INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 10, (2024) E-ISSN: 2222-6990

Scams Issues among Elderly: A Conceptual Paper

Nurul Faqihah Saifuddin[2], Balqis Musa[2], Nurin Sofiya Zakaria[2], Nur Farhana Othman[2], Andito Dwicahyo Putera[2], Puvaneswaran Kunasekaran[1,2], Mohd Roslan Rosnon[1,2], & Muhammad Afiq Abdul Razak[2] & Rahimah Ibrahim[1,2]

[1]Malaysian Research Institute on Ageing, Universiti Putra Malaysia, Serdang, [2]Faculty of Human Ecology, Universiti Putra Malaysia, Serdang

Corresponding Author Email: puvaneswaran@upm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i10/23268 DOI:10.6007/IJARBSS/v14-i10/23268

Published Date: 19 October 2024

Abstract

This study aims to identify and analyse the key factors of scams among the elderly. In the context of rapid technological advancement, the elderly are particularly vulnerable to scams due to their limited technological knowledge and inherent trust in others which threaten their well-being. Existing literature highlights that elderly are frequent targets of online scams due to declining cognitive abilities and social isolation. The analysis encompasses a comprehensive review of relevant studies and demographic data to explore the factors contributing to scams targeting the elderly. This paper identifies four factors that make the elderly expose to scams which are (i) cognitive decline; (ii) social isolation; (iii) non-technologies savvy and; (iv) financial stability. There are five types of scams that target older people which are (i) government impersonation scams; (ii) sweepstakes and lottery scams; (iii) robocalls and phone scams; (iv) computer tech support scams and; (v) grandparents' scams. This study shows the impact of scams on the (i) financial and (ii) emotional security of the elderly. This paper provides valuable insights for readers on the mechanisms of scams targeting the elderly and offers a foundation for developing effective preventive measures and educational initiatives to protect this vulnerable population.

Keywords: Scams, Technology, Elderly, Financial, Emotional

Introduction

In an era of rapid technological advancement, fraud targeting the elderly poses a significant challenge in modern society. Scammers often find the elderly to be easy targets due to their limited technological knowledge and tendency to trust others. These scams not only threaten seniors' financial security but also cause serious emotional repercussions. To protect seniors from fraud, effective preventive measures and widespread education about the risks are essential. Understanding scammers' tactics and collaborating with governments, consumer protection agencies, and society can increase protections for the elderly and prevent

unnecessary harm. Nisa, Nisak, & Fatia (2023) stated, "The elderly are the group most often victims of digital crime and are vulnerable to consuming and spreading fake news" (p. 1).

Scammers are preying on the emotional vulnerabilities of elderly to achieve their own fraudulent goals. They often take advantage of elderly who may feel isolated or depressed. They exploit those feelings by creating a sense of urgency or fear which makes it easier for them to manipulate and defraud elderly. Technological advancements have made it easier for scammers to reach a broader audience and create more convincing facades such as fake websites or official-looking emails. Falling victim to these scams can devastate elderly financially and emotionally. Many may lose their life savings, face financial ruin, and lose trust in others. Additionally, the emotional toll of realising they have been deceived can lead to feelings of shame, humiliation, and even depression.

Ultimately, protecting the elderly population from scams requires a collective effort from individuals, communities, and authorities to ensure their safety, security and well-being. Sinaga (2022) believes that the elderly limitations in processing information in the digital space disturb their psychological well-being which making them more susceptible to fraud, improper protection of personal data and provocation by false news in the digital space. In this study, literature review is analysed systematically to explore the key types, factors and effect of scam among the elderly. The factors are gathered from various local and international academic journals related to ageing studies. Several secondary data mainly on demographic profile were also analysed to understand the issue.

Literature Review

An online scam is a fraudulent scheme conducted over the internet, intending to deceive individuals into divulging personal, financial, or sensitive information, or directly stealing their money. These scams can manifest in various ways, including phishing emails, fake online stores, sophisticated fraudulent dating profiles, and investment opportunities that seem too good to be true (Puram, Kaparthi & Rayaprolu, 2011). Elder financial abuse refers to any harmful conduct targeting individuals who are 60 years of age or older. While the definition of an older person varies by country, it typically aligns with the retirement age in most places (Nurfadhilah et al., 2021). The study by Pranggono & Arabo (2020) highlights how the global COVID-19 pandemic has led to a surge in cybersecurity problems. Cybercriminals seized the opportunity to make quick profits, resulting in a notable increase in cybercrime activity.

