of online financial crime, internet behaviour and their relationship.," *European Journal of Criminology,* vol. 18, no. 2, pp. 213-234, 2019.

[28] S. Cook, L. Giommoni, N. Pareja, M. Levi and M. Williams, "Fear of economic cybercrime across europe: a multilevel application of routine activity theory.," *The British Journal of Criminology,* vol. 63, no. 2, pp. 384-406, 2022.

[29] M. Habili, O. Muharremi and M. Hoxhaj, "Analysis of the variables influencing people's propensity to use online banking services in albania.," *International Journal of Finance & Banking Studies ,* vol. 11, no. 4, 2023.

[30] R. Chakraborty, J. Lee, S. Bagchi-Sen, S. Upadhyaya and H. Rao, "Online shopping intention in the context of data breach in online retail stores: an examination of older and younger adults.," *Decision Support Systems,* vol. 83, pp. 47-56, 2016.

[31] C. Barroso, M. Valle and M. Vinaras-Abad, "The role of the internet in later life autonomy: silver surfers in spain.," *Humanities and Social Sciences Communications,* vol. 10, no. 1, 2023.

[32] N. Saqib, "The transformation of financial system and its impact on consumers: case study of pakistan.," *Journal of Applied Finance and Banking,* vol. 5, no. 1, pp. 87-98, 2018.

[33] P. Chaudry, L. Cesareo and A. Pastore, "Resolving the jeopardies of consumer demand: revisiting demarketing concepts.," *Business Horizons,* vol. 62, no. 5, 2019.

[34] C. Heller, L. Ekstam, M. Haak, S. Schmidt and B. Slaug, "Exploring housing policies in five swedish municipalities: alternatives and priorities.," *BMC Public Health,* vol. 22, no. 1, 2022.

[35] R. Jena, "Factors impacting senior citizens' adoption of e-banking post covid-19 pandemic: an empirical study from india.," *Journal of Risk and Financial Management,* vol. 16, no. 9, p. 380, 2023.

[36] M. Arcand, S. Tep, I. Brun and L. Rajobelina, "Mobile banking service quality and customer relationships.," *The International Journal of Bank Marketing,* vol. 35, no. 7, pp. 1068-1089, 2017.

[37] S. Hua, Y. Yu-dong and Z. Tao, "How different types of financial service providers support small- and medium- enterprises under the impact of covid-19 pandemic: from the perspective of expectancy theory.," *Frontiers of Business Research in China,* vol. 14, no. 1, 2020.

[38] J. Manzano, C. Navarre, C. Mafe and S. Blas, "Key drivers of internet banking services use.," *Online Information Review,* vol. 33, no. 4, pp. 672-695, 2009.

[39] S. Purkait, "Phishing counter measures and their effectiveness – literature review.," *Information Management & Computer Security,* vol. 20, no. 5, pp. 384-420, 2012.

[40] A. Mahmood, M. Imran and K. Aidil, "Modeling individual beliefs to transfigure technology readiness into technology acceptance in financial institutions.," *Sage Open,* vol. 13, no. 1, 2023.

[41] J. Jang and H. Kim, "Diverging influences of usability in online authentication system: the role of culture (us vs korea).," *The International Journal of Bank Marketing,* vol. 40, no. 2, pp. 384-400, 2022.

[42] L. Rajaobelina, I. Brun, L. Ricard and B. C. Cloutier, "Not all elderly are the same: fostering trust through mobile banking service experience.," *The International Journal of Bank Marketing,* vol. 39, no. 1, pp. 85-106, 2020.

[43] S. Anjali and Laxmi, "Study on digitalization of banking in rural areas of haryana," *Journal of Propulsion Technology,* vol. 44, no. 4, pp. 5467-5475, 2023.

[44] I. Bojang and L. Ceesay, "Consumer susceptibility to e-banking services: evidence from retail banking sector of the gambia.," *European Journal of Business Management and Research,* vol. 5, no. 2, 2020.