International Journal of Religion
2024
Volume: 5| Number 11 | pp. 3130 – 3141
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/28kb8w07

Scam Awareness Gaps: A Survey on Malaysian Youth's Digital Habits and Knowledge

Fidlizan Muhammad[1], Ahmad Zakirullah Mohammed Shaarani[2], Mohd Yahya Mohd Hussin[3], Salwa Amirah Awang[4] and Rozilah Hamdan[5]

Abstract

This study examines the demographic profile, digital behavior, and scam awareness of participants, in order to provide valuable insights into their vulnerability to online scams. A survey was conducted by distributing questionnaires to 520 youths in which 482 of them responded. The survey was designed based on guidelines from various authorities addressing scam issues. The results indicate that most respondents have not attended scam awareness events, highlighting a gap in educational outreach. Social media use is prevalent, with significant engagement on platforms like TikTok and Telegram. Notably, 51% of respondents have encountered scammers through digital communications, underscoring the widespread nature of the issue. The findings on information and data literacy reveal that most respondents exercise prudent caution by verifying the authenticity of information before updating personal data. Data security practices are generally positive, with most respondents using different IDs and passwords for applications, although 28% still use the same PIN for multiple cards. Parental communication about scams is inconsistent, with 46.3% of respondents reported that they were never informed by their parents. In terms of problem-solving, 95.9% ignore phishing SMS messages, and 60.8% had made reports of scam incidents, though the rest by 39.2% feel too embarrassed to do so. These results highlight the need for targeted educational initiatives to enhance scam awareness and digital literacy, especially in urban areas and among individuals with high social media engagement. Ongoing efforts to promote security-conscious behaviors and improve parental communication about online safety are essential for empowering individuals against scams.

Keywords: *Scams, Knowledge, Awareness, Data Literacy and Security, Communication and Problem-solving.*

INTRODUCTION

Scams have caused enormous financial losses globally. The enduring and widespread issue of scams affects individuals, businesses, and governments globally (Hanoch & Wood, 2021). These fraudulent activities take various forms and often lure unsuspecting victims with promises of significant returns on investment (Chariri et al., 2018) or involve threats of police, customs, and tax office investigations, prompting individuals (Khadijah & Syahrul 2018; Rizal, 2020, Wilson et al. 2023) to relinquish their hard-earned income. Despite increased awareness and efforts to combat scam crimes, their proliferation continues, driven by the growing prevalence of online platforms and the increasing sophistication of fraudsters (Ma & McKinnon, 2022). Several factors have been identified as contributing to the ongoing persistence of this problem. These elements include less rigorous regulations and enforcement mechanisms to deter financial scams (Monroe et al., 2010), a lack of access to financial education, susceptibility to influences driven by greed and a lack of empathy, and the potential to yield to persuasion and the extravagant lifestyle of friends or acquaintances (Lev et al., 2022).

Numerous researchers propose that ongoing education or literacy regarding scams is a vital mechanism to address this issue (Kasim et al., 2020; Mohd Padil et al., 2022). Early implementation of this approach exposes the public to the tactics or modes of operation employed by scammers. The multitude of reported and investigated cases offers authorities the opportunity to heighten awareness about scams and the latest tactics, particularly among the youth. Scammers utilize diverse strategies to ensnare victims. Individuals who have fallen

[1] Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia. Email: fidlizan@fpe.upsi.edu.my, (Corresponding Author)

[2] Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia, Email: zakirullah@fpe.upsi.edu.my

[3] Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia, Email: yahya@fpe.upsi.edu.my

[4] Politeknik Sultan Azlan Shah, Behrang Stesen, 35950, Behrang Stesen, Perak, Malaysia, Email: salwa@psas.edu.my

[5] The Credit Counselling and Debt Management Agency, Kuala Lumpur, Malaysia, Email: rozilah.h@akpk.org.my

victim to scams perceive themselves as vulnerable, easily deceived, and possessing a nonchalant attitude (Wilson et al., 2023). Public education is imperative for heightening awareness, facilitating informed decision-making, and minimizing the risk of scams.

Malaysia has implemented various efforts to address the issue of scams (Ahmad, et al. 2023). On October 14, 2022, a collaborative effort between the National Anti-Financial Crime Centre (NFCC), the Royal Malaysia Police (PDRM), Bank Negara Malaysia (BNM), the Malaysian Communications and Multimedia Commission (MCMC), as well as financial institutions and telecommunications industries, established an integrated operation centre known as the National Scam Response Centre (NSRC). This serves as the operational hub to coordinate strategic responses to online financial fraud by tracking stolen funds and taking immediate enforcement actions against criminals.

Bank Negara Malaysia has implemented several measures to raise awareness among consumers regarding this issue. The Financial Consumer Alert (FCA) serves as a guide to enhance public awareness of entities or schemes that have been mistakenly perceived or appear to be licensed or regulated by Bank Negara Malaysia (BNM). Due to the evolving methods used by scammers, BNM consistently intensifies efforts and takes steps to combat scams by introducing additional controls and safeguards periodically. These include transitioning from SMS One Time Passwords (OTP) to more secure forms of authentication for online activities or transactions, tightening fraud detection rules and triggers to block suspected scam transactions. Additionally, customers will be asked to confirm the authenticity of such transactions before they are unblocked. Further measures involve restricting transactions to a single mobile or secure device for the authentication of online banking transactions, among others (Nor Shamsiah, 2022).

