INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 14, Issue 4, (2024) E-ISSN: 2225-8329

The Impact of Financial Literacy on Online Financial Scam Victimization

Mohd Akbal Qamas Abdul Basir, Mohamed Hisham Dato Haji Yahya, Hasri Mustaffa, Wei Ni Soh

School of Business and Economics, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Corresponding Author: Email: mohdakbalqamas@gmail.com

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v14-i4/23589 DOI:10.6007/IJARAFMS/v14-i4/23589

Published Online: 27 December 2024

Abstract

The rise in online financial scams has raised concerns and highlighted the need for a deeper comprehension of the factors contributing to victimization. This research examines the financial literacy levels among victims and investigates how financial literacy influences the likelihood of falling prey to online financial scams. Data was collected through in-depth interviews with fourteen (14) police officers from Jabatan Siasatan Jenayah Komersial Bukit Aman, who have encountered cases of financial scams and supported by the document analysis involving Police Report. Thematic analysis utilizing Nvivo 12 software was employed to analyze the data. Surprisingly, the study reveals that victims exhibit different levels of financial literacy among the victims which influence the susceptibility to online financial scams. Moreover, the findings able to explore common types of financial scams in Malaysia. Moreover, the study identifies awareness campaigns as a key measure in combating online financial scams. The findings emphasize the importance of financial literacy in determining susceptibility to online scams and provide valuable insights for policymakers, regulators, and enforcement agencies tackling this pervasive issue.

Keywords: Financial Literacy, Victimization, Online Financial Scam, Improvement Procedures, Awareness Campaigns

Introduction

In Malaysia, online banking was introduced in June 2000 when Bank Negara Malaysia issued guidelines for licensed banking institutions to offer Internet banking services. The rise of online banking is a global phenomenon, with millions of people around the world using this technology to manage their finances. Statista (2024) reported that as of May 2022, more than 66% of internet users in Malaysia were utilizing online banking. The number of digital payment users in the country is projected to grow by 35.37% from 2024 to 2028, reaching a total of 31.02 million users. One of the key drivers of this growth is the increasing use of mobile devices to access online banking services. As more individuals adopt this technology, financial institutions are adapting to meet their customers' needs by investing in digital

infrastructure and developing new online banking products and services. The trend towards online banking is likely to continue in the coming years as more consumers recognize the benefits of this technology. According to a report by MyCERT (2024), there were 5,917 cases of cybercrime reported in 2023. Of these, the most reported type of cybercrime was fraud, with 3,705 cases, which accounted for 62% of all reported cases.

In his Budget 2023 presentation, Malaysian Prime Minister Dato Seri Anwar bin Ibrahim highlighted the significant issue of online financial scams, with over 25,000 cases in 2022 resulting in RM850 million in losses. To combat this, the government has allocated RM10 million to the National Scam Response Centre (NSRC) for operating grants. While the establishment of the NSRC is a positive step, the lack of a uniform policy among financial institutions remains a concern.

Despite multiple programs held by the Malaysian Government to cater for this issue, the citizens are still at risk of becoming the victims. Financial literacy is an important survival skill that everyone should possess but is lacking among Malaysians (Aziz & Kassim, 2020). Malaysians are unaware of their low level of financial literacy. Thus, this research focuses on the financial literacy level and the impact of online financial scams on victims in Malaysia. Previous studies have shown that financial literacy among teenagers is low in most countries, including the United States. This may be because young people have not lived through difficult financial times, such as high inflation, making it difficult for them to answer financial literacy questions correctly.

Literature Review

Financial Literacy and Victimization in Malaysia

Lusardi and Mitchell (2007) defined Financial Literacy as a process which includes a) financial information gathering, b) financial confidence and skills development, c) awareness of opportunities and risks, d) the learning of suitable resources for assistance, as well as e) actions taken to improve one's financial situation. The research focuses on a group of individuals, including both active workers and retirees, who exhibit a significant lack of preparedness and financial literacy proficiency. The significance of financial literacy is underscored by the potential repercussions of financial mismanagement, which can lead individuals into the detrimental cycle of indebtedness.

Financial literacy refers to an individual's understanding and knowledge of financial concepts, which can be assessed by examining various aspects of financial knowledge. Numerous studies on financial literacy indicate that even in developed countries, the general population often lacks sufficient financial literacy to make informed financial decisions (Kumar & Kumar, 2023). For instance, individuals with low financial literacy are less likely to participate in the stock market, pay attention to retirement planning, face budgetary conflicts, and resort to informal borrowing.

Huston (2010), in her analysis of existing studies regarding measuring financial literacy, revealed 3 main barriers to measuring financial literacy, which are 1) The absence of a clear conceptualization and definition of financial literacy, 2) Issues related to the content and 3) Interpretation of measurement instruments, with first one as the most important. A significant proportion of studies, nearly three-quarters, failed to elaborate on the construct

they employed, while the rest presented varying definitions, incorporating elements such as knowledge, ability, and outcomes.

Throughout the last decade, Malaysia has achieved notable strides in promoting financial inclusion and has implemented nationwide initiatives for enhancing financial education to elevate the financial capabilities of its populace. Serving as the principal proponent of the financial literacy agenda in Malaysia, BNM has been actively championing financial literacy through diverse communication channels. BNM has implemented various initiatives to ensure that the Malaysian populace benefits from awareness programs related to financial literacy. For example, The Financial Education Network (FEN) inaugurated Financial Literacy Month 2022 (FLM2022) at Sasana Kijang, BNM, on October 1, 2022. FLM2022 serves as an annual flagship event designed to heighten consumer awareness of importance financial issues and enhance financial literacy among Malaysians.

