INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 2, (2025) E-ISSN: 2222-6990

A Qualitative Approach of KAP Model Against Online Scam in Malaysia

[1]*Salbiah Nur Shahrul Azmi, [2]Zurairah Jais, [3]Shahrul Niza Samsudin, [4]Noor Fariza Mohd Hasini, [5]Nor Izzuani Izhar, [6]Nor Ainee Idris, [7]Azwan Amirulsyafiq Abu Hassan

[1,2,3,4]Faculty of Business, Hospitality & Technology, Universiti Islam Melaka, Kuala Sungai Baru, 78200 Melaka, Malaysia [5,6]Academy of Language Studies and Translation, Universiti Islam Melaka, Kuala Sungai Baru, 78200 Melaka, Malaysia, [7]Royal Malaysia Police, Seberang Perai Tengah, Pulau Pinang, Malaysia

Corresponding Author Email: salbiahnur@unimel.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i2/24701 DOI:10.6007/IJARBSS/v15-i2/24701

Published Date: 15 February 2025

Abstract

This study aims to examine the online scam phenomena in Malaysia by emphasizing consumers' knowledge, attitude and practice (KAP) against the threat of the crime. Statistic shows the increment of online scam cases with various modus operandi used by cyber criminals, among them are online purchase scams and investment scams. By using qualitative approach, this study has interviewed Royal Malaysia Police (RMP) Investigation Officers and scam victims in order to gain deep insights and their experiences. The result of this study has given a clear picture towards consumers' level of awareness and the steps that can be taken in reducing the risks from becoming the victim of online scam crime. The finding from this study is hoped to contribute to the development of strategic online scam prevention that is more effective particularly in Malaysia.

Keywords: Online Scam, KAP Model, Knowledge, Attitude, Practice

Introduction

Online scam has become a critical issue in Malaysia, in line with the increase of internet use and digital technology. According to a report by Cyber Security Malaysia, the number of online scam cases have increased significantly in the recent years. This shows how serious the threat is to the society (CyberSecurity Malaysia, 2023). MyCERT Cyber999 conducted by Cyber Security Malaysia has recorded that online scam has retained the top chart of cyber security incident with the total number of cases 3,087 from the overall 4,898 cases in the mentioned year. Online scam includes various forms such as scam through fake websites, e-mail phishing and telecommunication scams. Society which has not enough knowledge about online security measures tends to be the victims to this state-of-the-art modus operandi.

In Malaysia, though there are continuous efforts done to give exposure to the society regarding online scams, there are still gaps between rising case statistics, efforts done and academic findings in this crime scope. Research gaps are divided into three: firstly, it is related to the understanding regarding online scam is still fragmented, in addition to previous studies focused more on certain aspects without giving a complete description about this phenomenon. As an example, a study done by Dinya Solihati et al., (2023) showed that online scams are developing in terms of forms and strategies, however, the understanding about the various types of scams and its effects on various sectors are still insufficient.

Secondly, the responds towards online scams, in terms of rules, technology as well as users' awareness still do not show sufficient effectiveness. A study by Koibichuk et al., (2021) found that there are increment in cyber security measures, cyber criminals are able to exploit certain weaknesses, showing that the existed respond strategies have to be refined and renewed. In addition, users' responds towards this threat are usually inconsistent, due to lack of awareness or deep understanding about the risks faced. Thirdly, although there are prevention measures being introduced, the effectiveness about these measures is being questioned. In a study by Alias et al., (2022), it was found that several prevention measures used by finance sectors showed no success in preventing the online scams. This shows the urgent need to identify and develop a more holistic and effective prevention measures which do not only rely on technology but also users' education and the increment of regulation control.

Although there are awareness campaigns and initiatives taken by the authority, the number of online scams still show a concerning increment. Latest statistics shows that online scams have become a popular modus operandi among cyber criminals with various new tactics that is created to confuse and trap victims (MCMC, 2023). The main problem identified is lack of awareness and deep understanding among internet users about the risks and the early signs of online scams. This creates an urgent need for an in-depth study about the level of knowledge, attitude and practice (KAP) of the users against online scams. Without a clear understanding about how users respond and the security measures they take, it is difficult for the authority and policy maker to create effective strategies to curb this problem. Thus, in order to bridge the relevant gap, the objectives of the study are as follows:

1. To investigate online scams in depth.
2. To explore the responses against online scams.
3. To identify appropriate preventive measures against online scam.

