Information Management and Business Review (ISSN 2220-3796)
Vol. 16, No. 4, pp. 1-11, Dec 2024

A Correlation Analysis of the KAP Model against Online Scam Crimes in Malaysia

[1]Noor Fariza Mohd Hasini, [1]Salbiah Nur Shahrul Azmi*, [1]Zurairah Jais, [1]Shahrul Niza Samsudin,
[2]Nor Izzuani Izhar, [2]Nor Ainee Idris, [3]Azwan Amirulsyafiq Abu Hassan
[1]Faculty of Business, Hospitality & Technology, Islamic University Melaka, Malaysia
[2]Academy of Language Studies and Translation, Islamic University Melaka, Malaysia
[3]Royal Malaysia Police, Malaysia
*salbiahnur@unimel.edu.my
Corresponding Author: Salbiah Nur Shahrul Azmi

Abstract: This study aims to analyze consumers' Knowledge, Attitude, and Practices (KAP) Model of online scam crimes in Malaysia following the increase in crime cases that have become a concern. By using a quantitative approach, data were collected through questionnaires and analyzed by using SPSS software to identify the relation between demography, internet usage, and consumers' cautious behavior. The KAP Model is adopted as the main framework to comprehend the consumers' interaction with their digital surroundings. The findings of this study show there are positive correlations between age, education, and awareness of online scam crimes. The findings also found that there are strong relations between internet users and social media with consumers' preventive behavior. This study aims to identify the gap in the literature about psychosocial factors that influence consumers' awareness. The result of this study is hoped to be a guide to the policymakers and the authorities in designing more effective prevention strategies to protect consumers from the threat of online scams as well as enhance digital literacy among Malaysians.

Keywords: O*nline scam, KAP model, knowledge, attitude, practice*

1. Introduction

In this sophisticated digital era, online scams have been one of the major threats faced by internet users around the world, including in Malaysia. According to a current report, online scam cases have shown a disturbing increase, with various types of scams such as phishing, financial fraud, and identity theft that have become prevalent. This situation has urged researchers to delve deep into understanding how internet users can protect themselves against these threats. One of the approaches used is the KAP Model (Knowledge, Attitudes, Practices) adapted from research related to cyber security and now is being implemented into the study of online scams.

The National Security Council (NSC) on 4th of March 2024 has reported 107,716 online scam cases detected from 2020 until 2023. These scam cases involved losses of RM 3.2 billion and until January 2024, several 131 hotline numbers involving fraud activities have been terminated. Although various parties such as the Royal Malaysia Police (PDRM) in collaboration with the government and government agencies have disseminated information about the modus operandi of online scams, it has not been fully effective.

Therefore, this study is not only substantial in comprehending the influential factors and the cautious behavior of internet users but also plays a role in developing more effective preventive strategies. In the context of Malaysia, where the level of digital literacy varies according to demographics, this study can contribute to public policy and awareness campaigns. By identifying how education and age can influence awareness of online scams, this study can help in structuring targeted educational programs to reduce scam risks among internet users.

Based on the background of the research population which focuses on respondents from among the faculty members (Faculty of Business, Hospitality and Technology), Islamic University Melaka, Malaysia, the following is the statistics of cases and losses from cybercrimes in Melaka in the year 2023.

Table 1: Statistics of Cases and Losses from Cyber Crimes Melaka Contingent 2023

No.	Modus operandi	Number of Cases	Number of Losses (RM)
1.	Online purchasing scam	528	5,963,514.62
2.	Non-existent investment scams	296	21,844,890.68
3.	Non-existent loan scams	259	1,885,451.29
4.	Other cyber scams;		
	● TAC scams	221	3,611,713.54
	● Contest scams		
	● Other cyber-related scams		
5.	Phone scams	156	5,900,861.58
6.	Love/parcel scams	46	730,279.43
7.	Job offer scams	45	561,638.87
8.	Impersonation scams	20	52,500.00
	Total	**1571**	**40,550,850.01**