The recent surge in such scams in Malaysia has been attributed to the widespread impact of the COVID-19 pandemic. According to Salleh (2022), the surge in online fraud cases is related to job scams, loan scams, and investment scams. All the scams that have occurred are related to the recent implementation of the Movement Control Order (MCO) in Malaysia. Yin (2022) reported a 25% spike from the previous year, with a significant uptick in investment scams during the pandemic, fueled by movement restrictions that prompted individuals to seek additional income sources.

Financial literacy is a key factor in preventing individuals from falling victim to investment scams and in promoting financial well-being and knowledge about money (Sabri & Zakaria, 2015). Chariri et al. (2018) found a positive relationship between an individual's level of financial literacy and their ability to detect investment scams. Research indicates that many investment scam victims have limited investment knowledge (Venkatesan & Venkataraman, 2018), as they are unaware of the various tactics used by scammers. Consequently, individuals with better financial market knowledge are more capable of making sound investment decisions. They understand the importance of saving, particularly for retirement, and investing in financial assets to build future wealth.

Being a victim of fraud can have severe consequences on various levels, including economic, physical, and psychological well-being. In terms of identity theft, it was found out that every victim lost, on average, about $1000 (Abbott & McGrath, 2016). In the modern world, the Internet has become an integral part of people's lives, and living comfortably often requires Internet access. Criminals have consequently devised multiple methods to exploit the characteristics of the internet for profit. Given the relative ease of replicating someone's online identity, some criminals pose as legitimate individuals to deceive internet users into revealing sensitive information like passwords and credit card details.

Research Methodology

This study collected data from multiple sources to explore financial literacy in relation to online financial scam victimization. A semi-structured interview protocol was employed as the tool to guide interviews regarding the victimization of online financial scams. The semi-structured interview approach, as described by Kvale and Brinkmann (2009), sought to capture the interviewees' descriptions of their life experiences to uncover the essence of the discussed phenomena (p. 3). The Interviews were conducted in English to facilitate effective

communication. However, recognizing the diverse backgrounds and varying levels of education among the respondents, a decision was made to permit responses in Bahasa Malaysia. Malay constitutes one of the native ethnicities, accounting for approximately 60% of Malaysia's population (Mahadin, 2021).

The participants in this study were chosen using a purposive sampling technique. Participants were selected through a criterion sampling process, which required them to fulfill a set of criteria to be eligible to participate (Savin-Baden & Major, 2013). Commercial Crime Investigation Department was selected for the study as they fulfilled the criterion of the study and were willing to participate. The determination of the sample size in this research follows Clarke and Braun (2013) recommendation, which suggests that a range of 6 to 15 participants is appropriate for conducting thematic analysis in research projects. The final sample includes fourteen police officers from the Commercial Crime Investigation Department, Bukit Aman from different departments, ranging from different levels of officers.

Researcher acquired the police reports for the document review from a reputable and reliable online platform. Document broadly includes various materials, spanning from traditional texts to visual sources like photographs, videos, and films (Merriam & Tisdell, 2016). Visual materials, much like written documents, offer valuable content for qualitative analysis (Flick, 2018). The police reports collected for this study had to meet specific criteria before they could be included. These criteria include providing comprehensive report coverage, covering information about scams, and being available on an online platform. While more than 50 police reports were initially gathered from various sources, only 36 of them met all the necessary criteria. The data collected from these reports included information such as location, gender, age, race, occupation, type of scam and modus operandi.

NVivo has been chosen for analyzing extensive transcriptions and other documents to enhance data analysis (Gibbs, 2002). This software is used for initial coding, categorizing, and developing themes from the data (Strauss, 1987). Moreover, it supports an eco-friendly data management process, replacing traditional paper and pencil methods (Alam, 2020).

Findings and Discussions

In this study, the researcher has collected data from fourteen respondents, and all of them have been utilized for the study, as shown in Table 4.1. Guest et al. (2006) found the data saturation regarding the homogenous people at the 12th respondent. Despite having multiple backgrounds, the respondents were significantly related to the area of study, which includes the direct involvement with the victims.

Table 4.1
Demographic of Respondents

RESPONDENTS	EDUCATION LEVEL	POSITION	SERVICE YEAR	FIELD OF QUALIFICATION
Respondent 1	Master's Degree	Deputy Superintendent of Police (DSP)	17	IT & Business Administration
Respondent 2	Master's Degree	Deputy Superintendent of Police (DSP)	18	Forensic Accounting
Respondent 3	Bachelor's Degree	Assistant Superintendent of Police (ASP)	10	Economy
Respondent 4	Master's Degree	Deputy Superintendent of Police (DSP)	21	Accounting
Respondent 5	Bachelor's Degree	Inspector (INSP)	19	Business admin
Respondent 6	Master's Degree	Assistant Superintendent of Police (ASP)	10	Information Management
Respondent 7	STPM	Deputy Superintendent of Police (DSP)	27	Not Stated
Respondent 8	Bachelor's Degree	Assistant Superintendent of Police (ASP)	14	Business Administration
Respondent 9	Master's Degree	Superintendent (SUPT)	16	Law
Respondent 10	Master's Degree	Assistant Superintendent of Police (ASP)	15	Development Management
Respondent 11	Bachelor's Degree	Assistant Superintendent of Police (ASP)	9	Business Management
Respondent 12	Bachelor's Degree	Inspector (INSP)	8	Computer Science
Respondent 13	Bachelor's Degree	Inspector (INSP)	7	Business Administration
Respondent 14	Master's Degree	Inspector (INSP)	6	Public Administration

Source: Developed by author

In addition, the police report was included to improve the understanding of the cases. Thirty-six reports were specifically selected for their relevance to the research topic, which is online scam. Each of the selected reports is assigned a label ranging from R#1 to R#36, as indicated in Table 4.2.