Literature Review

Online scam

In Malaysia, the increment of online scam crimes is tangible evidence on the seriousness of this threat. In 2022, according to statistics produced by the Malaysia government the total of loss due to online scams are RM 1.73 billion and between January until September 2023 also increased to RM 687 million or 29 percent compared to the same duration in 2022 (Majlis Keselamatan Negara, 2024). These statistics shows a more increasingly urgent threat, which needs a quick and effective action from all parties.

This issue comes from lack of awareness and being indifference among society. Although there are many awareness campaigns done by the authority such as the Royal Malaysia Police (RMP), there are still people who fall victims due to lack of knowledge regarding this crime modus operandi. Therefore, society's understanding about the prevention measures of online scams must be enhanced continuously, because the tactics and modus operandi of this crime are always changing. This gives an emphasis towards the continuous education and more aggressive awareness initiatives to protect the society from being the victims of online scams.

According to RMP (2024), this online scam crime refers to the action of the criminals, also known as online scammers, who do not face with the victims, using third party identities to do their scams (mule account), and do not involve physical violence. There are eight online scam crimes' modus operandi such as online shopping scams, non-existent loan scams, investment scams, love scams, part-time job-offer scams, application scams and impostor scams. Besides that, Abdul Karim & Lyndon (2023) have listed types of online scams globally such as cyber extortion, breach of user personal data, user identity theft, psychological and mental harassment and cyber bully and pretending to get data based on a well-known organization.

This issue has shown how important it is a continuous action to educate the society about the online scam crime risks and to enhance the level of cyber security. The society has to be more proactive in protecting themselves from being scam victims by utilizing educational resources and provided information by the authority. With the enhancement oof awareness and knowledge, it is hoped that the number of online scam crime can be reduced in the future.

Model of Knowledge, Attitude and Practice (KAP Model)

The model of Knowledge, Attitude and Practice has proved its importance in understanding and overcoming this issue. it integrates three main components: knowledge about cyber-crime, attitude towards cyber -crime prevention and online security practice. Knowledge plays an important role in an individual's life where the more knowledge we possess the more influence it plays in changing someone's attitude. A changed attitude will bring to an increase of confidence, thus, affecting a person's practice. Knowledge is considered as the main element, because without knowledge, a person is unable to act based on information gained. Recent studies have shown the significant increment of knowledge about cyber-crimes is related to risk reduction from being online scam crimes. This knowledge includes the understanding on various types of scam that exist, the technics used by scammers, and the ways to identify and avoid from the threats. This is proved by Pitchan et al., (2022) in their study who find that the young people who possess knowledge and awareness are able to protect themselves from being cyber-crime victims and able to face risks from online shopping.

Other than that, digital citizenship also has significant impact regarding the awareness and cyber-crime prevention among higher learning institution students and the result from this study shows that the knowledge about digital law and digital communication skills are important in reducing cybercrimes. In relation to a study done by De Kimpe et al., (2021) indicates that an individual who are well informed about online security tend to feel less vulnerable against cyber-crime and less likely to take security measures. Even, this is proved

from a study done by Abdul Wahab et al., (2023) saying that knowledge and society's awareness is correlated with online scam crime cases which are still at large.

Meanwhile, the attitude factor, an individual's attitude towards cyber-crime prevention, plays an important role in KAP model. The change of attitude of an individual will encourage them towards the change of behavior because human behavior has close relation to attitude. When attitude change, behavior will indirectly change. In this case, the change of attitude happens when an individual gain new knowledge. This idea is supported by the behavioral cognitive-rational model, which mentions that human changes their behavior after they receive and assess new information rationally (Hagger et al., 2020). A positive attitude towards cyber security includes the preparation to practice security measures and a high perception towards the important issue of cyber security. A proactive attitude towards cybersecurity also can reduce the tendency to become a victim of online scams. In addition, Abdul Wahab et al., (2023) also emphasize that the lack of vigilance among the community contributes to the increase in online scam cases. Therefore, the community needs to adopt a curious attitude and be more aware of current developments, including new tactics and modus operandi of cybercrime.