Reyes et al (2007), explained on the concept and understanding of cybercrime and discussed various aspects such as law enforcement and prosecution. According to them, any intentional act where the victim suffers or could suffer a loss, while the perpetrator benefits or gains, is considered a computer crime. Financial exploitation has been associated with age-related vulnerabilities, including a general decline in mental or physical health, cognitive and neuropsychological impairments, financial concerns, social isolation, loneliness, and lack of family support (Weissberger et al., 2020; Boyle, 2020). Online scams encompass deceitful activities or tactics employed by groups or individuals to illicitly obtain money or goods from unsuspecting individuals. With the increasing global exposure and globalisation of the Internet, online scams have proliferated. It's crucial to raise public awareness and encourage scepticism toward individuals online, as their true identities are often unknown (Shah, 2020).

According to Nurul Huda et al (2021), more than fifty percent of older persons utilise the Internet today, and this percentage is steadily rising. This increase calls for more research into the cybersecurity problems and difficulties that older people face. Seniors typically lack knowledge about technology, which deters them from learning about new security precautions. A lot of older people have health problems or physical limitations that make it hard for them to use new technology; they frequently need help to operate new equipment. Their gadgets are usually not adequately safeguarded as a result. Moreover, according to a Consumer Financial Protection Bureau (2022), elder financial exploitation whose estimated losses range from $2.9 billion to $36.5 billion annually is becoming more commonplace and is being dubbed the crime of the 21st century because of the yearly drops in victimisation rates and losses. The extent to which elder financial exploitation occurs is unknown, based on research conducted online. This is especially clear from the yearly losses and victimisation rates roughly 1 in 24 occurrences of elder abuse are thought to be recorded, based on estimates. Furthermore, according to Consumer Financial Protection Bureau (2022) a investigation on 2017 shows the average loss suffered by a senior American who falls victim to elder financial exploitation is close to $34,200. Thus, attempts and actual losses of more than $6 billion occurred between 2013 and 2017.

Morgan & Tapp (2024) mentioned that financial fraud causes elderly persons to lose about $36 billion annually. Based on data gathered by the FBI's Internet Crime Complaint Centre, 105,301 fraud cases targeting individuals 60 years of age or above were documented in 2020. Ueno et al (2022), mentioned that there were 16,851 recorded scam instances in Japan in 2019, resulting in a total harm amounting to 31.58 billion JPY, or 305.7 million USD. Elderly people made up 83.7% of the victims in these cases, and older adults are more likely than the general US population to fall victim to consumer fraud.

Methodology

The methodology for this conceptual paper involves review of existing literature and data sources to address the multifaceted issue of scams among the elderly. By synthesizing insights from academic journals and secondary data analysis, this paper develops a comprehensive conceptual framework about scams issues among aging population such as types of scams, factors of scam and impacts of scams. This framework is critically analyzed to assess its relevance and contribution to understanding the scams issues among the elderly. This paper provides valuable insights for readers on the mechanisms of scams targeting the elderly and offers a foundation for developing effective preventive measures and educational initiatives to protect this vulnerable population.

Scam among Elderly in Malaysia

According to the Royal Malaysia Police, cybercrimes in the country have increased by 50% over the past two years. This surge is primarily attributed to scammers' ability to exploit technological advancements and leverage various loopholes, allowing them to deceive their victims with new tactics (Button & Cross, 2017). It is undeniable that, in this era of globalisation, technological innovation is advancing rapidly alongside global population growth. The swift pace of the digital age has significantly transformed various aspects of life, particularly in terms of living arrangements and lifestyles (Kostić, 2022). There are many types of scams among the ageing population in Malaysia. One of the most famous scam issues in Malaysia is the Macau scam. According to the Central Bank of Malaysia, a Macau scam is when

an individual may receive phone calls from scammers who impersonate bank representatives or public officials. These scammers aim to deceive recipients into divulging personal banking information or transferring funds to third-party accounts. Based on the Ministry of Communication and Multimedia, Taiwanese and Chinese syndicates operate the Macau Scam by utilising international and local calls from Hong Kong, as well as local Malaysian bank accounts, to collect funds from victims' accounts. The extracted money is then converted into cash and transferred overseas through money changer services. This technique, known as Voice Phishing, involves the use of Voice over Internet Protocol (VoIP) technology, which enables callers to display any phone number to deceive victims.