Table 4.2
Police Report Summary

No	State	Year	Gender	Occupation	Type of Fraud
R#1	Negeri Sembilan	2022	Male	Takaful Agent	Unauthorized Transaction
R#2	Selangor	2019	Male	Technician	Fake Transaction
R#3	Johor	2022	Male	Business	Cheating Store Money
R#4	Selangor	2022	Woman	N/A	Car Rental Fraudulent
R#5	Selangor	2022	Woman	Housewife	Job Scam
R#6	Selangor	2015	Male	Hotel Helper	Home Rental Deposit
R#7	Negeri Sembilan	2022	Woman	Student	Ponzi Scheme
R#8	Negeri Sembilan	2022	Male	Lorry Driver	Ponzi Scheme
R#9	Kelantan	N/A	N/A	N/A	Borrowing Money/Loan
R#10	Kuala Lumpur	2019	Woman	Salesman	Misuse of Card Credit Transactions
R#11	Melaka	2020	Male	Business	Online Purchase fraudulent
R#12	Kuala Lumpur	2020	Male	N/A	Online Purchase fraudulent
R#13	Kedah	2020	Woman	Marketing Manager	Offline Purchase Fraudulent
R#14	Terengganu	2022	Male	N/A	Offline Purchase Fraudulent
R#15	Sarawak	2022	N/A	N/A	Investment Fraud
R#16	Sarawak	2022	Male	Unemployed	Use of Identity
R#17	Selangor	2020	Male	Technician	Use of Identity
R#18	Melaka	2021	Male	Salesman	Use of Identity
R#19	Kuala Lumpur	2022	Male	Self-employed	Use of Identity
R#20	Kelantan	2021	Male	Retiree	Use of Identity
R#21	Johor	2017	Woman	Custom Officer	Macau Scam
R#22	Johor	2022	Male	Doctor	Macau Scam
R#23	Johor	2014	Male	N/A	*Kutu*
R#24	Kuala Lumpur	2019	Woman	Business	Mule Account
R#25	Johor Bahru	2009	Male	Welder	Lost of I/C
R#26	Kuala Lumpur	2022	Male	N/A	Job Scam
R#27	Selangor	2022	Male	Canteen Operator	E-wallet Hack
R#28	Selangor	2019	Male	Teacher	Home Rental Deposit
R#29	Selangor	2022	Male	Company Director	Fake Receipt
R#30	Selangor	2022	Male	Student	Purchase of Old Coins
R#31	Sabah	2021	Male	Old Money Collector	N/A
R#32	Johor	2019	Male	Driver	N/A
R#33	Selangor	2022	Woman	Content Moderator	N/A
R#34	Selangor	2020	Woman	Online Business	N/A
R#35	Selangor	2022	Woman	N/A	N/A
R#36	Pahang	2020	Male	N/A	N/A

Source: Developed by author

Financial Literacy Levels

The findings revealed that participants who dealt with the scam victims of scams felt Malaysians generally were susceptible to scams, easily fooled. Participants has varying opinion regarding the level of financial literacy posed by the victims as illustrated in Table 4.3. Extracts from interviews with police officers have been included in the result section. The varying levels of literacy among each victim will determine their involvement in this victimization.

Table 4.3
Level of Financial Literacy

Theme	Categories
Level of financial literacy	High level • Excellent Financial Management • Understanding of financial conceptions • Selection of safer financial products Low level • Financial exclusion • Lack of understanding of financial knowledge • High risk lending & debt accumulation

Source: Developed by author

High Level

A high level of financial literacy refers to a comprehensive understanding of various financial concepts, tools and practices. Individuals with high levels of financial literacy have the knowledge and skills necessary to make sound financial decisions regarding their finances, as noted by Gathergood and Weber (2017), who found that individuals with high levels of financial literacy are more likely to be able to avoid fraud-related losses as they can select appropriate and safer financial products.

Victims know how to control their finances and where to invest their money. Respondent 1 said, "...*they know how to control their finances…".* Respondent 1's comment that victims know how to control their finances confirms that a high level of financial literacy helps to correctly assess the seriousness of the scam. A high level of literacy among victims might hinder them from becoming victims. Engels et al. (2019) confirmed that people with high levels of literacy can detect scams. A high level of financial knowledge gives them a better understanding of the financial market and economic laws.

Respondents linked the high level of literacy to their excellent financial management and lack of financial problems, as Respondent 6 noted, "…*They have good financial management, no financial problems…*". When analyzing the cases dealt with by police officers, the level of financial management exhibited by the victims becomes apparent through their responses during investigations. Victims' ability to articulate and respond to questions during the inquiry serves as an indicator of their level of financial literacy. Respondent 9 stated that victims have an above-average level of financial literacy, *"These people have above-average financial literacy".* As mentioned by Mohamad et al., (2024), a person with adequate financial literacy is more likely to manage their money effectively due to access to diverse financial options, which helps them achieve financial well-being.