From the perspective of practice, the practice of online security is a practical manifestation from knowledge and attitude. This includes the use of security software, the management of safe password and being careful in e-mail interaction and suspicious messages. According to Uthoff (2022), practice refers to the way a person applies their knowledge through action. When a knowledge is understood deeply, attitude and practice can enhance the quality of action and encourage the process of awareness (Mahmud & Siarap, 2013). It shows that these practices directly influence an individual effectiveness in avoiding online scams. Moreover, a study done by Priya & Ranganathan (2022) proposes one of the ways to enhance the level of people's awareness about cyber security is through playing cards which means involving the development of gaming platform that enables the players to learn about various cyber-attacks and defend mechanism. Meanwhile, based on the result of a research by Elena et al., (2021), about the role or responsibility of a certified auditor in reducing the effect of cyber scams where they need to give more emphasize on training, courses and awareness workshops to prevent the incidents caused by human errors particularly in the financial sector which is always the target of cyber scams on its employees in the department. Abdul Wahab et al., (2023) also say that an individual begins to know or learns about a practice and later develop a positive attitude towards it.

Methodology

This section will explain research design, research instruments, analysis unit, sampling and research analysis method.

Research Design

Qualitative research design is selected in order to gain detailed and deep explanation about the experience of the participants because the researchers only have a general idea related to the research topic. Therefore, the concept of the research design will develop when the researchers start to understand the background and research topic content through exploration and research which is done directly towards the participants.

Instrument and Analysis Unit and Research Sampling

The researchers are the main instrument in collecting and analyzing data. Data collected by the researchers through interview question kit which is developed based on secondary sources which was tested and given directly to the research analysis unit i.e. Investigating Officer (RMP) and directly involved victims in the online scams based on cases that occurred in Malaysia. The type of interview questions is semi structured and is used based on modifications that happen during the research.

Research Analysis Method

In a qualitative research that uses purpose sampling, the suitable data analysis method is important in ensuring deep understanding about the phenomena being studied. Thus, thematic analysis is used because of its flexible characteristic and able to help in identifying the main theme in research data. The first step involves reading and understanding data as a whole for the process of identifying the collected data. Next, data that are identified will be coded according to suitable category or theme. In order to develop a theme in the third step, the codes that were categorized will be organized into a wider theme. Lastly, those themes will be connected to research objectives as well as KAP model that is used to interpret the themes.

Results

The results of the study are divided into interviews with investigating officer and victim involved in online scams.

Results of Interviews with Investigating Officer (RMP)

The interview questions were categorized into three themes i.e. knowledge, attitude and practice. Thus, this section has recorded the research findings from the interview that are asked towards the Investigative Officer of the Commercial Crime Investigation Department, RMP regarding online scams. The summary of the findings from the interview questions are as follows:

Table 1
Findings from Interview Session with Investigative Officer of The Commercial Crime Investigation Department, RMP

Theme 1: Knowledge (K)	
Objective 1: Investigating online scams in depth.	
Q1	What is the meaning of online scam?
A1	Scam which does not face to face between the scammer and the victim, using mule account or third-party account, and does not use physical violence because there was no meeting was made with the victim.
Q2	What efforts are made by the RMP in giving exposure to the society regarding online scam?
A2	Exhibitions and awareness programs involving talks related to online scam crime
Q3	What is the common modus operandi usually used by the scammers to do online scam?

A3 Among 8 popular online scams in Malaysia such as apk application scam, phone scam or macau scam, love scam/parcel scam, online shopping scam/e-commerce crime, non-existent loan, investment scam, part-time job-offer scams, impostor scam.

i) Apk application: apk link will be given through Whatsapp. Then, the scammer will extract the victims' Whatsapp contacts to make the scam by asking to borrow money. Victims who click on the related link will then be the scam victims.

ii) Phone scam: a scam through a phone call. The scammer will disguise as coming from government or private agencies such as from RMP, Malaysian Anti-Corruption Commission (MACC), and J&T Express for the purpose of intimidating the victims. In order to solve problems created by scammers, victims will be threatened such as bank account will be frozen and linked to AMLA. The scammers will ask the victims to make money transfer to the given account number (they will vanish after getting the money). There are victims who are willing to make a loan because of panic being threatened to make the transfer.

iii) Love scam/parcel scam: victims will meet the scammers through social media and establish a romantic relationship with the victims. Then, the scammers will tell the victims that gifts will be sent through parcel. Then, the victims will get a phone call saying that the parcel is stuck somewhere causing the parcel to be unable to be delivered. However, the victim is suggested to make money transfer to solve the problem. Most victims are lonely women, women who are alone or aged women. Victims among men are caused by business scam.

