Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Exploring the Prevalence of Online Fraud Through Social Media in Malaysia

Nor Athiyah Abdullah[1], Siti Hazyanti Mohd Hashim[2*], Lim Kai Heng[3]
1,2 ,3 School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia
Corresponding author. E-mail address: sitihazyanti@usm.my

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Introduction: Social media and private messaging apps are crucial in Malaysia's daily lives, with a population of 32.98 million and 29.55 million users in 2022. However, these platforms have become effective tools for targeting Malaysians for online fraud, with over 90,000 cases from 2017 to 2021 resulting in losses totalling RM3.3 billion. Many Malaysians have been victims, causing psychological problems and additional losses

Objectives: This study aims to identify factors contributing to online fraud, increase awareness among Malaysians, investigate victim experiences on social media, and determine prevention solutions.

Methods: The research uses questionnaires and literature reviews to provide guidelines for authorities to act on online fraud

Results: Results show that factors such as extra income, purchasing products online at a cheaper price, scammers pretending to be trusted, and high salary offers contribute to online fraud. The results can help authorities make better decisions about acting and informing Malaysians about online fraud.

Conclusions: The government, MCMC, family, friends, partners, and colleagues can help increase awareness. Additionally, not sharing sensitive personal information, downloading unverified apps, clicking on suspicious links, and responding to unsolicited calls or messages can help prevent online fraud.

Keywords: Social media, Online fraud, Awareness of online fraud

INTRODUCTION

Every aspect of Malaysian life, from work and leisure to socialising and business, is impacted by social media and private messaging applications. With a total of 32.98 million users in January 2022, or 91.7% of the country's population. Malaysians have reason to be proud of the effectiveness and efficiency of social media platforms (Kemp 2022) Texting, social networking, video viewing, voice and video chatting, and information gathering were the top five internet activities in 2020, according to a poll by the Malaysian Communications and Multimedia Commission (MCMC) (Malaysian Communications and Multimedia Commission 2020).

The COVID-19 epidemic and lockdown have increased internet use and online shopping to carry out everyday tasks and meet basic necessities. The newest COVID-19 Standard Operating Procedure (SOP), current information, work, study, purchase basic necessities, socialise, and more have led to a meteoric rise in internet and social media use among Malaysians (Malaysian Industrial Development Authority 2020) Cybercrime is on the rise in tandem with the proliferation of online information sharing (McKinsey & Company 2022). This means that fraudsters are finding more and more ways to use social media and private chat applications to facilitate online fraud. Scammers prey on Malaysians using social media and messaging applications, committing online fraud for their own gain. Scammers in Malaysia conduct a wide variety of online fraud crimes, including frauds involving social networking, romance, employment, job modelling, investments, and more (David 2022).

The prevalence of many forms of online fraud, which is difficult to prevent, has made it a hot subject in Malaysian media and online communities. Data from the Bukit Aman Commercial Crime Investigation Department (CCID) shows that the number of incidents of internet fraud has surged by 60.6% in the last decade (Bernama 2021). Moreover, between 2017 and 2021, the Bukit Aman Commercial Crime Investigation Department (CCID) uncovered almost 90,000 instances of internet fraud, with a total loss of RM3.3 billion (The Star 2022). Scammers' ease in taking advantage of Malaysians is evident. The increasing number of Malaysians falling prey to online fraud puts their mental health at risk, not to mention their bank accounts and other financial resources. More than 46% of Malaysians surveyed by telecom firm Telenor Group said they had fallen prey to internet fraud sometime in the past. Because of their lack of education about internet fraud and inadequate social media security measures, most Malaysian residents are easy prey for con artists. Numerous measures and investigations are required to forestall the perpetuation of online fraud in Malaysia, given the alarming increase in both the number of victims and reporting of such incidents. Therefore, this research aims to identify the main variables that contribute to online fraud, find out how informed Malaysians are about online fraud, look at victim experiences on social media, and find out how to avoid online fraud.

LITERATURE REVIEW

This section primarily discussed previous research on online fraud, with a focus on the use of social media platforms and the efforts to increase awareness about online fraud.

2.1 Social media and private messaging apps

Social media and private messaging apps have increased users rapidly because it brings a lot of conveniences to people's lives and makes people's lives where people stay connected online, entertainment and information exchange. These platforms allow easy access to news, communication, product promotion, and content sharing worldwide. According to Global social media statistics research 2022, 4.7 billion users, 59% of the global population, engage on social media (Chaffey 2022). In Malaysia, social media and private messaging apps play an essential role in Malaysians' daily basis in business, entertainment, socializing, working, and more. Malaysians can take pride in social media and private messaging apps' proficiency with a population of 32.98 million because there were 30.25 million users in January 2022 which is 91.7 percent of the total population in Malaysia (Asia Pac 2022). Due to the COVID-19 pandemic and lockdown, social media and private messaging apps became tools that people constantly use to share information. Social media's speed in spreading information led to increased usage, aiding Malaysians in staying updated, working, and socializing (MIDA 2020). Yet, this surge also amplified online fraud, with scammers exploiting social media's reach. This rise in fraud causes psychological distress, financial losses, and other issues for users.

