ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2025.1833.154

CYBERCRIME VULNERABILITY AMONG OLDER ADULTS IN MALAYSIA IN THE CONTEXT OF DIGITAL DECEPTION

Kian-Lam Tan[1*], Jayaeswari Sangaralingam[2], Lau Pei Mey[3], Premalatha Karupiah[4], Chen-Kim Lim[5]

*[*1]School of Digital Technology, Wawasan Open University, Penang Malaysia. Email: andrewtan@wou.edu.my, orcid: https://orcid.org/0000-0003-1627-7437*
[2]School of Digital Technology, Wawasan Open University, Penang Malaysia. Email: jayaeswaris@wou.edu.my, orcid: https://orcid.org/0009-0001-3114-6788
[3]School of Digital Technology, Wawasan Open University, Penang Malaysia. Email: pmlau@wou.edu.my, orcid: https://orcid.org/0000-0002-8787-803X
[4]School of Social Sciences, Universiti Sains Malaysia, Penang, Malaysia. Email: prema@usm.my, orcid: https://orcid.org/0000-0002-0604-9310
[5]Institute for Environment and Development (LESTARI), Universiti Kebangsaan Malaysia, Bangi, Malaysia. Email: kim@ukm.edu.my, orcid: https://orcid.org/0000-0003-4353-4128

Received: April 23, 2025; Revised: July 29, 2025; Accepted: August 27, 2025; Published: September 12, 2025

SUMMARY

This study explores the growing phenomenon of cybercrime targeting older adult individuals in Malaysia, a demographic increasingly susceptible due to factors such as limited digital literacy, social isolation, and perceived financial stability. Drawing upon Routine Activity Theory and Social Engineering Theory, the research investigates the situational and psychological vulnerabilities that expose senior citizens to scams, particularly phishing, identity theft, and impersonation-based fraud. Utilizing a phenomenological qualitative approach, interviews were conducted with 13 Malaysian seniors aged 60 and above to examine their personal experiences, awareness levels, and emotional responses related to cybercrime victimization. Findings revealed that while only a minority had been direct victims, the emotional toll—including trauma, shame, and anxiety—was significant across the board. Scam tactics often involved impersonation of authority figures and manipulation through urgency or emotional grooming. The study emphasizes the dual impact of cybercrime: financial losses and long-term psychological distress. It concludes that current institutional measures, though important, must be supplemented by age-targeted education, simplified security tools, and psychosocial support to effectively mitigate risks. This research provides critical insights for policymakers, financial institutions, and digital educators in building inclusive and safer online environments for Malaysia's aging population.

Key words: *cybercrime, older adult victims, online scams, social engineering, financial exploitation, cybersecurity awareness, psychological impact.*

INTRODUCTION

In the past two decades, the term cybercrime has risen in prominence. Cybercrime communities have evolved from IRC channels to forums and cryptomarkets, and are increasingly moving to mobile chat

platforms. Cybercrime definition can be summed up as any criminal activities (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data. [24] described cybercrime as "any illegal action that involves the use of a computer or the internet as a tool or a target or it can be both".

In a seminal paper by [16] titled 'An inquiry into the nature and causes of the wealth of internet miscreants', the authors analyzed data that was gathered over seven months in the Internet Relay Chat (IRC) rooms on activities on cybercrime. They observed chats that were inclined to credit card fraud, identity theft, spamming, phishing, online credential theft, and the sale of compromised hosts. What used to be hacking for fun started to be hacking for profit. And today, almost 17 years later, reports of cybercrime have evolved from the days of IRC to cryptomarkets, online scams to phone/ mobile scams [6].

In Malaysia, news of scams and cyber-victims are reported regularly in the media with such headlines "Senior citizens lose over RM227,000 in credit card, investment scams in Pahang." [29]. A total of 51,631 online fraud cases were reported in Malaysia between 2019 and 2021 involving a total loss of RM1.61 billion [21]. Number of cybercrime cases reported in Malaysia from 2021 to June 2022 total of 31,169 [3]. According to Prime Minister Datuk Seri Anwar Ibrahim, The Edge Malaysia reported that cybercrime caused losses exceeding RM1.22 billion from January to October 2024 [31].