Based on New Straits Times (2024), there have been 494 reported cases of impersonation scams nationwide since January 1, resulting in total losses of RM238,732. Additionally, Malay Mail (2024), reported that senior citizens in Malaysia lost RM552.5 million to online scams between 2021 and 2023, according to Bukit Aman Commercial Crime Investigation Department (JSJK) director Datuk Seri Ramli Mohamed Yoosuf. He noted that these scams affected 5,533 elderly victims, making up 6.4% of the 86,266 online scam victims recorded during this period, with total losses amounting to RM2.7 billion. Despite the lower number of elderly victims compared to other age groups, the financial losses they experienced were significantly higher. Furthermore, New Straits Times (2023) reported a case where a 70-year-old from Kanowit lost RM120,000 after being deceived by scammers who falsely claimed he had won a RM300,000 lottery, requiring an upfront payment before receiving his winnings.

While Bernama (2023), reported that a 69-year-old man was contacted via Facebook by an individual pretending to be a bank officer in March 2023. The fake bank officer requested the victim to pose as a relative of a deceased person who had allegedly deposited US$26,700,000 (about RM 126 million). The victim was promised half of this amount. The suspect then introduced a 'lawyer' who would supposedly manage all required payments, including taxes, levy charges, and anti-laundering fees. Following these instructions, the victim used his savings and made 70 transactions into 26 different bank accounts from May 9, 2023 to March 11, 2024, but never received any promised payment. Thus, the public must verify the legitimacy of such calls with the police or relevant agencies immediately. Other issues reported by Bernama (2024), is the housewife lost over RM1.09 million after investing in a stock scheme promoted on social media, which promised high returns in a short period. After initially investing a small amount and receiving the promised profit, the victim continued to invest up to RM1.09 million. However, despite the initial returns, subsequent profits ceased, and attempts to contact the suspect were unsuccessful.

Types of Scams

Government Impersonation Scams

Imposter scammers employ various methods to deceive individuals into believing they are interacting with authoritative figures. Using phone calls, text messages, or emails, these scammers create an appearance of legitimacy, often falsifying caller ID to display official government or business numbers. Their primary aim is identity theft, achieved through soliciting money, gift cards, or personal information from victims. Genuine government agencies typically initiate contact through formal letters, making unexpected communication through other channels a red flag for potential scams. Among the prevalent scams are IRS

imposter schemes, where fraudsters falsely claim tax debts and may issue threats, and Social Security imposter scams, which involve false claims regarding benefits (United State Government, 2024).

According to the Australian Competition and Consumer Commission (2023), scammers frequently impersonate trusted entities like businesses, friends, or family members to extract money or personal details. These imposters deceive individuals into believing they represent reputable organisations, including police, government agencies, banks, and well- known corporations. They may even assume the identity of a victim's acquaintance. Utilising technology, scammers manipulate caller IDs to resemble legitimate numbers and craft text messages that seamlessly integrate into ongoing conversations with genuine organisations.

Imposter scammers exploit various channels like phone calls, texts, and emails to impersonate authoritative figures or agencies (United State Government, 2024). They manipulate caller IDs to appear legitimate, often targeting vulnerable groups like older adults who may be less familiar with digital security. This demographic is at heightened risk in countries such as Indonesia, where platforms like WhatsApp and Facebook are used extensively but digital security knowledge remains limited (Jumrana & Cecep, 2023).

