ASI
Asia Social Issues

E-ISSN: 2774-0315

https://doi.org/10.48048/asi.2025.274566

Aging And Vulnerability: The Psychological Ramification of Financial Fraud on Seniors

Khemtida Petchtam

Faculty of Social Sciences and Humanities, Mahidol University, Nakhon Pathom 73170, Thailand

Corresponding author's e-mail: khemtida.pet@mahidol.ac.th

Abstract The aging population in Thailand is proliferating, with significant effects on social, economic, and health systems. This study aims to investigate the impact of financial fraud on senior females' mental health in the Phra Khanong district of Bangkok, Thailand. It identifies the types of fraud experienced by seniors and their psychological consequences, primarily focusing on stress, anxiety, and depression. The researcher used mixed methods to explore senior females' experiences with financial fraud. Data collection tools included the Kessler Psychological Distress Scale (K-10) to assess the level of distress, General Anxiety Disorder-7 (GAD-7) to measure anxiety levels, Patient Health Questionnaire-9 (PHQ-9) to evaluate depression severity, and in-depth Interviews to provide qualitative insights into personal experiences with fraud. The findings indicated a high prevalence of financial fraud among the sample, with the most common phishing scams via text messages and social media (70%). Victims of financial fraud exhibited higher levels of distress, anxiety, and depression compared to non-victims. Specifically, the mean distress score was markedly higher in the fraud group, highlighting the severe emotional impacts of financial exploitation. These findings call for urgent legislative action, increased public awareness, innovation, and collaboration with financial institutions to protect this vulnerable population from financial exploitation. Future research should expand the geographical scope of the study and incorporate longitudinal designs to understand better the long-term psychological effects of financial fraud on seniors. By prioritizing the psychological well-being of elderly individuals, society can better protect one of its most vulnerable populations from the detrimental effects of financial exploitation.

Keywords Digital technology; Financial fraud; Mental health; Phra Khanong district; Psychological impact; Seniors

Received: *June 5, 2024*
Revised: *August 1, 2024*
Accepted: *November 5, 2024*

Introduction

Financial fraud refers to illegal acts committed to deceive or cheat victims out of money or assets. It encompasses a range of activities, including scams, unauthorized use of financial information, and identity theft. Seniors are particularly vulnerable to such fraud due to cognitive decline, social isolation, and, often, a substantial amount of accumulated wealth. Financial fraud targeting seniors is a growing concern worldwide, characterized by the exploitation of older adults for financial gain through deceptive practices. According to the Federal Trade Commission (FTC), older adults in the United States lost over $1 billion in fraud in 2020, with a median individual loss of $1,500 (Federal Trade Commission, 2021). The situation is similarly dire globally, with studies indicating that up to 20% of seniors have been victims of financial fraud (National Council on Aging, 2021). In the European Union, the European Commission has reported a significant increase in fraud cases targeting the elderly, particularly during the COVID-19 pandemic (European Commission, 2021). According to the Office of the National Economic and Social Development Council (NESDC), approximately 10% of seniors in Thailand have experienced some form of financial exploitation (NESDC, 2022). Additionally, the Thai Ministry of Social Development and Human Security reports an increasing trend in reported cases, with a significant rise in online fraud targeting elderly individuals (Ministry of Social Development and Human Security, 2023).

Seniors are particularly vulnerable to financial fraud due to cognitive decline, social isolation, unfamiliarity with digital technology, and trust in others, which collectively create an environment where they are more susceptible to scams. As people age, they experience cognitive decline, affecting memory, judgment, and decision-making abilities (Lichtenberg, 2016). This decline causes more difficulty for seniors in recognizing and avoiding scams. The natural reduction in cognitive function leads to a decreased ability to process complex information and recognize fraudulent schemes, making seniors prime targets for scammers who exploit these vulnerabilities. Isolation may lead to loneliness, and criminals often exploit this by posing as friendly companions or trustworthy individuals (DeLiema et al., 2017). Scammers use this perceived friendship to gain trust and manipulate seniors into providing personal information or financial resources. Many older adults are not as familiar with the latest digital security practices or how to recognize phishing emails, fraudulent websites, or scam phone calls (Anderson, 2019). Scammers exploit seniors' unfamiliarity with technology, making it easier to deceive them through fake tech support calls or phishing emails that ask for personal information. They target seniors because they perceived them as having significant assets, such as savings, retirement funds, and home equity (Kemp & Mosqueda, 2020). This perception, combined with the factors mentioned above, makes seniors an attractive target for various types of financial fraud, including investment scams, lottery fraud, and identity theft.

Financial fraud against seniors is a significant issue with wide-ranging impacts on individuals, families, and society. This type of fraud involves deceitful schemes designed to trick seniors into giving away their money or personal information, often leading to severe financial, emotional, and even physical consequences. One of the primary reasons financial fraud against seniors is particularly concerning is the vulnerability of the demographic. Seniors often have accumulated significant assets over their lifetimes, making them attractive targets for fraudsters (National Council on Aging, 2023). The emotional and psychological impact of being defrauded is devastating, leading to a loss of independence and trust, as well as increased feelings of shame and depression (Lichtenberg et al., 2013). Financial fraud against seniors in Thailand has seen a marked increase, particularly with the rise of online scams. According to the Thai Ministry of Digital Economy and Society, there has been a significant uptick in reports of online fraud targeting older adults in recent years (Ministry of Digital Economy and Society, 2021). These scams often involve fraudulent emails, fake websites, and deceptive phone calls, where perpetrators impersonate government officials or reputable companies to extract money from unsuspecting victims. A study by the National Institute of Development

Administration (NIDA) revealed that Thai seniors lost an estimated 1.5 billion baths to various forms of financial fraud in 2020 alone (NIDA, 2020). This figure highlights the economic impact of such crimes on the elderly population.