iv) Online shopping scam/e-commerce crime: this is among the commercial crimes that happens the most. It happens when the victim is given an account number to make online payment for a n ordered goods, then, when the ordered goods is not delivered, the victim is unable to contact the seller because the scammer no longer use the number anymore.

v) Non-existent loan: this modus operandi rarely happens among students. For the first situation usually, victim will find loan from the internet and follow instruction on the platform. Victim is usually being contacted to further discuss about the intended loan. However, victim is asked to pay for the duty stamp, process money and other costs into the mule account and usually victim will follow scammers' instruction because they think this is to ease the loan process. In this case victim will only deal through phone and never meet the scammers. All company details in order to convince the victim that are shown by the scammers are fake. In the end, the victim suffers the loss due to the forefront payment and does not get the amount of the promised loan.

Meanwhile, for the second situation, the victim will surrender all personal details to do the online loan and only be given the loan less than the agreed amount. Then, the victim will be threatened to pay the loan installments with high rate interests within less than one month from the date of the loan. Not only the victim will be threatened, but also the victim's acquaintances or family will be threatened. Such criminals are also known as loan sharks, the '*Ah long'* scammers.

vi) Investment scams: This is also among the top commercial crimes. Usually, the victim will be set into a Whatsapp or telegram group and most of the victims involved are caused by greed. Most schemes use the excuse of charging fees to obtain returns from the investment in question; however, once the payment is made, the scammers typically ask the victim to add more money because the purported investment returns have supposedly increased. All evidence to convince the victim will be included in the group by the scammer posing as an investor at the same time. In the end, the victim does not receive the promised investment

returns.

vii) Job offer scams: This type of scam occurs when the victim receives a WhatsApp message or an online job offer. Usually, the victim will be asked to make a payment supposedly to buy the goods they want to sell first and be promised a refund of the payment along with a commission. However, the true concept of online work is that there are no fees to be made by employees or victims.

viii) Scams impersonating acquaintances: Usually, the person who receives the apk will click the link, so all the recipient's contact data will be stolen by scammers. The next scammer will impersonate the victim's acquaintance to borrow money and request assistance. The scammer will use the victim's acquaintance's profile but with a different number.

Among all modus operandi, investment scam recorded the highest losses as in the case of situation 1, the report involved losses reaching millions of ringgits.

Q4 In your opinion, based on the latest crime trends, what is the level of awareness and knowledge of the public towards online scam?

A4 The level of public awareness and knowledge, especially related to modus operandi, is still lacking despite efforts to spread awareness and this can be proven based on crime statistics that have increased from year to year. It can also be proven that some of the victims involved are mostly professional workers such as teachers.

Theme 2: Attitude (A)

Objective 2: Exploring responses to online scams.

Q1 Through the efforts undertaken by the RMP, is there any positive or negative feedback from the community?

A1 In combating the issue of online scam, the RMP has conducted numerous crime prevention campaigns such as talks and town halls. As a result of these prevention campaigns, the RMP has received positive feedback from the community, largely due to the community's lack of knowledge regarding online scam.

Q2 Is this online scam crime a result of the society's careless attitude or due to a lack of awareness and knowledge regarding online scams?

A2 Lack of knowledge regarding fraud trends and the greed of fraud victims.

Q3 Is it possible that the public has knowledge about online scam, but due to the urgency of the situation, they are caught up in the crime of online scam?

A3 Yes, this can be proven for instance if the community continues to take online loans without any prior verification with the bank and other financial institutions, leading them to fall into the trap of online loan sharks.

Theme 3: Practice (P)

Objective 3: Identifying appropriate preventive measures against online scam.