2.2 Online fraud

Online fraud, a form of cybercrime, exploits the internet to defraud individuals through tactics like fake tech support calls, phishing emails, deceptive websites and more (Norton 2022). It spans malware attacks, email schemes, and phishing attempts, targeting sensitive data and money (National Crime Victim Law Institute 2010). Social media and private messaging apps are used by billions of users around the world. According to Wira Prabowo Madjid, he mentioned that Southeast Asia is one of the biggest regional social media users around the world (Madjid 2021). In 2022, Facebook is the most famous social media apps in all Southeast Asian countries (statista 2022). In Malaysia, there are many social media and private messaging apps used by Malaysians daily such as WhatsApp, Facebook, Twitter, Messenger, Instagram, and Telegram (CK Wong 2018). Scammers leverage these social media and private messaging apps due to their accessibility and affordability. The Royal Malaysia Police reported a total of 71,833 scams, amounting to more than RM5.2 billion losses, was reported in two years in Malaysia (Salleh 2022). In Singapore, the police mentioned that the scam victims lost more than $633.3 million in 2021 which cause the sum total loss to be almost 2.5 times in the previous year (David Sun 2022). In Thailand, the Office of the National Economic and Social Development Council (NESDC) pointed out that the online scams in Thailand increase rapidly, so the scam victims lost more than THB 1 billion (The Nation 2022).

2.3 Familiarity, Trust and Awareness towards online fraud

Jusoh, W.N.H.W., and Nizar, N.M.S., 2022, examined the awareness of Malaysian Muslim university students about scams. The survey aimed to gauge risk understanding, including consumer awareness during online transactions. The results of Jusoh, W.N.H.W., and Nizar, N.M.S., 2022, showed that:

i. Most students are aware of online scams.
ii. Most students have a good understanding of the types of online fraud in Malaysia.
iii. Most students know how to differentiate between original calls and scam calls.
iv. Many students know how to respond to calls from strangers.
v. Most students do not share personal details easily with strangers.
vi. Many students do not easily make friends with strangers.
vii. Most students do not trust the profile images of strangers on social media platforms.

The study highlighted that most Malaysian Muslim female university students have a high awareness level of online fraud because most of them use religion when using the Internet. However, it is an imbalanced sample size as the female has 158 respondents, which equals 80.6% of respondents, while the male has 37 respondents, which equals 19.4% of respondents.

In addition, Zahari, A.I., Bilu, R., and Said, J., 2019, identified the main factors that contribute to online purchases from the experience of online fraud victims. The study was highlighted that;

i. Familiarity with sellers boosts trust, as higher familiarity correlates with increased trust levels.
ii. Trust in sellers impacts online purchase intentions, as it underpins buyer-seller relationships.
iii. User awareness of online shopping shapes perceptions and influences purchase intent.
iv. Customer confidence in sellers affects purchase intent and is tied to belief in product delivery.

The authors also discussed the impacts:

i. Familiarity affects purchase intent, often high and reduced for specific websites
ii. Trust is vital, influenced by familiarity, building trust with online sellers
iii. Awareness of cybercrime risk is initially low but increases after becoming a victim
iv. Confidence is tied to product knowledge, influencing purchase decisions

The conclusion is that familiarity, confidence, and trust affect e-commerce trustworthiness. Awareness is lacking among fraud victims. However, the study's limited sample size (7 phone interviews) does not conclusively establish the relationship between familiarity, confidence, trust, and e-commerce trustworthiness.

2.4 Common types of online fraud on social media and private messaging apps in Malaysia

There are some common types of online fraud on social media and private messaging apps with major factors in Malaysia as follows:

i. BigPay scam

BigPay is a mobile payment app under AirAsia's parent company Capital A Berhad, offers a versatile virtual prepaid card enabling global spending, transfers, bill payments, and more (BigPay 2019). Thus, the scammer takes advantage of the features in BigPay app for their benefit. Scammers impersonate BigPay employees to send a fake BigPay employee ID and contact the BigPay users through WhatsApp (BigPay 2020). By using WhatsApp, scammers can use unknown phone numbers to perform unsolicited calls. Scammers ask and get login links, one-time passwords, bank account details, identity card numbers, and personal information from the BigPay users by using the excuses. Although BigPay gives the warnings, scammers still have not given up on this tactic and continue to commit online fraud (malay mail 2020).

ii. Lottery and Prize scams

Lottery and Prize scams deceive victims by falsely claiming they've won without participating (Scamwatch Radar n.d.). Scammers use the excuses for the fees like taxes or insurance to exploit victims, collecting money and delaying payouts. To claim prizes, victims share personal info and transfer fees, only to receive fake checks. Deposited checks bounce, leaving victims with losses, and scammers with personal data for identity theft and account misuse. Pahang Commercial Crime Investigation Department head mentioned the victim claimed he transferred more than RM65, 000 to a scammer who claimed was able to predict the lottery number that would win him RM1.1 billion (Bernama 2021).

iii. Online shopping scams (Social commerce fraud)