In 2023, seniors aged 60 and older reported significant financial losses due to various types of fraud. The FBI's Internet Crime Complaint Center (IC3) noted that tech support scams were the most frequently reported, affecting nearly 18,000 elderly victims (Federal Bureau of Investigation, 2023). Although less common, investment scams were the most financially devastating, costing seniors over $1.2 billion in 2023 and other prevalent fraud, including business email compromise, romance scams, government impersonation, and personal data breaches (Federal Bureau of Investigation, 2023). Additionally, the National Institute of Justice (NIJ) reports that consumer products and services fraud is the most common type of financial fraud experienced by seniors. Financial abuse is a significant component of elder abuse, with seniors losing over $36 billion annually to various forms of financial exploitation, including scams perpetrated by relatives and caregivers (National Institute of Justice, 2023). Comparative data from the FTC's Consumer Sentinel Network (CSN) reveal that fraud and identity theft remain the leading complaints among older adults. In 2022, fraud accounted for 46% of all reports, with identity theft comprising 21.5%; imposter scams were the most frequently reported, followed by credit card fraud, the most common identity theft type for those over 60 (Comparitech, 2024). This study primarily focuses on senior women due to demographic trends. Women generally have a longer life expectancy than men, resulting in a larger population of senior women (World Health Organization, 2021). Exploring the psychological ramifications of financial fraud on senior females in Thailand is important; this study was designed as a pilot project focusing on Phra Khanong district with research questions are (1) What types of financial fraud do female seniors experience in the Phra Khanong district, Bangkok, Thailand? and (2) Are fraud caused victims to have stress, anxiety, and depression? The research hypothesis is that elderly individuals who have experienced fraud are more likely to suffer from mental health problems compared to those who have not experienced fraud.

Literature review

The global population of senior females

As of recent estimates, the global population includes a significant and growing number of senior females, defined as women aged 60 and above. According to the United Nations Department of Economic and Social Affairs, approximately 700 million people aged 60 years or over worldwide, with women comprising about 55% of this demographic (United Nations Department of Economic and Social Affairs, 2022). The gender disparity increases with age, particularly in the oldest age groups, due to higher female life expectancy. The distribution of senior females varies significantly across different regions. In more developed regions, the proportion of the population aged 60 and above is much higher compared to less developed regions. Europe has the highest percentage of older females, with about 25% of its female population over 60 (World Health Organization [WHO], 2021).

In contrast, Africa has the lowest proportion, at approximately 5% (United Nations, 2022). According to WHO (2021), women tend to live longer than men but often spend their later years in poor health due to chronic illnesses such as osteoporosis, arthritis, and dementia. Senior women are more likely to live alone, increasing the risks of social isolation and loneliness, which can exacerbate mental health issues.

Seniors' vulnerability

Individuals may experience cognitive decline as they age, impairing their ability to process information, make decisions, and recognize fraud. Cognitive impairments, such as dementia or mild cognitive impairment, make seniors more susceptible to fraud due to not fully understanding the complexities of financial transactions or detecting deceitful tactics used by fraudsters. Many seniors

live alone or are socially isolated, which increases their vulnerability to fraud. Scammers exploit seniors' loneliness by posing as friends or trusted individuals, gaining the senior's trust before committing fraud. The naivety of modern technology and online security practices make seniors an easy target for online scams, such as phishing emails, fraudulent websites, and other cybercrimes (James, 2016). The financial stability of many seniors, who have accumulated savings, pensions, and assets over their lifetimes, makes them attractive targets for fraud (AARP, 2020). Scammers know seniors often have access to significant funds and use various schemes to exploit this, including investment fraud, lottery scams, and identity theft.

Online shopping scam

An increase in scams has parallelled the rise of online shopping. According to the Federal Trade Commission (FTC), consumers reported losses of over $1.9 billion from online shopping scams in 2020, a sharp increase from previous years (Federal Trade Commission, 2021). These scams are prevalent across various platforms, including social media, email, and fake websites, making it increasingly difficult for consumers to distinguish between legitimate and fraudulent sellers. Seniors are becoming more active online, with a significant rise in internet usage among those aged 65 and older. The increased online presence, with a lack of familiarity with digital security practices, makes them prime targets for online shopping scams (Anderson, 2020). Online shopping scams targeting seniors involve fake websites that mimic legitimate online stores. The fraudulent sites entice victims with attractive deals on popular products. Once victims make a purchase, scammers either fail to deliver the product or deliver an item significantly different from what was advertised. A study by the Thai Police's Technology Crime Suppression Division (TCSD) revealed that seniors accounted for nearly 30% of all victims of online shopping fraud in 2023 (Technology Crime Suppression Division, 2023).

Phishing scam via text message

Phishing scams via text messages, often called "smishing," involve fraudsters sending a deceptive text message to individuals, aiming to steal sensitive information such as personal identification numbers, passwords, and financial details. Smishing scams operate by sending messages that appear to be from legitimate sources, such as banks, government agencies, or well-known companies. These messages include a sense of urgency, compelling the recipient to act quickly by clicking on a link or calling a phone number provided in the message. Once the victim interacts with the link or phone number, they are directed to a fraudulent website designed to harvest personal information or to unknowingly download malicious software onto their device (Ablon, 2018). The prevalence of smishing has increased in recent years, paralleling the broader rise in cybercrime. Seniors are disproportionately affected by text message phishing scams. A study shows that individuals over 60 are more likely to fall victim to scams and suffer higher financial losses than the younger age group (Federal Trade Commission, 2021). The report highlighted that in 2020, seniors reported losing over $300 million to various fraud schemes, with phishing being a significant contributor. In Thailand, the number of seniors using mobile phones has increased significantly, which has led to a rise in SMS phishing incidents. According to a report by the Thai Bankers' Association (2022), there has been a marked increase in phishing scams targeting seniors, particularly those involving text messages.