Sweepstakes and Lottery Scams

According to the Federal Trade Commission (2021), fake prize, sweepstakes, and lottery scams involve fraudulent communications claiming that recipients have won prizes such as electronics or vehicles. These scams become evident when victims are asked to pay fees or provide financial information to receive their prizes. Key indicators include demands for payment, false promises of increased winning odds through payments, and requests for sensitive financial data. Scammers often masquerade as government entities or reputable businesses to enhance credibility, employ mass messaging to target numerous individuals, and employ urgency tactics to elicit immediate responses. Additionally, scammers may send counterfeit checks, requesting recipients to return a portion of the funds, aiming to deceive individuals into disclosing personal information or making payments under false pretences. Federal Trade Commission (2021), warns about scams promising prizes like iPads or cars, requiring recipients to pay fees or disclose financial information. Elderly individuals, particularly susceptible due to their empathy and limited digital literacy, are often targeted through emotional manipulation tactics (Robinson & Edwards, 2024). This demographic's vulnerability is further exacerbated by their high usage of mobile devices for social media and messaging, where scams can easily proliferate (Jumrana & Cecep, 2023).

Robocalls And Phone Scams

The Federal Trade Commission (2023), identifies robocalls as automated calls featuring pre-recorded messages rather than live operators, frequently employed illegally to promote products or services, and often involved in fraudulent activities. Scams include the auto warranty hoax, where scammers falsely assert the need for extended car warranties; the Amazon suspicious charge ploy, where individuals impersonate Amazon representatives to report fictitious charges; and the Social Security Administration scam, where fraudsters pretend to be SSA officials claiming enforcement actions against recipients. Other common schemes involve pretending to be Apple tech support, utility companies, offering student loan relief, or representing governmental or financial institutions offering reduced interest rates.

Recipients are advised to disconnect immediately from such calls or delete associated messages to avoid engagement. According to the Federal Trade Commission (2023), illegal robocalls pose significant risks, including auto warranty scams and fraudulent calls pretending to be from Amazon or the Social Security Administration. These scams exploit trust and urgency, which are effective tactics against the elderly who are targeted for their willingness to help and lack of familiarity with such deceptive practices (Button et al., 2017).

Computer Tech Support Scams

According to the Federal Trade Commission (2022), tech support scams involve deceiving individuals into believing their computers have severe issues, such as viruses, and then charging for unnecessary repair services. Payment is typically requested through irreversible methods like wire transfers, gift cards, prepaid cards, cryptocurrency, or money transfer apps. Tactics employed include impersonating technicians from reputable companies over phone calls, presenting pop-up alerts that mimic legitimate system or antivirus notifications, and placing online advertisements or search engine listings to attract victims. Recognizing these tactics is essential to avoid falling victim to tech support fraud. Tech support scams, as highlighted by the Federal Trade Commission (2022), deceive victims into paying for unnecessary services by fabricating computer issues. Scammers exploit the elderly's trust in perceived authority figures and their willingness to resolve perceived problems swiftly, often through payment methods that are difficult to trace or reverse (Robinson & Edwards, 2024).

The Grandparents' Scam

Exploiting the trust and emotions of grandparents, grandkid and family scams involve impersonating distressed loved ones needing financial assistance, such as bail or medical expenses. Scammers employ various strategies, including accessing personal information from social media or using voice cloning technology to replicate family members' voices. These scams often involve urgent pleas for secrecy and immediate payment, typically through methods that are difficult to trace or reverse, such as wire transfers, cryptocurrency, or gift cards. Federal Trade Commission (2019; 2024) stated that awareness of these tactics is critical for potential victims, who are advised to verify callers' identities independently and avoid disclosing sensitive information over the phone.

Factors Scam among Elderly

Scammers often target the elderly due to several factor. First, cognitive decline significantly increases their risk of scams among elderly. Elderly struggle with decision-making, memory, and judgment as their cognitive functioning deteriorates with age (Ebner et al., 2022). This cognitive decline makes them difficult to identify and respond to fraudulent schemes. For example, memory issues may lead them to provide personal information to scammers when they mistakenly believing they are interacting with trusted family members. The impaired ability to assess risks and recognize inconsistencies in scammers' stories further exacerbates their vulnerability. Next, elderly individuals who are financially stable are prime targets for fraud. Many seniors have accumulated assets over their lifetimes and have reliable income sources such as pensions. Scammers are drawn to these individuals due to their wealth and financial resources. Past research highlighted that elderly with substantial lifetime wealth are at a higher risk of being targeted by scams promising high returns on investments or posing as financial advisors (Phelan, O'Donnell & McCarthy, 2023). Additionally, elderly who often have a charitable disposition are particularly vulnerable to scams which pretend to be

legitimate charities and asking for donations. This vulnerability is heightened when their cognitive abilities are impaired and making it harder for them to recognize the scam.