The Ministry of Communications and Digital Malaysia (KKD) reported that Malaysians lost almost RM600 million in the year 2022, an increase of approximately 17%, due to scams and cybercrimes [2]. Financial scams have been on the rise since the onset of the pandemic, almost a total of RM2 billion accumulated from 2019 to 2022 [30]. There were a total of 2520 network security incidents reported to the Malaysian Communications and Multimedia Commission (MCMC) through the Network Security Center in 2020 [8] [12]. The majority of the incidents reported was website defacement and this was followed by phishing.

As the population ages and becomes increasingly connected to the digital world, internet-based victimization of senior citizens is becoming more evident. Reports indicate that seniors account for 6.4% of total cyber scam victims. However, their financial losses are significantly higher compared to other groups. Between 2021 and 2023, scams resulted in total losses of RM2.7 billion, with senior citizens losing half a billion Ringgit, representing 20 percent of the total losses, according to Bukit Aman Commercial Crime Investigation Department (CCID) director Comm Datuk Seri Ramli Mohamed Yoosuf [29].

Senior citizens may be at a higher risk of falling victim to cybercrime due to their limited familiarity with technology, as well as a tendency to be more trusting and less likely to question suspicious activities. This vulnerability makes them attractive and easy targets for online predators seeking to exploit their financial resources, personal information, and emotional well-being [33]. The consequences of cybercrime can be devastating, resulting in financial loss and privacy breaches. Ultimately, victims often experience emotional distress, social isolation, and a diminished quality of life [19].

PROBLEM STATEMENT

The topic of cybersecurity and its impact on older adult individuals is often overlooked in research and discussions. While extensive literature focuses on the cybersecurity concerns of young people and working adults, the unique challenges faced by the older adult receive significantly less attention. Consequently, there are only a limited number of academic articles that specifically explore cybersecurity issues among the older adult [22].

The exploitation of senior citizens through scams, particularly cybercrime, is costing the nation's older adult millions of dollars annually, with the number of victims rising at an alarming rate. This paper aims to examine the experiences and vulnerability of older adult individuals to cybercrime and explore their perceptions of cybercrime victimization within the Malaysian context.

This study aimed to provide policymakers, practitioners, and researchers with a deeper understanding of the prevalence, causes, and potential solutions to the financial exploitation of the older adult in a consumer context. The study had three specific objectives: (1) To identify the types of cybercrime that affect the older adult in Malaysia; (2) To examine the key factors that make the older adult vulnerable to cybercrime; and (3) To assess the impact of cybercrime on the older adult, focusing on both financial losses and emotional well-being.

Research Objectives / Questions / Hypotheses

The research questions are as follows:

R1: What types of cybercrime do the older adult in Malaysia fall victim to?

R2: What are the critical factors that make the older adult vulnerable to cybercrime?

R3: What are the consequences of cybercrime on the older adult, both in terms of financial losses and emotional well-being?

LITERATURE REVIEW

Since the start of the new millennium, the use of information technology and the internet has surged dramatically. People of all ages and genders now spend a significant portion of their time online. The benefits of internet usage are undeniable—it facilitates daily tasks, enables remote work, and allows banking transactions to be completed from the comfort of home [10]. However, alongside these advantages, there are also risks, particularly for the most vulnerable members of society, the senior citizens, who are often targeted by cybercrime.

Malaysia's Ministry of Digital states on its official website that there is no single comprehensive definition of cybercrime. However, it identifies three main categories of cybercrime. First, when information and communications technology (ICT) systems and intellectual property are targeted for exploitation, intrusion, identity theft, and information theft. Second, when ICT devices are used as tools to commit crimes. Lastly, when ICT devices serve as platforms or mediums for carrying out criminal activities.

The older adult is more vulnerable to scams and the factors that contribute to these were identified as older adults are less experiences with technology and are not as confident dealing with technology compared to the younger generation [15]; aging as a contributor to diminishing sensitivity and poorer or slower decision-making capabilities (Oliveira et al., 2017); and reduced psychological well-being, lessened cognitive function, and lower health and financial literacy makes the older adult more susceptible to scams [18].

Besides that, [25] reiterated that any intentional act online where the victim suffers financial loss or would suffer loss while the offender profits, constitute a cybercrime offense. Notably, financial exploitation has been associated with the older adult victims who are more susceptible to cybercrime due to factors such declining mental and physical health, reduced cognitive ability, social isolation, lack of family and social support [34].

Online scams and phone scams have become a global issue. According to Jorij Abraham, Managing Director of the Global Anti-Scam Alliance, financial losses exceeded USD 1 trillion within a year August 2022 to August 2023), as reported at the Global Anti-Scam Summit [32]. Further to this, the Consumer Financial Protection Bureau (2022) reported an estimated loss between $2.9 billion to $36.5 billion annually on exploitation focusing on the older adult, earning it the reputation of being the "crime of the 21st century".