Online shopping scams are one of the most famous online fraud cases because most scammers use the anonymous nature of the internet to trap shoppers. It involves scammers pretending to be online sellers, selling the products on social media platforms, or using a fake shopping website or a fake advertisement on an authorized retailer site (Scamwatch Radar n.d.). Scammers use social media platforms, fake websites, or fake advertisements to promote products or services. Once the victim sends money for products, they may receive fake products or never receive their ordered products. According to the Inspector-General of Police, he mentioned that there were 8,162 online shopping scams involving losses totaling RM58 million from January to October 2021 (Perimbanayagam 2021).

iv. Job scams (Employment scams)

Job scams, also known as employment scams, are common online fraud cases that happened in Malaysia and South-East Asia countries. Job scams come in the form of work-from-home jobs, home-based jobs, work-abroad jobs, and more. Scammers attract victims with enticing pay and minimal effort on platforms like job sites and social media (Jobstore 2021). During the COVID-19 pandemic and lockdown, job scams increased rapidly in Malaysia because many Malaysians lost their jobs and income. Scammers have taken advantage of increased unemployment rates and new opportunities during the COVID-19 pandemic and lockdown to advertise fake job listings to desperate job seekers. Malaysia's Commercial Crime Investigation Department reported RM4.6 million losses from job scams from January to August 2021 (malay mail 2021). In 2022, many job seekers are being lured by offers of high pay in the countries like Cambodia, Thailand, and Myanmar through the job opportunities overseas via social media platforms (TheStar 2022).

v. Romance scams (Catfish crimes or Internet love scams)

Romance scams, also known as catfish crimes, are also common online fraud cases that happened in Malaysia by targeting single or lonely individuals online through social media, private messaging, and dating apps (Natalie Khoo 2022). These romance scammers use attractive profile pictures on social media to win their victims hearts and gain their trust by building fake relationships. After they have established trust, scammers request money from their victims for travel expenses, fees, personal crises, or other emergency expenses. Some scammers may do so as an attempt at manipulation, revenge, or entertainment rather than for money. According to the Royal Malaysia Police (PDRM), the cases of romance scams are on the rise nationally because the data shows a total of 1,535 love scams reported in 2019 and a total of 1,535 love scams reported in 2020 (Akmal Hakim 2021).

vi. Modeling scam

Modeling scams commonly target females, but they could affect anyone, regardless of gender (KSChang 2022). Scammers may pretend to be a modeling agency, photographer, and more that can offer them a casting or modeling job with higher pay and no experience needed. Scammers may send the requirements and details about the modeling job through WhatsApp, Facebook, Messenger, or Instagram and then proceed to request an amount of money for securing the job or ask for nude photos for the portfolio. After receiving nude photos, they threaten the victims and use these photos for their own benefit. According to Joanna Joseph, she found that many women have fallen prey to these scammers because scammers are using the high-paying modeling job to attract them to capture the required poses in photos (June 2022).

vii. Investment scams (Money games / Cryptocurrency investment)

Investment scams are one of the most famous online fraud cases that promise big payouts, quick money, or guaranteed high returns without any risks (Moneysmart n.d.). Common investment scams include cryptocurrency scams, money game scams, Ponzi schemes, celebrity endorsement scams, and more. Most scammers used cryptocurrency and forex investment scams to trap victims during the COVID-19 pandemic. The government of Malaysia allows the members to withdraw RM10,000 in the Employees Provident Fund account, so scammers have taken this opportunity to target the EPF members for their investment scams. The Securities Commission Malaysia (SC) found that most scammers use the messaging application Telegram to promote and perform investment scams (The Malaysian Reserve 2022). They also received more than 2000 complaints about illegal investment schemes or scams in September 2021 (The Malaysian Reserve 2021) .To avoid scams: (1) Beware of easy money offers, (2) Be cautious with personal info requests from strangers, (3) Skepticism towards offers for little effort, and (4) Watch for untraceable employers.

viii. Online romance scams (Catfish crime / Internet love scams)
Shaari, A.H., Kamaluddin, M.R., Fauzi, W.F.P., and Mohd, M., 2019 discuss the pattern of deceptive language and strategies used in online romance scams in Malaysia. The Scammers Persuasive Techniques Model outlines seven steps which are to create attractive accounts and send friend requests, build trust by sharing stories and showing interest in victims' backgrounds. Third is develop a hyper-personal relationship by sharing personal information. Fourth, manipulate victims' emotions to focus on the relationship. Five, request small amounts of money. Six is playing different roles, and seven is request larger sums, lowering the amount if needed (Monica T Whitty 2015). Brown, P., Levinson, S.C., and Levinson, S.C., 1987 identified three stages for Online Romance Scams. Initial stage is scammers create attractive profiles, build relationships, and gather victim information. The Pre-attraction stage, scammers use romantic communication to build trust and emotional connection, and last stage - scammers execute the scam, requesting money using various excuses. The authors also highlight strategies specific to romance scams involving Malaysian victims which are use local names and places, associate with well-known companies and use local languages and religious references.

Besides that, Jumrah, M.H., Hossin, A., and Nissanto, N., 2019, explore catfish crime among single mothers in Kota Kinabalu, Sabah. Catfish crime involves individuals using fake identities to exploit victims in cyber-love scams. The result highlights that Facebook is the main communication tool for catfish and victims due to its accessibility. There are two main factors contributing to catfish crime which are social environment and interpersonal attraction. The Social environment themes include silence, mass media, partners, and self-esteem. Interpersonal attraction themes encompass physical attraction, the introductory period, ability, and equation attractiveness. Catfish analyze victims' backgrounds and personalities before ensnaring them and the Catfish create comfortable conversation patterns to lure victims, particularly single mothers.