As a result, the banking industry has implemented an awareness campaign to educate consumers. As part of the campaign, the banking industry encourages the public to remember three simple steps to stay safe and avoid falling victim to scams: STOP, THINK, BLOCK, when they receive any calls, messages, or emails from unknown parties. The tagline *"Ingat 3 Saat OK"* and the hashtag *#JanganKenaScam* will be adopted by all members of banks as part of a cohesive and targeted nationwide campaign. This aims to ensure that the public is consistently informed and equipped with the necessary information and awareness regarding the various modus operandi employed by scammers. It also emphasizes best practices to keep themselves safe online, making it more challenging for scammers to succeed in luring victims.

The Royal Malaysia Police (RMP), under The Commercial Crime Investigation Department (CCID), established on December 1, 2004, has implemented various methods to raise awareness among the public regarding scam crimes. Based on information and reports from victims of scam crimes, the RMP has created a database of phone numbers and account numbers of known scammers called *"SemakMule"* through the website https://semakmule.rmp.gov.my (RMP, online). Through this website, individuals can verify the authenticity of received information to reduce the risk of involvement in such crimes. For the same purpose, the Royal Malaysia Police's Cyber Crime Alert has recently issued a comprehensive guidebook on scam crimes prevalent in Malaysia. This guidebook provides insights into the modus operandi employed by scammers and offers advice and tips to help individuals avoid falling victim to scams (RMP, online). Due to the efforts made by relevant agencies to raise awareness about scam crimes, the issue is whether it is known or recognized by the public. To ensure the success of efforts to address this crime, awareness among the youth is crucial. Research has indicated that the younger demographic within the society, particularly young generations, may be susceptible to the risks associated with illicit investment schemes (Jack & Ibekwe, 2018; Ibekwe & Oli, 2020). Pursuing unrealistic financial goals could prompt them to participate in deceptive investment schemes, driven by the desire to achieve wealth quickly and effortlessly (Jack & Ibekwe, 2018). Therefore, this study aims to identify the level of knowledge among young people regarding this crime as a measure to the success of government-led campaigns that have been implemented.

LITERATURE REVIEW

Scams represent malicious endeavours aimed at manipulating individuals and can take various forms. These deceitful activities aim to deceive individuals into engaging in harmful actions or divulging sensitive information. Scammers frequently utilize social engineering techniques to influence their targets, employing strategies such

as creating a sense of urgency, offering rewards or prizes, or posing as a trusted authority (Wilson et al., 2023). Community awareness of scams can help reduce the risk of falling victim to this crime (Puram et al., 2011). This criminal activity involves the participation of both parties. Experienced scammers, typically aged between 30 and 38, engaged in such acts as a form of revenge or self-gratification. On the other hand, younger scammers (20-24 years old) were often attracted to a luxurious lifestyle and influenced by their more experienced counterparts (Tambe Ebot & Siponen, 2014).

According to Cressey (1973) and Alavi et al. (2020), three elements that drive individuals to commit fraud namely; pressure, opportunity, and rationalization. Pressure is often financial, and individuals facing such pressure may try to solve their problems without external help. The second element is opportunity, which arises when a lack of internal control provides a scammer with access to commit fraud. The third component is rationalization, where scammers come up with reasons to justify their actions, often believing that their wrongdoings are not illegal or immoral (Omar et al., 2016). For victims, the unavoidable exposure to the internet and prevalent use of social media today create opportunities for criminals to ensnare them using various tactics

Awareness of scam crimes can be obtained through reading, experience, or education. Insufficient knowledge and awareness may prompt younger generations to engage in fraudulent scams due to enticing offers (Mohd Padil et al., 2022). Holtfreter et al. (2010) found that individuals with lower levels of self-control are more vulnerable to fraud, especially when they cannot resist the allure of a luxurious lifestyle presented by fraudsters. Therefore, financial literacy equips individuals with the skills, motivation, and confidence to apply information and understanding in decision-making across various financial contexts (Lusardi et al., 2020). Youths can enhance their awareness of scams through education, whether at schools or universities, among other means (Mishra and Kumar, 2019; Beal & Delpachitra, 2003). Gui et al. (2021) discovered that a simple educational flyer outlining the risk-return trade-off can alter investment decisions once individuals become aware of the high risk associated with high-return financial products. As a result, introducing the younger generation to financial management education at an early stage to foster disciplined spending can serve as a preventive measure against falling victim to scam crimes. (Mohd Padil et al. 2022).

To reduce the risk of falling victim to online scams, individuals should acquaint themselves with the common tactics employed by cybercriminals, such as phishing emails, counterfeit websites, and social engineering strategies (Puram et al., 2011). Additionally, it is crucial to exercise caution during online purchases and verify the legitimacy of websites and sellers before disclosing personal or payment information (Baker, 1999; Liu et al., 2022). Educational campaigns and awareness initiatives play a pivotal role in enhancing consumer awareness, thereby preventing individuals from succumbing to online scams and frauds. By augmenting knowledge and understanding of prevalent risks and tactics used by cybercriminals, individuals can enhance their ability to safeguard both themselves and their personal information during online transactions (Wilson et al. 2023).