Types of cybercrime in Malaysia

According to [14] report, a total of 6,209 cybercrime cases were reported. The highest number of cases involved fraud, with 4,219 cases, followed by incidents categorized as content-related. In the first quarter of 2025, fraud cases alone numbered 1,126, while content-related cases amounted to 195. The most common types of cybercrimes in Malaysia are listed below:

Phishing

According to the FBI's 2022 report, phishing is the most prevalent form of cybercrime, with its occurrence increasing by over 1000% since 2018. A phishing attack involves a website that appears to be genuine and legitimate but is actually designed to capture personal information and exploit it to harm the victim. The modus operandi of the offender is to send an email supposedly from the bank or service provider with the intention to trick the victim in disclosing confidential information as such passwords or personal data for example: full name; NRIC, username and such [9].

Scammer (Love scam / Macau scam)

Love scam targets predominantly single senior professional females who have money. The offender will be friend the victim by email or messages. The offender will shower the victim with attention, giving them time as they usually target lonely ladies who just want someone to talk to. The offender takes their time to garner trust from the victims and eventually will start giving some stories to say they are in financial difficulty because of business and they need some money and they promise to pay back. The other common scam is that the scammer will say they have sent gifts to the victim but it is now held at the immigration and need the victim to pay some amount of money before they can receive their gift/parcel. On the other hand, the Macau scam as explained by the Royal Police of Malaysia, are usually done by locals or foreigners who contact the victims usually via phone and offer them lucky draws or pretend to be bank official to scam the victims [17].

Identity theft

An identity theft happens when the offender steals the information of the victim and pretends to be the victim to commit crime. The victim's confidential or personal data such as their name, NRIC, address and such are used by the offender to either commit unlawful crimes or use these data to apply for loans or borrow money from loan sharks. With the widely used internet technology it is easier for the offender to access to personal data especially when we use unsecured Wi-Fi in public places [1].

Underpinning Theory

Theories related to cybersecurity scams can be broadly grouped as firstly, theories that discusses what motivates the scammer and secondly, theories that explains why the older adults fall victim to these scams. Some theories related to cybersecurity scams such as the socioemotional selectivity theory, cognitive aging theory, and social engineering theory. This study looked at two set of theories, the Routine Activity Theory and the Social Engineering Theory to understand the vulnerability of older adult individuals to cybercrime in Malaysia.

The Routine Activity Theory [11], suggests that crime occurs when there is a motivated offender, a suitable target and there is an absence of someone or something that can prevent the crime. The theory highlights on how the offender exploits opportunities and are motivated when they come across a vulnerable target in the older adult who is not well versed with the internet or who lacks knowledge in cybercrime risks [26]. Older adult individuals often meet these criteria due to predictable routines and lifestyles, financial stability, and limited digital literacy. In the context of growing online fraud and phone scams, these characteristics make older adults more susceptible to becoming targets. During the COVID-19 pandemic, increased digital reliance and social isolation created additional opportunities for cyber offenders, particularly among seniors with limited support systems [5].

Social Engineering theory is based on the concept of an offender manipulating people into breaking security procedures, which is one of the core modus operandi played by the offender in cybercrime. The offender uses psychological manipulation on the vulnerable older adults into performing actions such as giving away passwords or disclosing personal information and such. The offender persuades their targeted victims to divulge sensitive information to grant them unauthorized access or they create a false sense of trust or urgency that deceives the victims. Common tactics include imitating authority figures, creating urgency, and offering small initial rewards to build trust. These methods align with established models of scam behavior, such as [36] Scammers Persuasive Techniques Model, which outlines the gradual grooming process used to exploit victims.

Together, these frameworks offer a twofold perspective: Routine Activity Theory highlights the situational conditions that make older adult individuals vulnerable, while Social Engineering Theory explains the manipulative strategies offenders use. Applying these theories enables a structured analysis of how technological, psychological, and social factors intersect to increase the risk of cybercrime among the older adult.

RESEARCH METHODOLOGY

This study employed a phenomenological research design, a qualitative approach focused on exploring individuals' experiences, perceptions, and the meanings they ascribe to them. [13] recommended a sample size of five to 20 participants for phenomenological research, using the snowball sampling method to identify participants. The participant profile consisted of Malaysian senior citizens aged 60 and above who had either been exposed to internet scams or were victims of cybercrime. In Malaysia, individuals aged 60 and above are classified as older adult, aligning with the definition established by the World Assembly on Ageing in 1982 [23].