Q1	What preventive measures can be suggested to avoid online scam?
A1	Among the preventive measures that can be taken are; - Don't panic, ask questions and don't act on your own. Be aware and share the calls or scams received with family members or close acquaintances as most victims do not tell their problems because they have been threatened by scammers. - Don't share bank information with third parties. - Do not entertain messages received by the RMP, MACC or any agency that uses private numbers. Usually, government agencies especially will not give instructions for money transfers. - Do not click on suspicious links. - Create double verification and use phone call tracking apps such as whos call or true caller. - Use a mule check to find out the legitimacy of the account number provided by the scammer. - Be aware of scams information - Avoid becoming an account mule - Make purchases on trusted platforms and apply for loans in person at offices licensed by the Central Bank of Malaysia (BNM) or Ministry of Housing and Local Government (KPKT). - Contact the National Scam Response Centre (NSRC) at 997 for fraud or scams that occurs within 24 hours so that the mule account or perpetrator will be frozen immediately.
Q2	Are the existing laws sufficient to address scam crimes?
A2	So far, the existing legal provisions are sufficient to overcome the crime of online scam. However, the challenge of tracking down cybercriminals is more challenging than face-to-face crime. Online scam is different from face-to-face fraud because face-to-face fraud makes it easier to track down criminals if there is physical evidence such as photographs, vehicle number plates and so on. This is in line with a higher percentage of cybercrime than face-to-face crime at 80%. The first step that the RMP will take to track down online criminals is to check the account owner. Then the account will be frozen and the account owner will be interrogated.
Q3	What is the impact of online scam crime on the country?
A3	Overall, this crime contributes to significant losses and undoubtedly affects the financial well-being of society. Online scam has increased alongside technological advancements as online scammers become more sophisticated and exploit technological weaknesses. It is not impossible that in the future, crimes involving the use of AI will occur.

Source: Author's compilation

Results of Interviews with Victim

The interview questions have been categorized into 3 themes, namely knowledge, attitude, and practice. Therefore, this section records the findings of the study from the interviews conducted with victims who have been involved in online scam. The analysis of the findings from the questions posed is as follows;

Table 2
Findings from The Interview Session with Victim Who Have Been Involved in Online Scam

Theme 1: Knowledge (K)	
Objective 1: Investigating online scams in depth.	
Q1	Do you have knowledge regarding online scams before becoming a victim of this scam?
A1	To be honest.... I'm used to hearing cases of online scams. However, my knowledge is limited as I have been entangled in this scam.
Q2	Do you know and are you aware of the modus operandi used by scammers?
A2	In my case, I did not know and was not aware of the modus operandi used by the scammers. What I knew at that time, I needed money and I did a Google search related to online loans because I thought it was a simple and fast method.
Q3	In your opinion, are the efforts undertaken by the authorities sufficient to provide awareness and knowledge regarding online scams?
A3	In my opinion, efforts to provide awareness should be expanded in the workplace regardless of the government or private sector because many victims are also among individuals who are employed and have income but are exposed to the risk of being scammed.
Theme 2: Attitude (A)	
Objective 2: Exploring responses to online scams.	
Q1	What caused you to become a victim of online scam? Could you please share your experience?
A1	I did an online loan search on Google and clicked on several links to the service provider's site. Through several surveys conducted, I was attracted to an online loan offer by a company that I thought was registered, but after realizing that I was a victim of scams, I found out that the company was not legitimate and not registered as a licensed money lending provider. I have provided all the necessary information for the purpose of the loan and without me realising that all the data on my mobile phone has been stolen by scammers. This is a consequence of the link I clicked on the website of the non-existent loan provider.
Q2	Have you taken into account personal data security or link security factors before falling victim to online scams?
A2	I admit that I was careless and did not take into account the security of personal data or links at that time. What I do know, how easy it would be to take out an online loan that doesn't have to go through strict procedures like a bank.
Q3	Has the compelling circumstance factor caused you to fall for online scams without thinking about the link security factor?

A3	Yes. It's right because what I know is that I want to earn money in a short time. However, not all of the promised loan amounts were given by the scammers. They give an amount that is less than the agreed amount and manipulate the amount.
Q4	Did the scammer threaten you? What is the form of the threat?
A4	Yes... to me and my family. They have sent threats on WhatsApp to me and my family that they got from the data stolen through contacts on my phone. They requested my family to repay the borrowed amount with a multiplied sum and they also manipulated the transaction evidence by stating that I had borrowed a large amount.
Theme 3: Practice (P)	
Objective 3: Identifying appropriate preventive measures against online scam.	
Q1	What steps have been taken upon realizing that you have become a victim of online scam?
A1	I have collected all the evidence of the conversations and payment transactions that have been made to the scammer. I took all the evidence to the police station to make a report of threats and threats as my family and I had paid more than we should have but were still threatened by the scammer. Then, our family acted to block the numbers used by the scammer and changed the phone number. I have also changed the device I am using to prevent the scammer from tracking me and my contacts. This was on the advice of PPIM which I contacted for advice on the problem I was facing.
Q2	Is the existing legislation sufficient to address online scam crimes today?
A2	The existing laws are sufficient but for me, the exposure related to the modus operandi of scammers needs to be expanded because in my case, I am not aware and do not know about the modus operandi of these scammers.
Q3	What is the impact of this scam crime on your life?
A3	The impact is huge because it does not only involve me but my family and they are in a state of trauma with the threats given. From that day on, it was no longer easy for me to press any link given by any party. I also no longer believe in any online loans and will only take loans with banks.