Source: PDRM Melaka (2024)

Problem Statement

Online scams have become a concerning global phenomenon, with a far-reaching impact on individuals and organizations. In Malaysia, the increase in online scam cases mirrors the global trend, where more advanced technology has become an opportunity for cybercriminals to exploit the weakness of internet users. Abdul Wahab, Pitchan, & Salman, (2023) mention that since 2014, reports of the MCMC have ascertained that one of the main challenges of the technological world in Malaysia today is the occurrence of online crimes resultant of various social media networks that open up opportunities to criminals to commit online scams. This issue is supported by an article disseminated by the National Security Council on March 18th, 2024 where they reported 34,497 frauds (scams) involving RM 1.218 billion of losses as well as 12,851 charges of cases being recorded nationwide in 2023. Based on these statistics, several 6,434 investigation papers were opened throughout the year 2023 through the National Scams Report Centre (NSRC) involving RM 105 million in losses.

Due to this, multiple efforts have been made by the PDRM such as providing a portal for Mule Check to inspect telephone and banking account numbers that are involved and CCID Infoline service to channel information related to this crime. Besides that, there are 1610 campaigns and 3727 speeches have been organized in 2023 to spread awareness regarding this online scam crime. This issue is not in line with the context of research in Malaysia because there is not so much research done regarding online scams that is being talked about in line with the increment of case statistics every year.

Moreover, since there are increments in the effort to educate consumers about the risks of online scams, the level of digital literacy among Malaysians is inadequate to overcome this threat effectively. There are many researchers such as Bashir et al. (2022), Patil and Arra (2022), Althibyani and Al-Zahrani (2023), Kimpe et al (2022), and Abdul Wahab et al., (2023), where they indicate that lacking knowledge in preventing and the attitude in avoiding from becoming the victim of online scams are the main factors contributing to this crime.

Therefore, this study is conducted with three main objectives by adapting the KAP Model against online scam crimes. Specifically, the objectives are:

- To study the correlation between knowledge and online scams.
- To identify the correlation between attitude and online scams.
- To study the correlation between preventive measures and online scams.

2. Literature Review

Online Scam Crimes

The rapid advancement of technology has made easy access to information digitally. However, the study by Abdul Wahab et al., (2023) shows that there are negative effects towards technology users since there are irresponsible parties who take advantage by committing online scam crimes. In 2022, according to statistics published by the Malaysian government, the total number of losses due to online scams is RM 1.73 billion and between January to September 2023 it has increased to RM 687 million or 29 percent in comparison to the same duration in 2022 (National Security Council, 2024).

This happens because of society's lack of awareness and knowledge about online scam crimes. The Royal Malaysia Police (PDRM) through its Commercial Crime Investigation Department (CCID) has executed numerous security campaigns in giving explanations about the criminal modus operandi. According to CCID Bukit Aman, 3,689 crime prevention programs have been organized between January and May this year to enhance understanding and awareness in society. This activity must be done continuously because the tactics and modus operandi of online scam crimes are always changing. Bashir et al. (2022) also emphasized the importance of these campaigns in helping people understand the way the crime is committed.

Abdul Wahab et al., (2023) referring to a source by PDRM in 2022, have identified seven main modus operandi of online crimes including online purchasing scams, non-existent loan scams, non-existent investment scams, African scams, Macau scams, Business Email Compromise (BEC), and scam through SMS. Besides that, Abdul Karim & Lyndon (2023) have listed down several online scam crimes globally, such as cyber extortion, breach of user personal data, identity theft, psychological disorders, mental and cyberbullying as well as scams by using the name of well-known organizations in obtaining data.