A total of 13 individuals over the age of 60 (eight females and five males) were identified and interviewed for this study. Participation was voluntary, and the snowball sampling technique was used to recruit participants. The participant pool comprised a diverse group of older adult individuals of both genders and various ethnic, cultural, and socio-economic backgrounds to document and explore experiences of older adults from diverse background. Before the main research began, a pilot study was conducted to ensure that the interview questions effectively elicited the desired information. This pilot study helped refine the interview process by eliminating ambiguous questions and incorporating additional probing questions.

The data collection and analysis process were adapted as new ideas or patterns emerged. An informed consent was obtained prior to the interview. Detailed descriptions of participant's experiences, feelings and perceptions was recorded with the participants' consent and transcribed for analysis. Each interview session was between 30 to 45 minutes. Questions were framed to ask the participants on their experience of receiving a scam call, their personal experiences or incidents where they or someone they know fell victim, their knowledge of online security and protecting themselves from cybercrimes. The timeframe for data collection was approximately 6 months. Thematic analysis will be performed to identify and interpret patterns and themes from the qualitative data using NVivo software.

RESULTS

Types of cybercrimes

The participants in this study shared experiences related to various types of cybercrime. However, not all were direct victims of the cybercrimes they described. Only two participants had personally experienced cybercrime, while one recounted an incident involving a friend. The others had either been targeted by attempted cybercrimes or had encountered fraudulent activities without falling victim. With the exception of one participant, all shared experiences related to phone call scams, whereas only one individual reported an attempted cybercrime involving text messages. Among the phone call scams, the highest number (five cases) involved fraudulent calls from individuals posing as bank representatives, primarily related to banking or credit card activities. Table 1 summarizes the different types of scams

reported by the participants, with banking-related impersonation scams being the most common. This was followed by three cases each involving calls from individuals claiming to represent authorities, such as the income tax department, and calls related to package deliveries or product-related scams.

Table 1. Types of Phone Call Scams Reported by Participants

Type of Scam	Description	Number of Cases
Banking / Credit Card Scam (Bank Rep Impersonation)	Caller impersonates a bank officer to steal account or OTP details.	5
Authorities Impersonation (e.g., Income Tax Department)	Caller pretends to be from government bodies to intimidate victims.	3
Package Delivery / Product-related Scam	Fake delivery calls or product refund requests used as scam bait.	3
Text Message Scam	Fraudulent messages prompting clicks on malicious links.	1

Reasons why older adult people are vulnerable?

The participants in this study identified several factors that contribute to the heightened vulnerability of older adult individuals to cybercrime. Table 2 presents the key vulnerability factors cited by the participants, including financial stability and limited digital awareness [27]. These factors are based on the participants' perceptions of susceptibility to cyber threats. One key reason older adults fall victim to phone scams is their greater likelihood of answering phone calls compared to the younger generation. One participant, C, associated this tendency with feelings of loneliness. According to C, individuals who experience loneliness are more inclined to answer unknown calls and engage with scammers, thereby increasing their susceptibility. This initial interaction serves as an entry point, creating opportunities for fraudulent activities to unfold. C explained,

One is the senior people are lonely. Lonely old people, so they need someone to talk to when they have these rare calls coming in. Uh, so they want to talk…

Table 2. Perceived Factors Contributing to Vulnerability to Cybercrime

Factor	Description	Number of Mentions
Answers Unknown Phone Calls (Linked to Loneliness)	Older adults are more likely to answer unknown calls due to social isolation and desire for interaction.	1
Lack of Awareness of Smartphone Risks	Limited understanding of threats like malicious links or apps.	1
Poor Recognition of Digital Threats	Difficulty detecting scams or recognizing suspicious digital behavior.	3
Perceived Financial Stability (Pension / Savings)	Older adults perceived as financially secure, making them attractive targets.	5

Another participant, F, identified a lack of awareness regarding the risks associated with smartphone use as a key factor contributing to the vulnerability of older adult individuals to cybercrime. Many older adults may not fully comprehend the potential dangers posed by links in messages or websites. Additionally, their limited familiarity with smartphone functionalities increases the likelihood of accidental interactions, such as unintentionally clicking on malicious links or opening fraudulent applications, which can further expose them to cyber threats.