In addition, the paper by Hamsi, A.S., Bahry, F.D.S., Tobi, S.N.M., and Masrom, M., 2015 discusses ethical theories of the Kantianism, Social Contract Theory, Rule and Act Utilitarianism that collectively agree on the moral wrongness of online love scams, which breach cyber laws. There are some interconnecting factors and solutions highlighted which are misuse of student visas for scams, requiring collaboration between embassies, the National Police, and the Immigration Department. Second is an anti-fraud companies using advanced technology to track financial identity fraud. Third is stricter financial security measures to prevent fraud. Forth is review and enhancement of Cyber Law Acts by the Malaysian Government; and five is an imposition of limits and controls on internet access. Despite these proposed solutions, internet love scam cases continue to rise in Malaysia, highlighting a gap between theory and implementation.

2.5 Online shopping scams (Social commerce fraud)

Romero (2020) examines social commerce fraud in Malaysia, where scammers exploit social media platforms due to low startup costs, direct buyer connections, and instant payments. The study suggests preventive measures such as researching sellers, prioritizing registered companies, reviewing buyer feedback, ensuring transparency, using secure platforms, and opting for cash-on-delivery. However, the study's limited demographic with 92.6% female and predominantly Malay restricts generalizability across Malaysia's diverse population. Okorie et al. (2020) focus on preventing social media scams in Singapore, recommending user precautions like verifying payments, using secure networks, installing antivirus software, and educating users. Additionally, they propose broader anti-fraud measures, including targeted prevention campaigns, affordable detection programs, international collaboration, frequent anti-fraud campaigns, and enhanced government training. Despite these efforts, Okorie et al. (2020) acknowledge that scammers continuously adapt, making it challenging to curb the rising number of online fraud cases in Singapore.

METHODS

In this study, a quantitative method has been used and applied in exploratory research as primary data. The purpose of quantitative research is to have a better understanding of the social world through primary data (questionnaire surveys) and secondary data. The primary data for this study is collected using a questionnaire because the questionnaire can reach many respondents, save costs and time, and collect the data, it brings convenience for statistical processing and analysis, and the results can be easy to quantify. The study has used convenience sampling because it is best used for exploratory research. Therefore, an online questionnaire survey will be distributed to Malaysians who use social media and private messaging apps online. Besides that, the secondary data for this study will be gathered data and information from various resources. The secondary data can help the researcher to have a better understanding of the factors that contribute to the latest online fraud.

There are some steps that have been utilized to lead this study (Fig. 1.). Firstly, the initial step is to identify the problems of the research on online fraud via social media, and then the research can define the scope, research questions, and research objectives based on the identified problems. Next, the researcher needs to start collecting secondary data by reviewing journal papers, newspapers, articles, and more on online fraud via social media, so it can help identify the research gaps in the previous research that reviewed the existing literature. Then, the researcher will use Google Forms to design an online questionnaire survey to collect the primary data from the targeted Malaysian respondents through social media and private messaging apps. After that, the researcher will conduct a pilot study to assess the validity and reliability of the tool for the study. The gathered data will be analyzed using statistical data analysis tools like the Statistical Package for the Social Sciences (SPSS). Based on the results, guidelines for this study will be proposed. Finally, the researcher will discuss the findings and provide some future recommendations for future research.

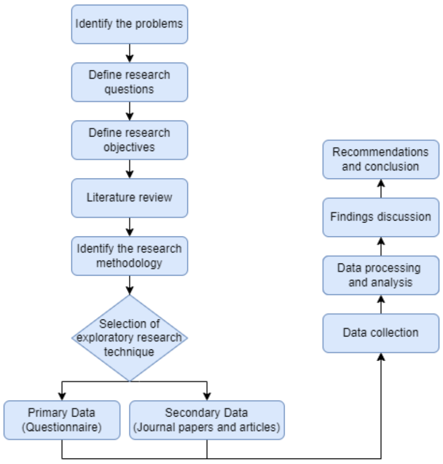
Identify the problems
Define research questions
Define research objectives
Literature review
Identify the research methodology
Selection of exploratory research technique
Primary Data (Questionnaire)
Secondary Data (Journal papers and articles)
Data collection
Data processing and analysis
Findings discussion
Recommendations and conclusion

Fig. 1. The research process of this study

RESULTS

4.1 Demographic profile

The questionnaire is designed on Google Forms and distributed to a total of 150 Malaysian respondents who are on social media or private messaging apps. There are eight respondents who provided invalid responses in this study because they answered they had been contacted by scammers while the respondents answered they did not face online fraud on social media or private messaging apps, which causes invalid data and responses. Due to invalid data and responses, eight records were deleted during the pre-processing. The questionnaires were collected from 142 respondents as shown in Table 1 below.

Table 1: The demographic profile of this study

Demographic Profile (N=142)	Frequency	Percent %
Gender		
Male	68	47.9%
Female	74	52.1%

The questionnaire is distributed to 150 Malaysians who are social media or private messaging users. From Table 1, it shows the respondents who took part in the questionnaire were 47.9% male and 52.1% female.

