Anatomy of Phone Scams: Victims' Recall on the Communication Phrases used by Phone Scammers

Farhanim Mohamad Asri and Tengku Elena Tengku Mahamad(✉)

Universiti Teknologi MARA, Selangor, Malaysia
tengku.elena@uitm.edu.my

Abstract. Scam activities has existed long before the advent of modern technology and today, it is still a growing concern that is happening across the globe due to the fast-growing technologies such as phones, the internet, and social media. Modern scams can either be physical (i.e., phone scam) or online (i.e., e-mail scam). Although many researchers have attempted to understand the cause and outcomes of phone scams however, very little research to date have attempted to identify the communication phrases used by scammers as part of their strategy to lure victims. Thus, this paper aims to identify the common phrases used by scammers during their modus operandi. Furthermore, this paper explores factors that may explain how and why victims fall for the scammers' scheme. Based on eight semi-structured interviews with victims of phone scams living in the state of Selangor, we discovered that the different scammers who had scammed the participants used similar communication phrases when trying to trick them out of their money. Phrases such as 'You have an overdue..', 'I can help you..', or 'Let's settle this together' was commonly used. Contrary to what has often been assumed, the victims are aware of the danger of falling victim to a scam. However, trust and panic are the main factors that made them fall victim. The results also represent a further step towards developing a strategy to combat scam activities by providing information on the language and communication used during communication exchanges between the scammers and the victims.

Keywords: Communication · Phone scams · Recall · Scammers · Victims

1 Introduction

Scam activities are not new and in fact, for many years it has been difficult to tackle globally. One of the common type of scams is phone scams. Phone scams have become a major problem in many countries with Australians reported a record of AUD$211 million in losses to scams in 2021 with phone based scams accounted for over AUD$63.6 million of the losses [1]. In Singapore, a study by cloud communicators provider Toku found that three-quarters of Singaporeans had received a scam call this year and with 10 per cent of them falling prey and suffering monetary loss [2].

Like other countries, Malaysia is not free from phone scams. In 2019, Malaysia was reported to have one of the highest numbers of scam cases in the world as a total of 63

© The Author(s) 2023
A. Ismail et al. (Eds.): i-COME 2022, ASSEHR 769, pp. 498–509, 2023.
https://doi.org/10.2991/978-2-38476-098-5_43

per cent spam calls are identified as fraudulent based on a data released by Truecaller [3]. Also, it has been reported that within three months in 2021, Malaysian lost over US$9 million to spam calls [4]. Those who are susceptible to become victim are those closer to retirement ages, and who are less tech-savvy [4].

In general, these fraudulent phone calls often involve the caller impersonating as a high-level government agency or law enforcement officer and utilises a combination of psychological techniques (i.e., trust, scarcity and urgency) in order to convince victims to reveal confidential information [5] and extort payment from them [6]. In the case of Malaysia, the scammer would claim to be an officer from a government body such as the police, customs department, Bank Negara Malaysia, the courts, or from private bodies such as banking institutions [4].

Investigating phone scams activity is a constant concern within the government bodies and private sectors [7] in an effort to combat this illegal activity. It is worth noting that scammers have adopted various techniques in defrauding their victims. Scammers induce an emotional reaction, often fear, from victims [8].

Phone scams happen in many forms, but they appear to make repetitive promises and threats or expect to pay for certain ways. It may be challenging to recognise the motives of an unsolicited caller instantly. Anyone may be caught unaware of a phone scam. Therefore this study aims to extend the literature that specifically examines the concern of telephony fraud by identifying common phrases used by the scammers.

1.1 Problem Statement

Malaysia is among the top 20 countries that is most affected by phone scam activities [9]. Most of the scam calls in Malaysia are from financial services (21 per cent), insurance (10 per cent), operators (five per cent), and debt collectors (one per cent) [9]. Other forms and formats used by the scammers include sales calls, surveys, political calls, subscriptions, and health promotional calls from companies [10].

A larger syndicate in the country called ‘Macau Scams’ originating from syndicates in Taiwan and China is also on the prowl in the country [11, 12]. The modus operandi of Macau scammers is to make threatening phone calls and disguising as police officers, tax agents, central bank workers, and others, claiming that the person who picked up the call is implicated in a criminal offence and being investigated [13]. Many have fallen victim to the Macau Scam syndicate for instance, a 30-year-old teacher lost RM254,600 [14], a 60-year-old housewife lost RM247,642 and a 21-year-old student lost RM12,000 after they were duped by the syndicate members [15].