Low Level

In the other hand, Sukumaran (2015) suggested that low Financial Literacy correlates with financial exclusion and speculate that a lack of understanding of financial systems and concepts makes individuals more vulnerable to economic exploitation. This vulnerability may include practices such as high-risk lending and accumulating debt. The statement by Respondent 10 below supported the low level of knowledge among the victims.

"So, people's knowledge about finance is quite low because commercial crime is always advertised on social media". **Respondent 10**

In addition, according to Respondent 14, the literacy level remains significantly low despite the implementation of many awareness activities by law enforcement agencies aimed at educating potential victims.

"Hmm, for me personally, the victims' literacy level is very low despite the campaigns carried out by the PDRM and governments. There are still others who are deceived, most of them are professionals". **Respondent 14**

In summary, it is clear from the police interviews that there are differences in the financial literacy level among the victims. Statements from the police officers have confirmed that the victims possess low levels and high levels of financial literacy. All the respondents discussed their encounters with scam victims and were able to identify their level of financial literacy.

Type of Online Financial Scams

There are many types of online financial scams today, each operated by scammers utilizing various financial instruments. Financial scams can occur to anyone in various circumstances. Each respondent in the study encountered different types of scams, with each individual experiencing scams specific to their respective divisions. The analysis from the interviews revealed five common types of online financial scam in Malaysia and illustrated in Figure 4.6.

Table 4.4
Type of Online Financial Scams

Themes	Categories
Type of scams	Macau Scam • Impersonation of government officer • Intimidation of committing crime E-Commerce Scam • Deliberate misrepresentation of something • Lack of control • Impulsive financial decisions Cryptocurrency Investment Fraud • Deceive investors and steal their funds • Fever detection trails by the authorities • Negligence of the risk Ponzi Investment Scam • Building trust among the victims • Lucrative money making • Easily susceptible to returns on investments Non-Existence Loan Scam • Financially desperate • Ignorant towards abnormal transaction

Source: Developed by author

Macau Scam

The Macau Scam, often known as the Phone Scam, was also referenced by Respondent 10. He stated how the fraudster deceived the victims by impersonating as LHDN or police officers. The fraudster will reach out to the victims and impersonate them as an official while intimidating them by alleging them to have committed a crime. Later, the fraudster will provide the victims instructions on how to transfer a specific sum of money to an official account to facilitate an investigation.

"Macau Scam (Phone Scam) disguised as LHDN officers. They will tell the victim that they involved in illegal activities such as drugs. .... However, they disguised as Police Officers to intimidate and build trust solely for the purpose of money transfer." **Respondent 10**

The existence and validity of the Macau Scam are substantiated by the case detailed in the police report R#21. In this incident, the victim, who is working as a doctor, was contacted by someone claiming to be a Pos Laju Officer, informing them of a suspicious package involving ICs and bank cards of other people. The excerpt from the police report is provided below.

"I want to make a police report regarding a fraud case that occurred involving myself on XX.XX.XXXX, which also involved a bank transaction amounting to RM 2,200. At 3.00 pm, while I was working, I received a phone call from the number +6014-xxxxxx and was connected to a Pos Laju officer named RXXXXX bXX RXXXX (PSXXXXXX employee ID), who stated that a parcel under my name as the sender had been blocked for sending prohibited items, namely 1 IC card and 5 Maybank cards from the Taman Ipoh Post Office, Perak on XX.XX.XXXX to be sent to the Sarawak Main Post Office, Kuching, Sarawak, with the recipient being AXXXX HX." **R#21**

The modus operandi then has been discussed by Respondent 11 regarding the Pos Laju parcel Modus Operandi.

"As an example of the Macau Scam, we will receive a call from JnT or Postlaju, and become panic when we were informed of the prohibited item detected from the parcel. The culprit will call and impose that the call is from immigration and due to the following matters and will further transfer it to the predefined police station. The victim will start to panic. There were walkie-talkie played on the background. The victims will start to be panic. The scammers will try to offer help by lodging the police report online. They will show the arrest warrant. That's the beginning of them transferring money to the scammer because they know they don't want to be charged." **Respondent 11**

E-Commerce Fraud

E-Commerce frauds take place on online shopping platforms, e-marketplaces, or social media. It aimed to deliberate misrepresentation of something with the goal of tricking another party into obtaining money. Victims are persuaded to pay for promised goods and services and invest in financial institutions. Holtfreter et al. (2008) found that individuals with a lack of control made purchases online more frequently, which may increase their risk of falling victim to online fraud.

Respondent 3 mentioned about the E-Commerce Fraud during the interview.

"For fraud victims, there are various types of fraud, e-commerce, buying goods, and so on. The victims have money and they want to get something from the internet yet they are cheated." **Respondent 3**

Respondent 11 and Respondent 13 also mentioned the E-Commerce scam along with other scam types.

"…E-Commerce (Online Purchase), Online Investment, Phone Scam (Macau Scam). Love scam…" **Respondent 11**

"…E-commerce, Online purchase fraud, Macau scam (Phone Scam), parcel scam, investment scam…" **Respondent 13**

Two cases that were listed in the police report serve as the basis for the proof of the modus operandi. The identified case numbers are R#12, R#13.

Case R#12 involves a purchase of a Bosch brand washing machine online through an advertisement seen on Facebook for the price of RM1,750.00. The buyer was provided with a tracking number after making the payment but later found that the tracking number was invalid. Subsequently, when attempting to contact again, the phone number had been blocked.