Model of Knowledge, Attitude and Practice (KAP Model)

The Model of Knowledge, Attitude, and Practice (KAP Model) has been proven to be important in understanding and handling the issue more effectively. This model uses the combination of three main elements: knowledge about cybercrimes, attitude towards the prevention of cybercrimes, and the practice of online security. As for the aspect of knowledge, the latest research shows that the increase in knowledge about cybercrimes has significantly reduced the risks of being online scam victims. The knowledge includes understanding the types of crimes, the techniques used by scammers, as well as the methods to identify and avoid those threats. The study by Patil and Arra (2022) emphasizes the importance of cybersecurity education in raising awareness and understanding among the public. When Althibyani and Al-Zahrani (2023) did a study on the effect of digital citizenship on awareness and cybercrime prevention among higher education students, it was found that knowledge about digital laws and digital communication skills play important roles in reducing cybercrimes. Other than that, a study by Kimpe et al. (2022) found that any individual who feels he is well informed about online security tends to feel less prone to cybercrimes and is unlikely to take inadequate precautionary measures.

This is proved through a finding in a study by Abdul Wahab et al., (2023) where society's knowledge and awareness have a close correlation with the increase of online scam cases that are still at large. This is in line with the KAP Model introduced by Bennett (1976) where he outlines some important assumptions. Among them are: (i) the increment of one's knowledge will lead to the change of attitude; (ii) when knowledge increases, attitude and practice will change towards a more positive direction; and (iii) the more frequent an individual is exposed to a message, highly likely the message will influence the individual.

Next, an individual attitude toward cybercrime prevention also plays an important role in the KAP Model. This attitude comprises the readiness of the individual to practice safety precaution measures and the perception of the importance of cyber security issues. Besides that, Abdul Wahab et al. (2023) emphasized that unwary public attitudes can contribute to the increment of online scam crime cases. The study also divided the factor of attitude into two main themes: public opinion towards online scam crime prevention campaigns, as well as the feelings and emotions of the public towards the campaigns.

The findings of the study show that informants have a very positive opinion towards the campaigns and voluntarily get involved, assuming as an anticipated opportunity to increase knowledge and enhance cyber security skills. They think that such campaigns not only have to be continued in the future but also to enlarge their scope to be able to reach more individuals because the advantages are significant in enhancing awareness and community resilience against sophisticated cyber threats.

From the perspective of practice, the practice of online security is a practical manifestation of an individual's knowledge and attitude for example the use of security software, strong password management, and vigilance during interaction with suspicious emails or messages. Meanwhile, a study by Priya and Ranganathaan (2022) proposed that one of the ways to increase public awareness about cyber security is through a specially designed card, where this platform helps the players to learn about the various types of cyber-attacks as well as defense mechanisms. Other than that, a study by Simona Tache et al. (2021) about the role and responsibility of a certified auditor in reducing the effect of cyber scams emphasizes the importance of training, courses, and awareness workshops, particularly in financial sectors that frequently becoming the target of cyber scams towards the members in the organization.

Abdul Wahab et al., (2023) also mentioned that an individual will start to understand or learn a certain practice, and later build a positive attitude towards the practice. In the study, the researchers have classified those practices into two main themes, namely society's action towards the campaign and society's attitude towards the campaigns. The results of the study showed that the informants responded positively such as commitment to join upcoming campaigns and invite other people to join as well. Other than that, the informants share messages or information that they have during the campaign with family and friends so that they receive the same knowledge. The informants take cautious measures to avoid them from being online scam crime victims, similar to the advice being imparted during the campaign. Moreover, the informants are always vigilant, which is emphasized in the campaign so as not to fall victim to online scams.

Practices like this are very essential to protect ourselves and others from the cybercrime threat which is increasing in the digital era nowadays. Positive practices that are cultivated through the campaigns not only help individuals avoid being online scam victims but also strengthen society's awareness about the importance of protecting personal information on digital platforms. In a wider context, the practices of sharing information and experiences from this campaign have the potential to create a larger awareness network in the community. By this, the effort to combat cybercrime becomes a collective responsibility, where every individual plays an important role in ensuring cyber security in an individual and society.