Source: Author's compilation

Discussions

This study provides an overview and depth of the online scams' phenomena in Malaysia, highlighting how the KAP (Knowledge, Attitudes and Practices) Model can shed light on the awareness and prevention measures of online fraud crimes among consumers. For the first objective, interviews with RMP Investigating Officers and scam victims proved that consumers' knowledge of the modus operandi of fraud is still lacking despite various awareness campaigns conducted by RMP. It can be demonstrated through the findings of the interviews that the RMP has conducted exhibitions and awareness programs aimed at exposing the community to the trends and modus operandi of online scam crimes. From the victims' perspective, they acknowledge that they do not possess in-depth knowledge regarding the modus operandi of scammers, despite having heard about online scam cases.

These findings are consistent with the studies by Abdul Wahab et al., (2023), and De Kimpe et al., (2021), which found that the knowledge and awareness of the community are related to the ongoing prevalence of online scam crimes.

Secondly, the attitudes of consumers who are careless or influenced by urgent circumstances also contribute to those who are victims of scams. For example, online loan scams and the use of unchecked harmful links indicate weaknesses in terms of user knowledge and attitudes. Therefore, to address the second objective, the findings of this study concur with the research by Abdul Wahab et al., (2023), which also emphasizes that the lack of vigilance among the community contributes to the increase in online scam cases. Furthermore, the attitude of greed has also been found to encourage the tendency of victims to fall prey to the scams of scammers. As a result, the victim's attitudes of greed, desperation, carelessness, and disregard for personal data security invite danger when the victim is threatened by scammers, simultaneously dragging the victim's family into the situation. However, the preventive measures recommended by the RMP and the victims, such as not acting alone and using security applications to screen calls and account numbers, can help reduce the risk of online scams. Behavioural change occurs when individuals acquire new knowledge, which is also in line with the cognitive-rational behavioural change model, indicating that humans alter their behaviour after receiving and rationally evaluating new information (Hagger et al., 2020). The recommendations put forward by RMP and the victims need to be considered in order to indicates that a proactive attitude towards cyber security can reduce the tendency to become a victim of online scams.

The findings for the third objective also confirm that education related to cyber security and online scam needs to be strengthened, particularly in providing users with a deeper understanding of cyber threats and how to protect themselves from becoming victims. Although the existing laws are sufficient, the level of awareness and the proactive attitude of the community towards cyber security need to be enhanced. Scammers are becoming increasingly aggressive and utilizing advanced technology in executing their tactics, including the use of third-party identities and psychological threats to trap victims. As a result, the need to devise more holistic preventive measures is high. This is supported by studies such as Uthoff (2022) which emphasize that practice refers to how an individual applies their knowledge through actions. Furthermore, when knowledge is understood more deeply, attitudes and practices can enhance the quality of actions and promote the process of awareness (Mahmud & Siarap, 2013). In this case, the victim has taken heed by exercising caution and not easily trusting any online offers, in line with the findings by Abdul Wahab et al., (2023) which add that an individual begins to know or learn about a particular practice and subsequently fosters a positive attitude towards it.

Overall, this study successfully addresses the research objectives to gain an in-depth understanding of online scam, explore responses to online scam, and identify appropriate preventive measures against online fraud by interviewing participants directly involved with this crime. Thus, the proposed research framework based on discussions from the results of the research conducted is as follows;