My thought is that an older citizen is not really aware, but this can happen to anyone. So, they don't really know what is there, but they are easy to be bullied by all these scammers.

Participant I, J and K shared a similar view, emphasizing that older individuals may struggle with recognizing digital threats and are therefore more susceptible to online scams. Participant I shared,

Awareness, not much awareness out there. Especially with older generation like me. I, at least read the paper every day, but how many people my age or older are doing that? We don't watch TV much also. But by watching TV too, we might not have any awareness.

Five participants, B, C, G, H and L identified that older adult people are targeted because of their financial stability. Many older adults have accumulated savings or receive pensions, making them attractive targets for cybercriminals. This financial security increases their likelihood of being targeted for scams, as perpetrators perceive them as having disposable income that can be exploited. L explained that,

I also think because they like know this person has money. They can pay for whatever money they have to because whenever it's like, oh, this civil servant got money.

However, it is important to note that the factors mentioned above are based on the participants' perceptions rather than direct experiences. To gain a deeper understanding of the vulnerabilities of older adult individuals, it is crucial to scrutinize the experiences of the two participants who were actual victims of cybercrime. Analyzing their firsthand encounters can provide more concrete insights into the specific factors that contributed to their victimization. The following section will examine their experiences in detail.

Participant A lost approximately RM12,000 in a phone scam, highlighting how shock and fear were used to deceive and manipulate him into divulging sensitive information. The scammer called around 3 p.m., a time when many people (especially older people) typically take an afternoon nap. Upon waking abruptly to the call, he was startled to hear that his bank card was allegedly being used fraudulently. The caller, claiming to be from his bank, created a sense of urgency, making it difficult for him to process the information clearly. While still disoriented, he was asked to provide various details, including a one-time password (OTP) and short messaging system (SMS) verification codes. In his state of shock, he unknowingly complied, only realizing the deception when his daughter intervened and warned him against sharing such information. He immediately ended the call, and they promptly filed a police report. However, within just fifteen minutes, five or six unauthorized transactions had already been made, resulting in the loss of his money.

Participant D recounted a markedly different experience, in which scammers exploited a deceptive reward system to gain her trust before coercing her into financial losses. Initially, she was asked to complete a series of tasks with the promise of receiving commissions. For the first few tasks, she was indeed compensated, reinforcing her confidence in the scheme. However, the scammers later demanded that she transfers money, claiming it was required to pay a service tax. They further intimidated her by threatening legal consequences from the income tax department if she failed to comply. They also showed 'official letter' from the income tax department to convince her to pay the required amount. Overwhelmed by fear and anxiety, she ultimately lost RM72,000 (USD 16,000). Reflecting on the incident, she described feeling as though she had been under a spell, unable to fully grasp the extent of her losses until after the fact.

Although she reported the crime to the police, she was informed that the perpetrators could not be apprehended, as they had used mule accounts to facilitate the scam. Mule accounts are bank accounts used by criminals to launder stolen money, often belonging to individuals who allow their accounts to be used, either knowingly or unknowingly, in exchange for a small commission. Because these accounts frequently change hands and are difficult to trace, authorities face significant challenges in tracking down the actual perpetrators and recovering lost funds [20].

Tangible and intangible consequences

Victims of cybercrime or attempted cybercrime experience both tangible and intangible consequences. Table 3 highlights the emotional and financial consequences of cybercrime experienced or observed by participants. The most significant tangible consequence is financial loss. For some individuals, this loss can be devastating, potentially depleting their life savings and causing long-term financial instability.

Others, however, may experience only a limited loss and are able to recover more easily. The severity of the impact varies depending on the extent of the fraud and the victim's financial situation.

Table 3. Tangible and Intangible Consequences of Cybercrime Victimization

Consequences Type	Description	Number of Mentions
Financial Loss	Direct monetary loss, ranging from minor amounts to substantial savings (e.g., RM12,000, RM72,000)	2
Fear and Anxiety	Psychological distress and insecurity when using digital financial tools or receiving unknown calls.	3
Trauma	Lasting emotional impact, including intrusive thoughts and hyper-vigilance even years after the incident.	3
Shame and Self-Blame	Feelings of embarrassment, humiliation, or perceived foolishness after being deceived.	2

However, the intangible consequences of cybercrime are equally significant. Participants reported experiencing trauma after falling victim to cybercrime or attempted cybercrime, leading to heightened fear and anxiety regarding any financial or banking-related interactions on their smartphones. This fear places them in a challenging position, as modern banking increasingly relies on mobile applications for transactions, making it difficult for them to navigate daily financial activities with confidence.