Email phishing

Email phishing is a prevalent form of cybercrime that involves fraudulent attempts to obtain sensitive information by disguising oneself as a trustworthy entity in electronic communications. Phishing emails include links to fake websites designed to look like legitimate ones, where victims are prompted to enter their information. Additionally, phishing emails contain malicious attachments that,

when opened, install malware on the recipient's device, further compromising their security (Krebs, 2020). Spear-phishing is a more targeted form of phishing where attackers tailor their messages to specific individuals or organizations, often using personal information to make the emails more convincing (Symantec, 2018). In Thailand, email phishing is particularly acute due to the rapid digitalization of services and the increasing Internet use among seniors (Chou, 2021). These attacks primarily aim for financial gain, with cybercriminals seeking access to bank accounts, credit card details, and other personal information. A study by Kshetri (2022) highlights that seniors are likely to fall victim to phishing scams due to a lack of awareness about cyber threats, limited digital literacy, loneliness, and trust in authoritative-looking emails. These emails often use persuasive language and create a sense of urgency to prompt immediate action, making it difficult for seniors to recognize the scam. Statistical data from the Thai Ministry of Digital Economy and Society indicates a 30% increase in reported phishing cases targeting seniors in the past year (Ministry of Digital Economy and Society, 2023). This increase is attributed to the COVID-19 pandemic, which forced many seniors to rely more heavily on digital communication and online services, exposing them to greater cyber risks.

Psychological impact

Victims of financial fraud frequently experience intense feelings of shame and guilt. They may blame themselves for falling prey to the scam, believing they should have been more cautious or knowledgeable. The self-blame led to severe emotional distress, including anxiety, depression, and loss of self-esteem (Button et al., 2014). Anxiety is a typical response, manifesting because of stress and fear associated with the loss of financial stability and breach of trust. Feelings of shame and guilt can exacerbate anxiety in seniors, as they often blame themselves for falling victim to scams (Cross, 2019). The relationship between financial fraud and depression in seniors can be both a cause and a consequence. The stress of losing financial security can trigger depressive episodes, while pre-existing depression can impair judgment, making individuals more susceptible to scams. The psychological impact is often exacerbated by the reactions of others, who may view the victim as gullible or irresponsible. Victims of financial fraud frequently experience a range of negative emotions, including anger, fear, and guilt. These emotional responses can intensify stress, leading to more serious mental health issues such as anxiety and depression. Feeling deceived can undermine a senior's trust and security, increasing stress levels (Lachs & Berman, 2011). Research indicates that the emotional distress caused by financial fraud leads to decreased life satisfaction and overall well-being (DeLiema, 2018). The constant worry about financial stability and the potential inability to recover lost funds can lead to chronic stress, which has been linked to various health problems, including cardiovascular diseases and a weakened immune system (American Psychological Association, 2023).

Fraud theory

Fraud theory is a comprehensive framework for understanding the motivations, mechanisms, and prevention of fraudulent activities. Buller and Burgoon developed the interpersonal fraud theory in 1996, which describes online fraud in four stages: fraudulent online messages, the assessment of the authenticity of the information, the generation of trust, and decision-making errors (Burgoon & Buller, 2015). A previous study found that online fraud is associated with seniors' mental health status, cognitive ability, extroversion level, trust level, self-control, security, and perceived control (Shang et al., 2022). Nevertheless, researchers have found that older adults are not linked to a higher possibility of being deceived. Many studies indicate that seniors are more likely to become victims of fraud, mainly because of psychological factors.

Fraudulent theories of elderly abuse emphasize the risk factors of both the victim and the perpetrator. Situational factors also influence the risk of victimization. According to the routine activity theory developed by Cohen and Felson in 1979, criminal acts result from the convergence of three

factors: the offender, the suitable target, and the absence of capable guardians (DeLiema, 2018). As opposed to concentrating on the demographic characteristics of victims, routine activity theory emphasizes the offender's day-to-day activities, behaviors, and opportunities to come into contact with susceptible targets. Although the researcher initially developed it to address street crimes, they can also apply it to financial crimes. Criminals access thousands of potential victims with minimal supervision by purchasing online goods over the phone, through an application, or via social media. A study indicates that seniors who purchase products online are at high risk of fraud (DeLiema, 2018). The lack of self-control is another factor that increases the risk of fraud victimization.

Research methodology

Study design and area

Financial fraud targeting seniors has become a significant concern globally. This study aimed to explore the types of fraud and their impact on mental health among female seniors aged 60-70 in Phra Khanong district. Understanding these impacts requires various qualitative and quantitative approaches to provide a comprehensive analysis. Quantitative tools were standardized instruments to collect levels of anxiety, depression, and stress and identify demographic variables such as age and socioeconomic status. The qualitative tool was an in-depth interview. The researcher conducted semi-structured interviews with seniors to gain a deeper understanding of the personal experiences and psychological ramifications of financial fraud. Subjects were recruited in public places that were safe and convenient to ensure their safety and convenience. The researcher used the snowball technique to collect data. The researcher held interviews at public locations, consulted participants' families, and administered surveys with their permission.

Data collection tools

K-10

This study divides into four parts. Part 1 was the Kessler Psychological Distress Scale (K10) to screen the respondents' stress levels. The K-10 included a 10-item questionnaire designed to measure anxiety and depression, each related to an emotional state, with a five-level response scale. The researcher designed K-10 to be self-administered or interview-administered, with the ending and weighted kappa scores ranging from 0.42 to 0.74, indicating that the test is reliable (Kessler, 2023). A score between 10 and 19 indicates well-being, a score between 20 and 24 indicates mild distress, a score between 25 and 29 indicates moderate distress, and a score between 30 and 50 indicates severe distress.

In-depth interview

Part 2, an open-ended, in-depth interview questionnaire, was used to gather information about financial fraud. The researcher asked respondents to assess whether they had been victimized by cybercrime through social media fraud, banking fraud, e-mail fraud, ransomware attacks, phishing scams via text message, or identity theft. The researcher examined in-depth respondents' experiences and perceptions of cybercrime. Considering the vulnerability of the respondents, eleven questions were read to them.