Various studies have examined users' knowledge in utilizing technology to protect themselves from scam crimes. Research conducted by Chaudhry et al. (2016) and Maimon et al. (2023) investigates into email fraud or phishing. This involves criminals employing persuasive techniques to deceive individuals into divulging personal or sensitive information or making payments to the fraudster. These techniques often involve a rich and emotional narrative that exploits the victim's emotions, such as greed or fear. Establishing trust is indeed another crucial aspect of social engineering attacks. Cybercriminals may employ various techniques to appear trustworthy, including using professional-looking websites or email addresses, providing seemingly legitimate contact information, or posing as known or respected authority figures. Phishing emails may use language creating a sense of urgency, urging the victim to act quickly or risk missing out on a supposed opportunity. To counter these fraudulent emails, individuals need to be aware of common phishing tactics and exercise caution when opening emails or clicking on links.

Numerous studies have highlighted a significant gap in the knowledge and awareness of many individuals when it comes to recognizing and avoiding potential risks and scams in online transactions, spanning online marketplaces and e-wallets (Hamsi et al., 2015; Zahari et al., 2019). In Malaysia, widespread online shopping scams involve counterfeit websites promoted through social media, leading to incidents where victims either receive mismatched products or none at all. Scammers entice consumers with significantly lower-priced

products, employing tactics that spur impulsive purchases. The surge in social media use amplifies the prevalence of online shopping, offering scammers ample opportunities to exploit consumers for both money and personal information. Some scammers also aim to obtain sensitive details by soliciting bank information or encouraging sign-up forms during purchases (Nor Hasaliza et al., 2023). To mitigate the risk of falling victim to online scams, individuals must familiarize themselves with the common tactics employed by cybercriminals. Exercising caution during online purchases and ensuring the legitimacy of websites and sellers before divulging personal or payment information are equally crucial.

Educational campaigns and initiatives aimed at raising awareness can play a pivotal role in enhancing public understanding, thereby preventing individuals from becoming susceptible to scams and frauds. In the context of avoiding scams, people can safeguard themselves by adopting a cautious approach when considering scammer offers and meticulously examining all associated information (Baucus & Mitteness, 2016). The main challenge authorities face in addressing scam crimes is providing understanding and awareness to the public. While many are familiar with the campaigns designed to tackle this issue, individuals can be caught off guard and succumb to scams when becoming addicted or vulnerable on the internet (Khadijah et al. 2018). This vulnerability, shared by others, highlights the ongoing challenges in educating and raising awareness among the public to effectively combat scam crimes (Wilson et al. 2023). Despite the reporting of this crime in the mass media, the recurring frequency of this issue proves that victims and some members of the community are unaware of the problem and unable to apply methods to address the promoted scams (Button et al., 2014; Whitty & Buchanan, 2016; Whitty, 2020)

RESEARCH METHODOLOGY

Measurement Instrument

Due to the absence of available questionnaires in previous research, the measurement scale utilized in this study was self-developed, drawing guidance from the book or guidelines provided by the Commercial Crime Investigation Department (CCID), Royal Malaysia Police (RMP), published in December 2022 under the title "*Trend Terkini Jenayah Komersil.*" The document is accessible online at *https://heyzine.com/flip-book/cb606d5783.html* (RMP, 2022). The constructs and items were meticulously crafted in alignment with the study's objectives, research questions, and the target group of respondents. Drawing from literature related to scam topics, the study identified 29 items and five knowledge constructs for questionnaire development: data literacy, digital content, data security, communication, and problem-solving. Part A of the questionnaire pertains to demographic information provided by the respondents. In Part B, all respondents were required to indicate their knowledge levels for the five constructs in the survey. Most items presented to respondents were in the form of a two-response scale, requiring them to choose the appropriate action or respond with yes or no. Some items in the digital content construct utilized a three-point likert scale, ranging from disagree (1) to strongly agree (3).

This survey was conducted face-to-face with respondents over a period of 4 months from May to September 2023. A total of 520 survey forms were distributed to the youths during this timeframe. As a result, 482 survey forms were received with complete responses. The collected data were analysed using IBM SPSS Statistics version 29.