Non technology savvy also a crucial factor of scams among elderly. Many elderly lack familiarity with digital technology and online security practices make them vulnerable to scams (Kemp & Perez, 2023). This lack of digital literacy makes them vulnerable to internet-based scams such as phishing or fraudulent tech support offers. Without adequate understanding of online threats, they are more likely to fall for schemes designed to exploit their lack of technological knowledge (Ebner et al., 2022). Next, Social isolation is one of the factors that make the elderly easily susceptible to scams. As elderly individuals often live alone, especially after their children have started their own families, they may experience loneliness and a strong desire for social interaction. This isolation makes them more susceptible to scammers who exploit their need for companionship by pretending to be friendly and trustworthy individuals (Kemp & Perez, 2023). The lack of a supportive social network also means they may not have others to consult or warn them about potential scams, making them more likely to fall victim (DeLiema, 2018).

Impact of Scams on Elderly

According to Kemp & Perez (2023), elderly experience more severe non-financial consequences from fraud even though they are less likely to incur financial losses. These non-financial impacts include emotions such as anger, embarrassment, irritation, stress, and adverse physical health effects. Kemp & Perez (2023), stated that 68.5% of fraud victims reported feeling irritated, 55.6% felt angry, 30.4% experienced stress, 15.7% felt embarrassed and 6.2% suffered from negative physical health consequences. This shows that elderly are most affected by these specific non-financial impacts compared to other age groups.

This aligns with previous research on victim blaming and the fear of incompetence in a digital society. Prior studies have indicated that older adults, even those who are fraud victims, often describe those defrauded as greedy, gullible, or naïve, which attributes some responsibility to the victims themselves (Button, Lewis & Tapley, 2014). Such discourses can amplify the feelings of anger and embarrassment identified in the study. Additionally, elderly sometimes fear that their family and friends will perceive them as incapable of managing their personal affairs after falling victim to fraud that leading to concerns about losing control over their finances. These worries can intensify the negative emotional and psychological impacts of consumer fraud. Furthermore, elderly generally have poorer physical health, but the emotional and psychological effects of fraud are more likely to manifest or exacerbate existing physical issues. This may explain the higher likelihood of negative physical effects from fraud among those aged sixty-five or over (Kemp & Pérez, 2023).

