COVID-19: A PRISMATIC VIEW

Editors
Che Mahzan Ahmad
Mazni Buyong
Saodah Wok
Zeti Azreen Ahmad

COMET
COMMUNICATION AND MEDIA CENTER

COVID-19: A PRISMATIC VIEW

Editors
Che Mahzan Ahmad
Mazni Buyong
Saodah Wok
Zeti Azreen Ahmad

Publisher
Communication and Media Centre (COMET),
Department of Communication,
AbdulHamid AbuSulayman (AHAS) Kulliyyah of Islamic
Revealed Knowledge and Human Sciences,
International Islamic University Malaysia

Year of Publication
2022

COMET
COMMUNICATION AND MEDIA CENTER

Published by COMET, Department of Communication, AbdulHamid AbuSulayman Kulliyyah of Islamic Revealed Knowledge and Human Sciences (AHAS KIRKHS), International Islamic University Malaysia, Gombak, Kuala Lumpur.

ISBN: 9789671987704

Editors: Che Mahzan Ahmad, Mazni Buyong, Saodah Wok and Zeti Azreen Ahmad
Layout Designer: Nur Aina Athirah binti Mahyuddin

Communication and Media Centre (COMET) was established in March 2015. The centre is dedicated to the field of media and communication studies. It produces scholarly research work that addresses both academic and societal needs. COMET is championed by the Department of Communication that is under AbdulHamid AbuSulayman Kulliyyah of Islamic Revealed Knowledge and Human Sciences (AHAS KIRKHS), International Islamic University Malaysia (IIUM).

Contents

Contents

Preface

Keynote Speech by Datuk Dr. Hishamshah Bin Mohd Ibrahim
Deputy Director of Health (Research and Technical Support), Ministry of Health, Malaysia.

Allow me to express my gratitude to the organiser of the 2nd Communication Research Seminar (CORENA) for the honour of delivering this morning's keynote address.

It has been almost two years since COVID-19 emerged at the end of 2019. Countries all over the world are at various stages of disease mitigation. As of November 30, 2021, Malaysia recorded 2,632,782 total COVID-19 cases, with 2,537,204 recoveries. Since the emerging of the pandemic, the Malaysian public has been dependent on both local and international authorities and media for information related to COVID-19. Various strategies have been adopted by the MOH in an effort to convince the people about COVID-19 since the pandemic outbreak. The COVID-19 health crisis has introduced new challenges to effective health information delivery around the world. In the context of COVID-19, this is exacerbated by the misinformation and disinformation surfacing on social media. However, in a pandemic situation, there is an increased reliance on the government and health authorities to manage the problem. The need to provide clear, consistent, and credible information surrounding the COVID-19 pandemic is key to disease mitigation and control.

Although information is available through various local and international sources, the MOH Malaysia and the Malaysian National Security Council (NSC) are the official sources responsible for communicating information about COVID-19 and its control in the country. As such, both the MOH and NSC have made concerted efforts to maintain a consistent and reliable flow of information to the public through both traditional and new media sources. Credible spokespeople from the MOH and NSC are chosen to deliver COVID-19 updates to ensure the clarity, trustworthiness, and congruence of information.

Official information and local updates on the disease were broadcast via press conferences and regular messaging through multiple telecommunication channels, including traditional media, digital media platforms, and social media. In Malaysia, these channels includes government and privately owned media. The provision of platforms to facilitate the people to access the latest information related to COVID-19 is frequently updated. Not only limited to one-way communication, even interactive sessions and virtual are conducted continuously such as webinar on the easy access social media platforms. This is to empower the people to obtain information from authentic and reliable sources. The encouraging response proves that the people continue to depend on the government to obtain authentic sources of information.

Malaysia followed the WHO's Coronavirus Disease 2019 (COVID-19) Strategic Preparedness and Response Plan (WHO SPRP) guideline, focusing on nine pillars encompassing public health areas central to preparedness and response activities such as country-level coordination, planning, and monitoring, risk communication and community engagement, surveillance, rapid response teams, case investigation and so forth. We had proper systems in place designated units to monitor the case statistics and surveillance systems. The nation's involvement and contributions to surge capacity, surveillance activities, delivery of medical services as well as COVID-19 related physical and digital infrastructure such as mobile applications for COVID-19 contact tracing and updates, were achieved with our MOH CPRC working closely with centralised coordination council (i.e., National Security Council, NSC) consisting of multiple ministries where MOH provided advice based on the evolving COVID-19 situation, as well as collaborations with other countries, non-government organisations, private sectors, and the public.

MOH played a vital role in warranting maximum readiness to contain the spread of the virus and was transparent in handling the pandemic by providing sufficient and up-to-date information to the public through major social media information platforms including the Official Portal of the MOH, creation of a special Facebook user account called the Crisis Preparedness and Response Centre (CRPC), Kementerian Kesihatan Malaysia (KKM), and CRPC KKM Telegram (My Government, 2020). The Ministry also constantly emphasised awareness programmes for public on important preventive measures such as wearing of mask, practise of physical distancing and hand hygiene to minimise transmission of COVID-19. These were achieved by dissemination of information through in infographics and simple diagrams to reach the public easily. MOH also conducted community mobilisation and reach out programmes.

to educate and create awareness among public on importance of preventive measures. In addition, various infographics associated with COVID-19 especially on statistics of current cases and latest issues were prepared daily and uploaded onto the website. The MOH also conducted daily press briefings, conference recordings, and has published relevant news on COVID-19 to increase public engagement and ensure public awareness and access to accurate information.