Explanation of Constructs

The explanation related to the five constructs used in this study as follows;

Table 1: Explanation of the five Constructs

Constructs	Explanation	Source
Information and Data Literacy	This dimension focuses on individuals' ability to locate, evaluate, and effectively use information and data from various sources. It includes skills such as assessing the credibility of information, understanding data sources, and critically analysing information for relevance and accuracy. In the context of knowledge scams, information and data literacy are crucial for recognizing trustworthy sources, distinguishing between	Wei et al. (2021); Zainal Abidin et al. (2018), Teitcher et al. (2015)

	legitimate and fraudulent information, and making informed decisions based on reliable data	
Digital Contents	Digital content refers to the creation, sharing, and consumption of multimedia materials in digital formats. This dimension explores how young individuals engage with and produce digital content. It includes activities such as blogging, video creation, and social media participation. Understanding digital content creation is important in the context of knowledge scams, as individuals may encounter deceptive content online, and being able to discern authentic and reliable information from misleading or fraudulent content is essential	Cross & Layt (2022); Ali & Mohd Zaharon(2024); Pratt et al. (2010)
Data Security	Data security involves practices and measures implemented to protect sensitive information from unauthorized access, disclosure, alteration, or destruction. This dimension assesses individuals' awareness and adherence to security measures to safeguard their personal and sensitive data. This includes using strong and unique passwords, employing encryption methods, being cautious about sharing personal information, and staying informed about cybersecurity threats	Arachchilage & Love (2014); Baruh & Popescu (2017);Chen et al. (2017); Robb & Wendel (2023)
Communication	Communication, in the context of your research, examines how individuals interact and share information in various online platforms and social settings. It encompasses both the effectiveness and security of digital communication. This dimension explores whether individuals use secure communication channels, are cautious about sharing personal information online, and engage in respectful and responsible online communication. Effective communication skills are vital for avoiding potential scams and fraudulent activities	Hipgrave (2013); Cross & Layt (2022), Azianura et al. (2019).
Problem-solving	Problem-solving refers to the ability to analyse and resolve challenges, especially those encountered in digital environments. This dimension assesses how well individuals can identify and address issues related to online scams and deceptive practices. Problem-solving skills include recognizing and avoiding potential scams, seeking help or guidance when needed, and adapting to new technologies and tools to mitigate risks	Kuo et al. (2014); Kubilay et al. (2023); Aung & Mon (2020)

These dimensions collectively provide a comprehensive understanding of the factors influencing youths' susceptibility to knowledge scams and their ability to navigate the digital landscape securely and effectively. The research will shed light on the strengths and weaknesses in each dimension, offering insights for educational and awareness programs tailored to the specific needs of Malaysian youth

RESEARCH FINDINGS

Demographic Profile of Respondent

As shown in Table 2, the survey results provide valuable insights into the characteristics of the participants. Most of the respondents are female (62.7%), while males account for 37.3%. In terms of where they live, a significant majority (65.6%) are in urban areas, while 34.4% are in suburb/rural locations. Regarding their exposure to educational events about scams, a large percentage (84.6%) have not attended any lectures or workshops, indicating a potential gap in scam awareness efforts. In terms of social media use, a substantial number have accounts on different platforms, such as Facebook (40.2%), TikTok (58.2%), Telegram (56.2%), and X (Twitter) (29.3%). Notably, a significant portion of the respondents (50.8%) has encountered scammers through emails, SMS, or other messages, highlighting a prevalent issue that requires attention. These findings underscore the diverse demographics and experiences of the participants, emphasizing the need for targeted awareness campaigns and educational initiatives, especially for those who have yet to participate in anti-scam events.

Table 2: Demographic Profile of Respondents

Demographic Profile	n	%
Gender		
Male	180	37.3
Female	302	62.7
Residential Location		

Urban/ City	316	65.6
Suburb / Rural	166	34.4
Have you ever attended a lecture/workshop related to scams		
Yes	74	15.4
No	408	84.6
Do you have a social media account? (Yes)		
Facebook	194	40.2
Tiktok	281	58.2
Telegram	271	56.2
X (Twitter)	141	29.3
Have you ever received emails, SMS, or other messages from scammers?		
Yes	245	50.8
No	237	49.2

Source: Survey

Constructs Findings

The results of the analysis of the five study constructs, namely information and data literacy, digital content, data security, communication, and problem-solving, are explained in subtopics (i) to (iv)

Information and Data Literacy

The analysis of scam data in Table 3 highlights the key trends on how individuals respond to potential threats. A majority (56.6%), demonstrate prudent caution when receiving requests to update personal information, opting not to click and ignore the potentially suspicious prompts. Furthermore, an impressive 96.7% show a strong inclination toward trust verification, preferring to consult with friends, family, or teachers before updating any information. This underscores a commendable awareness of potential risks associated with personal data.

Table 3: Findings on Information and Data Literacy

No	Statements	Answer	N	%
1.	You receive information through email, SMS, WhatsApp group, or a website link to update personal information. What is your action?	Click and update personal information	209	43.4
		Do not click and ignore	273	56.6
2.	You receive information through email, SMS, WhatsApp group, or a website link to update personal information. What is your action	Proceed to update the information	16	3.3
		Verify its authenticity (consult with friends, family, teachers, etc.)	466	96.7
3.	A close friend sends you a website link to update your personal information. What is your action?	Immediately click and update the information	9	1.9
		Inquire with your friend first	473	98.1
4.	Someone in a social media group (WhatsApp, Telegram, TikTok, etc.) sends a link offering a substantial prize. What is your action?	Immediately click and update my personal information	19	3.9
		Do not click and ignore the link	463	96.1
5.	If you receive a phone call from a bank institution requesting your identification number, bank account number, or card details, what should you do?	Provide the required information to the bank officer	23	4.8
		End the call and do not provide any requested information	459	95.2
6.	Storing passwords in a notebook or contact list in your phone is a secure method?	True	258	53.5
		False	224	46.5
7.	What is the best way to use social media to avoid scams?	Avoid using social media altogether	51	10.6
		Be cautious when using social media and avoid sharing personal information	431	89.4