Participant B shared his experience,

After you've completed the [scam] call, you put down the phone, so actually we are confused. I mean, it's shocking. You know, suddenly someone is calling you asking for some details and you panic a bit first. You don't see this because you don't get this very kind of call every day.

Participant H shared her experience,

When I was almost scammed, I was shaken. Luckily, I woke up. But the thought I could have lost my money, scares me. I am more scared than I am angry.

Participant D described experiencing lasting trauma even years after the incident, highlighting the enduring psychological impact of cybercrime.

OK, emotionally it affected me a lot for the first time. I think until now it's still in my head and once in a while it will come into my head, so I think, like I said, it's a good lesson for me to keep me aware of whatever next time. Don't go into this kind of thing.

I think this happened in 2021, October.

In addition to trauma, participants noted that victims often experience a profound sense of shame. Participant C expressed that had he fallen victim to a scam, he would have experienced intense feelings of shame and self-blame. He noted that being deceived in such a manner would have made him feel not only embarrassed but also unintelligent for failing to recognize the scam. This perspective highlights the deep psychological burden associated with cybercrime victimization, where individuals often internalize blame despite the sophisticated tactics used by perpetrators.

Participant H shared her sister's experience, explaining that feelings of shame have prevented her from openly discussing the incident.

My sister now is better but she still doesn't want to talk to us about this. She is very sensitive when we discuss about scam. I don't know if she feels she was stupid to lose the money or what she feels.

Overall, the findings of this study highlight the various types of cybercrime encountered by the participants, the factors contributing to the vulnerability of the older adult to such crimes, and the

tangible and intangible consequences they endure as a result.

DISCUSSION

The findings of this study align with existing literature on cybercrime vulnerability among the older adult, particularly in the Malaysian context. The prevalence of phone scams involving impersonation of bank officials or government authorities (e.g., income tax department) underscores the exploitation of trust and authority—a hallmark of social engineering tactics. Recent research [7] demonstrates that telephone scams disproportionately target older adults by weaponizing fear and urgency, bypassing rational decision-making through psychological manipulation. This aligns with Participant A's experience of being coerced into sharing OTPs during a disoriented state. Similarly, Participant D's case reflects the "foot-in-the-door" technique, where initial small rewards build trust before escalating demands, a strategy aligned with the Scammers Persuasive Techniques Model [36]. Whitty's model, which explains how scammers groom victims through incremental trust-building phases, is evident in Participant D's experience: early financial rewards established credibility, enabling later exploitation through threats of legal action.

The Routine Activity Theory further explains the targeting of older adult individuals as "suitable targets" due to their perceived financial stability and lack of capable guardianship. Participants highlighted that seniors' accumulated savings or pensions make them attractive to offenders, while limited digital literacy and slower cognitive processing [18] reduce their ability to act as their own guardians. [7] corroborate this, identifying that older adults' reliance on landlines or mobile phones—coupled with isolation—creates a "perfect storm" for fraudsters to exploit. These theoretical connections are summarized in Table 4.

Bank Negara Malaysia's (BNM) security measures, such as replacing SMS OTPs with app-based authentication and cooling-off periods for new e-banking registrations, directly address vulnerabilities identified in this study. For instance, Participant A's loss of RM12,000 via SMS OTP theft could be mitigated by stricter authentication methods. However, these measures must be complemented by targeted education for older adult users, as technological transitions (e.g., app-based systems) may inadvertently exclude those unfamiliar with smartphones.

The emotional consequences reported—trauma, shame, and social withdrawal—mirror global findings on the psychological toll of cybercrime. [5] argue that the shift in routine activities since the pandemic created new opportunities for cybercriminals, with older populations particularly affected due to increased online exposure and limited digital literacy. This is evident in Participant D's enduring anxiety and Participant H's sister's reluctance to discuss her experience, highlighting the need for psychosocial support mechanisms alongside financial safeguards.