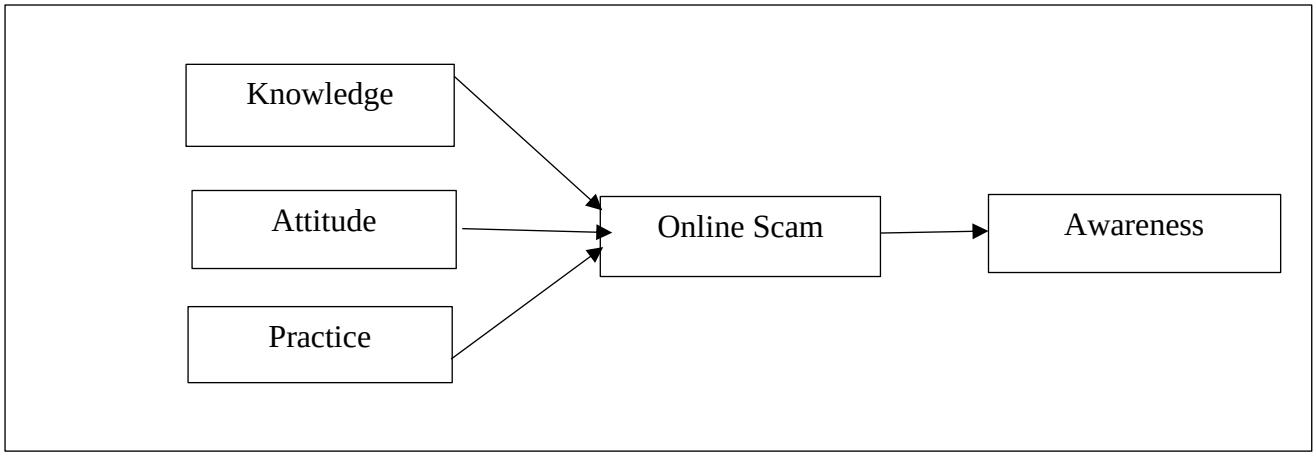

Figure 1. KAP Model Research Framework on Online Scams in Malaysia.
Source: Author's compilation

As discussed above, the KAP model is seen to be related to public awareness of online scams. This framework was formed from research results that showed variations in each factor in the KAP model, namely knowledge, attitude and practice.

Conclusions and Recommendations

Online scams represent a serious threat to cyber security in Malaysia, particularly with the increasing use of digital technology. This study found that a lack of knowledge, apathy, and weak security practices are the main factors that lead users to become victims of online scams. Although various preventive measures have been implemented, statistics indicate that online scam continues to rise. This further underscore the need to enhance public awareness regarding online scam and how individuals can protect themselves from becoming victims. The KAP model demonstrates that knowledge, attitudes, and practices are the key in developing a more effective response to this threat.

The following are recommendations to address the issue of online scams:

1. **Cyber security education:** Educational institutions and authorities need to collaborate to introduce cyber security modules in school and university curricula. Increasing knowledge, particularly regarding the modus operandi of online scam crimes, is essential to reduce the risk of users becoming victims.
2. **The organization of awareness campaigns more extensively:** The authorities need to intensify awareness campaign efforts involving various platforms, especially social media, briefings at the workplace, and campaigns within the community and society. This aims to ensure that information is conveyed effectively, particularly to those who are likely to be exposed to online scam.
3. **Accessible Safety Applications and Tools:** Users need to be exposed to security applications such as "Who's Call" or "True Caller" to identify suspicious calling numbers. Internet service providers can also play a role by offering security alert notifications to users.
4. **Development of a More Stringent Police and Legislation:** The authorities need to consider measures to streamline the enforcement of laws against cyber scammers, as well

as to leverage artificial intelligence (AI) technology to detect online fraudulent activities more quickly and effectively.

5. **Cooperation with Financial Institutions:** Financial institutions need to be more proactive in helping consumers to identify suspicious transactions and provide education on online scam crimes.

Lastly, in terms of contribution, this study has proposed the KAP Model Research Framework on Online Scams in Malaysia as shown in Figure 1. This framework has bridged the gap between theory and practice based on interviews conducted with individuals who are directly related to the study problem. The framework confirms that public awareness of online scams can be influenced by knowledge, attitude and practice factors. In addition, this study has also suggested several useful suggestions for further development in order to reduce the risk and impact of online scam crimes, as well as build a society that is more vigilant against cyber threats in the future. The interview method with parties directly involved in the research problem also contributed to providing in-depth knowledge and experience related to online scams in line with the stated study objectives.

Acknowledgements

This work was supported by Universiti Islam Melaka (UNIMEL) through the Incentive Research Grant (IRG) 2024/2025 (GPI/24/F3/07).