General Anxiety Disorder-7 (GAD-7)

The third part of the study was a rapid assessment of anxiety using a questionnaire or the GAD-7. The researcher widely used the test to determine the severity of initial anxiety symptoms. The questions were based on (DSM-IV-TR) criteria, and the scores ranged from "0" not at all to "3" almost every day (Bohlmeijer et al., 2021). Scores on the GAD-7 range from 0 to 21. GAD-7 scores of 0-4 indicate minimal anxiety, 5-9 indicate mild anxiety, 10-14 indicate moderate anxiety, and greater than 15 indicate severe anxiety. The higher the GAD-7 score, the greater the level of functional impairment.

Patient Health Questionnaire (PHQ-9)

Doctors in the United Kingdom developed the PHQ-9 questionnaire, used as part four of this study. The test has been validated for monitoring and diagnosing depression. Despite this, this study is intended for research purposes only. The scale ranges from 0 to 3, from not at all to nearly daily. The interpretations of total scores are 0-4 minimal depression, 5-9 mild depression, 10-14 moderate depression, 15-19 moderately severe depression, and 20-27 severe depression.

Ethical approval

Ethical approval was obtained before data collection began. The aim is to protect the respondents of this research. The Committee for Research Ethics (Social Sciences) of Mahidol University, Thailand, has approved this study (No. 2022/129/(B1)). The researcher obtained written informed consent from all respondents prior to enrolment in the study. Respondents were aware of the study's purpose and were willing to participate.

Statistical analyses

This study performed a descriptive statistical analysis to summarize the participant characteristics. In addition, to investigate the impact of fraud on mental health, the study performed an independent sample t-test. Although the sample size of 30 is minimally acceptable for t-tests, this study additionally performed a bootstrap t-test to cross-check the reliability and validity of t-test results (Andrei, 2021). The researcher conducted the bootstrap t-test using 1,000 replicates, and statistical significance was set at a p-value of 0.05 in this study. All statistical analyses in this study were conducted using IBM SPSS Statistics version 20.

Results

Table 1 provides a summary of the participant characteristics. Only one person (3.33%) was between the ages of 69 and 70, but the majority (36.67%) were between the ages of 63 and 65. Another 33.33% were between 66 and 68, and 26.67% were between 60 and 62. Most respondents (66.67%) live with family members, while 30% and 3.33% live with their spouses and children. The majority of the sample size holds a Bachelor's degree (60%), followed by those with a Master's degree (16.67%). A smaller percentage of individuals have completed primary school (13.33%) and associate degree (6.67%), with the lowest percentage having only completed secondary school (3.33%).

16.67%, 13.33%, 6.67%, and 3.33%—approximately eight out of thirty respondents' monthly income is between 25,000 and 35,000 THB. Five respondents (16.67%) reported having no monthly income. Twenty-six respondents (N=30) reported experiencing fraud, the majority of which were phishing scams via text message (70%) and social media scams involving e-mail (16.67%).

Regarding mental health, the mean of distress (K-10 score), anxiety (GAD-7 score), and depression (PHQ-9 score) were 23.30, 13.90, and 17.13, respectively. Furthermore, these mean scores were higher among participants who experienced fraud (phishing scams via text messages or social media, including e-mail scams) than those who did not. Specifically, the mean of distress among the fraud group was 24.42, while that among the no-fraud group was 16.00. Regarding anxiety and depression, the means for the fraud group were 14.23 and 17.27, while those for the no-fraud group were 11.75 and 16.25, respectively. These results indicate that fraud could negatively affect mental health among participants.

Table 2 presents the t-test results to evaluate the impact of fraud on mental health. The results indicated that distress and anxiety were statistically significant among three mental health indicators in both general and bootstrap t-tests. For distress, the mean difference between the fraud and no-fraud groups was -8.423, with a p-value of 0.001. This indicates that the participants who experienced fraud

(either phishing scams via text message or social media, including e-mail scams) had a significantly higher level of distress than those who did not experience fraud.

Table 1 Participant characteristics (n=30)

Participant Characteristics	**Frequency**	**Percent**
Age		
60–62 years	8	26.67
63–65 years	11	36.67
66–68 years	10	33.33
69–70 years	1	3.33
Living arrangement		
Husband	9	30.00
Husband and children	1	3.33
Family members	20	66.67
Education		
Primary school	4	13.33
Secondary school	1	3.33
Associate degree	2	6.67
Bachelor's degree	18	60.00
Master's degree	5	16.67
Income		
No income	5	16.67
Below 10,000 baht	4	13.33
10,000 - 2,5000 baht	13	43.33
25,000 - 3,5000 baht	8	26.67
Type of Fraud		
No fraud	4	13.33
Type 1: Phishing scam via text message	21	70.00
Type 2: Social media, including e-mail scam	5	16.67

Participant Mental Health	**Mean**	**Std. Dev.**	**Min**	**Max**
Distress (K-10 score)	23.30	6.72	11.00	38.00
No fraud	16.00	3.46	11.00	19.00
Fraud types 1 and 2	24.42	6.41	13.00	38.00
Anxiety (GAD-7 score)	13.90	3.24	10.00	22.00
No fraud	11.75	2.22	10.00	15.00
Fraud types 1 and 2	14.23	3.28	10.00	22.00
Depression (PHQ-9 score)	17.13	3.20	13.00	26.00
No fraud	16.25	2.06	14.00	18.00
Fraud types 1 and 2	17.27	3.35	13.00	26.00

For anxiety, the mean difference between the fraud and no-fraud groups was -2.481, with a p-value of 0.041 and 0.005 in general and bootstrap t-tests, respectively, indicating that the level of anxiety among participants who experienced fraud was significantly higher than that among those who

did not. Regarding depression, the negative mean difference (-1.019) indicated that the level of depression among participants who experienced fraud was higher than that among those who did not. However, this relationship was not statistically significant. In sum, the results overall indicated that fraud could significantly increase the level of distress and anxiety among participants, but not depression.