4.2 Analysis on the awareness of online fraud

In this section, descriptive statistics were used to summarize respondents' awareness of online fraud, utilizing a 5-point Likert (1 = Strongly Disagree, 5 = Strongly Agree). Table 2 displays the results for seven questions regarding online fraud awareness. The mean scores ranged from 3.47 to 3.91, indicating a generally high level of awareness among Malaysian social media users. Standard deviation values between 0.837 and 1.183 suggest the data is normally distributed with moderate variability. Overall, the descriptive analysis shows that most respondents agree with the statements about online fraud, demonstrating a strong awareness of the risks when using social media and private messaging apps.

Table 2: The descriptive analysis on the awareness of online fraud

Questions on the awareness of online fraud (N=142)	**N**	**Min**	**Max**	**Mean**	**Std. Deviation**
Q1. I am aware of online fraud on social media or private messaging apps.	142	1	5	3.77	0.837
Q2. I am aware of the latest online fraud on social media or private messaging apps.	142	1	5	3.47	1.070
Q3. I do not easily be friends with strangers on any social media or private messaging apps without finding out first.	142	1	5	3.71	1.095
Q4. I do not easily provide my personal information to a stranger on social media or private messaging apps.	142	1	5	3.91	1.024
Q5. I do not easily respond to unsolicited calls or messages from strangers on any social media or private messaging apps.	142	1	5	3.70	1.103
Q6. I do not easily trust strangers on any social media or private messaging apps.	142	1	5	3.77	1.027
Q7. Awareness of online fraud can help to prevent becoming an online fraud victim on social media and private message apps.	142	1	5	3.62	1.183

In Table 3, it shows the role that can be played in raising awareness of online fraud based on the multiple selections made by the respondents. The result shows that more than half of the respondents have selected the government of Malaysia and the Malaysian Communications and Multimedia Commission (MCMC), Family, Friends, Partners, and Colleagues because they can help raise awareness of online fraud. And also, the result shows that 38.7% of the respondents selected the Royal Malaysia Police (Polis Diraja Malaysia) and 20.4% of the respondents selected the Non- Governmental organization (NGO), which can help to conclude that the Non-governmental organization (NGO) has a minority chance compared to other roles that can help in raising awareness of online fraud. In short, the government of Malaysia and the Malaysian Communications and Multimedia Commission (MCMC), Family, Friends, Partners, and Colleagues are playing a vital role that can help increase awareness of online fraud.

Table 3: The role that can help in raising awareness of online fraud based on the multiple selections

The awareness of online fraud (N=142)		Frequency	Percent %
In your opinion, who are playing a vital role that can help in raising awareness of online fraud?	The government of Malaysia	85	59.9%
	Malaysian Communications and Multimedia Commission (MCMC)	75	52.8%
	Royal Malaysia Police (Polis Diraja Malaysia)	55	38.7%

	Family	75	52.8%
	Friends, Partners, and Colleagues	76	53.5%
	Non-Governmental Organisation (NGO)	29	20.4%

4.3 Analysis on the prevention solutions to online fraud

Most respondents rely on newspapers, magazines, social media, and private messaging apps for online fraud prevention solutions, indicating that these platforms are effective for rapidly sharing information with the public. Key preventive measures include avoiding sharing sensitive information, not downloading unverified apps, not clicking on suspicious links, and ignoring unsolicited messages or calls. Additionally, most respondents agree that the Malaysian government, the Malaysian Communications and Multimedia Commission (MCMC), and the Royal Malaysia Police play crucial roles in preventing online fraud. Facebook, preferred by 88.7% of respondents, is identified as the most suitable platform for sharing prevention solutions due to its wide usage, with Instagram also seen as effective by 62%. These platforms can help reduce the number of social media users falling victim to online fraud.

Table 4: The results of prevent solutions that can help to reduce online fraud cases

The prevention solutions to online fraud (N=142)		**Frequency**	**Percent %**
Which source did you get the prevention solutions to online fraud?	Radio	52	36.6%
	Newspaper and magazines	72	50.7%
	Television	62	43.7%
	Official websites	61	43%
	Social media and private messaging apps	109	76.8%
	Peers or family members	1	0.7%
In your opinion, what type of prevention or solutions can help to prevent and solve the problems of online fraud on social media or private messaging apps?	Install and connect the Virtual Private Network app (VPN)	38	26.8%
	Install and use the Mobile Antivirus Protection app	37	26.1%
	Browse on authorized websites only	62	43.7%
	Do not share sensitive personal information with anyone	97	68.3%
	Do not download unverified apps on social media and private messaging apps	72	50.7%
	Do not click on suspicious links	98	69%
	Do not respond to unsolicited calls or messages	89	62.7%
	Improve Cyber Law Acts	62	43.7%
In your opinion, who is playing a vital role in helping to prevent online fraud?	The government of Malaysia	98	69%