In light of recent events in Malaysia, it has becoming extremely difficult to ignore the existence of phone scams activity that leave traumatised effect on the victims. However, due to the modus operandi for scams is constantly changing, making it difficult to inform the public about the various forms of scams [5]. It is not known how the communication used by the scammers were very effective in scamming people even though there were a lot of empirical study about scams activities have been conducted. It has become the concern of the relevant parties throughout the country. A primary concern of phone scams is the phrases used by the scammers to lure people until they become one of the victims.

Past studies suggested that most of the scams that many fall victim to is the Internet Scam or Online Fraud [16, 17]. One of the scam is called Online Romance Scam [16, 18]. These scammers primarily target individuals who are looking for potential relationships as victims, via the dating websites, apps or social media, by pretending to be prospective partners [16]. Scammers generally create fake online accounts meant to attract victims. They start by professing a deep feeling for the victim and encouraging them to communicate to them secretly. As soon as the scammer has gained the victim's trust, they begin to ask for money by saying that they need funds for some kind of personal emergency [16]. Other studies have attempted to improve psychological understanding of why people fall victim to scams activity [19, 20].

What we know about scams is largely derived from studies conducted on Internet Scam and Online Fraud. The precise strategy of it is a much-debated topic among authors in many countries. However, the issue of phone scams has grown in importance in light of recent surprising facts regarding Macau Scam. To date, there has been little discussion about phone scam activities that is operating in Malaysia.

Although many research has been carried out on phone scams (e.g., [6, 21]), no single study exists which aims to study the communication in the view of phrases. Most of the work carried out on phone scams ignores the possibility that communication phrases used by scammers can be useful to identify potential scammers. Also, studies that have been conducted mostly looked at samples in Western countries (e.g., [6, 22]). Therefore, this study attempted to identify phrases used by scammers during their phone scam activities in Malaysia. This study is important in order to educate the general public on how to identify fraudulent calls through the communication phrases used by them. By being able to identify these phrases, scam cases may potentially be reduced.

1.2 Research Questions

Being financially scammed can leave emotional scars to the victim. It can make the victim feel foolish and ashamed. However, there is lack of understanding and knowledge that anyone can fall victim to a scam. Therefore this study aims to answer three research questions:

(1) Why do people fall victim to phone scams?
(2) How do scammers convince their victims over the phone?
(3) What are the communication phrases used by phone scammers to lure their victims?

2 Purpose of Study

The purpose of this study was to explore the tactics used by phone scammers to lure their victims by obtaining in-depth understanding of: (1) communication phrases uses by phone scammers; (2) the methods often used by the scammers; and (3) reasons for people falling for scams. It is hoped that this in-depth understanding would be beneficial to create awareness to the society in preventing them from falling victim. This study focused on the perspectives of eight phone victims living in the state of Selangor.

This study is expected to achieve several outcomes. Firstly, it is hoped that the findings would be beneficial to society as a whole to increase their awareness on the

strategies used by scammers when manipulating their victims through phone calls. It may help them to identify phone scams immediately after a few familiar phrases uttered by the scammer.

Secondly, the relevance of this research is that it may help authorities to reduce the number of phone-scam activities in Malaysia by preventing victims from falling for their schemes. They can reveal the communication phrases used by the scammers and their tricks to lure the victims. The expeditious process of investigating scam crimes also could be increased.

3 Research Methods

The research conducted used a qualitative approach to collect non-numerical data (words) to answer the research questions [23, 24]. Many researchers have utilised qualitative as a method of study to gain insight to the thoughts and feelings of study participants, which can help them develop an understanding of the significance that people relate to their experiences [24]. Qualitative research is based on the idea that reality is subjective as human being perceives everything individually and differently [25].

In this case, this study utilised the qualitative method of research in order to gain insight on the victims' perception on the scam activities as well as their 'first-hand' experience on being a victim. Once the interviews were conducted, they were then transcribed. The researchers then carried out a qualitative thematic analysis. The themes were then divided into major themes and sub-themes.