"…while browsing Facebook at home, I came across an account named EXXXXXXX EXXXXXXXXX, which advertised electrical appliances for sale. Intrigued, I initiated contact with the owner of the account, identified as 1/M Chinese, via messenger, expressing interest in purchasing a Bosch washing machine priced at RM1,750.00. Following discussions, I agreed to the purchase and proceeded to deposit the agreed amount into the seller's AmBank account (2XXXXXXXXXXX AXXX SXXX HXX BXXX). Subsequently, the seller provided a tracking number (EDP 334877896MY PosLaju). However, upon attempting to track the shipment, I discovered that the provided tracking number was incorrect. All attempts to contact the seller proved futile, as he had blocked me on messenger. Based on these circumstances, I believe I have been deceived. Therefore, I am filing this report to the police for their information and to pursue further actions, as I have suffered a loss of RM1,750.00…" **R#12**

Case R#13 involves the abuse of store information for scam purposes. All purchases are strictly online. If cash purchases are desired, one must visit the physical store. The information used includes the store name and registration number. No cash losses have been reported. The excerpt from the police report is provided below.

"I am writing on behalf of AXXX CXXXXXX SXXXXX (M) Sdn Bhd, located at No 2XX-2XX JXXXX KXXXX XX X, TXXXX PXX XXXX XX XX XXXX RXXXXX KXX XX XXX AXXX SXXXX in Kedah, to report an incident. Over the past few days, we have received complaints from individuals who claim to have made purchases from our store through an online platform. It's worth noting that our company requires customers to visit our premises for purchases, and all transactions are conducted in person. Upon investigation, I discovered that a Facebook account under the name MX EXXXXXXXXX has been operating a business using our store's address. Furthermore, the registration number provided by this account matches our company's registration number

(No: 8XXXXX-XX), albeit with different addresses. This leads me to suspect that someone may have forged documents for fraudulent purposes…" **R#13**

Cryptocurrency Investment Fraud

These scams take advantage of the growing popularity and potential profitability of cryptocurrencies to deceive investors and steal their funds. Respondent 2 repeatedly mentioned the involvement of the Cryptocurrency scams in Malaysia.

"And of course, the last thing is that what happens to this financial instrument in this e-wallet is cross border. You can easily convert from ringgit to Vietnamese Dong. Vietnamese Dong can be converted to RMB, and then RMB can be converted to whatever currency they want. Lastly, they will convert to cryptocurrency because there is an integration between each currency with cryptocurrency, in one e-wallet or three e-wallets. That's why the investigation will be tough." **Respondent 2**

Respondent 3 highlighted Cryptocurrency investment fraud during the interview, noting that many victims of investment fraud use cryptocurrency as the medium for scams. The use of cryptocurrency provides scammers with an easier means to conduct fraudulent activities, as authorities may have fewer trails to detect such activities.

"Most of the victims are involved with investment fraud cases, digital finance involving cryptocurrency investments". **Respondent 3**

Respondent 4, who is head of the investigation unit regarding cryptocurrency crime, commented that despite of what type of platform they are trading, including cryptocurrency, the negligence of the risk becomes the factor of the victimization.

"We don't care what type of platform victims are using, crypto or stock, of course, everyone wants to get rich. However, in terms of buying, our own attitude, being unmindful will open up for risks to be scammed. Those are the difference between greed and carelessness. If they are careless, they need to be careful and stop sharing information. Yet, for greed, I can't say much. They will say, lucky I only invested a little". **Respondent 4**

Ponzi Investment Scheme

Respondent 2 expressed the belief that Ponzi schemes are considered serious crimes, and he categorizes them within the classification of serious scams, alongside the Macau Scam," *…Online scam victims have many categories, the main scam category includes Macau scam and Ponzi scam…".* He also compared the Ponzi scheme to the investment fraud. Due to the nature of the scam, which involves building trust among the victims in order to obtain a bigger return, he confirmed the association of both scams," *Just to add, Ponzi is an investment scam. They like MLM or binary level systems. The binary level is interesting as they do nothing, but downlines will get income."*.

Respondent 12, who is experienced in multimedia crime, insisted that the department has listed out Ponzi scheme as one of the main online financial frauds. The department dealt with the cases regarding the involvement of multimedia and cybercrime. The Ponzi scheme is among the top online financial scams as it appeared to be the first out of the list.

"Multimedia PDRM has highlighted 6 main modus operandi of online financial scams. Firstly, Ponzi scam, second is love scam, next is e-commerce, e-financial crime, including phishing: business email compromise. Number 5, we have Non-Existence Loan and lastly, we have online investment scams." **Respondent 12**

The researcher has examined police reports thoroughly and found two examples related to the Ponzi scheme, which are R#7 and R#15. For R#7, a student came across an investment advertisement on the Telegram app offering a return of RM10,000.00 with an initial investment of RM1,000.00 within 3 hours. Without much consideration, the victim deposited money into the provided account. The excerpt is provided below.