	Malaysian Communications and Multimedia Commission (MCMC)	97	68.3%
	Royal Malaysia Police (Polis Diraja Malaysia)	70	49.3%
	Non-Governmental Organisation (NGO)	43	30.3%
	Influencers	33	23.2%
	Social media apps	1	0.7%
	Family	1	0.7%
	Self	1	0.7%
In your opinion, which type of social media or private messaging app is suitable for sharing the prevention solutions to online fraud?	Facebook	126	88.7%
	Messenger	32	22.5%
	WhatsApp	49	34.5%
	Instagram	88	62%
	Telegram	31	21.8%
	Twitter	63	44.4%
	Tiktok	2	1.4%
	Douyin (China Tiktok)	2	1.4%
	RED (Xiaohongshu)	1	0.7%

Table 5 highlights the reasons for using social media and private messaging apps, as well as the factors contributing to online fraud based on respondents' multiple selections. Most respondents use these apps for socializing, entertainment, and staying updated with news, with 56.3% engaging in online shopping, 24.6% seeking job opportunities, and 15.5% using them for dating. The table also reveals key factors contributing to online fraud, such as the lure of easy money, cheaper online purchases, scammers impersonating trusted individuals, and high salary offers. Identifying these factors can assist the Malaysian government and Royal Malaysia Police in better understanding and addressing the causes of online fraud.

Table 5: The results of prevent solutions that can help to reduce online fraud cases

The factors contributing to online fraud (N=142)		Frequency	Percent %
What are the reasons that you use social media and private messaging apps?	Socializing	109	76.8%
	Entertainment	112	78.9%
	Dating	22	15.5%
	Online shopping	80	56.3%
	Jobs	35	24.6%
	Latest news and information	88	62%
In your opinion, what are the factors that may contribute to online fraud?	To earn extra income (easy money)	93	65.5%
	Purchase the products online at a cheaper price	90	63.4%
	Scammers pretend to be someone I know and trust	78	54.9%

	Lottery, sweepstakes and competition scams	42	29.6%
	High salary job offer	52	36.6%
	Find a partner for a relationship	41	28.9%
	Lack of knowledge	1	0.7%

Table 6 presents the types of online fraud experienced by respondents on social media or private messaging apps. The most common scams include online shopping scams (42.9%), investment scams (31.6%), lottery and prize scams (27.6%), and job scams (28.6%). Other scams, such as romance scams (13.2%), modeling scams (11.2%), Big Pay scams (3.1%), and fake mobile apps or online game scams (1%), were less frequent. The findings highlight that scammers primarily use platforms like Facebook, Messenger, WhatsApp, and Instagram due to their large base of active Malaysian users. This suggests a need for the Malaysian government to collaborate with Facebook Inc. to provide scam alerts on these platforms, helping to warn and protect social media users from fraud.

Table 6: The results of prevent solutions that can help to reduce online fraud cases

The online fraud victim experiences on social media (N=98)		Frequency	Percent %
What type of online fraud did you face in social media or private messaging apps?	Investment scam	31	31.6%
	Lottery and Prize scam	27	27.6%
	Online shopping scam	42	42.9%
	Job scam (Employment scam)	28	28.6%
	Romance scam (Online dating scam)	11	11.2%
	Modelling scam	8	8.2%
	Big Pay scam	3	3.1%
	Call scam	1	1%
	Fake mobile apps scam	1	1%
	Online game scam	1	1%
Which type of social media or private messaging applications did you face online fraud?	Facebook	51	52%
	Messenger	22	22.4%
	WhatsApp	50	51%
	Instagram	27	27.6%
	Telegram	9	9.2%
	Twitter	3	3.1%
	Discord	2	1%
	Dating app	1	1%
	Tiktok	1	1%

From Table 7, it shows the total loss to the scammers from online fraud. The result shows that the majority of the respondents do not have to perform any transactions with the scammers, so they do not have any losses to the scammers. While 23.5% of the respondents lost below RM 1,000 and 27.6% of the respondents lost RM 1,000–RM 4,999 to the scammers, And also, 10.2% of the respondents lost RM5,000–RM 9,999, and 4.1% lost more than RM10,000, respectively.

Table 7: The results of total loss to the scammers

The online fraud victim experiences on social media (N=98)	Frequency	Percent
How much is your loss to the scammers?		
RM 0 (Transactions have not been made to the scammers)	34	34.7%
Below RM 1,000	23	23.5%
RM 1,000 - RM 4,999	27	27.6%
RM 5,000 - RM 9,999	10	10.2%
More than RM 10,000	4	4.1%

From Table 8 above, it shows the total loss to the scammers from online fraud. The result shows that the majority of the respondents do not have to perform any transactions with the scammers, so they do not have any losses to the scammers. While 23.5% o Based on Table 8 below, it shows the result of the impacts after being scammed based on the multiple selections made by the respondents. The result shows that the majority of the respondents have emotional problems after being scammed by the scammers. Besides that, the result shows that 31.6% of the respondents have financial impact, 17.3% of the respondents have psychological problems, 9.2% of the respondents have health problems, 9.2% of the respondents feel nothing, 1% of respondents are losing trust in online shopping, 1% of the respondents lost their game account, and 1% of the respondents are losing their original job. In brief, most respondents have emotional problems after being scammed by the scammers, so the authorities can create a team to help the victims address their emotional problems.