Source: Survey

In scenarios involving close friends sharing website links or enticing prizes on social media, respondents exhibit a high level of trust and awareness. An overwhelming 98.1% inquire with their friend before clicking on a link, while 96.1% wisely avoid clicking on links offering substantial prizes. These responses indicate a collective awareness of the risks associated with both familiar and unfamiliar online interactions. The findings also reveal

a sensible approach to potential phishing attempts through phone calls, with 95.2% choosing not to provide requested information. However, there is room for improvement in password security awareness, as 46.5% still consider storing passwords in a notebook or contact list on a phone as secure. Finally, a significant 89.4% emphasize caution and avoiding the sharing of personal information when using social media, reinforcing the need for ongoing education and awareness campaigns to empower individuals against potential scams.

Digital Content

The analysis of the data on digital content-related variables provides valuable insights into individuals' perceptions and behaviours in the context of online scams as shown in Table 4. A substantial 73.0% strongly agree that scammers often use fake websites to deceive victims, showcasing a high level of awareness regarding the prevalence of this deceptive tactic. Additionally, respondents express a cautious stance toward websites selling goods using images of popular icons or idols, with 37.6% strongly agreeing that such sites can be trusted. However, a notable 22.2% disagree, indicating a significant level of scepticism towards these platforms

Table 4: Findings on Digital Content

No	Statements	Answer	N	%
1.	Scammers often use fake websites to deceive victims	Strongly Agree	352	73.0
		Partially Agree	113	23.4
		Disagree	17	3.5
2.	Websites selling goods using images of popular icons or idols can be trusted?	Strongly Agree	181	37.6
		Partially Agree	194	40.2
		Disagree	107	22.2
3.	Sharing home addresses and phone numbers openly on social media does pose a danger to me?	Strongly Agree	283	58.7
		Partially Agree	141	29.3
		Disagree	58	12.0
4.	There are many fake website links that resemble genuine websites today. Do you know these differences?	Strongly Know	100	20.7
		Partially Know	219	45.4
		Do not Know	163	33.8
5.	A social media friend invites you to join a savings scheme with a small initial investment and high returns. Do you trust the scheme	Trust and join the scheme immediately 100%	14	2.9
		Do not trust 100%, but might join if the investment is small	103	21.4
		Do not trust 100%	365	75.7
6.	What action would you take for each scheme?			
	a. Capital RM50, profit RM 100	Join	36	7.5
		Do not Join	446	92.5
	b. Capital RM100, profit RM500	Join	18	3.7
		Do not Join	464	96.3
	c. Capital RM500, Profit RM5000	Join	10	2.1
		Do not Join	472	97.9

Source: Survey

Concerns about personal safety emerge in the context of social media, with 58.7% strongly agreeing that openly sharing home addresses and phone numbers poses a danger. Regarding the ability to differentiate between genuine and fake website links, a majority (45.4%) only partially know the differences, emphasizing the need for increased awareness and digital literacy. When evaluating trust in a saving scheme proposed by a social media friend, a majority (75.7%) do not trust the scheme 100%. This scepticism is further reflected in respondents' actions regarding various investment scenarios, where a substantial percentage (92.5% to 97.9%) choose not to join schemes with different capital and profit combinations. These findings underscore the importance of enhancing digital literacy and promoting cautious behaviour in the face of potential online scams. Ongoing education and awareness efforts are crucial to empower individuals to navigate the digital landscape safely

Data Security

The analysis of data security measures in Table 5 indicates positive trends in how people safeguard themselves from potential threats. A large majority (79.5%) show a strong awareness of security by using different IDs and passwords for applications, recognizing the importance of diverse login information for better data protection. When managing multiple ATM and bank credit cards, the majority (71.6%) wisely opt for different PIN numbers, demonstrating a cautious approach to financial security. However, the data also highlights the need for increased awareness, as 28.4% use the same PIN number.

Table 5: Findings on Data Security

No	Statements	Answer	N	%
1.	In using applications, what safety measure do you use	Use the same ID and password	99	20.5
		Use different ID and password	383	79.5
2.	If I have many ATM and bank credit cards, what safety measure do you use?	Use the same PIN number	137	28.4
		Use different PIN numbers	345	71.6
3.	For internet safety purposes, what do you usually do?	Use the same ID and password	120	24.9
		Use different ID and password	362	75.1
4.	You receive an email from an unknown individual informing you that your bank account has a problem. What is your action	Call the number provided in the email	36	7.5
		Ignore the email	446	92.5
5.	While browsing the internet, an ad pops up telling you that you have won a substantial prize. What is your action	Click on the advertisement	23	4.8
		Ignore the advertisement	459	95.2
6.	You don't have any credit card. However, you receive an SMS to call certain number? What is your action?	Call the provided number immediately	22	4.6
		Ignore the SMS	460	95.4

Source: Survey

In terms of internet safety, a substantial 75.1% prioritize security by using different IDs and passwords, indicating a positive inclination towards securing online accounts with varied login information. Additionally, respondents show a wise response to potential phishing attempts and enticing advertisements by choosing to ignore them, underlining a prudent attitude in avoiding potential scams. Overall, these findings emphasize the importance of promoting security-conscious behaviours and continuous awareness initiatives for comprehensive data protection in the digital age.