The data for this study was collected from eight participants representing the community of scam victims in the state of Selangor. Due to the large population in Selangor, the purposive sampling method was used. Purposive sampling reflects a set of sampling techniques based on the researcher's judgement in the selection of units (i.e., Malaysians citizen (male or female) who have experienced in losing money due to phone scams activity and Malaysian victims who have made at least one transaction to the scammers) to be analysed [26]. Purposive sampling is also known as judgmental or selective sampling categorised in non-probability sampling [27]. The sampling design is based on the researcher's judgement as to who would provide the appropriate results for the objective analysis to achieve [28].

The researchers selected the samples based on their own judgement and purpose of the research, looking for the victims which refers to an individual who have experienced in losing money due to a phone scam activity. The participation requirements were as follows: Malaysian citizen (male or female) who have experienced in losing money due to phone scam activities, Malaysian victim who have made at least one transaction to the scammers, and Malaysian victim who are willing to share their experience with the researchers.

Furthermore, the researchers made use of Internet search and telephonic inquiry to reach victims for potential data collection. Most of the first communication with the potential participants took place via email or through social networking sites (SNS) including WhatsApp and Telegram. After the researchers managed to get their approval to participate in the research, the participants were then contacted via phone. The interview date, time and location was then set up. The participants were given the consent form for

them to read the details about this research and for them to understand the potential risks (if any) if they were to participate in this research. The participants were told that the research is voluntary and that they can withdraw from participating in this research at any time. To protect the identity of the victims, they were all identified using pseudonyms such as Victim 1, Victim 2, Victim 3 and so forth.

As this research was conducted during the spread of the COVID-19 virus, the interview sessions were all held virtually via phone or Google Meet platform depending on the preferences of the participants. The interviews were conducted in English and recorded with the participants' consent. The interviews were conducted between 45 min to one hour.

4 Findings

4.1 Knowledge About Phone Scams in Malaysia

Based on the research conducted, data suggests that all of the participants are aware of the scam activities operating in Malaysia (i.e., Victim 1, Victim 2, Victim 3, Victim 4, Victim 5, Victim 6, Victim 7 and Victim 8). The participants have some knowledge and understanding on what scam is about. Two of the participants indicated that scam is an activity by someone anonymous who targets other people's money. For instance, Victim 4 explained:

> 'The very first thing comes in my mind regarding scam is actually any procedures or actions taken by one irresponsible individual towards his victim to gather their money in an illegal...illegal use.'

Victim 3 on the other hand mentioned that scam is considered a syndicate and it operates mostly in Kuala Lumpur and targets people who are desperately seeking for job despite of their age.

Scammers often use few medium such as phone calls, the Internet, social media (e.g., WhatsApp) and even face-to-face. According to four of the eight victims interviewed, (i.e. Victim 1, Victim 2, Victim 3, and Victim 7) they noticed that currently Malaysia is famous for phone scam activities instead of other mediums. Victim 2 said:

> 'But mostly *uh* in Malaysia, people kept getting tricks by this scam phone calls rather than other medium.'

Victim 7 on the other hand explained:

> 'Yes, there's so many scam calls these days. Every now and then me and my family get calls from scammers. It's a shame I fell for one of the calls.'

News and information about scams activities can be obtained by mainstream media, social media (e.g., Facebook and Twitter), and also from families and friends. In all cases, the participants reported that they received phone calls scam and resulted in some money loses. All the participants were encountered with different scenario of phone calls scam. Victim 1 shared her experienced about her being scammed by a scammer who

impersonated as a police officer who claimed that she will be sued for not parking her car at the proper parking space. This is in line with past research which had indicated that scammers often pose as police officers or other authorities (e.g., [13]).

A different scenario happened to Victim 2 where she received a call from someone impersonating as a bank officer. The 'bank officer' claimed that some money was mistakenly transferred to her bank account during the bank's system downtime. Similar to Victim 2, Victim 5 was conned a phony bank officer. However, the situation was quite extensive where the scammer knew that the victim is handling her grandfather's bank account. The experience was shared by Victim 5:

> 'I was at home and I had gotten a call by this one person he claims himself to be Encik Arman and he said that my grandfather's bank account number was forced to freeze due to some suspicious transaction.'