Table 2 Results of T-Test to examine the impact of fraud on mental health

			95% CI			
Variables	**Mean Diff.**	**Std. Err.**	**Lower Limit**	**Upper Limit**	**t-score**	**p-value**
Distress (K-10 score)						
General t-test (n=30)	-8.423	2.301	-13.029	-3.818	-3.661	0.001*
Bootstrap t-test (replicate=1,000)	-8.423	1.435	-11.000	-5.646		0.001*
Anxiety (GAD-7 score)						
General t-test (n=30)	-2.481	1.187	-4.857	-0.104	-2.090	0.041*
Bootstrap t-test (replicate=1,000)	-2.481	0.843	-4.065	-0.722		0.005*
Depression (PHQ-9 score)						
General t-test (n=30)	-1.019	1.209	-3.439	1.401	-0.843	0.403
Bootstrap t-test (replicate=1,000)	-1.019	0.826	-2.672	0.619		0.220

Note: * = statistically significant at 0.05.

Discussion

Phishing scams via text messages have emerged as one of the most prevalent types of fraud in this study. The rise in prevalence is attributable to the increasing reliance on mobile communication and the relative ease with which scammers can target large numbers of victims. Phishing scams typically involve fraudulent messages that appear to be from legitimate sources, such as banks, government agencies, or well-known companies, and they often prompt recipients to provide sensitive information like passwords, credit card numbers, or Thai IDs. Scammers' messages send a sense of urgency or fear to provoke immediate action. They claim a limited response time to avoid severe consequences, such as account suspension or financial loss. The tactic manipulates psychological responses to urgency and fear, reducing the likelihood of critical thinking and increasing the chances of compliance (Button et al., 2014). Another common approach is the promise of rewards, prizes, or exclusive deals. These messages encourage recipients to click links or provide personal information to claim the offer. The allure of a significant reward can cloud judgment and lead victims to act without considering the potential risks (Marett & Joshi, 2009). Some smishing attacks involve sending malicious attachments that, when opened, install malware on the recipient's device. Scammers use the malware to steal personal information, monitor activities, or gain unauthorized access to the device. The use of malware escalates the potential damage of the scam (Symantec Corporation, 2018). Scammers sometimes pose as customer support representatives from reputable companies, offering help with non-existent issues. Scammers ask for personal information or remote access to the victim's device under the guise of helping. This tactic exploits victims' trust in customer support services and willingness to resolve issues promptly (Krebs, 2016).

Twenty-one out of thirty participants were victims of phishing scams via text message. A study by Proofpoint, a cybersecurity firm, revealed that 74% of organizations experienced phishing attacks in 2020, with a notable increase in mobile phishing attempts (Proofpoint, 2021). The report underscored that attackers exploit the trust users place in their mobile services and the hurried nature of text message communication. In addition to organizational reports, academic research supports the prevalence of text message phishing scams. A study examined the psychological factors influencing susceptibility to phishing attacks and found that the concise nature of text messages, combined with the immediacy of mobile communication, makes individuals more likely to fall for these scams (Oliveira et al., 2021). The study suggested that text message phishing is particularly effective because it exploits users' tendencies to respond quickly to messages on their mobile devices without thorough scrutiny. Reports indicate that phishing attempts via SMS increased by 25% in Thailand in 2023, with a significant portion of the targets being individuals over 60 (CyberSecurity Malaysia, 2023).

Social media and email scams targeting seniors are a growing concern globally. Seniors are vulnerable to financial fraud due to various factors, such as limited digital literacy, isolation, and trust in others. Social media platforms have become breeding grounds for various types of scams. One common tactic involves creating fake profiles that impersonate friends or family members to gain the victim's trust. Once scammers establish trust, they request money for emergencies, share links to malicious websites, or promote fake investment opportunities. Email scams are another prevalent form of fraud targeting seniors. These scams often involve emails that appear to be from legitimate institutions asking the victim to provide personal information or click on malicious links. Scammers targeted two subjects in this study through fake e-commerce websites. The website appeared professional and offered popular clothes at heavily discounted prices, targeting seniors through social media ads. Victims were required to pay upfront via bank transfer. However, after payment, the ordered items never arrived. Three subjects received an email that appeared to be from a well-known online retailer, notifying them of an order they had not placed. The email included a link to cancel the order, leading to a fake website that captured their login credentials and credit card information. The scammers subsequently made unauthorized purchases using their credit cards.

The psychological impact of financial crimes on seniors is profound. Financial loss led to a cascade of negative emotions. One of the immediate psychological impacts of financial fraud on seniors is emotional distress. Other negative emotions include anger, shame, guilt, and sadness. These feelings lead to a significant decline in overall well-being and life satisfaction. The sense of betrayal exacerbates negative emotions, leading to a more profound sense of personal violation. Financial fraud precipitates mental health issues among seniors. Depression and anxiety were the typical responses to financial loss and the stress associated with fraud. The results of this study show that victims of financial fraud had higher rates of stress and anxiety compared to non-victims. Local studies in Thailand corroborate that the financial strain and stress from fraud lead to long-term mental health challenges (Somchai, 2019). There is evidence suggesting that stress and trauma associated with financial fraud accelerate cognitive decline in seniors. A study by the Journal of Elder Abuse and Neglect (2018) found that victims of financial exploitation showed signs of cognitive impairment faster than their non-exploited counterparts. This is particularly concerning in Thailand, where the aging population is growing, and resources for mental health support are limited (Channarong, 2019).

Stress, anxiety, and depression significantly affect seniors' mental health globally, and financial fraud exacerbates these conditions. In Thailand, these mental health challenges are prevalent among the elderly population, who are particularly vulnerable to scams. Aging brings about numerous stressors, such as declining health, loss of loved ones, and financial instability. These stressors can lead to anxiety and depression, significantly impacting the quality of life. A study found that 31.3% of Thai elderly reported depressive symptoms, and 28.4% experienced anxiety (Wongpakaran et al.,

2019). These figures indicate that a substantial portion of the senior population is struggling with mental health issues.