3. Methodology

This study uses a quantitative design by using the questionnaire distribution to collect data. Data in this study is obtained through the use of a questionnaire form that is structured based on secondary sources that have been tested, then gathered and processed by using the Statistical Package for Social Sciences (SPSS) software. In this study, descriptive analysis and correlation were done. Correlation analysis was used to understand the relationship between KAP Model and online scams. Furthermore, the findings from the study were analyzed by using a descriptive analysis method, aimed to analyze data that is received from the questionnaire form filled in by the respondents.

This research uses a simple random sampling method. Simple random probability sampling is a sampling technique where every member of the population has the same opportunity to be selected as a research respondent. In sections B, C, D, and E, the questionnaires will be measured by using the Likert Scale with five levels for respondents to indicate their level of agreement with the statements provided, where 1 indicates strongly disagree and 5 indicates strongly agree.

The distribution of the questionnaires is done through the Google Form platform and the findings of this study will be analysed. The population for this study is 413 among the Faculty of Business, Hospitality and

Technology members, Islamic University Melaka, Malaysia. By referring to the Krejcie and Morgan (1970) sample size determination table, the sample size for this study is 201.

Table 2: Distribution of Questionnaires

Aspects	No. of Questions
Section A: Respondents' Background	8
Section B: Online Scams	4
Section C: Knowledge Related to Online Scams	5
Section D: Attitude Towards Online Scams	5
Section E: Steps to Overcome Online Scams	5
No. of Questions	**27**

Source: Author's Illustration

The selection of respondents from among the faculty members is relevant referring to the victim list recorded in Melaka as follows:

Table 3: Statistics of Cyber Crime Victims According to Contingent Occupation Melaka Year 2023

No.	Occupation		2023	
			No. of Cases	Total of Losses (RM)
1.	Government	Teachers	47	1,294,020.72
		Health	26	404,103.68
		Police	14	40,990.00
		Military	7	35,698.00
		Others	139	2,268,665.79
2.	Private		732	11,176,617.71
3.	Students		143	1,010,618.22
4.	Businessmen		139	8,683,181.72
5.	Business		20	241,504.80
6.	Domestic Engineers		16	390,312.77
7.	Entrepreneur		166	4,022,700.18
8.	Pensioners		122	10,982,436.42
	Total		**1571**	**40,550,850.01**

Source: PDRM Melaka (2024)

4. Findings

This section elaborates on the findings from the research from the descriptive analysis and correlation generated through SPSS.

Descriptive Analysis Findings

The results from the displayed descriptive analysis in the tables depict a whole picture of the research respondents based on several variables of demography and attitude. Below is a brief elaboration for every variable:

Table 4: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Men	79	39.3	39.3	39.3
	Woman	122	60.7	60.7	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 5: Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-20	93	46.3	46.3	46.3
	21-30	92	45.8	45.8	92.0
	31-40	9	4.5	4.5	96.5
	41-50	7	3.5	3.5	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 6: Level of Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SPM	9	4.5	4.5	4.5
	STPM	2	1.0	1.0	5.5
	Diploma	100	49.8	49.8	55.2
	Bachelor's Degree	79	39.3	39.3	94.5
	Master's Degree	10	5.0	5.0	99.5
	Doctor of Philosophy	1	.5	.5	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 7: Internet Usage in a Day

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than 2 hours a day	3	1.5	1.5	1.5
	3-4 hours a day	32	15.9	15.9	17.4
	5-6 hours a day	64	31.8	31.8	49.3
	more than 6 hours a day	102	50.7	50.7	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 8: Daily Use of Social Media

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than 2 hours a day	16	8.0	8.0	8.0
	3-4 hours a day	67	33.3	33.3	41.3
	5-6 hours a day	45	22.4	22.4	63.7
	more than 6 hours a day	73	36.3	36.3	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 9: Frequency of Using the Application

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facebook	35	17.4	17.4	17.4
	Instagram	58	28.9	28.9	46.3
	Whatsapp	52	25.9	25.9	72.1
	Tiktok	32	15.9	15.9	88.1
	Telegram	14	7.0	7.0	95.0