As for job seekers such as Victim 3 and 4, they experienced quite a different scenario. First, the scammer approached the victims by sending all the details via WhatsApp. After a while, the victims received a call from the scammer explaining more about the job and also setting up for the interview session. However, in order to secure the jobs, both victims were required to deposit the money first. According to both victims, they had deposited some money with Victim 3 depositing 100 Malaysian Ringgit, and Victim 4, 200 Malaysian Ringgit. Victim 3 offered an explanation on how the scammer introduced their company by saying that:

> 'The way he introduces and explain about the company details were very convincing. He said that it is an international company based on the overseas and has long operated in Malaysia.'

4.2 Research Questions

Despite some effort by the government and the media to create awareness on scam activities in Malaysia, many still fall victim into these schemes. Perhaps the reason why the victims were not aware that they were communicating with a scammer is that people tend to easily trust a stranger who is trying to be kind and sympathetic towards the problem that people face.

Reasons for people to fall victim to scams may vary according to the individual and surprisingly the scammers are able to predict people. According to [29], high trust in the center of scams has been reported to be one of the factors that affect why people fall victim to scams. It may seem like they are able to read people's mind but in reality, it is one of their strategies or modus operandi to trick their victims. Scammer often do background research on the potential victims and provide some details about their target. The scammer used it to trigger people as Victim 5 reported:

> 'I assume triggering me was the way, he sounded so convincing and professional, like I said. He did not force me actually. However, he had all the exact details.'

Other reasons for people to fall into scam are normally because of the need to find a job. The scammer will impersonate as the manager or any high position holder in

a well-known company and offering a job. Talking about this type of scam, Victim 3 shared that he was desperately searching for a new job because during that time, he was terminated from the previous job for some reason. As for Victim 4, he said:

> 'I want to use extra money during that time because of personal reasons and they offer me a part time which is...which has gotten my attention'

Victim 8 was also terminated from his previous job and said in short, "I was looking for a job at the time and the caller said there was a job opening."

In different scenarios, the victims will be asked for the details such as full name, address, and even Identification Card (IC) Number. [30] mentioned that the scammers set up a fake recruitment agency and, as part of the registration process, collect all the personal information of the applicants. The scammers will used it and pretending that they are going to confirm the details. Victims will share their details with the scammer as they think the scammer can solve their problem. According to Victim 2, she said:

> 'I have like carelessly share my details out of the consciousness um I give the confirmation about full name, my IC number, my address.'

Same goes to Victim 4 who said, "I did share some of my personal details such as my name, address, and even my IC number." Meanwhile Victim 8 added, "Yes I gave my details. Name, IC, address."

Some of the victims were not aware that they are not allowed to share confidential information such as Transaction Authorization Code (TAC) or confirm their security number to others, especially strangers. Victim 5 mentioned that she had shared her grandfather's security number to the scammer who impersonated as a bank officer from CIMB Bank. Victim 5 explained in length:

> 'I believe that he would have known already, as he knew a lot about our details. But by the time he asked for the confirmation and permission for the security number, I thought he was only trying to ask permission so that I immediately tried to help and share the information.'

Four of the participants mentioned that trust are the main factors triggering them to give the money to the scammer. Trust rises to a level in which the scammer is considered to be very professional, and after that the level of trust continues the same though the perceived reputability can change. Almost all participants trusted the scammers during the conversation. Commenting on the factors triggering the victims, trust is the main factor as they said:

> 'I think because I am panic during that time. He said that he is a police officer and it makes me panic and trust him,' (Victim 1)
>
> 'Everything seems so real uh I put trust on the bank officer and let him to handle the issue regarding my account,' (Victim 2)
>
> 'They gained my trust during that time,' (Victim 4)
>
> 'I felt trust to him, and I actually thought that he really genuinely wanted to help me,' (Victim 5)

Next, the factor triggering the victims is panic situation. For example, Victim 1 thought that everything was real. She got panicked and scared that her husband will get upset if she did not pay for the compensation. Thus, she wanted to settle things immediately with the 'police officer' (the scammer). She became panic because during the conversation, the 'police officer' used a fierce tone to communicate with her and she had no room to ask anything. Victim 2 also said:

> 'During that time um I like not in the right state of mind. I am very anxious and panic at the same time because…uh besides um the scammer won't give me a chance to have a doubt on him by keep loads my brain with information that is not necessary and um create more panic for me to think about consequences I will face if I did not settle the issue immediately.