Communication

The analysis of communication-related variables in the scam data reveals insightful patterns in individuals' responses to different situations as presented in Table 6. When faced with a phone call from someone claiming to be a police officer, the majority (92.5%) demonstrates a prudent approach by choosing to end the conversation, showcasing a heightened awareness in avoiding potential scams and safeguarding personal information. Similarly, in a scenario involving the post office calling for a monetary deposit, a significant 96.5% dismiss the conversation and instructions, reflecting a cautious and informed stance toward potentially fraudulent activities.

Table 6: Findings on Communication

No	Statements	Answer	N	%
1.	A police officer calls and informs you that you are involved in a police case, such as smuggling, possessing illegal goods, having weapons, etc	Follow instructions and take the directed actions	36	7.5
		End the conversation and do not provide any requested information	442	92.5
2.	The post office calls you and informs you that a package has been sent, requiring you to deposit money into a specific account first	Follow instructions and deposit the requested money	17	3.5
		Disregard the conversation and instructions given	465	96.5
3.	You receive an email stating that you are lucky and have won a substantial prize, and you need to provide your identification and bank numbers	Follow instructions and take the directed actions	8	1.7
		Disregard the instructions and inform family and friends to be cautious	474	98.3
4.	An advertisement promotes a new product using an icon (influencer, YouTuber) you admire,	Click and join the group	39	8.1
		Ignore the advertisement	443	91.9

	inviting you to join a social media group (Telegram, TikTok, etc)			
5.	When a scam occurs, parents tell you about it	Always	102	21.2
		Sometimes	157	32.6
		Never	223	46.3

Source: Survey

In the context of email communications proclaiming substantial prize wins, individuals overwhelmingly (98.3%) adopt a sceptical approach by choosing to disregard the instructions and advising family and friends to exercise caution. This highlights a robust awareness of common tactics used by scammers to deceive recipients. Additionally, when faced with advertisements on social media promoting new products with admired icons, the majority (91.9%) exhibits discernment by choosing to ignore the advertisements, signalling a cautious and informed response to potentially deceptive promotions. Lastly, the findings reveal variability in parental communication about scams, with 46.3% reporting "never" being informed by their parents. This emphasizes a potential gap in parental guidance and underscores the critical need for ongoing efforts to promote awareness, communication, and education to empower individuals in recognizing and avoiding fraudulent activities

Problem-Solving

The analysis of problem-solving variables in the scam data provides valuable insights into individuals' decision-making and actions in various scam-related situations as summarised in the following table;

Table 7: Findings on Problem-solving

No	Statements	Answer	N	%
1.	You receive an SMS requesting your identification number, bank account number, and bank PIN. What is your action	Reply to the SMS and provide the information	20	4.1
		Ignore the SMS	462	95.9
2.	You buy an item online. Later, you are asked to provide additional information besides your address, such as your identification number, bank account number, and bank PIN	Do not proceed with the purchase	259	53.7
		Fill in the requested information	223	46.3
3.	If you become a victim of scams, what is your action	Inform a specific party	293	60.8
		Feel embarrassed and keep quiet	189	39.2
4.	You are contacted by someone who tells you that you have won an iPhone 14. However, you need to pay a shipping fee of RM150 first. What is your action?	Ignore the offer	278	57.7
		Pay the shipping fee	204	42.3
5.	You receive an urgent message from a friend through WhatsApp, Telegram, etc., asking to borrow a sum of money. What is your action?	Immediately lend money to your friend	32	6.6
		Call and inquire further with your friend first	450	93.4

Source: Survey

When faced with an SMS requesting sensitive information like identification number, bank account number, and bank PIN, the majority (95.9%) demonstrates a prudent approach by choosing to ignore the SMS, emphasizing a cautious response to potential phishing attempts and a commitment to protecting personal information. In the context of online purchases requiring additional personal information, a significant portion (53.7%) opts not to proceed with the purchase, showing a keen awareness of potential risks associated with sharing sensitive data. On the other hand, 46.3% fill in the requested information, suggesting a potential area for improvement in understanding and practicing online safety measures.

When asked about actions following a scam victimization, the majority (60.8%) indicates a proactive response by choosing to inform a specific party. In contrast, 39.2% express a sentiment of embarrassment and silence, revealing a potential emotional barrier that could hinder some individuals from seeking help or reporting scams.

These findings underscore the importance of promoting awareness, providing guidance on safe online practices, and addressing emotional aspects to enhance individuals' resilience against scams.