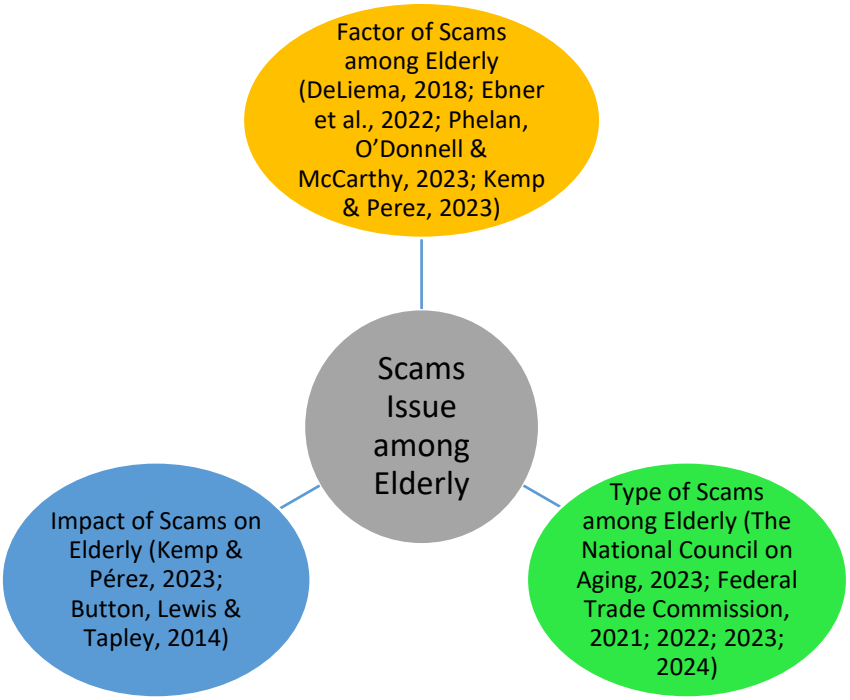

Figure 1: The Proposed Conceptual Framework on Scams Issues among Elderly

Conclusion

The landscape of scams targeting the elderly continues to evolve with advancements in technology. The psychological study on cognitive and affective changes linked with ageing and age-related stereotypes are some of the reasons why it is commonly considered that the prevalence and vulnerability of consumer fraud increase in old age (Ross, Grossmann & Schryer, 2014). Based on Figure 1, addressing scams targeting the elderly requires serious attention. Scammers are becoming increasingly sophisticated, employing a variety of tactics to exploit vulnerabilities such as social isolation, financial stability, cognitive decline, and lack of technological savvy. These tactics lead to significant emotional and financial suffering for the elderly. The effects are serious which eroding confidence and trust while frequently making pre-existing social and physical problems worse. A multifaceted strategy is needed to address this issue, one that involves educating and increasing awareness among the elderly, putting strong technology safeguards in place, strengthening social support networks and advocating for stricter enforcement of the law. DeLiema et al (2018), mention that if socioemotional characteristics, financial literacy and context are not as predictive of victimisation as they are, the consumer education messaging should emphasise teaching techniques for resisting persuasion. The elderly are a vulnerable group that society can safeguard more effectively by addressing the issues that make them more likely to fall victim to scams and advocating for preventive measures that will ensure their financial and emotional well-being in a digital world.

Recommendation

Scams that prey on the elderly must be addressed in a multidimensional approach that includes community support, technology intervention and education. It's critical to implement focused educational initiatives to increase older adults' knowledge of technology and teach them how to spot and avoid typical scams. It should be common practice to hold regular community workshops and lectures on cybersecurity, safe internet usage and how to

handle suspicious correspondence. It is important to develop and promote technological solutions, such as simple antivirus software, safe browsing extensions and user-friendly security products designed for the elderly. According to Ueno et al (2022), there are two integrated methods used in Japan to identify phone fraud which are actual time call data is analysed and the system immediately disconnects calls if fraud is suspected, recorded call data is analysed and then the system notifies the call receivers through phone call or email or by calling their pre-registered relatives during the call.

Furthermore, financial institutions should encourage the use of trustworthy financial advisors who can provide oversight and guidance to prevent illegal investments and transactions as well as implement additional protective measures for elderly customers such as transaction alerts and monitoring for unusual account activity. In addition, targeted protection within financial systems worldwide would allow prevention and early interventions due to the surge in frauds that can originate from outside sources (Phelan, O'Donnell & McCarthy, 2023). This includes sharing information about emerging threats, coordinating with law enforcement, and implementing advanced security technologies to safeguard elderly individuals from sophisticated scams that transcend national boundaries. These proactive measures can help in early intervention and prevention which ensuring a safer financial environment for elderly customers worldwide

Next, the creation of support groups and counselling services is crucial in providing victims with the emotional support they need to recover their trust and deal with the psychological effects of the scam. It is also suggested by Satchell et al (2022), that older persons' fear of crime is unfounded, but that its effects might be more severe due to related life events including deteriorating physical condition, losing a loved one, and having less money in retirement. Ensuring victims can readily seek assistance and report instances are ensured by providing clear and accessible reporting channels for elder fraud. By combining these strategies, society may make the elderly feel safer and more supported while also drastically lowering the frequency of scams that target them.

References

Australian Competition and Consumer Commission. (2023). *Impersonation scams*. Australian Competition and Consumer Commission.

Bernama. (2023, Jun 14). Senior citizens lose over RM2.2 mil to investment frauds. *Bernama.*

Bernama. (2023, April 10). Elderly vegetable trader loses nearly RM1 mil in phone scam. *Bernama.*

Boyle, D. A. (2020). Older adults and scam awareness: exploring vulnerability within geriatric oncology. *Exploitation, Financial, Older Adults, Scam, Geriatric, Patients with Cancer*, 24(4), 434-438.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*, 36-54.

Button, M., & Cross, C. (2017). Technology and fraud: The 'fraudogenic' consequences of the internet revolution. In McGuire, M. & Holt, T. (Eds.), *The Routledge Handbook of Technology, Crime and Justice*. Routledge.

Consumer Financial Protection Bureau. (2022). *Recovering from elder financial exploitation: A framework for policy and research.* Consumer Financial Protection Bureau.