As we all know that the Coronavirus disease (COVID-19) is the first pandemic in history in which technology and social media are being used on a massive scale to keep people safe, informed, productive and connected. At the same time, the technology we rely on to keep connected and informed is enabling and amplifying an infodemic that continues to undermine the global response and jeopardises measures to control the pandemic.

MOH through CPRC, Unit Komunikasi Korporat and Health Education Divisions and other relevant agencies in Malaysia such as NSC and Malaysian Communications and Multimedia Commission utilised both conventional and digital media to communicate with the public to allay these misconceptions. Authorities countered the non-scientific messages and misconception by providing fact and accurate messages through various channels; media spokesperson, social media platforms, daily press conferences etc. Information based on data and research finding are often disseminated to public in very informative manners through infographics, articles that were easy to understand. Despite these measures, rumours and fake news were still circulated privately in social media such as WhatsApp or Facebook posts that required clarification from MOH and these agencies. With the consistent and standardised presentation of information to the public from the beginning, misinformation and confusion were able to be avoided and therefore the public confidence in the government's handling of the pandemic had been strengthened.

Based on various research findings conducted by MOH through National Institutes for Health (NIH) on public's cognitive, affective and behavioural aspect towards COVID-19 throughout different phases; during initial period of COVID19 outbtreak and lockdowns, during the containment phases and during the severe outbreak phases highlighted high knowledge level among public on preventive measures, positive perceptions towards the importance of preventive measures and high compliance towards SOP. This indicates information provided by MOH is sufficient and easy to be understood by public. From the provision of correct information regarding the disease outbreak to the provision of COVID-19 vaccine information, our country is proud to be among the countries that achieved a high percentage of fully vaccinated citizens. 96.8 percent of the adult population has received two doses of COVID-19 vaccine injections and a total of 25,370,746 individuals or 77.7 percent of the total population have completed COVID-19 vaccine injections, as of 30 November 2021.

Recent study findings conducted in 2021 on the assessment of the continuity of compliance with the new norms, risk perceptions of COVID-19 infection, and vaccine acceptance still showed positive response from public in the aspect of knowledge and attitude however self- reported practices towards prevention measure showed a downward trend. Study of COVID-19 preventive message fatigue also showed that the people have reached a maximum level of information fatigue. Repeated messages carrying reminders of safe distancing practices, hand washing, wearing of masks, stay home pleas, potential COVID-19 complications and daily updates of morbidity and mortality data through various national and professional mass media channels can result in message and pandemic fatigue among public. Thus to address this communication challenges, MOH had strategise to incorporate diverse channels to reach audiences that include a mix of individual, interpersonal, organisational, and community and mass media channels and application of health literacy strategies by conveying most relevant and needed messages to the rightful target group in the forms that can be best understood by the group.

Apart from message dissemination strategies, the government also developed and urged the use of technology via mobile phone apps aimed to assist COVID-19 outbreak management and as a tool of communication with citizens, namely, MySejahtera. The widespread use of this apps indicates that citizens rely on and facilitate access to information both on the current situation of covid-19 and also on obtaining vaccination appointments. It is now a norm that we all scan the MySejahtera QR Code before we walk into any place. The existence of MySejahtera since the start of the pandemic and how it has evolved from a basic data capturing platform to a functional platform that can be used to manage and monitor Covid-19 patient is indeed applaudable. The MySejahtera app is a functional application whereby the CovidNow portal is basically completely informative. As we know communication can be in many forms and CovidNow is established to disseminate information that are specific and as a quick access for the public. MySejahtera and CovidNow are established for different purposes and functions.

A pandemic is not new to the world, however the nature of this pandemic and its' impact to people are quite exclusive and we are tackling it on a day- to day basis. Each new morning brings in new knowledge, each sunset leaves us behind with lessons learnt. So are the strategies that have been used to manage the pandemic in Malaysia. The Ministry of Health usually formulates strategies using evidences that have been produced by research. We also adopt many strategies that have been used internationally but always ensure that it is suited and customised for Malaysia. In terms of the success or failure of a strategy or the many policies adopted during the pandemic, we must all agree the nature of the pandemic is such that we had through trial and error strategies and we had continually improvise based on the latest development and we keep doing it till date. This is a process and these processes will not stop and at each point in time we will have to keep improving. So even if there are complaints from the public, we must all come to an understanding that there will be strategies that didn't seem quite suitable but be assured that the Ministry of Health has been striving to ensure to fulfil it's prime purpose which is service to the public. “Kami Sedia Membantu”.

Foreword

Prof Dato' Sri Dr. Syed Arabi bin Syed Abdullah Idid
Advisor,
Communication and Media Centre (COMET)
Department of Communication, AHAS KIRKHS,
IIUM

Friends and colleagues

السَّلَامُ عَلَيْكُمْ وَرَحْمَةُ اللّٰهِ وَبَرَكَاتُهُ

Praise be to Allah, for upon his Guidance and Mercy

I am very honour to be invited by COMET to make this forward.

COVID-19 has caused such misery and unhappiness the world over. Companies have collapsed, families have lost their loved ones, breadwinners have seen their income dwindle or slashed. There has been an absolute onslaught on the economy. One sees misery and unhappiness at every level. One must remember and recognise the individual and family's anxiety, anger, anguish, and despair as millions are out of work.