CONCLUSION AND RECOMMENDATION

In conclusion, the analysis of scam data across multiple variables has revealed important patterns in individuals' responses to potential threats. Overall, the majority of participants demonstrate commendable awareness and cautious behaviour, particularly in scenarios involving requests for personal information, phishing attempts, and potentially fraudulent activities. Notably, participants display a high level of scepticism and careful consideration when faced with suspicious online content, such as fake websites, enticing advertisements, and dubious social media schemes. However, there are areas for improvement, such as password security awareness and consistent parental communication about scams.

Based on the findings, several recommendations can enhance individuals' resilience against scams. Firstly, there is a need for continuous education and awareness campaigns, focusing on password security practices and the identification of fake websites. Additionally, efforts should be directed towards improving digital literacy to enable individuals to navigate online spaces securely. Parental involvement is crucial, and initiatives to encourage open communication about scams within families can bridge potential gaps in awareness. Furthermore, the study suggests the importance of emotional support and guidance for individuals who may feel embarrassed or reluctant to report scam incidents. Ongoing educational initiatives and awareness campaigns should be tailored to address these specific areas, empowering individuals to make informed and secure decisions in an evolving digital landscape.

Acknowledgement

This research has been carried out under Fundamental University Research Grant (commonly known as Geran Penyelidikan Universiti (2022-0147-107-01) provided by Universiti Pendidikan Sultan Idris. The authors would like to extend their gratitude to Research Management and Innovation Centre (RMIC) that helped managed the grant.

REFERENCES

Ahmad, Z.A., Mubin,A. N.N., & Arzeman, A. (2023). Content Analysis of Cybercrime Infographics. Jurnal Komunikasi: Malaysian Journal of Communication, 39(4), 501-519.

Alavi, K., Mahbob, M.M., & Azha Sooed, M.S., (2020). Strategi Komunikasi Penjenayah Cinta Siber Terhadap Wanita Profesional. Jurnal Komunikasi: Malaysian Journal of Communication, 36(3), 296-311.

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A Cyber Fraud: The Types, Implications and Governance. International Journal of Educational Reform, 3(1), 101-121. https://doi.org/10.1177/10567879221082966

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Aung, N.N., & Mon, H.H. (2020). Budgeting habit behavior of undergraduate students in Yangon University of Economics. Journal of the Myanmar Academy of Arts and Science, 18(8), 39-50.

Azianura, H.S., Rahim, M.K., Fariza, W.P., & Masnizah, M. (2019). Online-dating romance scam in Malaysia: An Analysis of Online Conversations between scammers and victims, Journal of Language Studies, 97-115.

Baker, C.R. (1999). An analysis of fraud on the Internet. Internet Research, 9(5), 348-360. https://doi.org/10.1108/10662249910297750

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management, New Media & Society, 19(4), 579-596.

Baucus, M. S., & Mitteness, C. R. (2016). Crowdfrauding: Avoiding Ponzi entrepreneurs when investing in new ventures. Business Horizons, 9(1), 37–50.

Beal, D., & Delpachitra, S. (2003). Financial literacy among Australian university students. Economic Papers: A Journal of Applied Economics and Policy, 22(1), 65-78.

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

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.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior, 70,291–302.

Cressey, D. R. (1973). Other People's Money. Montclair: Patterson Smith.

Cross, C., & Layt, R. (2022). I Suspect That the Pictures Are Stolen: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. Social Science Computer Review, 40(4), 955-973.

Gui, Z., Huang, Y., & Zhao, Z. (2021). Whom to educate? Financial literacy and investor awareness. China Economic Review, 67, 1-22.

Gordillo-Rodriguez, M. T., Pineda, A., & Gómez, J. D. F. (2023). Brand Community and Symbolic Interactionism: A Literature Review. Review of Communication Research, Vol.11, pp.1-32.

Hamsi, A. S., Tobi, S. N., & Masrom, M. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. Journal of Management Research, 7(2), 169-181.

Hanoch, Y., & Wood, S. (2021). The Scams Among Us: who Falss Prey and Why. Current Directions in Psychological Science, 30(3), 260-266.

Hipgrave, S. (2013). Smarter fraud investigations with big data analytics. Network Security 2013(12), 7-9.

Holtfreter, K., Reisig, M.D., Leeper Piquero, N., & Piquero, A.R. (2010). Low self-control and fraud: offending, victimization, and their overlap. Criminal Justice and Behavior, 37(2), 188-203.

Ibekwe, C.C., & Oli, N.P. (2020). Ponzi schemes and risks of patronage among undergraduates in tertiary institutions in Anambra state, South-East, Nigeria. International Journal of Management Studies and Social Science Research, 96-107.

Jack, J.T., & Ibekwe, C.C. (2018). Ponzi Schemes: An Analysis on Coping with Economic Recession in Nigeria. The Nigerian Journal of Sociology and Anthropology, 16(1), 72-90.

Kasim, E.S., Zin, N.M., Padil, H.M., & Omar, N. (2020). Ponzi scheme and its prevention: insights from Malaysia. Management and Accounting Review, 19(3), 89-118.

Khadijah, A., & Syahrul, M.A.S. (2018). Love Scam in Selangor: An Exploratory Research on Modus Operandi in Cyber Crime towards Professional Women. Jurnal Pembangunan Sosial, 21(Sept.), 105-122.