Based on a previous study conducted by [31], people tend to act in response on fraudulent communications because of several key factors and one of it is trust. The victims usually pay attention to interaction rather than focusing on the message content when the scammer impersonates an authority (e.g., police officer, customs officer, and bank officer). This study is consistent with that of [18] who indicated that scammers uses threats, warnings, and dares in making sure that the victims make a transaction.

4.3 Powerful Communication Phrases Used by Scammers

Communication is a tool to connect with others and it makes our life easier. However, communication also could bring negative impacts in our lives. In the emerging era of the Internet, people can search on people's information and details with a single click. According to all of the victims, the convincing self-introduction was the main factor that they did not hang up the call. The scammers put up on tricks by convincing the victims professionally. Upon introducing themselves and the victims' brief background, it made it easier for the victim to feel that the call was legitimate. Once the victims were 'hooked', the victims then fell into the trap of giving other confidential information or make a certain monetary transaction for the scammers.

During the interview, Victim 5 indicated that the scammer mentioned to the victim about accurate details related to the grandfather's bank account, including her grandmother's name and address. Victim 5 mentioned:

> 'He was approaching me with a formal introduction. He introduced himself and he sounded really professional for me. He was also prepared with every detail about my family, so that he could sound convincing.

Along with that, as for Victim 3 and 4, the scammer will be using other medium to approach the victims to catch their interest. It has been reported that over the years, the scammers were employed the same impersonation techniques [6] in recruitment fraud. After a while, the scammer gives a phone call to explain more details. Victim 4 said:

> 'They approached me on WhatsApp. Okay. So, the reason that...they approached me, because they knew that I was looking for a part time job during that time, for

my personal things, to get extra money, and then they call me and begin to explain almost two hours.'

Impersonating as someone else is easy for the scammer because the scammer is doing it as a routine. The scammer will impersonate as a bank or police officer, a manager, and such. The scammer will also make the victims trust the scammer to help them solve any issues with the hope that it will bring to an end. Victim 2 illustrates the situation and said that the phrases used by the scammer were:

'We make mistakes during the money transfer and you need to refund it back as it is not your money.'

'I can help you to solve this problem in much easier way. All you need to do is calm down and just follow my instruction.'

As for Victim 5, she commented that the scammer knows how to make people feel anxious and panic because the scammer will read all of the details about the victim. The scammer will try to convince people with the correct details and then say that the problem can be solved with the scammer's help. The phrases used by the scammer to her was:

'If you want this to be done at the bank, we may need to do an appointment, something like that. But I will only be in Malacca next week and go back to HQ, blah, blah and then he said that he doesn't mind if I don't mind.'

Victim 6 on the other hand explained, "This is HSBC Bank. You have an overdue charge in your HSBC credit card."

Scam activities are happening around the world every day. It has now become a routine, and the scammer almost has no obstacle to confront the victims throughout the incident. Simplest way to trigger the victim's interest was illustrated by Victim 4. Victim 4 recalled what the scammer had said:

'So, do you want to work to others and get money? Or do you want to work by yourself and makes money?'

The communication phrases used by the scammers was described as very convincing. It is somewhat surprising that during the communication, the victims said threat does not exist in the conversation. The scammers lure the victims to fall victims into their scam by communicating professionally and effectively. The phrases used by the scammer is usually patterned and structured before the conversations. For instance, Victim 6 recalled, "The scammer was very professional. His English was perfect. Who would've thought."

It seems as though scammers often use the phrase "I can help you" or "let's settle this together" to convince their victims. Scammers tend to make the victims feel the intimate relations between them. Thus, it makes the victims easily trust and act in accordance with the scammers' instructions. Victim 5 said that the scammer would make people team up with them. [30] found that the victims have one of the characteristics including being sensitive to certain psychological triggers which could establishing relationships. It can be seen that the victims mostly felt anxious when speaking to the scammers, and

this may be due to the communication tone used throughout the conversation. On the other hand, the scammer used impersonation to make the victims feel worried and panic.