"...I came across an investment opportunity on the Telegram application and then I contacted an individual named MXXXXXXXX RXXXX and was interested in taking the RM1,000.00 package that promised a return of RM10,000.00 after 3 hours. Subsequently, at approximately 1130 hrs, I transferred RM1,000.00 to the Bank Rakyat account under the name MXXX YXXXX with account number XXXXXXXXXX. Then, the individual asked for an additional RM3,000.00 as commission. At around 1500 Hrs, I transferred RM3,000.00 to the same account. After that, the individual requested another RM10,000.00 to activate my account, but I refused because I didn't have enough money. I requested a refund of my money, but he said he couldn't return it. Because of this, I went to the police station to file a report because I am dissatisfied with the individual. The total loss I experienced is RM4,000.00. This is my report." **R#7**

R#15 reported that he had been asked to pay a minimum of RM130.00 to join a healthcare plan. After transferring the money to the fraudster's account, he was invited to a WhatsApp group and was told that he needed to recruit additional members to double up his commissions. The commission will be given in accordance with how many new members are recruited. The excerpt is provided below.

"...I opened Facebook and found a message in my inbox from SXXXXXX GXXXX. In the message, he offered me a medical package and asked for a fee of RM130.00. I agreed and transferred the money to the given account, HXXX LXXXX BXXX (XXXXXXXXXX) under the name IXX CXXXXXX GXXXXX MXXXXXXXXX, and then I was added to a WhatsApp group. It was in this group that I learned about the program being run. I needed to recruit new members to earn commissions. I have been following this program, and I have invited my siblings and friends to join. Quite a few of them did. I managed to gather 94 people to join under me, and the program collected RM50,000.00 from these 94 people. Initially, the program was running smoothly. However, on XX/XX/XXXX around 2259 hrs, I found myself removed from the group, and my phone number was blocked by the group founder. I felt deceived. As a result, I have incurred a loss of RM7,000.00. The purpose of filing this report is to prevent any further undesirable incidents and to request the return of my money, as well as the money invested by my relatives and friends in the program. That concludes my report." **R#15**

Non-Existence Loan Scam

Non-Existence Loan scam has been discussed by Respondent 3 regarding the need to pay an upfront fee before receiving the borrowing funds. He insisted that in a few cases, the victims had already detected the abnormality of the transaction by depositing the money into the

individual account. However, they kept on with the transaction process to get the promised amount of money.

"For non-existent loan cases, victims make payments in advance, sometimes they pay lawyer's fees, and so on. For example, if they make a loan at an ABC Money Lending Company, a loan company, victims will then make payments to individual accounts; then, they should be aware that these payments are illegal transactions; why should they pay to personal accounts while dealing with the company." **Respondent 3**

The Non-Existence of Loan Scam was also discussed by Respondents 6 and 8 during the interview sessions.

"Pinjaman Tak Wujud (PWT) or non-existence loan, Macau scam, Love scam, Business Email Compromise (BEC) including phishing, few other modus operand (MO), and online shopping fraud." **Respondent 6**

"Macau scam, Ah Long, Pinjaman Tak Wujud (Non-Existence-Loan), parcel scam and e-commerce scam." **Respondent 8**

Respondent 13's observation about the evolution of non-existent loan scams into online platforms highlights the adaptability of scammers in the digital age. The use of online platforms allows scammers to carry out the same fraudulent schemes but with greater efficiency and reach. Victims can be targeted remotely, and the scams can be executed without the need for physical contact.

"Non-Existence Loan Scam through online platform. Traditionally, Ah-Long will need physical meetup to set up the approval process. Now, surely it can be carried out online" **Respondent 13.**

Improvement Procedure through Awareness

The discussion on this part mainly revolves around the improvement procedure of financial literacy for online financial scams. The interviews highlighted awareness, as depicted in Table 4.5 below.

Table 4.5
Improvement procedure through Awareness

Themes	Categories
Raising Awareness through various channel	• Utilization of Government TV channel • Radio and roadside signboard • Utilization of Social Media
Community-driven initiatives	• Online platforms such as Facebook, Twitter • Bolstering public safety and fostering social cohesion. • Tackle the underlying causes of crime • Fostering awareness about crime prevention methods
Targeted group exposure	• Empower individuals with knowledge, thereby boosting their confidence in avoiding scams
Confidentiality	• Data privacy protection • Banking information protection
Empowerment of Self Awareness	• Not taking things for granted and paying attention to the scams • Individual's introspective grasp of their thoughts, emotions, and actions • Individuals being vigilant and aware of their financial surroundings

Source : Developed by Author

According to Wilson et al. (2024), non-governmental entities, including community organizations and civil society groups, have the potential to enhance public safety by fostering awareness about crime prevention methods and tackling the underlying causes of crime, such as poverty, inequality, and social exclusion. Collaborating with government agencies and various stakeholders, these groups can formulate community-driven initiatives aimed at bolstering public safety and fostering social cohesion.

Respondent 2 commented that awareness involves public and private engagement, "*…involves public and private engagement where both of these engagements are required…".* Respondent 2 further explained that the enforcers have done campaigns on television. However, there are still victims being scammed "*…We have done some campaigns on TV related to financial literacy, but there are still people who are deceived…".* This comment implies the important of public awareness to heighten response efficacy among the victims. Respondent 4 echoed the statement by saying that the announcement has been made through social media, organized talks, as well as seminars for the targeted group.

"Police have been actively announced on social media, organizing talks and seminars for government staff and students". **Respondent 4**

To support the statement, Respondent 5 explained further that the awareness must be made visible to the targeted group "*…Public awareness can be improved through Facebook, social media, posters, social media, radio, television, roadside signboards where people are happy to see…".* Continuous exposure perhaps can help them to at least understand the scam itself.