	Other	10	5.0	5.0	100.0
	Total	201	100.0	100.0	

Source: Generated by SPSS

Table 10: Organizing Seminars Can Provide Awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	201	100.0	100.0	100.0

Source: Generated by SPSS

Of the total of 201 respondents, 39.3% were males and 60.7% were females. This shows that there are more female respondents in this study. The majority of respondents were between the ages of 18-20 (46.3%), followed by those aged 21-30 (45.8%). The age group of 31-40 years (4.5%) and 41-50 years (3.5%) is less. As for the level of education, respondents with a Diploma (49.8%) made up the largest group, followed by those with a Bachelor's Degree (39.3%). Only a small number of respondents had higher levels of education such as Master's Degree (5.0%) and Doctor of Philosophy (0.5%).

In addition to demographic data, the respondent behavior data such as daily internet usage indicates that the majority of respondents spend more than 6 hours per day online (50.7%). Meanwhile, 31.8% of respondents use the internet for 5-6 hours, and 15.9% for 3-4 hours. As for social media usage, findings show that 36.3% of respondents spend more than 6 hours per day on social media, followed by 33.3% who spend 3-4 hours per day. Additionally, data on the frequency of app usage reveals that Instagram (28.9%) and WhatsApp (25.9%) are the most commonly used apps by respondents, followed by Facebook (17.4%) and TikTok (15.9%). Ultimately, all respondents (100%) agree that efforts to raise awareness such as organizing seminars can help in educating about the threats of online scams.

Reliability

Table 11: Reliability Statistics

Cronbach's Alpha	N of Items
.936	19

Source: Generated by SPSS

The reliability statistics indicate a Cronbach's Alpha value of 0.936 for the 19 items, which constitute the list of questions for both dependent and independent variables. A Cronbach's Alpha of 0.936 indicates that the instrument used has an excellent level of reliability. Generally, an Alpha value above 0.7 is considered acceptable, and a value above 0.9 is considered excellent. Therefore, the instrument used in this study is highly consistent internally. This means that the items in the questionnaire or the test measure the same concept effectively, and their results remain stable when retested under the same conditions.

Correlation analysis findings

Pearson correlation is used to measure the strength and direction of the linear relationship between two variables to address the objective of this study. The findings for all three factors are as follows:

The Relationship between knowledge and online scam.

Table 12: Correlations

		DV	KNOWLEDGE
DV	Pearson Correlation	1	.589**
	Sig. (2-tailed)		.000
	N	201	201
KNOWLEDGE	Pearson Correlation	.589**	1

	Sig. (2-tailed)	.000	
	N	201	201

**. Correlation is significant at the 0.01 level (2-tailed).
Source: Generated by SPSS

For the first objective of the study, the correlation between DV and KNOWLEDGE was 0.589. This suggests that there is a moderately strong positive correlation between DV and KNOWLEDGE. A positive correlation means that when the KNOWLEDGE value increases, the DV value also tends to increase. From a significant point of view, a p-value (or Sig.) of 0.000 indicates that this correlation is very statistically significant because the p-value is smaller than 0.01. Therefore, there is a moderately strong positive correlation between the variables DV and KNOWLEDGE, and this correlation is statistically significant. This means that knowledge may have a positive effect on DV variables in the context of this study.

The Relationship between attitudes and online Scams.

Table 13: Correlations

		DV	ATTITUDE
DV	Pearson Correlation	1	.422**
	Sig. (2-tailed)		.000
	N	201	201
ATTITUDE	Pearson Correlation	.422**	1
	Sig. (2-tailed)	.000	
	N	201	201

**. Correlation is significant at the 0.01 level (2-tailed).
Source: Generated by SPSS

For the second objective of the study, the results of the analysis showed that the correlation between DV and ATTITUDE was 0.422. This suggests that there is a moderate positive correlation between DV and ATTITUDE. This positive association means that when the ATTITUDE value increases, the DV value also tends to increase, but not as strongly as the correlation in the previous analysis (DV and KNOWLEDGE). From a significant point of view, the value of p (or Sig.) is 0.000, indicating that this correlation is statistically significant. Therefore, there was a moderately positive correlation between the variables DV and ATTITUDE, and this correlation was statistically significant. Although this correlation is not as strong as the correlation between DV and KNOWLEDGE, it still suggests that attitude may have a positive influence on DV variables.