Given this picture, one can see that the threat posed by COVID-19 is not a medical and health problem only. It is more significant than a health problem. It is not a threat that only medical officers can solve. It is a security issue where nations are involved, where governments must take stern actions to avert further damage to the national economy and administration. The soldiers and security personnel oversee that citizens comply with the rules and SOPS to curb the infections. The banks see the need to allow some leeway in meeting debtor obligations. The landlords work out arrangements with their tenants to overcome the problems on monthly payments. The COVID-19 is a threat to society.

Society does acknowledge the contribution of the medical and health personnel. Still, I think we should also be looking at the broader picture as COVID-19 is a fight of humanity against an unwelcome disease. All members of society are involved in this big fight. The medical and health profession conducted research covering all aspects of the disease, resulting in the discovery of vaccinations. Other research findings are known to their fraternity to help society recover from the pandemic. Scholars in political science, sociology, psychology, counselling, economics, and communication conduct various research to help fight COVID-19. Social sciences mainly on social aspects such why there is opposition against vaccinations and wearing masks? How do families cope with domestic violence?

Social Science and Communication have made significant contributions in resolving the massive challenges arising out of the COVID-19 pandemic as a vastly better understanding of human and societal behaviour is essential to reduce viral transmission and maximise human safety and well-being. By training, these scholars have developed concepts and empirical generalizations to translate into research techniques for specific studies to handle the pandemic problem at hand.

Infection prevention and control require a fuller understanding of politics, international relations, philosophy, economics, psychology, and sociology. Areas that need more attention include scepticism and denial of vaccination, against wearing masks, and in cases, a refusal on the seriousness of COVID-19 itself. The impact on the families' well-being, mental health, and the increased domestic violence resulting from income reduction and unemployment would need psychological counselling and rehabilitation. Health campaigns would require communication understanding in reaching out to the right audience with the right messages.

Various social science scholars have found out the different impacts of lockdowns on ordinary people. Working from Home (WFH) has its attendant problems, with children unable to attend schools and being at home with their parents who play different roles not previously enacted during pre-pandemic.

Political science and polling surveys have measured peoples' confidence and trust in institutions, focusing on government performance and the day's leaders. Researchers use qualitative studies on the leadership qualities of their respective leaders in their society. Studies have been using quantitative and qualitative approaches in Malaysia, showing leadership traits and portraying leadership. Similar research approaches touched on the British prime minister's leadership, President Biden of the US, and President Duterte of the Philippines.

There has been tremendous research done by Social Science Scientists, including scholars in Communication. The research areas they cover are varied, broad and relevant. COVID-19 has been a common agenda for public opinion organizations. For the year 2020 and even 2021, COVID-19 has been a common topic by polling organizations asking the opinion of the general public, specific public on their concerns with COVID-19. They have measured the people's response toward government actions, feelings, and concerns as recorded by polling organizations in Africa, Latin America, Asia and Europe.

This book consist of selected papers presented in a Seminar organized by Communication and Research Centre (COMET), Department of Communication, International Islamic University, Malaysia held in 2021. This center is dedicated to the field of media and communication studies to produce scholarly and practice oriented research addressing both academic and societal needs. It is hope that more books will be published in the near future.

The Mediating Effect of Behavior on Cyber Resilience Towards Online Fraud Threats Among IIUM Students

Nur Hafifah Jamalludin, Saodah Wok, Nerawi Sedu &
Tengku Siti Aisha Tengku Azzman

INTRODUCTION

People start to see the importance of using online platforms in their professional and personal duties. This is in line with the advanced settings offered by the communication companies. As online platform has become a part of our life, there are challenges faced by the users, specifically, the active users of the online platforms. This is due to the increased cases of online fraud threats reported locally (Muniandy, Muniandy, & Samsudin, 2017) as well as internationally (Liang & Xue, 2009). The more users are attached to the online platforms, the higher chance for them to encounter the online fraud threats created by the perpetrators. This explains the reason behind choosing IIUM students as respondents for the study since they are the younger generation who attached to the online platforms for academic and personal purposes.

Online fraud threats can be defined as a form of Internet deception, where the purpose of the perpetrators is to obtain money and benefits from the intended targeted victims. There are two types of online fraud threats: financial fraud and identity theft (Krubhala, Niranjana & Priya, 2015). Financial fraud refers to the money-related transactions where the perpetrators use fraudulent techniques to gain profits from the victims. In addition, identity theft is a technique used by the perpetrators to utilise a person's identity to commit, aid or abet any unlawful activity. These two techniques of online fraud threats are closely related with the younger generation, specifically, students because they are active users of the online platforms. They frequently use online payment transactions or e-banking. However, lack of positive attitude and behaviour in seeking information from the authorities make them vulnerable to the threats created by the petpetrators (Radhakrisna & Pointon, 2007). The concern is whether they are capable to remain functioning after the stressful events. As such, the study aims to investigate the following objectives: (1) to identify the level of attitude, behavior, and cyber resilience towards online fraud threats; (2) to test the relationships between attitude, behavior, and cyber resilience towards online fraud threats;

and (3) to analyse the mediating effect of behavior between the attitude and cyber resilience towards online fraud threats.

LITERATURE REVIEW

The discussion will relate to the analysis of the study which requires specific steps to be followed for testing the mediating effect of behavior (mediator) on attitude (independent variable) with cyber resilience (dependent variable) towards online fraud threats.