Table 4. Alignment of Study Findings with Theoretical Models and Literature

Key Finding	Supporting Theory / Model	Reference or Related Literature
Use of fear and urgency in phone scams	Social Engineering Tactics / Persuasive Techniques	[36]; [7]
Gradual trust-building through small rewards before exploitation	Foot-in-the-Door Technique	[36]
Older adults targeted due to perceived wealth and low guardianship	Routine Activity Theory	[18]
Psychological impacts: fear, trauma, shame	Psychosocial Consequences of Cybercrime	[5]
Technological vulnerability due to smartphone unfamiliarity	Digital Divide in Elderly Populations	Supported in current literature (e.g., BNM, 2023)

A limitation of this study is its small sample size (n=13), which restricts generalizability. Future research could employ mixed methods to quantify vulnerability factors (e.g., correlating financial literacy with

scam susceptibility) across a larger demographic. Additionally, the reliance on self-reported data may introduce recall bias, suggesting the need for real-time monitoring of scam interactions.

CONCLUSION

This study clarifies the multifaceted vulnerability of Malaysian older adult to cybercrime, driven by technological unfamiliarity, social isolation, and financial attractiveness. Key findings reveal that online scams or phone scams—particularly those impersonating trusted institutions—are the most prevalent, exploiting seniors' trust and limited digital literacy. Financial losses and psychological trauma emerge as significant consequences, with long-term impacts on victims' well-being.

The study highlights the urgency of holistic interventions. While BNM's security measures are a critical step, their effectiveness hinges on parallel efforts to enhance older adult digital literacy through community workshops, simplified cybersecurity guides in native languages, and family-mediated education. Policymakers should also mandate banks to implement age-friendly authentication systems and establish trauma counseling services for victims.

This research contributes to the underexplored domain of older adult cybersecurity in Southeast Asia, offering actionable insights for Malaysia's aging population. Future studies should explore longitudinal trends in scam tactics and evaluate the efficacy of interventions like BNM's policies. By bridging institutional safeguards, public education, and emotional support, Malaysia can mitigate the rising tide of cybercrime against its older adult population.

REFERENCES

[1] Mohamad AR, Yaakop MR, Razif MA. The efficacy of the Malaysian Government's response towards cybercrime. Open Journal of Political Science. 2024 Jan 18;14(1):166-76. https://doi.org/10.4236/ojps.2024.141010

[2] Masoumeh H, Jahangiri S, Ali BH, Alireza K. A survey on existing digital divide between teachers and students of girl schools in astara county. International Journal of Academic Research in Business and Social Sciences. 2013 Nov 1;3(11):356. http://dx.doi.org/10.6007/IJARBSS/v3-i11/345

[3] Bernama. Number of cybercrime cases reported in Malaysia from 2021 to June 2022 total of 31,169. Bernama; 2022 Jul 27.

[4] Kassim NM. Effect of perceived security and perceived privacy towards trust and the influence on internet banking usage among Malaysians. International Academic Journal of Social Sciences. 2017;4(2):26-36.

[5] Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies. 2021 Feb 1;23(S1):S47-59. https://doi.org/10.1080/14616696.2020.1804973

[6] Amiri M, Akkasi A. Assessing security challenges in online social networks. International Academic Journal of Science and Engineering. 2015;2(4):1-0.

[7] Button M, Shepherd D, Hawkins C, Tapley J. Fear and phoning: Telephones, fraud, and older adults in the UK. International Review of Victimology. 2025 Jan;31(1):117-34. https://doi.org/10.1177/02697580241254399

[8] Peydayeshi Y, Karimi MR. Studying the relationship between emerging communication factors and religious beliefs. Int Acad J Innov Res. 2017;4(2):22–9.

[9] Chen W, Guo X, Chen Z, Zheng Z, Lu Y. Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem. InIjcai 2020 Jul (Vol. 7, pp. 4456-4462).

[10] Thasleena KF, Santhi P. Generational divide in digital banking: Comparing experience and expectation across Generations X, Y, and Z. Indian J Inf Sources Serv. 2025;15(2):268–74. https://doi.org/10.51983/ijiss-2025.IJISS.15.2.34

[11] Cohen LE, Felson M. Social change and crime rate trends: A routine activity approach. American sociological review. 1979 Aug 1:588-608. https://doi.org/10.2307/2094589

[12] Blazic BJ, Cigoj P, Blažič AJ. Web-Service Security and The Digital Skills of Users: An Exploratory Study of Countries in Europe. J. Internet Services Inf. Secur. 2023;13(3):41-57. https://doi.org/10.58346/JISIS.2023.I3.004

[13] Creswell JW, Poth CN. Qualitative inquiry and research design: Choosing among five approaches. Sage publications; 2016 Dec 19.