Kubilay E., Raiber E., Spantig L., Cahlíková J., & Kaaria L. (2023). Can you spot a scam? Measuring and improving scam identification ability. Journal of Development Economics,165, 1-10.

Kuo, F.-R., Chen, N.S., & Hwang, G.J. (2014). A creative thinking approach to enhancing the web-based problem solving performance of university students. Computers & Education, 72, 220–230. https://doi.org/10.1016/j.compedu.2013.11.005.

Lev, E., Maha, L.G., & Topliceanu, S.C. (2022). Financial frauds' victim profiles in developing countries. Frontiers in Psychology, 13, 1-14. doi: 10.3389/fpsyg.2022.999053

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontier In Psychology, 13, 927398. doi: 10.3389/fpsyg.2022.927398

Lusardi, A., Mitchell, O.S., & Curto, V. (2014). Financial literacy and financial sophistication in the older population", Journal of Pension Economics and Finance, 13(4), 347-366.

Ma, K.W.F., & McKinnon, T. (2022). COVID-19 and cyber fraud: emerging threats during the pandemic. Journal of Financial Crime, 29(2), 433-446.

Maimon, D., Howell, C.J., Moloney, M., & Park, Y.S. (2023). An Examination od email fraudsters' Modus Operandi. Crime & Delinquency, 69(11), 2329-2358.

Mishra, M.K. (2019). Financial Literacy and Education for improving Financial Skills (Nov 17, 2019), http://dx.doi.org/10.2139/ssrn.3488670.

Mohd Padil, H., Kasim, E.S., Muda, S., Ismail, N., & Md Zin, N. (2022). Financial literacy and awareness of investment scams among university students. Journal of Financial Crime, 29(1), 355-367.

Monroe, H., Carvajal, A., & Pattillo, C. (2010). Perils of Ponzi: regulators need to stop Ponzi schemes before they gain momentum, especially in developing countries. Finance and Development, 37-39

Nor Hasaliza, A.N., Shazleen, M., & Razali, M.R. (2023). Understanding the Social Commerce Scam And Consumers Self Disclosure. International Journal of Business and Technology Management, 5(2), 251-262.

Nor Shamsiah, M.Y. (2022). Governor's Speech at the Launching of Financial Crime Exhibition. Available at; https://www.bnm.gov.my/-/financial-crime-exhibition-speech-en

Omar, N., Said, R., & Johari, Z.A. (2016). Corporate crimes in Malaysia: a profile analysis. Journal of Financial Crime, 23(2), 257-272, doi: 10.1108/JFC-05-2014-0020.

Pratt, T.C., Holtfreter, K., & Reisig, M.D. (2010). Routine online activity and internet fraud targeting: extending the generality of routine activity theory. Journal of Research in Crime and Deliquency, 47(3), 267-296.

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

Rizal, M.A.R. (2020). Online scammers and their mules in Malaysia. Malaysian Journal of Law and Society, 26(1), pp. 65-72.

Robb, C.A., & Wendel, S. (2023). Who can you trust? Assessing vulnerability to digital imposter scams", Journal of Consumer Policy, 46, 27-51.

Royal Malaysia Police, RMP (2022). Trend Terkini Jenayah Komersil. Available at, https://heyzine.com/flip-book/cb606d5783.html

Royal Malaysia Police, RMP (online). #BeSmartStayAlert #LetsFightScammerTogether SCAM ALERT: GUNA SEMAK MULE SEBELUM TERUSKAN TRANSAKSI. Available at, https://www.rmp.gov.my/news-detail/2022/09/17/besmartstayalert-letsfightscammertogether-scam-alert-guna-semak-mule-sebelum-teruskan-transaksi

Tambe Ebot, A.C., & Siponen, M. (2014). Toward a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective". ICIS 2014 Proceedings. https://aisel.aisnet.org/icis2014/proceedings/GeneralIS/31

Teitcher, J.E., Bockting W.O., Bauermeister, J.A., Hoefer, C.J., Miner, M.H., & Klitzman, R.L. (2015). Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs. Journal of Law, Medicine & Ethics, 43(1), 116-33, doi: 10.1111/jlme.12200.

Wei, L., Peng, M., & Wu, W. (2021). Financial literacy and fraud detection Evidence from China", International Review of Economics & Finance, 76 (November), 478-494.

Whitty, M.T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims", European Journal on Criminal Policy and Research, 26(3),399-409.

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

Zahari, A. I., Bilu, R., & Said, J. (2019). The Role of Familiarity, Trust and Awareness Towards Online Fraud, Journal of Research and Opinion, 6(9),2470–2480, https://doi.org/10.15520/jro.v6i9.23.

Zainal Abidin, N., Kamaluddin, M.R., Shaari, A.H., Din, N., & Ramasamy, S. (2018). Pengetahuan dan Amalan Perlindungan Pengguna Facebook Wanita terhadap Penipuan Cinta di Malaysia. Jurnal Komunikasi: Malaysian Journal of Communication, 34(4), 113-133.