(1) Attitude and Cyber Resilience

Students who have positive attitude in developing cyber resilience will have an advantage in facing online fraud threats. This is because they are well versed on the techniques used by the perpetrators since they like to confirm and verify suspicious threats from the authority before further actions are taken (Arniyati, Johnson, & Storer, 2015). They like to double-check the message received from the suspicious sender through the official website or directly communicate with Malaysian Communications and Multimedia Commission (MCMC) for their advice (Radhakrisna & Pointon, 2007). Therefore, it implies that positive attitude contributes to develop cyber resilience towards online fraud threats created by the perpetrators. As such, this study crafts this hypothesis:

> H1: Attitude is positively correlated with cyber resilience towards online fraud threats.

(2) Attitude and Behaviour

As cyber resilience describes the capability to prepare for, adapt and recover from online fraud threats; it is students' responsibility to seek extra information like preventative tips from the authority to avoid being victims. Furthermore, they need to turn on their notification from MCMC to get latest updates, specifically on the online fraud threats (Yunos, Ab Hamid, Susanty & Ahmad, 2017). This contributes to the application of the safe online practices and at the same time helps to build protection of their personal data online. As such students who have positive attitude in preparing themselves for online fraud threats will also develop positive behaviour in facing sophisticated techniques used by the perpetrators to lure them into the trap (Chandarman & Van Niekerk, 2017). Therefore, this study postulates the following hypothesis:

> H2: Attitude is positively correlated with behaviour.

(3) Behavior and Cyber Resilience

Behaviour and cyber resilience is closely related, specifically in handling online fraud threats created by the perpetrators. Positive behavior towards online fraud threats is when the students applied the techniques shared by the authority when they are online. For example, they are more alert with any tricks imposed by the perpetrators by not simply clicking the pop-up ads or notification in their windows, especially when they are using free Wifi provided in the cafeteria or shopping mall (Slusky & Partow-Navid, 2012). Any shared information using the free Wifi on the online platforms will be visible to the third-party or perpetrators. As a result, their privacy is at risk as the perpetrators can easily obtain related-information to be utilised for their own interest. Therefore, having positive behaviour helps the students become cyber resilience users of the online platforms. As cyber resilience users of online platforms, their ability to predict the threats or intrusion from the perpetrators, cautious of the different types of malware, do some research on the suspicious sender or service provider before further actions are taken, while they always refer to the authority to verify the websites used by the perpetrators (Shaari, Kamaluddin, Paizi@Fauzi, & Mohd, 2019). With these online practices, they are safe to browse and use the online platforms. Hence, the following hypothesis is proposed:

H3: Behavior is positively correlated with cyber resilience towards online fraud threats

(4) Mediating Effect of Behaviour on Attitude with Cyber Resilience towards Online Fraud Threats

Behavior has the potential to mediate the relationship between attitude and cyber resilience towards online fraud threats. This is because positive attitude makes the students realise on the importance of safe online computing in their communication devices (Koong, Liu, Bai, & Wei, 2008). This means that they like to confirm or verify the authenticity of the sender or service provider from the authority before proceeding to the next steps. Furthermore, they can seek extra-knowledge like tips or techniques as a preparation to safeguard their data online (Yuliarti, AnggrenI, & Utari, 2018). Hence, it contributes to the positive behaviour where the students can directly apply the shared tips or techniques given by the authority. For example, which settings that they can turn on and types of data they can share with the service provider. Several studies (Norris, Brookes & Dowell, 2019; Poppleton, Lymperopoulou & Molina, 2021) support that positive attitude leads to a proper behaviour in handling online fraud threats; which in turn, develop cyber resilience where they are cautious and always prepare for any threat possibilities, able to adapt to the environment, and they are able to recover from the threats or attacks (Muniandy, Muniandy & Samsudin, 2017; Ngo, & Peternoster, 2011). Therefore, behaviour can mediate the relationship between attitude and cyber resilience towards online fraud threats. Based on the above reviewed studies, the following hypothesis is presented:

H4: Behavior mediates the relationship between attitude and cyber resilience towards online fraud threats.

The discussions of findings related to cyber resilience towards online fraud threats are based on the social exchange theory (SET).

Social Exchange Theory (SET)

Social exchange theory (SET) was developed in 1958 by Homan (Cropanzano & Mitchell, 2005). SET explains on the nature of human beings where they are more interested in seeking rewards; avoid punishment and using their rational in making decision on certain matters (Homan, 1958). This means that they need to choose something that brings them positive effects and maximise the reward gained. The two rewards emphasised in the SET are in the forms of: (a) material such as money, time and service; and (b) intangible material such as effort, social approval, love, pride, shame, respect, opportunity, and power.

Based on the explained characteristics of SET, it assumes students are encouraged to seek knowledge on cyber resilience to avoid being victims of online fraud threats. With such enthusiastic attitude and behavior, they are always prepared for the threats created by the perpetrators. This indicates that they placed the cyber-security as their top priority to safeguard their data online and to be cautious in allowing some settings on their communication devices.

Conceptual Framework

Based on the literature review, the relationships among the factors are depicted in the conceptual framework shown below (Figure 1).

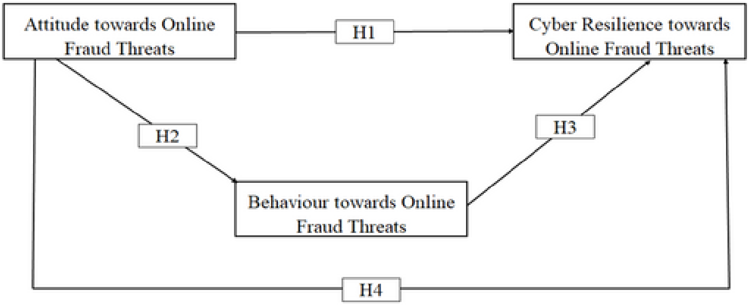

Attitude towards Online Fraud Threats
H1
Cyber Resilience towards Online Fraud Threats
H2
H3
Behaviour towards Online Fraud Threats
H4

Figure 1: Conceptual framework of the mediating effect of behavior on cyber resilience towards online fraud threats among IIUM students

Summary of the Hypotheses

Table 1 lists the hypotheses formulated for the study.