Table 8: The results of the impacts after being scammed based on the multiple selections

The online fraud victim experiences on social media (N=98)		Frequency	Percent %
What impacts did you face after being scammed by a scammer?	Financial impact	31	31.6%
	Emotional	54	55.1%
	Psychological problems	17	17.3%
	Health problems	9	9.2%
	Losing trust on online shopping	1	1%
	Lost game account	1	1%
	Lost original job	1	1%
	None	9	9.2%

DISCUSSION

This study presents a compelling examination of the prevalence of online fraud in Malaysia, particularly through social media and private messaging apps. While it effectively highlights key contributing factors, victim experiences, and potential preventive measures, certain critical issues remain underexplored. The study primarily relies on quantitative data from 142 respondents, which, while useful, may not fully capture the complexity of online fraud dynamics, such as psychological manipulation and evolving scam tactics. Additionally, the study's recommendations, including reliance on government and social media platforms for fraud prevention, overlook the potential limitations of enforcement and platform policies. Moreover, while the article acknowledges the emotional and financial toll on victims, it does not sufficiently explore long-term psychological consequences or the effectiveness of legal frameworks in deterring fraud. A more robust discussion integrating qualitative insights from victims and law enforcement, as well as comparative analysis with other Southeast Asian nations, would strengthen the study's findings and contribute to a more comprehensive understanding of online fraud in Malaysia. This study examines the increasing prevalence of online fraud via social media in Malaysia, focusing on public awareness, prevention strategies, contributing factors, and victim experiences. The findings indicate that Malaysians have high awareness of online fraud when using social media and private messaging apps, with government agencies, the Malaysian Communications and Multimedia Commission (MCMC), and personal networks playing crucial roles in raising awareness. Prevention measures include avoiding sharing personal information, not clicking on suspicious links, and strengthening Cyber Law Acts, with authorities utilizing newspapers, magazines, and social media to spread awareness. The study also identifies key factors contributing to online fraud, such as the pursuit of extra income, online shopping for cheap products, impersonation by scammers, and fraudulent job offers. Additionally, 69% of respondents reported scam encounters, primarily investment, lottery, online shopping, and job scams, often perpetrated via Facebook, Messenger, WhatsApp, and Instagram. Emotional distress is a common consequence for victims, emphasizing the need for government intervention, including potential collaboration with Facebook Inc. to implement scam alerts. However, the study acknowledges limitations, including the evolving nature of online fraud, a limited sample size, and a focus solely on Malaysia. Future research should explore fraud trends across Asia, expand sample sizes, and incorporate qualitative analysis for deeper insights.

ACKOWLEDGEMENT

The authors would like to acknowledge the financial support received from the Universiti Sains Malaysia grant (301/PKOMP/6315397).

REFRENCES

[1] 6 Common types of scams in Malaysia and the red flags to know to avoid them. (2021). BURO. https://www.buro247.my/lifestyle/insiders/types-of-scams-malaysia-red-flags.html

[2] Auto, H. (2022, February 16). Scam victims in S'pore lost $633.3 million in 2021 | The Straits Times. Www.straitstimes.com. https://www.straitstimes.com/singapore/courts-crime/victims-lost-6333-million-to-scams-in-2021

[3] Internet usage in Malaysia spikes as Covid-19 pushes more people to go online. (2020). MIDA | Malaysian Investment Development Authority. https://www.mida.gov.my/mida-news/internet-usage-in-malaysia-spikes-as-covid-19-pushes-more-people-to-go-online/

[4] Online Scams Articles | Norton Blog. (2025). Norton.com. https://us.norton.com/internetsecurity-online-scams.html#

[5] Ragananthini Vethasalam. (2022, December 4). Online scam issue tops list. The Star. https://www.thestar.com.my/news/nation/2022/12/05/online-scam-issue-tops-list

[6] The True Cost of Cyber Crime in Malaysia | Spectrum Edge. (2022, June 23). Spectrum-Edge. https://www.spectrum-edge.com/cyber-crime-in-malaysia/

[7] AsiaPac. (2022, August 3). Malaysia Digital Marketing 2022 | Insight | AsiaPac - Digital Marketing Agency Asia. AsiaPac. https://www.asiapacdigital.com/digital-marketing-insight/malaysia-digital-marketing-2022

[8] Basyir, M., & Hana Naz Harun. (2022, September 26). Online scam cases increasing in Malaysia. NST Online; New Straits Times. https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia

[9] Bernama. (2021, October 27). 15,935 online fraud cases, RM380mil in losses in first 9 months of 2021. Free Malaysia Today (FMT). https://www.freemalaysiatoday.com/category/nation/2021/10/27/15935-online-fraud-cases-rm380mil-in-losses-in-first-9-months-of-2021/

[10] Chaffey, D. (2025, February 14). Global Social Media Research Summary 2024. Smart Insights. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

[11] CK Wong. (2018). Top 5 social media platforms by total users in Malaysia. Silvermouse.com.my. https://blog.silvermouse.com.my/2018/09/top-5-social-media-platforms-malaysia.html

[12] Coppola, D. (2023, August 29). Global e-commerce Payment Fraud Losses 2021. Statista. https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

[13] David, A. (2022, August 4). RM5.2b in losses through online scams since 2020 | New Straits Times. NST Online. https://www.nst.com.my/news/crime-courts/2022/08/819331/rm52b-losses-through-online-scams-2020

