International Journal of Business and Society, Vol. 22 No. 3, 2021, 1589-1601

CYBERCRIME THREAT LANDSCAPE AMID THE MOVEMENT CONTROL ORDER IN MALAYSIA

N.K. Tharshini ♣
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

Zamri Hassan
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

Faizah Haji Mas'ud
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

ABSTRACT

The COVID-19 pandemic has evolved rapidly and affected almost all the world's countries, creating unprecedented chaos on human lives, physical health, mental wellbeing, and the world economy. During this time, digital space has become an indispensable global means of communication, entertainment, and social interaction. However, high reliance on digital tools increases the risk of being prey to cyberattacks. In order to explore the cybercrime threat landscape, empirical research was conducted to examine the shared experiences related to cybercrime threats during the enforcement of the Movement Control Order in Malaysia. Data was collected using an online survey among 332 respondents across Malaysia. The finding stipulated that most of the respondents comprised females aged between 18 and 28 years old. The result also indicated that majority of female became victims of online phishing/malware distribution [(M = 0.58, SD = 0.13); t (113) = 2.24, p = 0.02] and online sexual harassment [(M = 0.56, SD = 0.11); t (107) = 2.38, p = 0.01]. The understanding of cybercrime experiences faced by the public during MCO is essential to help law enforcement agencies to stay vigilant on issues related to public safety and security during unprecedented conditions.

Keywords: Cybercrime; COVID-19; Malaysia; Movement Control Order; Pandemic

Received: 31 July 2020
Accepted: 27 September 2021
https://doi.org/10.33736/ijbs.4323.2021

1. INTRODUCTION

Cybercrime is a global phenomenon perpetrated using technological devices. Intensive blooming in digitalisation has led cybercrime to become one of the fastest-growing threats in the world. The agenda of the cybercriminals primarily focuses on obtaining information related to intellectual property, business and commercial strategy, customer information (e.g. contact details, banking information, payment card details), and sensitive financial information (Norton Cybercrime Report, 2010). In 2019, the Internet Organised Crime Threat Assessment (IOCTA) published by the European Union Agency for Law Enforcement Cooperation (EUROPOL) revealed that the cybercrime landscape encompasses six significant domains. These domains are online child sexual

♣ Corresponding Author: Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak (UNIMAS), 94300, Kota Samarahan, Sarawak, Malaysia; Email: stharshini@unimas.my

exploitation, cyber-dependent crime, payment fraud, cross-cutting crime factors, criminal abuse through the Darknet, and convergence of cybercrime and terrorism (EUROPOL, 2019). According to Allodi (2017), most cybercriminals are freelancers who provide various services ranging from cash-out solutions, malware development, or self-made trading products on various platforms in the underground economy.

By using a false identity, cybercriminals can manipulate the end-users to perform specific tasks such as opening fake emails, messages, or documents, propagating them to an Operational Technology (OT) network (Jensen et al., 2017). Significantly, impersonation is effortlessly achievable in cyberspace. Hence, they utilise the ability of obscurity in the virtual space by creating mock-ups of trusted websites (e.g. technology brands/product brands), targeting potential victims. (Abbasi et al., 2010). The Source Credibility Theory indicates that the end-users who believed or fell into the trap of the impersonated person or organisation comply with cybercriminals' orders with much credence (Boss et al., 2015). Apart from impersonations, cybercriminals exploit the end-users by using the six persuasion principles, namely authority, consistency, liking, scarcity, reciprocity, and social proof, to obtain sensitive information from their victims (Ferreira et al., 2015).

The basic principle of scarcity explains that an object or item is perceivably more valuable if the availability is deficient (Naidoo, 2020). Certainly, this principle is practised by cybercriminals by taking advantage of the end user's vulnerability. For instance, they may claim that their counterfeit product is quickly running out of supply, creating the illusion of scarcity as a tactic to trap their "potential victims". According to the psychology of compliance literature, emotions play a vital function in compliance behaviour (Boss et al., 2015). For instance, cybercriminals impersonating a police officer might use "penalties" as a strategy to agitate the end-users to comply with their order. Similarly, Ferreira et al. (2015) stated that reciprocation is another technique cybercriminals use to con the end-user's compliance. For example, they might exploit the individuals' high sense of obligation or magnanimity by tricking them to participate in online donation scams or fake fundraising campaigns.

The fallout of the COVID-19 pandemic has a profound impact on the cybercrime threat landscape (Gradon, 2020; Naidoo, 2020), such as a decrease from 30% to 42% of robberies, murders, assaults, thefts, and burglaries in major cities across the United States following the "stay-at-home" orders (Coyne, 2020). EUROPOL (2020) reported that cybercriminals began exploiting the crisis by adopting different operation modes to diversify new criminal activities, replacing the traditional instrument of crime. Additionally, information gathered from Interpol (2020) disclosed that the COVID-19 crisis created a pathway for the cybercriminal to execute social engineering attacks (phishing emails), ransomware attacks, and malware distributions. Case in point, Interpol (2020) disclosed an escalation in online fraud on pharmaceutical products, such as hand sanitisers, surgical masks, vaccines, antiviral medication, and fake COVID-19 test kits. Notably, EUROPOL (2020) identified that the online activity of sexual predators has elevated during the lockdown period, especially against children who are more vulnerable and highly exposed to online/digital solutions.

In line with the difficult situation during the COVID-19 pandemic, the Malaysian government executed a partial lockdown nationwide known as the Movement Control Order (MCO). It was implemented under the Prevention and Control of Infectious Disease Act (1988) and the Police Act (1967) from 18th March 2020. As a result, the enforcement of MCO has amplified the cybercrime

rate in Malaysia during the COVID-19 pandemic. In March 2020, Malaysian authorities reported that 393 investigation papers (IPs) had been opened involving fraudulent withdrawals of Employees Provident Fund (EPF) and online sales of counterfeit face masks, causing approximately RM3 million loss (Malaysian National Cyber Security Agency, 2020). Moreover, in April 2020, the Malaysian National Cyber Security Agency (NACSA) has blocked fraudulent websites and malicious Android mobile apps used to manipulate the victims to disclose their internet banking details (Business Today, 2020). NACSA reported that most of the blocked malicious Android mobile apps could read mobile phone SMSes and steal the victim's TAC codes (Malaysian National Cyber Security Agency, 2020).

There is an influx of contraband cigarettes through various online platforms during MCO enforcement as many shops have run out of cigarettes (Kaur, 2020). Online gambling has escalated, particularly after the government of Malaysia offers cash assistance known as *Bantuan Prihatin Nasional* (BPN) to the public (Tee, 2020). Some cybercriminals manipulated the cash assistance opportunity by targeting and encouraging victims to gamble away their money. Moreover, the Federal Commercial Crime Investigation Department (FCCID) has identified around 501 cases of fraudulent face mask sales with a total loss of RM3.5 million between 18th March 2020 and 3rd April 2020 (Federal Commercial Crime Investigation Department, 2020). In these cases, most victims have dealt with the dealers via social media platforms such as Instagram, Facebook, WeChat, and WhatsApp. The FCCID further confirmed that the dealers blocked the victim's social media connection upon receiving the payment.

The NACSA (2020) reported that the sale of unregistered illegal medicine has increased during the MCO due to the high demand for "COVID-19 cure" from online consumers. A total number of 182 websites selling unregistered drugs for COVID-19 were blocked after receiving 38 complaints on the sales of pharmaceutical products (Malaysian National Cyber Security Agency, 2020). The *Op Pangae XIII*, carried out between 3rd March 2020 and 10th March 2020, identified around 360 social media accounts, 347 personal websites, and 585 e-marketplace links selling unregistered drugs during the MCO (Malaysian National Cyber Security Agency, 2020). The high reliance on digital tools, especially during the enforcement of MCO, has created an optimal environment for the dispersal of various types of cybercrime victimisation. Thus, this study examined the shared experiences related to cybercrime threats during the enforcement of MCO in Malaysia. Furthermore, this study aims to create awareness among community members on the risk of being a victim of cybercrime since everyone is becoming more technologically reliant than ever before.

2. LITERATURE REVIEW

The availability of digital tools combined with robust communication technology has significantly influenced many aspects of society. However, the proliferation of Information and Communication Technology (ICT) and increased Internet penetration have raised concerns about cybercrime victimisation (Symantec, 2018). The World Economic Forum (2019) has ranked cybercrime as the upmost five risks the globe faces. A report released by Segal (2020) from the Centre for Strategies and International Studies in collaboration with McAfee disclosed that countries such as Vietnam, Brazil, India, and North Korea are classified as cybercrime centres. Primarily, the majority of the cybercriminals have started using various social engineering techniques to penetrate the end-user's network security system. For instance, malware such as computer worms, viruses, ransomware,

trojan horses, spyware, and other malicious programs are being used to encrypt the victim's information (EUROPOL, 2020). Furthermore, some cybercriminals use phishing attacks (e.g. disguise email from a credit card company/online payment website/app/social networking site/online store) to steal personal data such as passwords, social security number, or bank account numbers (EUROPOL, 2020).

Various theories were developed in the field of criminology studies to elucidate the root cause of criminal behaviour in cyberspace exhaustively. In a broader sense, cyberspace is a virtual realm link by a network known as the Internet, the common medium that connects the entire world (Reich et al., 2012; Futter, 2016). The high trend of crime in cyberspace is related to the changes in the "routine activities" of everyday life postulated through the Routine Activity Theory (RAT) (Cohen & Felson, 1979). In general, RAT attempts to show that crime rates are not affected by the macro changes such as unemployment rates or economic recessions; instead, the general lifestyle of an individual leads someone to get involved in criminal activities (Holt & Bossler, 2008). Table 1 summarised the RAT and key sensitising concepts of RAT.

Table 1: RAT and Key Sensitising Concepts

Theory	Area	Sensitising Concept
Routine Activity Theory (RAT)	Situational factors	• Suitable target/victim • Online behaviour • Impersonation • People and technology vulnerabilities

Source: Cohen & Felson (1979); Holt & Bossler (2008).

RAT delineates that cybercriminals are readily seeking suitable opportunities to commit cybercrimes. A committed crime is connected with three distinct criteria such as exposure to motivate criminals, target suitability, and capable guardianship (Holt & Bossler, 2008). Moreover, ICT skills and hacking knowledge are prominent tools that enable cybercrimes to be carried out effortlessly (Nguyen, 2020). During the COVID-19 pandemic, cybercriminals eagerly wait to manipulate their potential victims as various individuals (target suitability) work from home. The high reliance on digital tools (exposure to motivate criminals) during the stay-at-home order creates an optimal environment for the cybercriminals to trap their potential victims since majority of individuals (e.g. students and employees) operate under an unsecured environment (capable guardianship) while using various types of digitals tools (e.g. Zoom, Shopee, Lazada, and WhatsApp).

The risk of cyberspace victimisation is anticipated to spiral during the stay-at-home order (Gradon, 2020; Naidoo, 2020). In essence, the high dependability on the Internet has enabled cybercriminals to lure their potential victims using various technological tools. These tools include online advertisement websites, social media websites, dating websites, marriage websites, bulletin boards, and emails (Button et al., 2014; Jayabalan et al., 2014; Maras, 2016). A substantial body of literature has suggested that the age factor plays a pivotal role in online fraud victimisation (Fredrickson et al., 2005; Arfi & Agarwal, 2013; Norris et al., 2019). Scholars have identified that due to the lack of self-control, young adults, particularly those in the age range between 18 to 25 years old, are more likely to become victims of online fraud (Roberts et al., 2012). Anecdotally,

low self-control and a high level of risk-taking are foreseen as the primary factors, which lead young adults to surf the dark web and purchase counterfeit items from the mock-ups of trusted websites. Moreover, this predicament inevitably increases their chances of being involved in unauthorised money transactions, ultimately expand the probability of being a victim of online fraud (Norris et al., 2019).

In terms of cyberspace victimisation, specific characteristic or habit of end-user will amplify their exposure to cybercriminals. Van Wilsem (2013) stated that the availability of personal particulars (e.g. photos, sexual orientation, relationship status, gender) in an instant messenger or social media is sufficient for cybercriminals to attack their prospective victims. Furthermore, habits such as engaging in online deviant behaviour (e.g. making rude comments and sending pictures of sexual nature) or communicating with strangers will heighten the probability of being a cybercrime victim (Henson et al., 2013). Additionally, a study conducted by Holtfreter and Meyers (2015) disclosed that end-users exhibiting low level of self-control, high level of engagement in remote shopping, frequent use of instant messaging, and possessing the habit of downloading music or films on an untrusted website are more likely to become victims of cybercrime.

Researchers have also noted that members of Generation Y are highly prone to become victims of cyberbullying and encounter sexual solicitation due to their lack of awareness of the risk for online victimisation and disclosure of information (Marchum et al., 2010; Bateman et al., 2011; Naidoo, 2020; Stickle & Felson, 2020). For instance, a typical Facebook profile allows users to share a diverse range of personal information, including gender, hometown, birth date, personal interest, and academic concentration. Others include relationship status, political affiliation, and name of partners; - somehow opening a pathway for the cybercriminals to trap their potential victims. In the bargain, Marchum et al. (2010) stated that young adults are more vulnerable to becoming victims of cybercrime, being highly dependent on technology and spending a big chunk of their time online than adults.

3. METHODOLOGY

3.1. Research Design

An online survey was conducted using Google Form in a bilingual version (English-Bahasa Malaysia) to examine the shared experiences on cybercrime victimisation during the enforcement of MCO. According to Ronchi and Kinsey (2011), using online survey is optimal to reach a larger population of respondents, eventually amplifying the chances of increased sample size. A total number of 21 closed-ended questions were developed focusing on cybercrime victimisation during the COVID-19 pandemic. The survey questions were comprehensibly phrased to increase respondents' understanding, reduce ambiguities, and facilitate quick responses.

The survey encompasses four main parts including; (i) demographic profile, (ii) malware distribution/phishing emails, (iii) online fraud, and (iii) online sexual harassment. The limitations regarding the methodological choice of closed-ended questions affecting the respondent's viewpoint (Reja et al., 2003) were addressed by permitting customised responses (e.g. other) to allow the respondent to add comments if necessary. Content validity and face validity were carried out to ensure the developed instrument reflects the measured phenomena. According to Oluwatayo

(2012), face validity is defined as a researcher's subjective judgment to verify the appropriateness and relevancy of a developed instrument. Meanwhile, content validity is carried out to check the instrument's accuracy (Anastasi & Urbina, 1997). In the context of this study, face validity was used to get feedback from the subject matter expert (panel). The summary of the panel's comments for face validity is shown in Table 2.

Table 2: Summary of the Panel's Comments for Face Validity

No	Comment (s)
1.	Improvise the sentence structure
2.	Reduce the number of an item
3.	Format acceptable

Upon receiving feedback from the panels, several amendments were made to the items (question) in the instrument. Subsequently, content validity was carried out using the Content Validity Index (CVI). A dichotomous rating of favourable or unfavourable was used to rate the validity of the content (Sangoseni et al., 2013). Lynn (1986) stated that an item is considered pertaining if the CVI score is above 0.78. Generally, favourable items (concise) were given a score of +1.00, whereas a score of +0.00 was given to unfavourable items (inapt question) (Masuwai et al., 2016; Sangoseni et al., 2013). For this study, a favourable rating by two expert panels and CVI greater than 0.78 indicated that the developed questions are relevant to the topic of the study. Table 3 shows the reliability value of the instrument.

Table 3: Reliability Value of Instrument

Variable	Cronbach Alpha (α); n = 332
Online Phishing/Malware Distribution	0.88
Online Fraud	0.60
Online Sexual Harassment	0.86

3.2. Procedure

The online survey form was disseminated to the public staying in East and West Malaysia via email and other social media platforms such as Facebook and WhatsApp. The survey period of the research officially begins between 8th May 2020 and 31st May 2020. Furthermore, a total number of 332 respondents participated in this study.

3.3. Data Analysis

The obtained data were analysed using Statistical Package for the Social Sciences (SPSS). T-test was used to analyse the differences between gender and cybercrime threat landscape during the enforcement of MCO in Malaysia.

3.4. Ethical Considerations

The Ethical Committee of the Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak, was consulted before conducting the online survey. Moreover, as a part of the ethical

consideration, the respondents' participation in this study is entirely voluntary, and all the responses were recorded anonymously. Besides, the purpose of the study was clearly stated in the Google Form, and respondents were also required to tick the "YES" checkbox as a sign of consenting to take part in this study. Additionally, no benefits or incentives were given to encourage participation.

4. RESULTS AND DISCUSSION

The result and discussion are presented in two main sub-sections, namely demographic profile and differences between gender and cybercrime threat landscape during the enforcement of MCO in Malaysia.

4.1. Demographic Profile

The demographic profile represents the basic information of the respondents who took part in this study. The descriptive analysis result showed that majority of the respondents were females (75%) aged between 18 and 28 years old (83.8%), and most of the respondents were Sarawakian (47.3%) that resided in the urban area (62.3%). Furthermore, the result stipulated that the majority of the respondents used a smartphone for Internet browsing (95.2%) and preferred using social media platforms, such as WhatsApp (92.2%), Facebook (71.1%), and Instagram (63.9%) to stay connected with others. The summary of demographic profile of the respondents is shown in Table 4.

Table 4: Demographic Profile

Profile	Frequency	Percentage (%)
Gender		
Male	83	25
Female	249	75
Age		
18-28 years	278	83.8
29-39 years	29	8.7
40-50 years	19	5.7
51 years and above	6	1.8
State		
Perlis	2	0.6
Kedah	6	1.8
Pulau Pinang	5	1.5
Perak	16	4.8
Selangor	37	11.1
Johor	5	1.5
Negeri Sembilan	7	2.1
Melaka	7	2.1
Pahang	3	1.0
Terengganu	29	8.7
Kelantan	11	3.3

Sabah	32	9.7
Sarawak	157	47.3
Federal Territory of Kuala Lumpur	15	4.5
Current Location		
Town Area	207	62.3
Rural Area	125	37.7
Most Used Device to Surf Internet		
Smartphone	316	95.2
Tablet	2	0.6
Laptop	9	2.7
Desktop	5	1.5
Most Used Social Media Platform		
Official email	62	18.7
Google email	118	35.5
WhatsApp	306	92.2

4.2. Differences between Gender and Cybercrime Threat Landscape

The result and discussion of this part are divided into two main sub-sections, including; (i) differences between gender and online phishing/malware distribution and (ii) differences between gender and online sexual harassment.

4.2.1. Differences between Gender and Online Phishing/Malware Distribution

There is a significant difference in the score for male (M = 0.54, SD = 0.10) and female respondents (M = 0.58, SD = 0.13); t (113) = 2.24, p = 0.02. The result indicated that most females became victims of online phishing/malware distribution compared to males. Moreover, the findings also depicted that cybercriminals sent harmful software and tried to hack the respondent's computer/smartphone/online account. Table 5 shows the summary of the T-test result.

Table 5: T-test of Differences between Gender and Online Phishing/Malware Distribution

Category	Gender	Mean	T-Value	Sig	Interpretation	Decision on Hypothesis
Online Phishing/Malware Distribution	Male Female	0.54 0.58	2.24	0.02	Significant difference	Rejected

Phishing is a web-based attack where the end-users (victims) are deceived of their private information. This crime involves the cybercriminal (phisher) fabricating a duplicate website and redirect the victims to obtain confidential details such as social security number, credit card number, or bank account details (Abbas et al., 2014). Vishwanath (2015) stated that individuals on Facebook regularly are more likely to fall prey to a phishing attack. Cybercriminals prefer to execute phishing attacks via email or instant message spoofing as individuals possess a habituated routine to check for emails and messages (Vishwanath, 2015). Notably, the result of this research

aligned with the study conducted by Boss et al. (2015), showing that females are more prone to become the victim of phishing attacks than males. In this study's context, since most of the respondents are female young adults (aged 18 to 28 years old), the vulnerability factor perceivably increases the possibility of being prey to phishing attacks. Supporting this statement, prior researchers have indicated that females have rapidly become victims of phishing attacks as they are more gullible compared to males (Lopes et al., 2003; Boss et al., 2015; Sun, 2016).

According to Sun (2016), cybercriminals (phishers) utilise various methods to target their victims. For instance, some phishers will send a random offer or malicious sale link specifically to females, knowing they are easily attracted to lower-price offers. Furthermore, the findings of this study indicate that gender and situation factors (stay-at-home order) may affect the outcomes of cybercrime victimisation. It was found that human vulnerability is way easier to attack than technical vulnerabilities during the stay-at-home order (Naidoo, 2020). For example, the enforcement of MCO entangled with limited human interaction might have led some of the respondents involved in this study to become victims of phishing attacks. This predicament is due to their dependency on utilising significantly increasing websites and applications to pay their bills, order food, or carry out online transactions during MCO.

4.2.2. Differences between Gender and Online Sexual Harassment

There is a significant difference in the score for male (M = 0.53, SD = 0.75) and female respondents (M = 0.56, SD = 0.11); t (107) = 2.38, p = 0.01. The result indicates that the majority of females become victims of online sexual harassment compared to males. Moreover, the findings depict that cybercriminals have sent sexual content messages/emoji's/images/videos via social media platforms and shared the respondent's personal information non-consensually. Table 6 shows a summary of the T-test result.

Table 6: T-Test of Differences between Gender and Online Sexual Harassment

Category	Gender	Mean	T-Value	Sig	Interpretation	Decision on Hypothesis
Online Sexual Harassment	Male Female	0.53 0.56	2.38	0.01	Significant difference	Rejected

The findings from this research coincide with previous studies indicating that most females have experienced online sexual harassment compared to their male counterparts (Baumgartner et al., 2010). Sexual harassment catalyses various psychological repercussions, ranging from sorrow, distress, depressive symptoms, and emotional distress. The same aftermath applies to the nature of sexual harassment occurring in online platforms, either in a private inbox or group chat. Significantly, young females are more vulnerable to become victims of cybercrimes as they spend more time being online than adult females (Jiloha, 2020). Moreover, a study conducted by Jiloha (2020) reported that females encountered a more comprehensive range of online sexual harassment compared to males. Furthermore, a report obtained from Interpol (2020) indicated that many young women experienced some form of sexual harassment (e.g. receiving sexually explicit messages or images) while using online dating sites or apps.

Sensation seeking (poor emotional regulation) and being impulsive (lack of control) is a common behavioural trait among young adults (Jain et al., 2020). Jain et al. (2020) stated that the desire to stay connected and obtain friend requests, likes or followers has resulted in young adolescents engaging in risky online behaviour including interacting with strangers, accepting friend requests from strangers, including too much personal information on the social media platform, or posting revealing pictures on Facebook, Instagram or WhatsApp. Overall, these critical risk factors might have perceivably increased the probability of female respondents in this study becoming victims of online sexual harassment during the stay-at-home order. Admittedly, this statement is supported by Ybarra et al. (2007), stating that disclosing personal information and posting revealing images escalate the risk of being a victim of online sexual harassment among females.

5. CONCLUSION & RECOMMENDATION

The result of this study unveiled that cybercriminals are consistently diversifying the cyberattack method by adapting themselves to situational changes during the enforcement of MCO in Malaysia. Admittedly, there is no single standalone solution to combat this issue in the realm of cybercrime. Thus, the end-users must be aware that expensive software alone is not enough to protect them from being victims of cyber threats. Hence, while using digital tools, the end-users must adhere to safety measures such as backing up online and offline files regularly and strengthening their home network by using strong passwords. Others safety measures include managing their social media profiles wisely and avoiding opening suspicious emails/attachments. Besides, government parties should take advantage of the resources and expertise of the private sectors in the fight against cybercrime. This idea can be achieved by developing a sustainable national cybersecurity campaign to raise public awareness of cyber activity's risk and impact. Moreover, future studies related to cybercrime victimisation should focus on the causal relations between various significant factors related to cybercrime by using The Partial Least Square path modelling. Furthermore, future studies should also expand to test on larger datasets from East and West Malaysia to obtain a more generalised understanding of the cybercrime landscape in Malaysia.

ACKNOWLEDGEMENT

The authors would like to acknowledge all the participants who took part in this study.

REFERENCES

Abbas, H., Mahmoodzahed, M. Q., Aslam Khan, F., & Pasha, M. (2014). Identifying an OpenID Anti-Phishing Scheme for Cyberspace. *Security and Communication Networks, 9,* 481-491.

Abbasi, A., Zhang, Z., Zimbra, D., & Chen, H. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly, 34*(3), 435-461.

Allodi, L. (2017). *Economic Factors of Vulnerability Trade and Exploitation: Empirical Evidence from a Prominent Russian Cybercrime Market*. Springer International Publishing.

Anastasi, A., & Urbina. S. (1997). *Psychological Testing* (7th ed). Upper Saddle River, NJ: Prentice Hall.

Arfi, N., & Agarwal, S. (2013). Knowledge of Cybercrime among Elderly. *International Journal of Scientific and Engineering Research*, *4*(7), 1463.

Bateman, P. J., Pike, J. C., & Butler, B. S. (2011). To Disclose or Not: Publicness in Social Networking Sites. *Information Technology & People*, *24*, 78-100.

Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted Online Sexual Solicitation and Risky Sexual of a Phishing Attack. *Journal of Computer-Mediated Communication*, *20*, 570-584.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviours. *MIS Quarterly*, *39*(4), 837-864.

Business Today. (2020). *KPMG: Hackers Exploiting Global Uncertainty during COVID-19 Pandemic.* https://www.businesstoday.com.my/2020/04/22/kpmg-hackers-exploiting-global-uncertainty-during-covid-19-pandemic/

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian and New Zealand Journal of Criminology*, *47*(3), 391-408.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608.

Coyne, M. (2020). *Crime Rates Across U.S. Drop Amid the Coronavirus Pandemic.* https://www.forbes.com/sites/marleycoyne/2020/04/11/crime-rates-across-us-drop-amid-the.

European Union Agency for Law Enforcement Cooperation. (EUROPOL) (2019). IOCTA. *Internet Organized Crime Threat Assessment.* The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/iocta-report

European Union Agency for Law Enforcement Cooperation. (EUROPOL) (2020). *Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis.* The Hague, The Netherlands: European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Federal Commercial Crime Investigation Department. (2020). *Jabatan Siasatan Jenayah Komersil.* https://www.rmp.gov.my/infor-korporate/jabatan---jabatan/jabatan-siasatan-jenayah-komersil

Ferreira, A., Coventry, L., & Lenzini, G. (2015). *Principles of Persuasion in Social Engineering and Their Use in Phishing*. Springer International Publishing.

Fredrickson, B. L., & Branigan, C. (2005). Positive Emotions Broaden the Scope of Attention and Thought-Action Repertoires. *Cognition and Emotion*, *19*(3), 313-332.

Futter, A. (2016). *Is Trident Safe from Cyber Attack?* https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf

Gradon, K. (2020). Crime in the Time of the Plague: Fake News Pandemic and the Challenges to Law-Enforcement and Intelligence Community. *Society Register*, *4*(2), 133-148.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Does Gender Matter in the Virtual World? Examining the Effect of Gender on the Link between Online Social Network Activity, Security, and Interpersonal Victimization. *Security Journal*, *26*(4), 315-330.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behaviour*, *30*(1), 1-25.

Holtfreter, K., & Meyers, T. J. (2015). Challenges for Cybercrime Theory, Research, and Policy. *Behavioural Emerging Situations*, 105-155. In G. C. Lajeunesse (Ed.), *The Norwich Review of International and Transnational Crime* (pp. 54-65). Norwich University: NUARI.

Interpol. (2020). *COVID-19 Crime: INTERPOL Issues New Guidelines for Law Enforcement.* https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-crime-INTERPOL-issues-new-guidelines-for-law-enforcement

Jain, S. & Agrawal, S. (2020). Perceived Vulnerability of Cyberbullying on Social Networking Sites: Effects of Security Measures, Addiction and Self-Disclosure. *Indian Growth and Development Review*, *14*(2), 149-171.

Jayabalan, P., Ibrahim, R., & Abdul Manaf, A. (2014). Understanding Cybercrime in Malaysia: An Overview. *Sains Humanika*, *2*(2), 109-115.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Jiloha, R. (2020). Internet Abuse: A Newer Form of Sexual Harassment. *Journal of Advanced Research in Psychology and Psychotherapy*, *3*(1), 13-18.

Kaur, M. (2020). *Online Gambling "Rampant" Since MCO Began.* Free Malaysia Today. https://www.freemalaysiatoday.com/category/nation/2020/04/06/online-gambling-rampant-since-mco-began/

Lopes, P. N, Salovey, P., & Straus, R. (2003). Emotional Intelligence, Personality, and the Perceived Quality of Social Relationships. *Personality and Individual Differences*, *35*(3), 641-658.

Lynn, M. R. (1986). Determination and Quantification of Content Validity. *Nursing Research*, *35*(6), 382-386.

Tee, K. (2020, April 6). *IGP Vows Crackdown on Rampant Cigarette Smuggling, Online Gambling During MCO.* Malay Mail. https://www.malaymail.com/news/malaysia/2020/04/06/igp-vows-crackdown-on-rampant-cigarette-smuggling-online-gambling-during-mc/1854103

Malaysian National Cyber Security Agency. (2020). *MyCERT – The Malaysian Computer Emergency Response Team.* https://www.cybersecurity.my/en/our_services/mycert/main/detail/2328/index.html

Maras, M. H. (2016). *Cyber Criminology*. New York: Oxford University Press.

Marchum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviours Using Routine Activity Theory. *Criminal Justice Review*, *35*, 412-437.

Masuwai, A., Mohd Tajudin, N., & Shah. N. S. (2016). Evaluating the Face and Content Validity of a Teaching Guiding Principles Instrument (TLGPI): A Perspective Study of Malaysian Teacher Educators. *Malaysian Journal of Society and Space*, *12*(3), 11-21.

Naidoo, R. (2020). A Multi-Level Influence Model of COVID-19 Themed Cybercrime. *European Journal of Information Systems*, *29*(3), 306-321.

Nguyen, T. V. (2020). Cybercrime in Vietnam: An Analysis on Routine Activity Theory. *International Journal of Cyber Criminology*, *14*(1), 156-173.

Norris, G., Brookes, A. & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, *19*(34), 231-245.

Norton Cybercrime Report. (2010). *Norton's Cybercrime Report: The Human Impact Reveals Global Cybercrime Epidemic and Our Hidden Hypocrisy.* https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-report-human-impact-reveals-global-cybercrime

Oluwatayo. J. A. (2012). Validity and Reliability Issues in Educational Research. *Journal of Educational and Social Research, 2*(2), 391-400.

Police Act. (1967). *Laws of Malaysia: Online Version of Updated Text of Print (Act 344).* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.ilo.org%2Fdyn%2Fnatlex%2Fdocs%2FELECTRONIC%2F103083%2F124971%2FF1234758774%2FMYS103083.pdf&clen=483809

Prevention and Control of Infectious Disease Act. (1988). *The Prevention and Control of Infectious Diseases (Measure Within the Infected Local Areas) Regulation 2020 – Containing the COVID-19 Outbreak in Malaysia.* https://www.christopherleeong.com/media/3887/clo_2020_03_the-prevention-and-control-of-infectious-diseases.pdf

Reich, P. C., & Gelbstein, E. (2012). *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilisation.* USA: Hershey.

Reja, U., Manfreda, K. L., Hlebec, V., & Vehovar, V. (2003). Open-Ended VS Closed-Ended Questions in Web Questionnaires. *Development Application Statistic*, *19*, 159-177.

Roberts, J. A., & Manolis, C. (2012). Cooking up a Recipe for Self-Control: The Three Ingredients of Self-Control and its Impact on Impulse Buying. *Journal of Marketing Theory and Practice*, *20*(2), 173-188.

Ronchi, E., & Kinsey, M. (2011). Evacuation Models of the Future: Insights from an Online Survey on User's Experiences and Needs. In J. Capote & D. Alvear (Eds.), *Proceedings of the Advanced Research Workshop: "Evacuation and Human Behaviour in Emergency Situations"* (pp. 145-155). Universidad de Cantabria.

Sangoseni, O., Hellman, M., & Hill, C. (2013). Development and Validation of a Questionnaire to Assess the Effect of Online Learning on Behaviours, Attitudes, and Clinical Practices of Physical Therapists in the United States Regarding Evidence-Based Clinical Practice. *The Internet Journal of Allied Health Sciences and Practice*, *11*(2), 113.

Segal, S. (2020). *Breaking Down the G20 COVID-19 Fiscal Response.* Centre for Strategies and International Studies (CSIS). https://www.csis.org/analysis/breaking-down-g20-covid-19-fiscal-response

Stickle, B. & Felson, M. (2020). Crime Rates in a Pandemic: The Largest Criminological Experiment in History. *American Journal of Criminal Justice, 45,* 525-536.

Sun, J. C. (2016). The Mediating Effect of Anti-Phishing Self-Efficacy between College: Internet Self-Efficacy and Anti-Phishing Behavior and Gender. *Computers in Human Behaviour, 59,* 12-14.

Symantec. (2018). *We Stop Threats Hiding in Plain Sight.* https://securitycloud.symantec.com/cc/#/landing

Van Wilsem, J. (2013). Bought It but Never Got It: Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168-178.

Vishwanath, A. (2015). Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcome. *Journal of Computer-Mediated Communication, 20*(5), 570-584.

World Economic Forum. (2019). *The Cybersecurity Guide for Leaders in Today's Digital World.* https://www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf

Ybarra, M. L., Mitchell, K. J., & Finkelhor, D. (2007). Internet Prevention Messages: Targeting the Right Online Behaviors. *Arch Paediatric Adolescent Medicine*, *161,* 138-45.