Table 1: Summary of hypotheses

No.	Hypothesis
H1:	Attitude is positively correlated with cyber resilience towards online fraud threats.
H2:	Attitude is positively correlated with behaviour.
H3:	Behaviour is positively correlated with cyber resilience towards online fraud threats.
H4:	Behaviour mediates the relationship between attitude and cyber resilience towards online fraud threats.

METHODOLOGY

A quantitative research design using a survey questionnaire was employed for the study. The quantitative research design helps the researcher to have an objective and accurate measurement (Wimmer& Dominick, 2014).

Population and Sampling Procedure

The respondents of the study consisted of IIUM undergraduate students from seven different Kulliyyah (faculties). The study employed the stratified random sampling procedure where it helped to (a) determine the divisions of the population involved and (b) divide it into smaller groups called strata. In this study, the population was divided into seven strata: (a) Ahmad Ibrahim Kulliyyah of Laws (AIKOL), (b) Kulliyyah of Architecture and

Environmental Design (KAED), (c) Kulliyyah of Education (KOED), (d) Kulliyyah of Economic and Management Sciences (KENMS), (e) Kulliyyah of Information and Communication Technology (KICT), (f) Kulliyyah of Engineering (KOE), and (g) Kulliyyah of Islamic Revealed Knowledge and Human Sciences (KIRKHS).

A total of 269 respondents participated in the study, consisting of 195 are females and 74 males aged 18 to 29 years old. In order to collect data among the students, permission had been approved by each department as well as the instructor from various courses in IIUM.

Data Collection Instrument

A questionnaire was used to collect data for the study from 1 December 2019 until 14 December 2019. There are six section with: (1) demographic information; (2) information on online fraud threats where the measured items were adapted from Koong, Liu and Wei's study (2015); (3) online payment methods where the measured items were adapted from Pradeep, Mukesh and Aditya's study (2011); (4) attitude towards online fraud threats where the measured items were adapted from Chandarman and Van Niekerk (2017); (5) behaviour towards online fraud threats where the measured items were adapted from Chandarman and Van Niekerk (2017); and (6) cyber resilience towards online fraud threats where the measured items were adapted from Yunos, Ab Hamid, Susanty and Ahmad (2017). The items were measured on a 5-point Likert scale where 1 = strongly disagree, 2 = disagree, 3 = slightly agree, 4 = agree and 5 = strongly agree.

Validity and Reliability

Pre-testing of the research instrument was conducted before the actual data collection started. Pre-testing is required because it able to detect problems in the research measurement. Thirty-one undergraduate students from seven different Kulliyyah completed the distributed questionnaire. Thus, based on the pre-test, minor changes or modifications were made to the questionnaire.

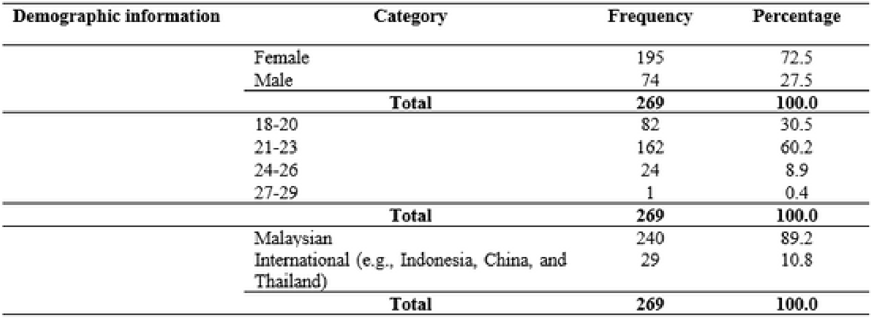
The reliability coefficients for all constructs are: (1) attitude, measured using 10 items with Cronbach's alpha of .869; (2) behaviour, measured using 10 items with Cronbach's alpha of .904, and (3) cyber resilience towards online fraud threats, measured using 10 items with Cronbach's alpha of .869. All the tested variables are reliable as the Cronbach's alpha values are above .700.

FINDINGS AND DISCUSSION

Demographic Chracteristics of Respondents

A total of 269 respondents participated in the study (Table 2). Most of the respondents are females (72.5%) while the rest are males (27.5%). Six in ten of the respondents (60.2%) aged ranged from 21 to 23 years old, followed by 18 to 20 years old (30.5%), and the rest (9.3%) belonged to the 24 and above age group. Majority all of the respondents are Malaysians (89.2%) and only 10.8% of them are the International students. For example, they are from Indonesia, China and Thailand.