The relationship between preventive measures and online scams.

Table 14: Correlations

		DV	PRACTICE
DV	Pearson Correlation	1	.565**
	Sig. (2-tailed)		.000
	N	201	201
PRACTICE	Pearson Correlation	.565**	1
	Sig. (2-tailed)	.000	
	N	201	201

**. Correlation is significant at the 0.01 level (2-tailed).
Source: Generated by SPSS

For the third objective of this study, the correlation result between the dependent variable (possibly the outcome variable) and PRACTICE is 0.565. This indicates a strong positive correlation between the dependent variable and PRACTICE. This positive correlation means that as the value of PRACTICE increases, the value of the dependent variable also tends to increase, with a similar strength of association as with DV and KNOWLEDGE in the initial analysis. In terms of significance, the p-value (or Sig.) of 0.000 indicates that this correlation is highly statistically significant. Thus, there was a moderately strong positive correlation between DV and PRACTICE, and this correlation was statistically significant indicating that PRACTICE may have a strong positive influence on the DV variable.

Discussion

This study aims to examine the relationship between consumers' knowledge, attitudes, and practices (KAP) and their awareness of online scams. The findings of the study showed that there was a significant positive correlation between all elements of KAP and consumers' cautious behavior towards the threat of online scams.

Knowledge

The correlation between knowledge and awareness of online scams is the strongest in this analysis ($r=0.589$, $p<0.01$). This indicates that increased knowledge among users plays a crucial role in enhancing their awareness of online scam risks. Sufficient knowledge about types of scams, modus operandi, and preventive measures enables individuals to act more vigilantly. These findings are consistent with previous studies by Patil and Arra (2022) that highlight the importance of cybersecurity education in improving users' understanding.

Attitude

Although the correlation between attitudes and awareness of online scams was more modest than knowledge ($r=0.422$, $p<0.01$), it still showed an important role in determining consumer caution. Positive attitudes towards digital safety measures such as trust in the effectiveness of awareness campaigns influence consumers' desire to practice proper preventive measures. Although attitudes are not as strong as the knowledge factor, this study supports the findings of Abdul Wahab et al. (2023) that proactive attitudes can reduce the risk of becoming a victim of online scams.

Practice

Online safety practices also show a significant correlation with cautious behavior ($r=0.565$, $p<0.01$). These findings suggest that users who follow safety measures such as using antivirus software, strong passwords, and avoiding suspicious links are better able to protect themselves from online scams. This aligns with a study by Simona Tache E. et al. (2021) which confirmed that good cybersecurity practices play a critical role in safeguarding users from cybercrime.

Research Implications and Gaps

The strong correlation between knowledge and safety practices indicates the need to strengthen cybersecurity education programs, especially among young and less educated individuals. However, this study found that the correlation between demographics such as education level and awareness of online scams still requires further research to understand its effects in more detail. Overall, the findings of this study confirm the importance of the KAP Model in understanding user behavior towards online safety. This study also suggests that an increase in awareness should be fostered through a broader cybersecurity education, promoting a positive attitude and continuous online safety practices among internet users in Malaysia.

5. Conclusion and Recommendations

This study successfully demonstrated a significant relationship between users' knowledge, attitudes, and practices towards online scam prevention in Malaysia, especially using the KAP model approach. The findings of the study showed that security knowledge and practices were key factors in increasing consumer awareness of online scams, while attitudes played a modest role in the study. This confirms that cybersecurity education is important in preventing online scams and protecting internet users.