5 Conclusion

This study examined the factors which are thought to contribute to the public to fall victim. There are two main factors which are trust and panic. This study contributes to existing knowledge of phone scam by providing details about the scammers' communication phrases to lure the victims. Although the current research is based on a small sample of participants, the findings suggest that it is essential to identify the communication phrases commonly used by phone scammers. This is to help predict the scam activities and prevent others from becoming a scam victim. Educating the public on how scammers operate will reducing the number of people falling into a scam scheme.

In terms of the selected research method, some limitations need to be acknowledged. First, the generalisability of these findings is limited due to the number of victims willing to participate because of the traumatised experience of losing some amount of money. Also, this study is based on the recall of victims therefore the exact words uttered by the scammers may not be accurate.

One of the strengths of this study is that it represents a comprehensive examination of almost the whole conversation of the scammers and the victims. The findings of this study are useful for authorities to create more effective awareness and disseminate a piece of accurate information by exposing the communication phrases used by the scammers.

Further studies on the current topic is required. Future researchers should investigate the extent of pattern and structure used by the scammers to lure their victims. In future work, it would also be essential to compare the experiences of individuals within the same demographic background such as age, gender, level of education, or occupation.

Acknowledgments. The authors would like to thank all participants for their involvement in this research. The authors would also like to thank the Faculty of Communication and Media Studies, Universiti Teknologi MARA for approving this research.

Authors' Contributions. Both authors have made substantial contributions to conception and design, data collection, and analysis. They have also equally been involved in drafting the manuscript and revising it critically.

References

1. Australian Competition & Consumer Commission (2021, September 27). Losses reported to Scamwatch exceed $211 million, phone scams exploding. [Media Release]. https://www.accc.gov.au/media-release/losses-reported-to-scamwatch-exceed-211-million-phone-scams-exploding
2. N. Md Nur. "Three-quarters of Singaporeans answered scam calles recently: Toku. *The Edge,* June 30, 2022. https://www.thesundaily.my/local/housewife-student-lose-over-rm250000-to-macau-scam-syndicate-YX9066199

3. A. Wong. "Malaysians on receiving end of world's biggest percentage of scam calls, new data claims."*The Sun Daily,* December 4, 2019. https://www.thesundaily.my/local/housewife-student-lose-over-rm250000-to-macau-scam-syndicate-YX9066199
4. D. J. Wong. "Within 3 months in 2021, Malaysians lost over US$9 million to spam calls." *Mashable SEA,* December 30, 2021. https://sea.mashable.com/life/18790/within-3-months-in-2021-malaysians-lost-over-us9-million-to-spam-calls
5. J. Lim. "Cover study: Consumers more vulnerable to scams during pandemic." *The Edge Malaysia*, October 7, 2020. https://www.theedgemarkets.com/article/cover-story-consumers-more-vulnerable-scams-during-pandemic
6. M. Bidgoli, J. Grossklags, "Hello. This is the IRS calling: A case study on scams, extortion, impersonation, and phone spoofing", 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, USA, 2017, pp. 57–69, doi: https://doi.org/10.1109/ECRIME.2017.7945055.
7. M. F. Mubarak, S. Yahya, A. Shaazi. M. A review of phone scam activities in Malaysia, in: Conference 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), 2019, pp.441–446. DOI: https://doi.org/10.1109/ICSEngT.2019.8906491.
8. G. Drevitch. "The phone scam targets psychologists." *Psychology Today*, October 26, 2021. https://www.psychologytoday.com/us/blog/the-fraud-crisis/202110/the-phone-scam-targets-psychologists
9. T. A. Yusof. "Malaysia in top 20 nations most affected by scam calls." *New Straits Times,* December 14, 2019. https://www.nst.com.my/news/nation/2019/12/547741/malaysia-top-20-nations-most-affected-scam-calls
10. Truecaller. "Most Malaysians are still susceptible to spam calls." *Focus Malaysia,* February 1, 2022. https://focusmalaysia.my/most-malaysians-are-still-susceptible-to-spam-calls/
11. Bernama. "Macau Scam's new tactic: A police notice to probe Macau Scam." *Free Malaysia Today*, June 13, 2022. https://www.freemalaysiatoday.com/category/nation/2022/06/13/macau-scams-new-tactic-a-police-notice-to-probe-macau-scam/
12. I. L. Hussein. "Penipuan dalam talian jadi jenayah komersil utama negara."*Berita Harian Online,* June 25, 2022. https://www.bharian.com.my/berita/nasional/2022/06/969890/penipuan-dalam-talian-jadi-jenayah-komersil-utama-negara
13. A. Shah. "Jamming the Macau scammers.*The Star,* February 21, 2022. https://www.thestar.com.my/news/nation/2022/02/21/mcmc-working-to-identify-and-block-macau-scam-calls
14. J. Riduan. "Teacher loses RM254,600 to Macau Scam syndicate.*New Straits Times,* April 3, 2022 https://www.nst.com.my/news/crime-courts/2022/04/785569/teacher-loses-rm254600-macau-scam-syndicate
15. Bernama. "Housewife, student lose over RM250,000 to Macau Scam syndicate." *The Sun Daily*, December 4, 2022. https://www.thesundaily.my/local/housewife-student-lose-over-rm250000-to-macau-scam-syndicate-YX9066199
16. M. E. Saad, S. N. Sheikh Abdullah, M. Z. Murah. Cyber romance scam victimization analysis using Routine Activity Theory versus Apriori Algorithm. *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, pp. 479–485, 2018, DOI: https://doi.org/10.14569/IJACSA.2018.091267.
17. A. I. Zahari, R. Bilu, J. Said. The role of familiarity, trust and awareness towards online fraud.*Journal of Research and Opinion*, vol. 6, no. 9, pp. 2470–2480, 2019, DOI: https://doi.org/10.15520/jro.v6i9.23.
18. A. H. Shaari, M. R. Kamaluddin, W. F. Paizi. Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, vol. 19, no. 1, pp. 97–115, 2019, DOI: https://doi.org/10.15520/jro.v6i9.23.
19. T. Sorell, M. Whitty. Online romance scams and victimhood. *Security Journal*, vol. 32, no. 3, pp. 342–361, 2019, DOI: https://doi.org/10.1057/s41284-019-00166-w