Many online platforms can be utilized to make effective awareness campaigns. The campaign will empower individuals with knowledge, thereby boosting their confidence in avoiding scams.

Respondent 11 and 12 consistently emphasized the importance of enhancing awareness pertaining to the preservation of data privacy. The respondent emphasized raising awareness to increase self-efficacy and implementing additional steps to safeguard against scams while also highlighting the potential for cost savings, ensuring the protection of banking and financial information should be seen as a paramount concern. Previous research indicates that individuals who have a better understanding of privacy concerns feel more empowered to control their personal information (Youn, 2009). To have confidence in the effectiveness of security measures, internet users must first feel sufficiently informed about the available measures.

"We need to increase awareness. People have to be sure on how to protect data security about bank information, banking and so on." **Respondent 12**

"Confidentiality in banking information, we always say that we as account holders cannot share our account information including password and online banking to third parties, including our own siblings, husband and wife, parents." **Respondent 11**

Self-awareness involves an individual's introspective grasp of their thoughts, emotions, and actions. The idea of self-awareness itself has been supported by Respondent 2.

"Therefore, private people need to work with people who are outside the group to inform them what is going on and to create self -awareness among them. When public and private awareness occurs, those in the "self -awareness category" will see the information and will be more aware of its impact on their finances, and what types of fraud occur. Thus, they can avoid falling victim to fraud." **Respondent 2**

Respondent 7 emphasized the importance of individuals being vigilant and aware of their financial surroundings. Awareness of protective tools was linked to a heightened perception of the mechanism's effectiveness. These results align with the findings of Hanus and Wu (2016) in their examination of desktop security behavior. Individuals who are not alert and proactive in safeguarding their finances may fall victim to scams, resulting in significant financial losses.

"That is why they need to be alert to their surroundings. Otherwise, they may lose everything they worked for due to their negligence. Moreover, some people are good at managing their finances, but at the same time, they become greedy." **Respondent 7**

Public awareness and self-awareness can intersect and influence each other. Individuals who possess a high level of self-awareness may contribute to public awareness by sharing their perspectives, experiences, and insights. Conversely, public awareness initiatives can promote and encourage self-awareness by prompting individuals to evaluate their beliefs, biases, and assumptions critically.

Respondent 10 believed that by not taking things for granted and paying attention to the scams, especially conducted by the CCID, one can reduce the tendency to become a scam victim.

"So, they need to have the self-awareness and understand about the scam. They need to know about it. Bear in mind that if somebody asked for the money, please refuse it ". Respondent 10

Conclusions and Recommendations

This study uncovers two distinct levels of financial literacy among the victims, ranging from high to low. It is noticeable that victims with high financial literacy levels fall for scams as these victims' displayed adeptness in financial management and possessed knowledge of effective investment strategies. Despite their high level of financial literacy, these victims may become victims due to a false sense of confidence in their ability to make informed financial decisions. According to the Protection Motivation Theory, financially literate victims may accurately perceive the severity of online financial scams yet still fall victim to them due to their perceived financial competence. Individuals with good financial knowledge may be vulnerable to scams due to the deceptive tactics employed by scammers.

On the other hand, victims with low levels of financial literacy often lack exposure to key components of financial literacy, such as debt management, income handling, and investment knowledge. This finding is consistent with the OECD's (2024) report, which highlights low financial literacy across various economic levels. A low level of financial literacy implies a lack of understanding of fundamental financial concepts, including debt management, income handling, behavioral aspects, and attitudes. Consequently, individuals with low literacy levels may struggle to make sound financial decisions. James et al. (2014) discovered that as financial literacy (FL) decreases, experiences of victimization increase. Similarly, study by Sukumaran (2015) suggest that low financial literacy level correlates with financial exclusion and speculate that a lack of understanding of financial systems and concepts makes individuals more vulnerable to economic exploitation. According to the Protection Motivation Theory, this vulnerability may include practices such as high-risk lending and accumulating debt. Based on these connections, researchers infer that financial literacy can influence victimization. This vulnerability can be attributed to their limited comprehension of financial instruments, leading to uninformed financial choices.

Five types of online scams commonly happen in Malaysia, which includes the Macau Scam, E-Commerce Scam, Crypto Currency Scam, Ponzi Scheme Scam, and Non-Existence Loan Scam. These scams are actively reported in Malaysia despite authorities' efforts to combat them. Most victims are unable to detect the scams they are experiencing due to limited knowledge and the constantly changing modus operandi. They only become aware of it when it involves financial loss.

The study emphasizes the effectiveness of awareness campaigns as a proven method to enhance the financial literacy level of victims and, by extension, the broader Malaysian population. These campaigns are designed to provide ongoing education to targeted groups, fostering greater understanding and exposure. However, there was limited assessment of its effectiveness in preventing or reducing fraud. Many parties involving enforcers, such as police

officers and policymakers, are encouraged to actively participate in spreading awareness initiatives. Furthermore, media channels can significantly contribute by ensuring the continuous visibility of awareness advertisements through platforms like television, newspapers, and online portals. This collaborative approach aims to empower individuals with the necessary knowledge and skills to make informed financial decisions and mitigate the risk of falling victim to scams.