Legislative measures are needed to protect seniors from financial fraud. Policymakers should strengthen legislation to protect seniors. This includes implementing stricter penalties for perpetrators and enhancing regulations to safeguard seniors' financial transactions. The mandatory reporting laws require financial institutions to report suspected cases of seniors' financial abuse to authorities (Deane, 2018). Organizations design effective public awareness campaigns are designed to educate seniors and caregivers about the risks and signs of financial fraud. The key components include education materials, workshops and seminars, media campaigns, community partnerships, and hotline support services. Research indicates that seniors participating in educational programs are more likely to recognize and avoid scams (Chongphaisal & Sumang, 2022). Collaboration with financial institutions plays a pivotal role in safeguarding the assets of seniors. Banks and other financial entities are often the first line of defense against fraud. Their collaboration with government agencies, non-profits, and the community is essential for creating a robust framework to prevent financial fraud. This collaboration takes several forms in Thailand, including information sharing, fraud detection training, and public awareness campaigns. Banks and financial institutions should employ advanced fraud detection systems that alert seniors to suspicious activities on their accounts (Brody, 2019). Community support network programs that pair seniors with younger individuals for mutual support can help bridge the technology gap and increase fraud awareness (Morrow-Howell, 2019). Collaboration between social workers, counselors, and law enforcement is crucial in addressing financial fraud targeting seniors. The collaborative approach ensures a comprehensive strategy to prevent, detect, and respond to fraud, leveraging the strengths and expertise of each stakeholder to protect vulnerable elderly populations. Implementing sophisticated AI and machine learning algorithms can enhance fraud detection capabilities. These systems can analyze transaction patterns to identify anomalies that indicate fraudulent activity. Banks and financial institutions might need to invest in these technologies to protect their customers. Utilizing biometric authentication methods, such as fingerprint, facial recognition, or iris scanning, can add an extra layer of security. These methods are more secure than traditional passwords and PINs, which can be easily compromised (Jain et al., 2011).

The limitations of this study are geographical limitations, cross-sectional design, and lack of a control group. This study focused on a specific district in Bangkok. While it provides valuable localized insights, the findings may not represent other regions in Thailand or cultural contexts. Expanding the geographical scope could yield more generalizable results. The study employs a cross-sectional design, capturing data at a single point in time. This approach needs to account for changes over time. Although the study compares victims and non-victims, a matched control group was absent, which limits the ability to draw strong causal inferences. Future research could include a control group matched to key demographic effects to better isolate financial fraud's effects. Building on the findings and addressing the limitations of this study, several areas warrant further research. Conducting longitudinal studies would help understand the long-term psychological effects of financial fraud on seniors. These studies could track changes in mental health over time and establish causal relationships. Future research should include more extensive and diverse samples across different regions of Thailand and other countries. This would enhance the generalizability of the findings and allow for cross-cultural comparisons. Given the increasing prevalence of online scams, studies should examine the role of technology and digital literacy in protecting seniors from financial fraud. Research could explore how training programs in digital skills can reduce vulnerability and improve the detection of scams.

Financial fraud is a growing concern globally, necessitating evidence-based strategies to mitigate its impact. Educational initiatives are crucial in preventing financial fraud. Studies show that

informed consumers are less likely to fall victim to scams. Organizations should focus on comprehensive educational programs that teach consumers about typical fraud schemes and how to recognize and avoid them (Anderson, 2021). Implementing advanced security technologies, such as multi-factor authentication (MFA) and biometric verification, can reduce the incidence of financial fraud. Research indicates that MFA can prevent up to 99.9% of automated cyber-attacks (Microsoft, 2019). Financial institutions should invest in advanced data analytics to detect and prevent fraud. Machine learning algorithms can identify unusual patterns and flag potential fraud before it occurs. According to a study by McKinsey and Company (2020), data analytics can reduce fraud losses by up to 50%. Collaboration among financial institutions, law enforcement agencies, and regulatory bodies is vital for fraud prevention. Sharing information about fraud trends and coordinating efforts can enhance the ability to detect and respond to fraud. The Financial Fraud Action UK (2019) highlights the importance of such collaboration in its annual report. By implementing these evidence-based strategies, it is possible to reduce the incidence and impact of financial fraud significantly.

Conclusion

Financial fraud targeting seniors is a global issue with significant psychological ramifications. Due to their cognitive decline, social isolation, unfamiliarity with digital technology, and accumulated wealth, seniors are particularly vulnerable. The impact of financial fraud extends beyond financial loss, affecting seniors' mental health and well-being. The study revealed that seniors were targeted through phishing scams via text messages and social media, with 70% of the respondents having experienced such fraud, leading to significant financial and emotional distress. The mean distress score (K-10) for fraud victims was significantly higher (24.42) than that of non-victims (16.00), indicating that experiencing fraud substantially increases psychological distress. The study found that victims had higher rates of stress and anxiety compared to non-victims, corroborating findings from other studies that financial strain and stress from fraud can lead to long-term mental health challenges. The stress and trauma associated with financial fraud can also accelerate cognitive decline in seniors, compounding the problem. This is particularly concerning in Thailand, where the aging population is growing, and resources for mental health support are limited. Addressing this problem requires approaches involving legislative measures, public awareness campaigns, and collaboration with financial institutions. Implementing these strategies can reduce the incidence and impact of financial fraud on the senior population, ensuring their financial and psychological well-being.

Acknowledgment

The research on "Aging and Vulnerability: The Psychological Ramification of Financial Fraud on Seniors" received a grant from the Faculty of Social Sciences and Humanities, Mahidol University. The researcher would like to sincerely thank the faculty for the grant, which provided the necessary funding for this study.