20. M. M. Button, C. M. N. Nicholls, J. Kerr, R. Owen, Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, vol. 47, no. 3, pp. 391–408, 2014, DOI: https://doi.org/10.1177/000486581452122
21. H. Tu, A. Doupé, Z. Zhao, G. J. Ahn. Users really do answer telephone scams. In 28th USENIX Security Symposium (USENIX Security 19), 2019, pp. 1327–1340.
22. S. Prasad, E. Bouma-Sims, A. K. Mylappan, B. Reaves. Who's calling? characterizing robocalls through audio and metadata analysis. In 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 397–414. 2020.
23. V. Pathak, B. Jena, S. Kalra. Qualitative research. *Perspectives in Clinical Research*, vol. 4, no. 3, pp. 192, 2013, DOI: https://doi.org/10.4103/2229-3485.115389
24. J. Sutton, Z. Austin. Qualitative research: Data collection, analysis, and management.*The Canadian Journal of Hospital Pharmacy,* vol. 68, no. 3, pp. 226–231, 2015, DOI: https://doi.org/10.4212/cjhp.v68i3.1456
25. A. J. Cropley. Introduction to Qualitative Research Methods. Riga, 2019.
26. G. Sharma. Pros and cons of different sampling techniques. *International Journal of Applied Research*, vol. 3, no. 7, pp. 749–752, 2017.
27. E. A. Crossman. Understanding purposive sampling: An overview of the method and its applications. *ThoughtCo,* September 28, 2018 https://www.thoughtco.com/purposive-sampling-3026727
28. I. Etikan, S. A., Musa, R. S., Alkassim. Comparison of Convenience Sampling and Purposive Sampling.*American Journal of Theoretical and Applied Statistics*, vol. 5, no. 1, pp. 1–4, 2015.
29. H. Y. Lu, S. Chan, W. Chai, S. M. Lau, M. Khader. Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention and Community Safety*, vol. 22, no. 4, pp. 313–330, 2020, DOI: https://doi.org/10.1057/s41300-020-00098-3
30. M. Stella. Deceiving the Deceived: An analysis of the United Nations Compensation Scam.*Journal of Literature, Languages and Linguistics*, vol. 23, pp. 1–7, 2016.
31. P. Fischer, S. E., Lea, K. M. Evans. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, vol. 43, no. 10, pp. 2060–2072, 2013, doi: https://doi.org/10.1111/jasp.12158

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.