Table 2: Demographic information

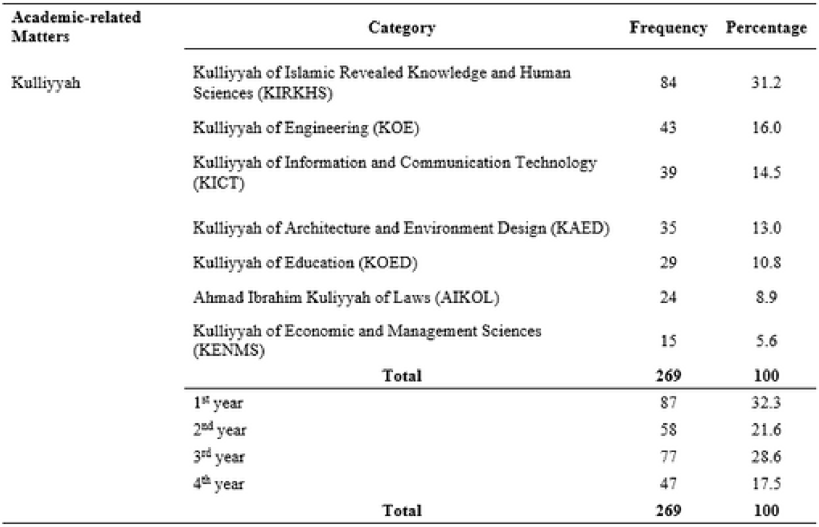


Demographic information	Category	Frequency	Percentage
	Female	195	72.5
	Male	74	27.5
	Total	**269**	**100.0**
	18-20	82	30.5
	21-23	162	60.2
	24-26	24	8.9
	27-29	1	0.4
	Total	**269**	**100.0**
	Malaysian	240	89.2
	International (e.g., Indonesia, China, and Thailand)	29	10.8
	Total	**269**	**100.0**

Academic-related matters consist of Kulliyyah and level of study (Table 3). Three in ten of the respondents (31.2%) are from KIRKHS; one tenth of them from KOE (16.0%), KICT (14.5%), KAED (13.0%), and KOED (10.8%).

Three in ten of the respondents (32.3%) are first year and more than one-fifth of them (28.6%) are from third year, 21.6% second year, while the rest (17.5%) are fourth year students. This means that each Kulliyyah has representation with different levels of study.

Table 3: Academic-related matters



Academic-related Matters	Category	Frequency	Percentage
Kulliyyah	Kulliyyah of Islamic Revealed Knowledge and Human Sciences (KIRKHS)	84	31.2
	Kulliyyah of Engineering (KOE)	43	16.0
	Kulliyyah of Information and Communication Technology (KICT)	39	14.5
	Kulliyyah of Architecture and Environment Design (KAED)	35	13.0
	Kulliyyah of Education (KOED)	29	10.8
	Ahmad Ibrahim Kuliyyah of Laws (AIKOL)	24	8.9
	Kulliyyah of Economic and Management Sciences (KENMS)	15	5.6
	Total	**269**	**100**
	1st year	87	32.3
	2nd year	58	21.6
	3rd year	77	28.6
	4th year	47	17.5
	Total	**269**	**100**

Level of Attitude, Behaviour, and Cyber Resilience towards Online Fraud Threats

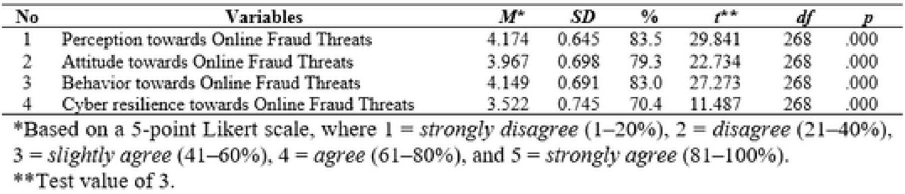
Table 4 presents the level of attitude, behavior, and cyber resilience towards online fraud threats. A one-sample t-test with a test value of 3 was used as the value.

The overall result for attitude is positive significant (M = 3.967, SD = 0.698; t(269) = 22.734, p = .000). It can be inferred that students are actively seeking for cyber resilience information to ensure that they are practicing a safe online computing to avoid being victims. Yunos, Ab Hamid, Susanty and Ahmad (2017) also found that adequate information on cyber resilience will help to safeguard students' personal data online.

In addition, having positive behaviour (M = 4.149, SD = 0.691; t(269) = 27.273, p = .000) helps students to be cautious users of the online platforms as they know what types of privacy setting that can be turn-on or off in their communication devices for their safety. Pradeep, Mukesh and Aditya's findings (2011) found that students started to realise the importance of applying and practicing cyber security when they are online to be a cyber resilient user avoid being victims of online fraud threats.

The overall cyber resilience is positive and significant (M = 3.522, SD = 0.745; t(269) = 11.487, p = .000). This means that they are prepared for the intrusion from the perpetrators. The most important is that they can bouce back where they can see the positive side of the challenges faced and learn from their mistakes. Al-Janabi (2016) found that students who develop cyber resilience will not get traumatic to use online platforms but they will cautiously deal with any threats imposed by the perpetrators in the future.

Table 4: One sample *t*-test on attitude, behavior, and cyber resilience towards online fraud threats



No	Variables	*M**	*SD*	%	*t***	*df*	*p*
1	Perception towards Online Fraud Threats	4.174	0.645	83.5	29.841	268	.000
2	Attitude towards Online Fraud Threats	3.967	0.698	79.3	22.734	268	.000
3	Behavior towards Online Fraud Threats	4.149	0.691	83.0	27.273	268	.000
4	Cyber resilience towards Online Fraud Threats	3.522	0.745	70.4	11.487	268	.000