References

Ablon, L. (2018). *Data thieves in action: Motivations and methods behind today's most notorious data heists*. Santa Monica, CA: RAND Corporation.

American Association of Retired Persons. (2020). *The financial exploitation of older adults: A review of the evidence*. Retrieved from https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/scope-elder-financial-exploitation.html

American Psychological Association. (2023). *Stress effects on the bo*dy. Retrieved from https://www.apa.org/topics/stress/body

Anderson, K. (2021). The role of consumer education in preventing financial fraud. *Journal of Financial Crime, 28*(3), 567-584.

Anderson, M. (2019). *Older adults and technology use*. Pew Research Center. Retrieved from https://www.pewresearch.org

Anderson, M. (2020). *Internet use among older adults: Key trends and statistics*. Pew Research Center. Retrieved from https://www.pewresearch.org

Andrei, F. (2021). *Bootstrap statistics-how it works around the limitations of simple statistical tests*. Towards Data Science.

Bohlmeijer, E. T., Kraiss, J. T., Watkins, P., & Dijkstra, M. (2021). Promoting gratitude as a resource for sustainable mental health: Results of a 3-armed randomized controlled trial up to 6 months follow-up. *J Happiness Stud, 22*, 1011-1032.

Brody, R. (2019). Financial fraud detection in the elderly. *Journal of Financial Crime, 26*(2), 371-383.

Burgoon, J., & Buller, D. (2015). Interpersonal deception theory. *Communication Theory, 6*(3), 203-242.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

Button, M., Nicholls, C.M., Keer, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408.

Channarong, S. (2019). Cognitive decline among elderly fraud victims in Thailand. *Asia Journal of Gerontology, 14*(1), 56-67.

Chongphaisal, P., & Sumang, K. (2022). Effectiveness of educational programs in preventing financial fraud among seniors in Thailand. *Journal of Elderly Studies, 15*(2), 45-58.

Chou, W. (2021). Digital literacy and the elderly in Thailand: Combating online scams. *Journal of Cybersecurity and Education, 15*(2), 78-92.

Comparitech. (2024). *Senior Scam Statistics 2024: Is elder fraud on the rise?* Retrieved from https://www.comparitech.com

Cross, C. (2019). But I have never sent them any money: Exploring the reporting of fraud victimisation to Action Fraud. *Criminology & Criminal Justice, 19*(4), 467-484.

CyberSecurity Malaysia. (2023). *Annual cybersecurity report*. Retrieved from https://www.cybersecurity.my/en/index.html

Deane, S. (2018). Financial exploitation of older adults. *Journal of Elder Abuse & Neglect, 30(*4), 290-305.

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

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2017). Exploring the risks and consequences of elder fraud victimization: evidence from the health and retirement study. Stanford, CA: Sandford Center on Longevity.

Federal Bureau of Investigation. (2023). Elderly fraud, in focus. Retrieved from https://www.fbi.gov

Federal Trade Commission. (2021). *Consumer sentinel network data book 2020*. Retrieved from https://www.ftc.gov/reports/consumer-sentimel-network-data-book-2020

Federal Trade Commission. (2021). *Protecting older consumers: A report of the FTC's elder fraud program*. Retrieved from https://www.ftc.gov/reports/protecting-older-consumers-report-ftcs-elder-fraud-program

Federal Trade Commission. (2021). *Protecting yourself from online shopping scams*. Retrieved from https://www.ftc.gov

Financial Fraud Action UK. (2019). *Annual fraud indicator*. Retrieved from https://www.financialfraudaction.org.uk

Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. New York, NY: Springer.

James, B. D. (2016). Cognitive and health-related risk factors of elder financial exploitation: A prospective longitudinal study. *JAMA Internal Medicine, 176*(7), 890-896.
Kemp, B., J., & Mosqueda, L.A. (2020). Elder financial exploitation: why financial professionals should care. *Journal of Financial Planning,33*(4), 32-40.
Kessler, R. C. (2023). Kessler psychological distress scale (K10). Clearwater, FL: Statistics Solutions.
Krebs, B. (2016). Spam Nation: The Inside Story of Organized Cybercrime from Global Epidemic to Your Front Door. Naperville, IL: Sourcebooks.
Krebs, B. (2020). Phishing and its impact on personal security. *Cyber Defenders, 15*(2), 89-104.
Kshetri, N. (2022). Cybersecurity threats to the elderly: A growing concern. *International Journal of Cyber Studies, 29*(3), 145-162.
Lachs, M. S., & Berman, J. (2011). *Under the radar: New York State elder abuse prevalence study*. New York, NY: Lifespan of Greater Rochester.
Lichtenberg, P. A. (2016). Financial decision-making and fraud vulnerability in older adults: Risk factors and prevention strategies. *Clinical Gerontologist, 39*(5), 421-428.
Lichtenberg, P. A., Stickney, L., & Paulson, D. (2013). Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist, 36*(2), 132-146.
Marett, K., & Joshi, K. (2009). The decision to share information and rumors: Examining the role of motivation in an online discussion forum. *Communications of the Association for Information System, 24*(1), 7.
McKinsey & Company. (2020). *Security key: An effective solution to phishing*. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/fighting-fraud-with-advanced-anlytics
Microsoft. (2019). *Multi-factor authentication: A powerful defense against financial fraud*. Retrieved from https://www.microsoft.com/en-us/security/blog/2019/08/20/multi-factor-authentication-99-0-effective/
Ministry of Digital Economy and Society. (2021). *Annual report on cybercrimes targeting seniors*. Bangkok, Thailand: Ministry of Digital Economy and Society.
Ministry of Digital Economy and Society. (2023). *Annual report on cybersecurity incidents in Thailand*. Bangkok, Thailand: Ministry of Digital Economy and Society.
Ministry of Social Development and Human Security. (2023). *Report on the rising trend of online fraud targeting seniors*. Bangkok, Thailand: Ministry of Social Development and Human
Morrow-Howell, N. (2019). Intergenerational programs and elder fraud prevention. *Journal of Intergenerational Relationships, 17*(4), 393-408.
National Council on Aging. (2021). *Financial scams targeting seniors*. Retrieved from https://www.ncoa.org/
National Council on Aging. (2023). *Top 10 financial scams targeting seniors*. Retrieved from https://www.ncoa.org/article/top-10-financial-scams-targeting-seniors
National Institute of Development Administration. (2020*). Financial losses due to fraud among Thai seniors*. Bangkok, Thailand: NIDA Press.
National Institute of Justice. (2023). *Examining financial fraud against older adults*. Retrieved from https://nij.ojp.gov
Office of the National Economic and Social Development Council. (2022). *Annual report on elder abuse and financial exploitation*. Bangkok, Thailand: Office of the National Economic and Social Development Council.
Oliveira, D., Rocha, H., Moraes, J., & Carrera, M. (2021). Understanding the psychology behind text message phishing: A study on the susceptibility factors. *Journal of Cybersecurity Research, 15*(2), 87-105.