References

Abdul Karim, M. Y., & Lyndon, N. (2023). Pandangan dunia pengguna perniagaan dalam talian tentang jenayah siber. Malaysian Journal of Social Sciences and Humanities (MJSSH), 8(7), e002392. https://doi.org/10.47405/mjssh.v8i7.2392

Abdul Wahab, E., Pitchan, M. A., & Salman, A. (2023). Pengetahuan, sikap dan amalan masyarakat di kuala lumpur terhadap kempen pencegahan jenayah penipuan dalam talian. Jurnal Komunikasi: Malaysian Journal of Communication, 39(1), 240–258. https://doi.org/10.17576/JKMJC-2023-3901-14

Alias, N. S., Mahamood, A. F., Tengku Yakob, T. K., Ramli, A. J., Affandy, H. B., & Abdul Manaf, A. R. (2022). Fenomena phishing di Malaysia: persepsi masyarakat, kesan dan kaedah mengatasi. Journal of Global Business and Social Entrepreneurship (GBSE), 8(24), 132–158. https://www.researchgate.net/publication/361205162_FENOMENA_PHISHING_DI_MALAYSIA_PERSEPSI_MASYARAKAT_KESAN_DAN_KAEDAH_MENGATASI

CyberSecurity Malaysia. (2023). Mid-Year Report Threat Landscape 2023. https://www.cybersecurity.my/data/content_files/26/2511.pdf

Hagger, M. S., Cameron, L. D., & Hamilton, K. (Ed.), & Hankonen, N., & Lintunen, T. (2020). Changing behavior: a theory-and evidence-based approach. In M. S. Hagger, L. D. Cameron, K. Hamilton, N. Hankonen, & T. Lintunen (Eds.), The Handbook of Behavior Change (pp. 1-14). Cambridge University Press. https://doi.org/10.1017/9781108677318.001

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K., (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808, https://doi.org/10.1080/0144929X.2021.1905066

Dinya Solihati, K., Rizki, M., & Sari, N. (2023). The role of the government to improve financial literacy in efforts to prevent the use of illegal online loans. The 4th International Conference on Governance, Public Administration, and Social Science, 2023, 670–687. https://doi.org/10.18502/kss.v8i11.13581

Koibichuk, V., Ostrovska, N., Kashiyeva, F., & Kwilinski, A. (2021). Innovation technology and cyber frauds risks of neobanks: gravity model analysis. Marketing and Management of Innovations, (1), 253–265. https://doi.org/10.21272/mmi.2021.1-19

Majlis Keselamatan Negara (2024). Scam Atas Talian, Jenayah Utama Abad Ke-21. https://www.mkn.gov.my/web/ms/2024/01/25/scam-atas-talian-jenayah-utama-abad-ke-21/

Malaysian Communications and Multimedia Commission (MCMC) (2023). Internet Users Survey 2022. https://www.mcmc.gov.my/skmmgovmy/media/General/IUS-2022.pdf

Mahmud, M. H., & Siarap, K., (2013). Kempen pencegahan H1N1: Kajian tentang pengetahuan, sikap dan amalan penduduk di Timur Laut Pulau Pinang. Jurnal Komunikasi: Malaysian Journal of Communication, 29(1), 127-140. https://journalarticle.ukm.my/6425/

Pitchan, M. A., Baco, M. A., Hassan, F., & Ghazali, A. H. A. (2022). Pengetahuan, sikap, amalan terhadap privasi maklumat & keselamatan pembelian barangan dalam talian oleh golongan belia. Jurnal Komunikasi: Malaysian Journal of Communication, 38(4), 250–267. https://doi.org/10.17576/JKMJC-2022-3804-14

Priya, P. M., & Ranganathan, A., (2022). Cyber Awareness Learning Imitation Environment (CALIE): A card game to provide cyber security awareness for various group of practitioners. International Journal of Advanced Networking and Applications, 14(02), 5334-5341. ISSN: 0975-0290. https://www.ijana.in/papers/V14I2-3.pdf

RMP Melaka. (2024). Statistik Jumlah Kes and Kerugian Jenayah Siber Kontinjen Melaka Tahun 2023.

RMP Melaka. (2024). Statistik Mangsa Jenayah Siber Mengikut Pekerjaan Kontinjen Melaka Tahun 2023.

Elena, S. T., Amalia, M. D., & Monica, M. D., (2021). The role of the chartered accountant in diminishing the effects of cyber fraud. Journal of Financial Studies, 6(11), 141-155. http://dx.doi.org/10.55654/JFS.2021.6.11.11

Uthoff, C. S. (2022). Cyber intelligence: actors, policies, and practices. Boulder, Colorado: Lynne Rienner Publishers, Inc.