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, *58*(4), 706-718.

Ebner, N. C., Pehlivanoglu, D., Polk, R., Turner, G. R., & Spreng, R. N. (2022) *Aging online: Rethinking the aging decision-maker in a digital era. In: A fresh look at fraud.* Routledge.

Federal Trade Commission. (2021). *Fake Prize, sweepstakes, and lottery scams.* United State Government.

Federal Trade Commission. (2022). *How to spot, avoid, and report tech support scams.* United State Government.

Federal Trade Commission. (2023). *Robocall scam examples*. United State Government.

Federal Communications Commission. (2024). *"Grandparent" scams get more sophisticated*. United State Government.

Federal Communications Commission. (2024). *Scammers use AI to enhance their family emergency schemes*. United State Government.

Jumrana J., & Cecep, I. (2023). Elderly digital resilience in responding to online fraud. *Proceedings of the Regional Seminar on Community Issues, Kendari, Province of Sulawesi Tenggara, Indonesia*. European Union Digital Library.

Kemp, S., & Pérez, N. E. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health,* 20(7), 1-17.

Kostić, J. O. (2022). Effects of using information and communication technologies on relationships with others and personal well-being*. Media Studies and Applied Ethics*, 3, 147-162.

Malay Mail (2024, May 27). Bukit Aman: Senior citizens lost over half a billion ringgit to online fraud from 2021 to 2023. *Malay Mail.*

Morgan, R. E., & Tapp, S. N. (2024). *Examining financial fraud against older adults.* National Institute of Social Justice.

New Straits Times (2024, January 21). 494 cases of impersonation scams reported nationwide since Jan 1, RM238,732 in losses**.** *New Straits Times.*

New Straits Times (2023, November 8). Elderly man loses RM120,000 in lottery scam. *New Straits Times.*

Nurfadhilah, C. A., Rojanah, K., Rahimah, I., & Muslihah, H. (2021). Elder financial abuse experience: A qualitative study from the perspective of older persons in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 11(8), 479–498.

Huda, N. K., Nor Aimuni, M. R., Farhan, Z., & Geogiana, B. (2021). Synthesizing cybersecurity issues and challenges for the elderly. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1775–1781.

Phelan, A., O'Donnell, D., & McCarthy, S. (2023). Financial abuse of older people by third parties in banking institutions: A qualitative exploration. *Ageing and Society*. 43(9), 2135-2156.

Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2), 1-6.

Puram, P. K., Kaparthi, M., & Rayaprolu, A. K. H. (2011). Online scams: Taking the fun out of the internet. *Indian Journal of Computer Science and Engineering*, 4(2), 559-565.

Reyes, A., O'Shea, K., Steele, J., Hansen, J. R., Jean, B. R., & Ralph, T. (2007). *Cyber crime investigations: Bridging the gaps between, security professionals, law enforcement, and prosecutors*. Syngress Publishing.

Robinson, J., & Edwards, M. (2024). Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments. *Security Journal*, 1- 24.

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Journal of the Association for Psychological Science*, *9*(4), 427–442.

Satchell, J., Craston, T., Drennan, V. M., Billings, J., & Serfaty, M. (2023). Psychological distress and interventions for older victims of crime: A systematic review. *Trauma, Violence & Abuse*, *24*(5), 3493–3512.

Shah, A. (2020). A Study of Online Scams: Examining the Behavior and Motivation Factors of Scammers and Victimization Consequences. In N. Suki & N. Suki (Eds.), *Leveraging Consumer Behavior and Psychology in the Digital Economy* (pp. 81-90). IGI Global.

Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsuoka, T. & Narumoto, J. (2022) Psychosocial characteristics of victims of special fraud among Japanese older adults: A cross-sectional study using scam vulnerability scale. *Frontier Psychology,* 13, 1-10.

United State Government (2024). *Imposter scams*. United State Government.

Weissberger, G. H., Mosqueda, L., Nguyen, A. L., Samek, A., Boyle, P. A., Nguyen, C. P., & Han, S. D. (2020). Physical and mental health correlates of perceived financial exploitation in older adults: Preliminary findings from the finance, cognition, and health in elders study. *Aging & Mental Health*, *24*(5), 740–746.