Proofpoint. (2021). *2021 State of the Phish*. Retrieved from https://www.proofpoint.com

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Front Psycho, 13*, 912242.

Somchai, K. (2019). Mental health effects of financial fraud on the elderly in Thailand. *That Journal of Psychiatry, 21*(4), 88-97.

Symantec Corporation. (2018). Internet Security Threat Report. Symantec Corporation. Technology Crime Suppression Division. (2023). Cybercrime statistics. Bangkok, Thailand: Technology Crime Suppression Division.

Symantec. (2018). *Internet security threat report*. Retrieved from https://www.symantec.com/security-center/threat-report

Thai Bankers' Association. (2022). *The impact of cybercrime on financial institutions in Thailand*. Nonthaburi, Thailand: Thai Bankers' Association.

United Nations Department of Economic and Social Affairs. (2022). *World population ageing 2022 highlights*. Retrieved from https://www.un.org/development/desa/pd/news/world-population-ageing-2022

United Nations. (2022). *World population prospects 2022*. Department of Economic and Social Affairs, Population Division. Retrieved from https://population.un.org/wpp/

Weissberger, G. H., Mosqueda, L., Nguyen, A. L., Boyle, P. A., Nguyen, C. P., and Han, S. D. (2018). The cognitive impacts of financial exploitation on seniors. *Journal of Elder Abuse & Neglect, 30*(4), 299-311.

Wongpakaran, N., Wongpakaran, T., Pinyopornpanish, M., Pinyopornpanish, K., Pengkaew, P., & Sirirak, T. (2019). Prevalence and associated factors of comorbid anxiety disorders in late-life depression: findings from geriatric tertiary outpatient settings. *Neuropsychiatric Disease and Treatment, Vol*(15), pp.199-204.

World Health Organization. (2021). *Global strategy and action plan on aging and health*. WHO. Retrieved from https://ww.who.int/ageing/global-strategy/en/

World Health Organization. (2021). *Life expectancy and healthy life expectancy*. Retrieved from https://www.who.int/data/gho/data/themes/mortality-and-global-health.estimates

Appendix 1 Descriptive Statistics of Each Question Item for Three Mental Health Indicators (n=30)

Variable	Mean	Std. Dev.	Min	Max
Psychological Distress (K-10)				
1. During the last 30 days, how often do you feel tired for no good reason?	2.87	1.14	1	5
2. During the last 30 days, how often did you feel nervous?	2.57	1.10	1	5
3. During the last 30 days, how often did you feel so nervous that nothing could calm you down?	2.40	1.04	1	4
4. During the last 30 days, how often did you feel hopeless?	2.17	1.21	1	5
5. During the last 30 days, about how often did you feel restless or fidgety?	2.50	1.07	1	4
6. During the last 30 days, how often did you feel so restless you could not sit still?	2.40	1.16	1	5
7. During the last 30 days, how often did you feel depressed?	2.23	1.14	1	5
8. During the last 30 days, how often did you feel that everything was an effort?	2.97	0.96	1	5
9. During the last 30 days, how often did you feel so sad that nothing could cheer you up?	1.80	1.06	1	4
10. During the last 30 days, how often did you feel worthless?	1.40	0.67	1	3
Anxiety (GAD-7)				
1. Over the last 2 weeks, feeling nervous, anxious, or on edge	2.07	0.52	1	3
2. Over the last 2 weeks, not being able to stop or control worrying	1.90	0.88	1	4
3. Over the last 2 weeks, worrying too much about different things	2.37	0.93	1	4
4. Over the last 2 weeks, trouble relaxing	2.00	0.98	1	4
5. Over the last 2 weeks, being so restless that it is hard to sit still	1.97	0.81	1	4
6. Over the last 2 weeks, becoming easily annoyed or irritable	2.20	0.81	1	4
7. Over the last 2 weeks, feeling afraid, as if something awful might happen	1.40	0.62	1	3
Depression (PHQ-9)				
1. Over the last 2 weeks, little interest of pleasure in doing things	2.17	0.59	1	3
2. Over the last 2 weeks, feeling down, depressed, or hopeless	1.60	0.81	1	3
3. Over the last 2 weeks, trouble falling asleep, staying asleep, or sleeping too much	2.47	0.78	1	4
4. Over the last 2 weeks, feeling tired or having little energy	2.33	0.88	1	4
5. Over the last 2 weeks, poor appetite or overeating	2.20	0.81	1	4
6. Over the last 2 weeks, feeling bad about yourself or that you are a failure or have let yourself or your family down	1.53	0.90	1	4
7. Over the last 2 weeks, trouble concentrating on things, such as reading the newspaper or watching TV	2.23	0.73	1	3
8. Over the last 2 weeks, moving or speaking slowly that other people could have noticed, or being fidgety or restless	1.60	0.77	1	3
9. Over the last 2 weeks, thoughts that you would be better off dead or hurting yourself in some way	1.00	0.00	1	1