[14] CyberSecurity Malaysia. Incident statistics 2024 Malaysia [Internet]. CyberSecurity Malaysia; 2024 Sep 13. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=87dc3238-293d-407d-9525-9426c3bea0dd

[15] Ebner NC, Ellis DM, Lin T, Rocha HA, Yang H, Dommaraju S, Soliman A, Woodard DL, Turner GR, Spreng RN, Oliveira DS. Uncovering susceptibility risk to online deception in aging. The Journals of Gerontology: Series B. 2020 Mar;75(3):522-33. https://doi.org/10.1093/geronb/gby036

[16] Franklin J, Perrig A, Paxson V, Savage S. An inquiry into the nature and causes of the wealth of internet miscreants. Ccs. 2007 Oct 29;7:375-88. https://doi.org/10.1145/1315245.1315292

[17] Ismail AI. Love Scam sasar mangsa kesunyian. Sinar Harian [Internet]. 2023. https://www.sinarharian.com.my/article/246957/berita/semasa/love-scam-sasar-mangsa-kesunyian

[18] James BD, Boyle PA, Bennett DA. Correlates of susceptibility to scams in older adults without dementia. Journal of elder abuse & neglect. 2014 Mar 15;26(2):107-22. https://doi.org/10.1080/08946566.2013.821809

[19] Rani MI, Zolkaflil S, Nazri SN. The trends and challenges of money mule investigation by Malaysian enforcement agency. International Journal of Business and Technopreneurship (IJBT). 2023;13(1):37-50. https://doi.org/10.58915/ijbt.v13i1.963

[20] New Straits Times. A total of 51,631 online fraud cases were reported in Malaysia between 2019 and 2021 involving a total loss of RM1.61 billion. New Straits Times; 2022 Mar 7. https://www.nst.com.my/news/crime-courts/2022/03/778569/over-rm16bil-lost-online-fraud-cases-2019-2021

[21] Zulkipli NH, Rashid NA, Zolkeplay AF, Buja AG. Synthesizing cybersecurity issues and challenges for the elderly. Turkish Journal of Computer and Mathematics Education. 2021;12(5):1775-82.

[22] Public Service Delivery and Local Government. The older adult/senior citizens. https://www.malaysia.gov.my/portal/content/30740

[23] Rahman, R. (2019). Cybercrime cases in a decade: The Malaysian experience. Independently published.

[24] Steele J, Reyes A, Brittson R, O'Shea K. Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors. Elsevier; 2011 Apr 18.

[25] Sasse S. "Motivation" and routine activities theory. Deviant Behavior. 2005 Nov 1;26(6):547-70. https://doi.org/10.1080/01639620500218260

[26] Wahid SD, Buja AG, Jono MN, Aziz AA. Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modeling. International Journal of Advanced Technology and Engineering Exploration. 2021 Jan;8(74):73. http://dx.doi.org/10.19101/IJATEE.2020.S1762116

[27] The Star. Seniors a prime target for scams. 2024 Jun 13 https://www.thestar.com.my/

[28] The Star. Senior citizens lose over RM227,000 in credit card, investment scams in Pahang. 2023 Feb 10. https://www.thestar.com.my/

[29] The Sun Daily. Safeguarding senior citizens from scams. 2023 Jun 22. https://www.thesundaily.my/

[30] The Edge Malaysia. Malaysia lost over RM1.22b to cybercrime from January to October 2024 — PM. 2024 Dec 3 https://theedgemalaysia.com/node/736320

[31] The Straits Times. $1.4 trillion lost to scams globally; S'pore victims lost the most on average: Study. 2024 Nov 13. https://www.straitstimes.com/

[32] Tripathi K, Cooper C. Cybercrime against older people during COVID19 pandemic. UCL JDI Special Series on COVID-19, (4). 2020 Apr.

[33] Weissberger GH, Mosqueda L, Nguyen AL, Samek A, Boyle PA, Nguyen CP, Han SD. Physical and mental health correlates of perceived financial exploitation in older adults: Preliminary findings from the Finance, Cognition, and Health in Elders Study (FINCHES). Aging & mental health. 2020 May 3;24(5):740-6. https://doi.org/10.1080/13607863.2019.1571020

[34] Whitty MT, Buchanan T. The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking. 2012 Mar 1;15(3):181-3. https://doi.org/10.1089/cyber.2011.0352

[35] Whitty MT. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British journal of criminology. 2013 Jul 1;53(4):665-84. https://doi.org/10.1093/bjc/azt009