This research offers significant contributions in theoretical, methodological, and practical aspects. This research builds on an established base in Protection Motivation Theory (PMT) to provide a robust theoretical foundation for understanding the complex interplay between financial literacy and victimization, which extends its application to the context of victimization in Malaysia. This study not only complements the theoretical literature but also advances methodological approaches in qualitative research. By focusing on short-lived and transient phenomena, such as the experience of scam victims, the study demonstrates the versatility of qualitative methods in capturing complex and dynamic social processes, which demonstrates the effectiveness of qualitative research in exploring phenomena that may not be adequately captured by quantitative approaches alone. The practical contributions of this research are significant, given the growing prevalence of online financial scam victimization, emphasizing the need to address these issues in educational curricula to include in school, awareness campaigns for policymakers, as well as an understanding of scam techniques by law enforcers. The future research recommends examining how personal values influence susceptibility to online scams, shaping risk perception and motivation for protective behaviors to inform effective prevention strategies.

References

Abbott, J., & McGrath, S. A. (2016). The effect of victimization severity on perceived risk of victimization: Analyses using an international sample. *Victims & Offenders, 12*(4), 587–609. https://doi.org/10.1080/15564886.2016.1208130

Alam, M. K. (2020). A systematic qualitative case study: Questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management*: *An International Journal, 16*(1). https://doi.org/10.1108/QROM-09-2019-1825

Aziz, N., & Kassim, S. (2020). Does financial literacy really matter for Malaysians? A review. *Advanced International Journal of Banking, Accounting and Finance, 2*, 13–20. https://doi.org/10.35631/AIJBAF.22002

Chariri, A., Sektiyani, W., Nurlina, N., & Wulandari, R. W. (2018). Individual characteristics, financial literacy and ability in detecting investment scams. *Jurnal Akuntansi Dan Auditing, 15*(1), 91–114.

Clarke, V., & Braun, V. (2013). *Successful qualitative research: A practical guide for beginners*.

Engels, C., Kumar, K., & Philip, D. (2019). Financial literacy and fraud detection. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3308537

Flick, U. (2018). *An introduction to qualitative research*. Sage.

Gathergood, J., & Weber, J. (2017). Financial literacy, present bias and alternative mortgage products. *Journal of Banking & Finance, 78*, 58–83. https://doi.org/10.1016/j.jbankfin.2017.01.022

Gibbs, G. (2002). *Qualitative data analysis: Explorations with NVivo*. Open University.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*, 2–16. https://doi.org/10.1080/10580530.2015.1117842

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Huston, S. J. (2010). The concept and measurement of financial literacy: Preliminary results from a new survey on financial literacy assessment. *Conference Presentation*, Academy of Financial Services Annual Conference, Anaheim, CA, October 9.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Susceptibility to scams scale. *PsycTESTS Dataset*. https://doi.org/10.1037/t62359-000

Kumar, V. V., & Kumar, J. S. (2023). Insights on financial literacy: A bibliometric analysis. *Managerial Finance, 49*(7), 1169–1201. https://doi.org/10.1108/mf-08-2022-0371

Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing* (2nd ed.). Sage Publications, Inc.

Lusardi, A., & Mitchell, O. (2007). Financial literacy and retirement preparedness: Evidence and implications for financial education. *Business Economics*, 35–44.

Mahadin, M. U. (2021). Malaysia demographic statistics first quarter 2021. Department of Statistics Malaysia. https://www.dosm.gov.my/v1/index.php

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey Bass.

Mohamad, R. K., Osman, Z., Ismail, Z., & Mohamad, L. (2024). Exploring Gender's True Impact on Financial Management Behaviour. *International Journal of Academic Research in Accounting Finance and Management Sciences, 14*(3). https://doi.org/10.6007/ijarafms/v14-i3/22273

MyCert. (2024). *Reported incidents based on General Incidents Classification Statistics 2023*. https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932

OECD. (2024). *PISA 2022 results (Volume IV)*. https://www.oecd-ilibrary.org

Sabri, M. F., & Zakaria, N. F. (2015). The influence of financial literacy, money attitude, financial strain and financial capability on young employees' financial well-being. *Pertanika Journal of Social Sciences and Humanities, 23*(4).

Salleh, M. B. (2022, August 5). PDRM: Over RM5.2 billion lost to scams in two years. *The Edge Malaysia.* Retrieved October 30, 2024, from https://theedgemalaysia.com/article/pdrm-over-rm52-billion-lost-scams-two-years

Savin-Baden, M., & Howell Major, C. (2013). Qualitative Research: The Essential Guide to Theory and Practice (1st ed.). Routledge. https://doi.org/10.4324/9781003377986

Statista. (2023). *Share of internet users who use online banking Malaysia 2022*. https://www.statista.com/statistics/788561/share-of-internet-users-who-use-online-banking-malaysia/

Strauss, A. L. (1987) Qualitative Analysis for Social Scientists. Cambridge University Press, New York. http://dx.doi.org/10.1017/CBO9780511557842

Sukumaran, K. (2015). Financial literacy -- Concept and practice. *DAWN: Journal for Contemporary Research in Management*, 59–65.

Venkatesan, T., & Venkataraman, R. (2018). Analysis of factors determining financial literacy using structural equation modelling. *SDMIMD Journal of Management, 9*(1), 19–29.

Vijay Kumar, V. M., & Senthil Kumar, J. P. (2023). Insights on financial literacy: A bibliometric analysis. *Managerial Finance, 49*(7), 1169–1201.

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime, 31*(5), 1140–1155. https://doi.org/10.1108/JFC-06-2023-0151

Yin, A. C. P. (2022, September 19). Securities Commission: 25% increase in reports of investment scams during COVID-19. *RinggitPlus.* https://ringgitplus.com

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x