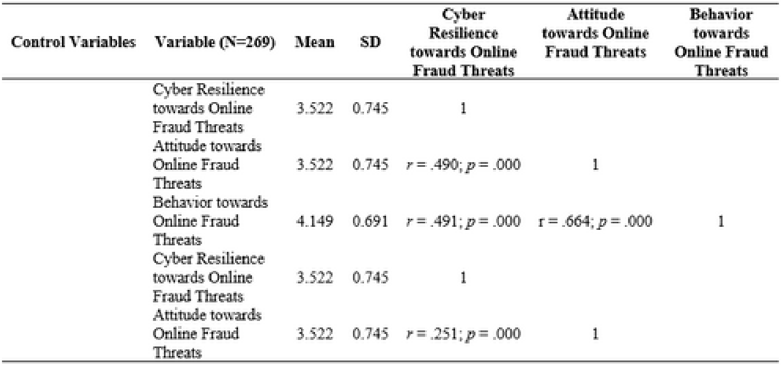
*Based on a 5-point Likert scale, where 1 = *strongly disagree* (1–20%), 2 = *disagree* (21–40%), 3 = *slightly agree* (41–60%), 4 = *agree* (61–80%), and 5 = *strongly agree* (81–100%).
**Test value of 3.

Hypothesis Testing

Relationship between Attitude, Behaviour and Cyber Resilience towards Online Fraud Threats

Two analyses were used to test the relationships between attitude, behavior and cyber resilience towards online fraud threats. The analyses involved are: (a) zero-order and partial correlation; and (b) hierarchical regression.

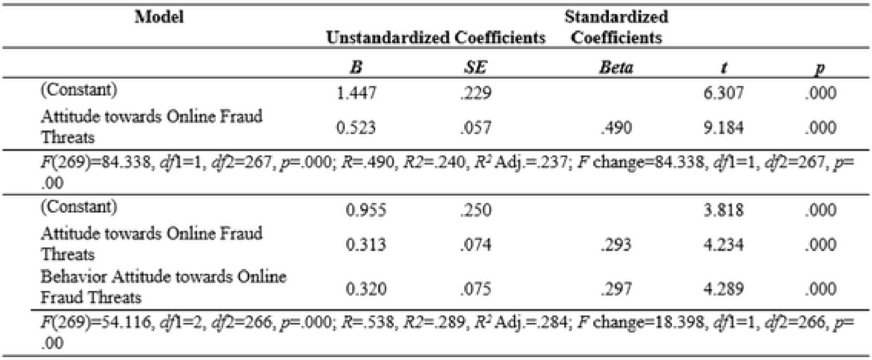
Table 5: Zero-order and partial correlation between behavior, attitude and cyber resilience towards online fraud threats



Control Variables	Variable (N=269)	Mean	SD	Cyber Resilience towards Online Fraud Threats	Attitude towards Online Fraud Threats	Behavior towards Online Fraud Threats
	Cyber Resilience towards Online Fraud Threats	3.522	0.745	1		
	Attitude towards Online Fraud Threats	3.522	0.745	*r* = .490; *p* = .000	1	
	Behavior towards Online Fraud Threats	4.149	0.691	*r* = .491; *p* = .000	r = .664; *p* = .000	1
	Cyber Resilience towards Online Fraud Threats	3.522	0.745	1		
	Attitude towards Online Fraud Threats	3.522	0.745	*r* = .251; *p* = .000	1	

Based on the results, all four hypotheses (H1, H2, H3, and H4) are supported as the correlation values are moderate significant. Hypothesis H1 (attitude is positively correlated with cyber resilience towards online fraud threats) is supported with a moderate significant correlation (r =.490; p=.000). Arniyati, Johnson and Storer (2015) found that positive attitude contributes to cyber resilience, provided that the students like to seek related information from the authority to confirm any suspicious activity. Hypothesis H2 (attitude is positively correlated with behavior) is also supported with a strong positive correlation (r=.664; p=.000). This means that students who have positive attitude and behaviour in handling online fraud are more likely to resist threats imposed by the perpetrators (Chandarman & Van Niekerk, 2017). In addition, the correlation between behaviour and cyber resilience towards online fraud threats (H3) is supported with a moderate significant correlation (r=.491; p=.000). This is in line with Slusky and Partow-Navid (2012) where they found that students who are eager to gain related information on cyber resilience will possess positive rewards as they know how to adjust with the stressful event created by the perpetrators. As all the criteria for mediating effect have been met where all the correlation tests are significant, thus, a hierarchical multiple regression analysis was performed (Table 6).

Table 6: Hierarchical regression analysis for cyber resilience towards online fraud threats with attitude and behavior



Model	Unstandardized Coefficients		Standardized Coefficients		
	B	*SE*	*Beta*	*t*	*p*
(Constant)	1.447	.229		6.307	.000
Attitude towards Online Fraud Threats	0.523	.057	.490	9.184	.000
F(269)=84.338, *df*1=1, *df*2=267, *p*=.000; *R*=.490, *R2*=.240, R^2 Adj.=.237; *F* change=84.338, *df*1=1, *df*2=267, *p*= .00					
(Constant)	0.955	.250		3.818	.000
Attitude towards Online Fraud Threats	0.313	.074	.293	4.234	.000
Behavior Attitude towards Online Fraud Threats	0.320	.075	.297	4.289	.000
F(269)=54.116, *df*1=2, *df*2=266, *p*=.000; *R*=.538, *R2*=.289, R^2 Adj.=.284; *F* change=18.398, *df*1=1, *df*2=266, *p*= .00					

The results show that behavior partially mediates the relationship between attitude and cyber resilience towards online fraud threats (H4). It is presented in the Beta weight reduction of .197 from Model 1(β=.490, t=9.184, p=.000) to Model 2 (β=.293, t=4.234, p=.000), yet their relationship is still significant. This is also supported by the reduction of the overall relationship F change=84.338 to F change=18.398; thus, H4 is partial supported. Yuliarti, AnggrenI, and Utari (2018) also stress on the behavior, specifically on the online platforms where students have to use the online platforms wisely and to practice safe online computing.