The following are suggestions to strengthen management and address online scams:

Cybersecurity Education Enhancement: The government and educational institutions need to expand public awareness campaigns, especially among young and less educated consumers. Cybersecurity courses should be incorporated into the official curriculum at the school and university levels.
Awareness Campaign through Social Media: Considering that most users spend more than 6 hours per day on social media, popular social media platforms like Instagram, TikTok, and WhatsApp can be used to disseminate information about online scam prevention.
Collaboration with the Private Sector: Internet service providers and technology companies need to be involved in anti-fraud campaigns by providing online cybersecurity warnings and educational resources to customers.
Online Scam Prevention Tool Development: The development of more user-friendly security software and online scam detection tools should be encouraged to help users identify threats and prevent online scam crimes from becoming more prevalent.
Advanced Studies: Further investigation needs to be conducted to examine in greater depth the impact of demographic factors such as age and education level on user attitudes towards cybersecurity, as well as a study on more specific trends in cyber scams in Malaysia.

With a more holistic and collaborative approach, online scam prevention measures in Malaysia can be further strengthened, reducing the risk of users falling victim to online scams.

Acknowledgment: The published article is the result of research funding awarded by Universiti Islam Melaka (UNIMEL) through the Incentive Research Grant (IRG) 2024/2025.

References

Abdul Karim, M. Y. & Lyndon, N. (2023). Panandgan 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 and Amalan Masyarakat di Kuala Lumpur Terhadap Kempen Pencegahan Jenayah Penipuan Dalam Talian. *Jurnal Komunikasi: Malaysian Journal of Communication*, *39*(1), 240–258

Althibyani, H.A. & Al-Zahrani, A.M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*, *15*, 11512. https://doi.org/10.3390/su151511512

Bashir, A., Azwardi, A., Soebyakto, B. B., Atiyatna, D. P., Hamidi, I., Hamira, H., & Dwi, R. S. (2022). Raising Awareness and Knowledge of Rural Communities against Lottery Fraud and Illegal Online Loans through Telephone and Short Message Services. *Sricommerce: Journal of Sriwijaya Community Services*, *3*(2), 89–96. https://doi.org/10.29259/jscs.v3i2.83

Bennett, C. F. (1976). Analyzing impacts of extension programs. Washington: U.S. Dept. of Agriculture, Extension Service.

Berita RTM (2024). 107, 716 Kes Penipuan dalam Talian Dikesan dari 2020 hingga 2023. https://berita.rtm.gov.my/nasional/senarai-berita-nasional/senarai-artikel/107-716-kes-penipuan-dalam-talian-dikesan-dari-2020-hingga-2023

De Kimpe, L., Walrave, M., Verdegem, P & Ponnet, K. (2022). 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, DOI: 10.1080/0144929X.2021.1905066

Jabatan Perangkaan Malaysia. (2022). *Poket Stats Negeri Melaka ST3 2022*

Kosmo (2024). 34, 497 Kes 'Scam' Babit Lebih RM 1.2 Bilion Kerugian pada 2023. https://www.kosmo.com.my/2024/03/18/34497-kes-scam-babit-lebih-rm1-2-bilion-kerugian-pada-2023/

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610

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/

Patil, K. and Arra, S. R. (2022). Detection of Phishing and User Awareness Training in Information Security: A Systematic Literature Review. 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, 2022, 780-786, doi: 10.1109/ICIPTM54933.2022.9753912

Priya, P. M. & Ranganathan, A. (2022). *Cyber* Awareness Learning Imitation Environment (CALIE): A Card Game to Provide Cyber Security Awareness for Various Groups of Practitioners Int. J. Advanced Networking and Applications, 14(02), 5334-5341.

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

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

Simona T. E., Magdalena, A. A. & Mihaela, D. M. (2021). The Role of The Chartered Accountant in Diminishing the Effects of Cyber *Fraud*. Journal of Financial Study, Valahia University of Targoviste, Romania