[14] Dermawan, A. (2024). Duck farms behind river pollution in Kedah. NST Online. https://www.nst.com.my/news/nation/2024/02/1015073/duck-farms-behind-river-pollution-kedah

[15] FMT. (2021, December 18). 5 common job scams you need to be wary of. 5 Common Job Scams You Need to Be Wary Of. https://www.freemalaysiatoday.com/category/leisure/2021/12/18/5-common-job-scams-you-need-to-be-wary-of/

[16] fortinet. (2023). What Is Internet Fraud? Types of Internet Fraud. Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

[17] Hakim, A. (2021, September 21). Love Scammers Are Impersonating "Tengku" Royalty To Trick Their Victims. TRP; TheRakyatPost. https://www.therakyatpost.com/news/2021/09/21/love-scammers-are-impersonating-tengku-royalty-to-trick-their-victims/

[18] InstituteProtecting, N. C. V. L., Enforcing, & Rights, A. V. (2010, July 27). What is "online fraud"? Law.lclark.edu. https://law.lclark.edu/live/news/6855-what-is-online-fraud

[19] J, J. (2019, October 17). What is BigPay? . Bigpayme. https://www.bigpayme.com/post/what-is-bigpay

[20] Kemp, S. (2022). Digital 2022: Malaysia. DataReportal. https://datareportal.com/reports/digital-2022-malaysia

[21] Mail, M. (2020, October 30). BigPay warns of scammers using its brand, advises public not to share any confidential information. Malay Mail ; Malay Mail. https://www.malaymail.com/news/malaysia/2020/10/30/bigpay-warns-of-scammers-using-its-brand-advises-public-not-to-share-any-co/1917743

[22] Mail, M. (2021, November). Bukit Aman warns of online scams offering lucrative jobs. Malay Mail ; Malay Mail. https://www.malaymail.com/news/malaysia/2021/11/01/bukit-aman-warns-of-online-scams-offering-lucrative-jobs/2017709

[23] MalaysiaTrend.com. (2025, March 7). MalaysiaTrend.com. https://www.malaysiatrend.com/msian-model-exposes-fake-talent-agencies-that-scam-women-for-nudes/

[24] McKinsey & Company. (2022, November 8). A new approach to fighting fraud while enhancing customer experience | McKinsey. Www.mckinsey.com. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience

[25] MCMC. (2020). Internet Users Survey 2020 88.7% Internet users in 2020. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Infographic.pdf

[26] Moneysmart. (2020). Investment scams - Moneysmart.gov.au. Moneysmart.gov.au; Moneysmart. https://moneysmart.gov.au/investment-warnings/investment-scams

[27] Nation, T. (2022, May 23). Online scams in Thailand rose sharply, inflicted over THB1 billion losses. Nationthailand. https://www.nationthailand.com/in-focus/40015870

[28] New Straits Times. (2021, September). Businessman parts with over RM65k in lottery scam. Retrieved from https://www.nst.com.my/news/crime-courts/2021/09/724755/businessman-parts-over-rm65k-lottery-scam

[29] *Over 90,000 online fraud cases from 2017-2021, involving RM3.3 bln losses*. (2022, October 3). Thesun.my. https://www.thesundaily.my/local/over-90000-online-fraud-cases-from-2017-2021-involving-rm33-bln-losses-FB8939070

[30] Perimbanayagam, K. (2021, November 8). Malaysians lost RM58 mil to online shopping scammers this year | New Straits Times. NST Online. https://www.nst.com.my/news/nation/2021/11/743575/malaysians-lost-rm58-mil-online-shopping-scammers-year

[31] *Fraud Is On the Rise, and It's Going to Get Worse*. (2022). Retrieved March 14, 2025, from https://www.darkreading.com/cyber-risk/fraud-is-on-the-rise-and-its-going-to-get-worse

[32] *SEA: top social media platforms by traffic share and country 2024 | Statista*. (2025). Retrieved March 14, 2025, from https://www.statista.com/statistics/1293253/sea-top-social-media-platforms-by-traffic-share-and-country/

[33] Tariq, Q. (2022). Police: Over 90,000 online fraud cases from 2017-2021, involving RM3.3bil losses. The Star. https://www.thestar.com.my/tech/tech-news/2022/03/11/over-90000-online-fraud-cases-from-2017-2021-involving-rm33bil-losses-police

[34] The Star Online. (2022, August 19). South-East Asia job scams ensnare three more HK victims, 23 in total. The Star. https://www.thestar.com.my/aseanplus/aseanplus-news/2022/08/19/south-east-asia-job-scams-ensnare-three-more-hk-victims-23-in-total

[35] Wira Madjid. (2021). The Importance of Social Media in South East Asia Countries. Academia.edu. https://www.academia.edu/72074861/The_Importance_of_Social_Media_in_South_East_Asia_Countries

[36] Nasira, N. F., Jynb, S. T. H., & Hashimc, S. H. M. (2022). Decomposition of subjective norms: Addressing the importance of normative influence in purchasing unsought product. International Journal of Academic Research in Business and Social Sciences, 12(11). https://doi.org/10.6007/ijarbss/v12-i11/15687