CONCLUSION

All the tested hypotheses for the study are supported with significant relationships. This means that attitude and behaviour are important contributors in developing cyber resilience users of online platforms; thus, helping them in facing online fraud threats created by the perpetrators. In addition, behavior is able to partially mediate the relationship between attitude and cyber resilience towards online fraud threats. This implies that behavior is a poweful construct in developing cyber resilience, specifically in handling numerous threats imposed by the perpetrators online. Therefore, future studies are suggested to test on cyber security as it is closely related to cyber resilience. Furthermore, it helps to determine the best predictor of cyber resilience towards online fraud threats. In addition, it is suggested to test the SET theory in a larger population like among the community instead of taking students as a sample size despite the fact that SET is applicable to the study.

AUTHORS' PROFILE

Nur Hafifah Jamalludin

A PhD candidate in the Department of Communication, IIUM with a Master's Degree of Human Sciences in Communication and a Bachelor's Degree of Human Sciences majoring is Mass Communication specialising in Public Relation. Her research interests include cyber resiliency, cyber-security, and social media usage specifically its impact on adults.

Email: *hafifahjamalludin@gmail.com*

Prof. Dr. Saodah Wok

Saodah Wok is a Professor in the Department of Communication, IIUM. She has her PhD in Mass Communication, University of Wisconsin-Madison. Her research interests include organisational communication, social sciences, media studies, and health communication.

Email: *wsaodah@iium.edu.my*

Dr Nerawi Sedu

Nerawi Sedu is an Assistant Professor at the Department of Communication, IIUM. He obtained a PhD in Journalism from the University of Queensland, Australia. His PhD thesis focused on the Islamic conceptualisation of press freedom, in the context of Malaysia. His research interests include media and communication, journalism and media system, and policy making

Email: *nerawi@iium.edu.my*

Dr. Tengku Siti Aisha Tengku Azzman

Tengku Siti Aisha Tengku Azzman is an Assistant Professor at the Department of Communication, IIUM. Her PhD is in Communication Studies from Kent State University. Her research interests include social media and communication technology, relational communication and quality of life, media studies, and intercultural communication.

Email: *taisha@iium.edu.my*

REFERENCES

Al-Janabi, S. (2016). A study of cyber security awareness in education environment in the Middle East. *Journal of Information and Knowledge Management*, 15(1), 2-30.

Arniyati, A., Johnson, C., & Storer, T. (2015). An investigation on organization cyber resilience. *International Journal of Computer and System Engineering*, 9(7), 2015.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, 20, 133-155.

Cropanzano, R., & Mitchell, S. M. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management*, 31(6), 875-900.

Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology*, 63, 597-606

Slusky, L., & Partow-Navid, P. (2012). Students' information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3-26.

Koong, K. S., Liu, C., Bai, S., & Wei, J. (2008). Occurrences of internet fraud in the USA. *International Journal of Services and Standards*, 4(1), 1-21.

Krubhala, P., Niranjana, P., & Priya, G. S. (2015). Online social network – A threat to privacy and security of human society. *International Journal of Scientific and Research Publications*, 5(4), 1-6.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 1(33), 71-90.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance and Cyber Security*, 2017, 1-14.

Ngo, T. F., & Peternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 773-793.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34, 231-245.

Poppleton, S., Lymperopoulou, K., & Molina, J. (2021). *Who suffers fraud? Understanding the fraud victim landscape*. Victims Commissioner. Retrieved from VC-Who-Suffers-Fraud-Report.pdf

Radhakrisna, G., & Pointon, L. D. (2007). Fraud in internet banking: A Malaysian legal perspective. *ResearchGate*, Volume 2007, 1-31.

Shaari, A. H., Kamaluddin, M. R., Paizi@Fauzi, W. F., & Mohd, M. (2019). Online dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online, Journal of Language Studies*, 19(1), 97-115. http://doi.org/10.17576/gema-2019-1901-06

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3-26.

Wimmer, R. D., & Dominick, J. R. (2014). *Mass media research: An introduction* (10th ed.). United States: Wadsworth Cengage Learning.

Yuliarti, M. S., Anggren, I. S., & Utari, P. (2018). Privacy and social media. *Advances in Social Sciences, Education and Humanities Research*, 260, 199-202.

Yunos, Z., Ab Hamid, R. S., & Ahmad, M. (2017). Cyber security situational awareness among students: A case study in Malaysia. *International Journal of Educational and Pedagogical Sciences*, 11(7), 1-7.

Acknowledgements

Distinguished officiator, keynote speaker, session chairpersons, technical reviewers, sponsors, presenters, participants, and all relevant parties and individuals who have contributed to the success of this event.

SPECIAL THANK YOU TO:

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue

KEMENTERIAN KESIHATAN
MALAYSIA

INTERNATIONAL COLLEGE
HATYAI CAMPUS
PRINCE OF SONGKLA UNIVERSITY

ABDULHAMID ABUSULAYMAN KULLIYYAH OF ISLAMIC REVEALED KNOWLEDGE AND HUMAN SCIENCES (AHAS KIRKHS)

TECHICAL SUPPORT AHAS KIRKHS

INFORMATION TECHNOLOGY DIVISION, INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA