INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 12, Issue 5, (2022) E-ISSN: 2222-6990

Level of Cybercrime Threat During the Outbreak of COVID-19 Pandemic: A Study in Malaysia

N. K. Tharshini, Faizah Haji Mas'ud, Zamri Hassan

Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

Email: stharshini@unimas.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i5/13142 DOI:10.6007/IJARBSS/v12-i5/13142

Published Date: 02 May 2022

Abstract

Cybercrime threat has shown a sudden increase during the enforced stay-at-home order due to the outbreak of the COVID-19 pandemic. Thus, empirical research was conducted in providing substantial evidence regarding the level of cybercrime threats in Malaysia during the outbreak of the COVID-19 pandemic. A quantitative approach was used to collect data among 332 respondents across Malaysia. The finding stipulated that a large number of respondents have experienced a high level of online phishing/malware distribution (72.9%), a moderate level of online fraud (69.2%), and a moderate level of online sexual harassment (87.7%). The move to explore the level of cybercrime threat experienced by the public during the outbreak of the COVID-19 pandemic is essential to detect, disrupt, and mitigate cybercrime threats during unprecedented situations.

Keywords: Cybercrime, Cybercriminals, COVID-19, Threat, Pandemic

Introduction

The outbreak of the COVID-19 pandemic has led to the emergence of various problems such as creation and consumption of false information, political hoaxes, transmission of misleading medical remedies for COVID-19, and fabrication of false conspiracy theories across the globe (Hansson et al., 2021; Tharshini et al., 2021). On the other hand, the outbreak of the COVID-19 pandemic has led many countries to issue "stay-at-home" orders to contain the spread of that virus resulting in a radical alteration to the individual's lifestyle. Some valid proof shows that violent crimes such as robberies, burglaries, murders, and thefts cases are reported to decline in major cities across the United States ranging from 30% to 42% following the decreased mobility due to the stay-at-home order (Hawdo et al., 2020). Consequently, the idling of society during the COVID-19 pandemic along with the advancement in digital technologies has created an optimal impact on the cybercrime threat landscape.

In general, cybercrime refers to illegal activities that use a computer or smartphone as its primary means of commission to intentionally cause harm against individuals or groups of

individuals (Chigada & Madzinga, 2021). According to Payne and Hadzhidimova (2018), cybercrime is classified as the second most reported crime across the world. Similarly, the National Institute of Communicable Diseases (2021) defined cybercrime as unauthorised computer-mediated activities toward an individual or a company with malicious intentions such as stealing or misusing information/data for personal gain. Pranggono and Arabo (2021) stated that the tremendous dependency on digital technology across all sectors attributed by remote working environments and stay-at-home orders during the COVID-19 pandemic has further upsurged the rate of cybercrime attacks across the globe.

According to Hawdo et al (2020); Pranggono et al (2021), dangerous online routine during the stay-at-home order, which includes surfing the dark web, visiting untrusted shopping websites, and playing online games increases the rate of cybercrime victimization. Moreover, the lack of security protocols for offsite connection also prompts cybercriminals to hack the internet-enabled devices, especially targeting those who work from remote locations (Hawdon et al., 2020; Payne et al., 2018; Quade, 2020). Furthermore, unsecured internet connections and less-reliable networks also increase the risk of cyberattacks for individuals working remotely from home (Chigada & Madzinga, 2021; Hansson et al., 2021).

With reference to the contagion impact of the COVID-19 pandemic, the government of Malaysia has decided to impose a nationwide lockdown pursuant to the Prevention and Control of Infectious Diseases Act 1988 and the Police Act 1987 (Jeyasingam, 2020). However, the high level of dependency on technology facilitation during the Movement Control Order (MCO) (also known as stay-at-home order) has amplified the cybercrime rate in Malaysia. Cyber Security Malaysia has disclosed that online sextortion cases have increased during MCO (Daily Express, 2020). A total number of 23 cases reported from 18 March 2020 until 14 April 2020 stated that some scammer has used pre-recorded webcam footage of beautiful women to lure the victims to disguise their identity (Daily Express, 2020). Besides, based on Pornhub's insights, Malaysia is reported to be in the top Asian country list surfing pornographic sites with the peak increasing to 24.4% on 25th March 2020 (during MCO) (Daily Express, 2020).

A statistic issued by the Malaysian Computer Emergency Response Team (MyCERT) shows that there was around 8,366 cybercrime cases reported in Malaysia from January 2020 to September 2020 (The Star, 2020). Additionally, cybercrime cases have particularly risen in Malaysia during the enforced MCO with a total number of 3,906 complaints being lodged to the Cyber999 Help Centre from 18th March 2020 to 30th June 2020 involving cyberbullying, attempts of hacking, cyber intrusion, and cyber fraud in urban areas with a high-speed of internet connection (The Star, 2020). Further to this, between January 2021 and May 2021, a total number of 4,615 cybersecurity incidents were reported to Cyber Security Malaysia for cases such as online fraud (3,299 cases), intrusion (765 cases), and distribution of malicious code to the computer and/or mobile phone (256 cases) (The Star, 2021).

The New Straits Times (2020) has reported that crime incidents related to Macau scams and impersonation of authorities, particularly posing as Central Bank of Malaysia and Malaysia Anti-Corruption Commission (MACC) personnel have increased by 65.3% involving losses of RM3.5 million during the MCO period (The New Straits Times, 2020). Furthermore, online loan scams have also skyrocketed since many people were financially affected due to job retrenchments in Malaysia during the COVID-19 pandemic (The New Straits Times, 2020). The

high reliance on digital tools, especially during the MCO has created an optimal environment for the dispersal of various types of cybercrime threats in Malaysia. Thus, this research sought to address the predominance level of cybercrime threat underwent by the public during the outbreak of the COVID-19 pandemic.

Literature Review

Based on the Rational Choice Theory, criminal behavior is the result of the systematic planning of an individual after considering the benefit and cost of their action (Marganski, 2019). Undoubtedly, when the benefit (e.g., feeling of superiority, revenge, instant gratification) outweighed the cost of action (getting punished, caught) an offense is very much likely to occur (Marganski, 2019). For instance, in the case of cyberstalking, the anonymity factor (benefit) allows the cybercriminals to reach out to a larger audience with minimal risk of detection or punishment (cost of action) (Marganski, 2019). Besides, mounting evidence related to the detrimental nature of cyberstalking toward the victims shows that those on the receiving end experience low quality of life, tend to change their school or work-related routines, develop negative psychological outcomes (e.g., depression, anxiety, PTSD, trauma), suffer financial repercussion, encounter suicidal ideation, or begin to distrust other individuals (Marganski, 2019). Furthermore, Marganski (2019) stated that cyberstalking has always been notoriously difficult to prosecute since most of the victims are reluctant to report those incidents due to social ramifications.

Advancement in digital technologies has transformed the way cybercriminals exploit the benefit of digital transformations by engaging in illicit activities such as internet luring. In general, internet luring is defined as a deceitful practice in which an individual tries to trick another person by using different types of online platforms such as social media forums, chat rooms, marriage websites, advertisement websites, employment websites, email, or bulletin boards to trap their potential victims (Maras, 2019). For instance, reports have shown that some child sex offenders pretended to be the same age as the child as a tactic to easily approach them (Maras, 2019). Similarly, females are easily lured by the cybercriminals through a variety of tricks including; (i) false promises of romantic relationship, (ii) fake employment opportunities with big remuneration in another country, or (iii) false promises to make them more famous (Maras, 2019). In addition to these, internet luring also victimizes females in various forms such as gender-based slur/harassment, cyberstalking, slut-shaming, sextortion, electronically enabled trafficking, and unsolicited pornography (Maras, 2019).

Online identify theft is the fastest-growing form of consumer fraud execution through advanced digital techniques such as “pharming” and “phishing” as a means of tricking their targeted victims (Quade, 2020). Additionally, online identity theft is prevalent in developed societies due to the high level of internet and mobile penetration in those societies (Quade, 2020). Likewise, cyberstalking is another form of rapidly rising cybercrime in the realm of cyberspace. Some researchers have classified cyberstalking as an innocuous behaviour in which someone violates the privacy of an individual causing greater distress and harm, especially for those on the receiving end (Hawdon et al., 2020; Payne et al., 2018). Growing evidence suggested that cyberstalking is a gender-based crime where males commonly play the role of a perpetrator whilst females disproportionately became the victims (Hawdon et al., 2020). Admittedly, the number of cyberstalkers is exponentially higher compared to physical stalkers since the former can hide under the veil of anonymity (Hansson et al., 2021).

Identically, young adults commonly fall victim to cyberstalking since they are more active on social media platforms compared to mature adults (Hawdon et al., 2020).
During the outbreak of the COVID-19 pandemic, cybercriminals have created numerous fake domains on the internet to deceive their potential victims (Checkpoint Risk Intelligence, 2020). Checkpoint Risk Intelligence (2020) stated that by the end of January 2020, around 4,000 domains related to Coronavirus were active, mostly from countries such as the United States, Russia, Italy, and Germany; from that total amount, 5% of the domains were suspicious, of which 3% of them were malicious domains used to obtain personal information for various nefarious intentions. Since many companies turned to cloud service platforms during the pandemic, cybercriminals have also attempted to disguise themselves by attacking those companies by using malware delivery (e.g., by sending hyperlink attachments) and phishing attacks (e.g., by sending phishing emails) (Palmer, 2020).

The advancement in the electronic medium has increased the rate of cybercrime victimization during the stay-at-home order (Kranenbarg et al., 2019). Both children and adults spent more time being online during this period due to the social isolation and boredom of being confined at home, eventually increasing the risk of becoming a victim of cybercrime (EUROPOL, 2020). Following this, Cook (2020) and Broadhurst et al. (2020) stated that new ransomware known as “CoronaVirus” and fake browsing application (related to medicine curing coronavirus) has been developed by cybercriminals to encrypt the data of the end-users. Besides, EUROPOL (2020) reports showed that most cybercriminals try to share intimate videos/photos of the victims, post offensive comments about the victims, or use spam emails, interactive websites, spyware, and Trojan to attack their victims during the stay-at-home order.

Objective

The objective of this study is to:

(i) Identify the level of cybercrime threat during the outbreak of the COVID-19 pandemic in Malaysia.

Methodology

To examine the level of cybercrime threats during the outbreak of the COVID-19 pandemic, an online survey was carried out using Google Form.

Research Instrument

A research instrument is an important tool to help the researcher in achieving the research objective. In this study, the level of cybercrime threats is measured by using the Cybercrime Experience during the Movement Control Order Questionnaire developed by Tharshini, Hassan, and Haji Mas’ud (2020). There are three main parts to this questionnaire namely; (i) online phishing/malware distribution, (ii) online fraud, and (iii) online sexual harassment.

Table 1 shows the reliability value of the research instrument.

Table 1
Reliability Value of the Research Instrument

Variable (s)	Cronbach Alpha (α); n = 332
Online Phishing/Malware Distribution	0.70
Online Fraud	0.78
Online Sexual Harassment	0.77

Procedure

Social media platforms such as Facebook, Telegram, and WhatsApp was used to disseminate the online survey form to the public. A total number of 332 respondents voluntarily took part in this study. Since data was collected using online tools, the researcher's name and email address was included in the Google form to enable the respondents to reach the person in charge if they have any query regarding the research.

Data Analysis

Data were analysed using Statistical Package for the Social Sciences (SPSS). Descriptive analyses were used to obtain information related to frequency and percentage.

Ethical Considerations

The participation of respondents in this study is completely voluntary and no incentives was given to encourage participation. Besides, it was made compulsory for all the respondents to tick the "YES" checkbox in the Google form that denotes their consent to take part in this study. Moreover, all responses from the respondents were recorded anonymously.

Result and Discussion

This section reports the result of the analysed data.

Level of Online Phishing/Malware Distribution

The result of the descriptive analysis shows that most members of the public experienced a high level (72.9%) of online phishing/malware distribution threats during the outbreak of the COVID-19 pandemic.

Table 2
Level of Online Phishing/Malware Distribution during MCO

Level	Frequency	Percentage (%)
Low	79	23.8
Moderate	11	3.3
High	242	72.9
TOTAL	**332**	**100**

Note: Low (<2.33), Moderate (2.34-3.67), High (3.68-5.00)

The implementation of MCO to curb the spread of the COVID-19 pandemic in Malaysia has opened a pathway for cybercriminals to target and attack new vulnerabilities from various walks of life. The high reliance on mobile phones, desktops, and laptops along with continuous engagement in social media activities, online banking, and online shopping during the stay-at-home order has greatly influenced the level of cybercrime victimization among the public. According to Malaysiakini (2020), the spike in internet usage during MCO has given an

opportunity for the cybercriminals to change their modus operandi to manipulate their potential victims, especially by creating and distributing fake domains, scams, and "COVID-19" themed phishing emails.

The findings of this research coincide with a report obtained from TechWire Asia (2020) reporting that issues pertaining to cybersecurity have become one of the top concerns during the enforcement of MCO in Malaysia. The National Cyber Security Agency (2020) disclosed that online threats in Malaysia have increased by 82.5% during the enforcement of MCO (involving online fraud, phishing email, and intrusion into unauthorised systems). Furthermore, the National Cyber Security Agency (2020) also stated that most cybercriminals have been using certain malicious domains which contain words such as "COVID-19", "Coronavirus" or "Corona" while sending phishing emails, attachments, and malicious URLs to lure their potential victims.

A large number of cybercriminals use online phishing as one of their tactics to lure their victims since many internet users are hooked to their social media platforms (e.g., Facebook, Instagram, Twitter, TikTok, Telegram, WhatsApp, etc.) and have been actively engaged in online shopping during the stay-at-home period (Tharshini et al., 2021; Naidoo, 2020). Moreover, since impersonation is easily achievable in cyberspace it became even easier for the cybercriminals to send online phishing/malware emails as a tactic to lure the victims (Naidoo, 2020). Furthermore, in the context of this study, risk factors such as lack of cybersecurity awareness and poor network configuration are also foreseen as one of the reasons that have caused majority of the respondents to fall victim to online phishing/malware distribution during the outbreak of the COVID-19 pandemic.

Level of Online Fraud

The result in Table 3 shows that majority of the members of the public have experienced a moderate level (72.9%) of online fraud threat during the outbreak of the COVID-19 pandemic.

Table 3
Level of Online Fraud during MCO

Level	Frequency	Percentage (%)
Low	45	13.6
Moderate	230	69.2
High	57	17.2
TOTAL	**332**	**100**

Note: Low (<2.33), Moderate (2.34-3.67), High (3.68-5.00)

The result of this research is aligned with a report obtained from The Star (2020) disclosing that online fraud has become one of the highest numbers of scams in Malaysia during MCO. Most of the online fraud cases that happened in Malaysia during MCO involved cases related to e-commerce fraud (with RM18 million in losses), fake bank loans (with RM18 million in losses), love scams (with RM18 million in losses), and Macau scams (with RM50 million in losses) (The Star, 2020). According to the International Criminal Police Organization (Interpol) (2020), some of the fraud tactics used by the online cybercriminals to lure their potential victims during the outbreak of the COVID-19 pandemic includes; (i) impersonating hospital officials, (ii) sending a request for payment to help someone who is infected by Coronavirus,

(iii) impersonating national or global health care authorities, and (iv) calling or emailing public requesting for their personal information to conduct COVID-19 screening.

Most online fraudsters carried out a well-planned and sophisticated strategy to con their potential victims, particularly related to fraudulent lotteries, romance scams, games scams, and prize draws scams (Ketchell, 2019). Broadhurst et al (2020) note that an individual is highly at-risk to become a victim of online fraud if they easily fall for persuasion (e.g., based on logic or emotional response). Furthermore, dispositional factors such as age, gender, education level, income, and individual characteristic (e.g., low self-control, high level of impulsivity, perceived loneliness) also increase the risk of an individual becoming the victim of online fraud (Norris et al., 2019).

In the context of this study, the drastic shift from retail purchasing to online purchasing due to the stay-at-home order is also foreseen as a potential risk and contributing factor to the rise of online fraud attacks during MCO in Malaysia. For instance, there is a significant change in the e-commerce landscape in Malaysia following the growing number of users utilising the marketplace purchases and mobile payments (e.g., food delivery, alternative transportation, e-groceries) due to the stay-at-home order. Undeniably, the use of e-commerce apps has opened a pathway for the fraudsters to manipulate the end-users since the payment/transaction taking place between the consumer and the vendor is anonymous to a certain extent, therefore increasing the risk of online fraud victimization (Reynolds, 2020).

Level of Online Sexual Harassment

The result in Table 4 depicts that majority of the members of the public have experienced a moderate (87.7%) level of online sexual harassment during the outbreak of the COVID-19 pandemic.

Table 4
Level of Online Sexual Harassment during MCO

Level	Frequency	Percentage (%)
Low	18	5.4
Moderate	291	87.7
High	23	6.9
TOTAL	**332**	**100**

Note: Low (<2.33), Moderate (2.34-3.67), High (3.68-5.00)

In general, online sexual harassment may come in various forms including sending abusive messages, sharing personal information, spreading sexual images without consent, or spreading malicious rumors about an individual (Nadim & Fladmoe, 2021). According to Jatmiko et al (2020), social media platforms are fertile ground for online sexual harassment to take place, particularly targeting adolescent females. Since the internet is a place that facilitates anonymity, most cybercriminals are able to target their victims based on physical appearance, gender, race, or ethnicity (Nadim & Fladmoe, 2021). Into the bargain, a textual analysis shows that online sexual harassment towards women tends to focus on sexualised and hyperbolic threats (Nadim & Fladmoe, 2021). On the contrary, a Twitter analysis depicts that a substantial amount of misogynistic languages such as “slut” and “whore” (which refer

to women as sexual objectification) were used while harassing women on social media platforms (Nadim & Fladmoe, 2021).

Nadim et al (2021) stated that many cybercriminals use fake female or male usernames in the chat room to trap their victims. In addition, on a daily basis users with female names received 100 threatening messages and/or sexually explicit messages on average whereas men only received 3.5 messages per day (Nadim & Fladmoe, 2021). Besides, the Pew Research Center (2014) has disclosed that both women and men experience different types of online harassment. For instance, women are more likely to experience online sexual harassment whereas men are more prone to experience name-calling and/or physical threats. Additionally, Mitchell et al (2014) stated that regular internet users who are nearly universal among individuals between the age range of 18 and 35 years old have experienced online sexual harassment at least once in their life.

The anonymity of the internet and the de-individualisation in cyberspace can diminish self-regulation and lead someone to engage in disinhibited behaviour such as sharing intimate information with strangers whom they meet online (Soo et al., 2012). According to Mitchell et al (2007); Soo et al (2012), the chances of receiving unwanted sexual solicitation are fairly high if an individual practices risky online habits such as including too much personal information on social media platforms, frequently posting revealing pictures, adding strangers to friends list, or frequently engaging in chatting with strangers in social media platforms. In the context of this study, the proliferation of online sexual harassment during the stay-at-home order clearly shows that digital gender abuse is likely to worsen, particularly among females, as the internet has become an absolute necessity in human life.

Limitation of Study

Due to the enforcement of MCO and social distancing conditions in Malaysia, data was collected using an online survey form. Thus, there are two main limitations in this study including:

(i) Absence of researcher: The respondent might have a different understanding or interpretations related to certain questions since the researcher was not present to provide explanations while the respondent was answering the questionnaire.

(ii) Limited respondents availability: Due to poor internet connection, some populations are less likely to respond to the online survey form, especially those who stay in rural areas with low internet speed.

Conclusion

The findings obtained from this study clearly show that cybercriminals are diversifying their modus operandi to trap their potential victims at a time when the world's attention is diverted toward the coronavirus. The results stipulated that a large number of respondents have experienced a high level of online phishing/malware distribution, a moderate level of online fraud, and a moderate level of online sexual harassment. Hence, it is crucial to improvise and protect important data and assets from cybercriminal attacks by leveraging a comprehensive approach to the existing cybersecurity system. Collaboration between law enforcement agencies, mobile phone companies, social network sites, internet service providers, social researchers, and other key players in the technology industry should hold promise to address

this issue. Furthermore, proactive steps must be taken by every member of the public, especially by not opening any attachment received via email from unknown senders, not providing personal information over email or phone calls to any unknown person, avoid downloading or clicking any links from unidentified sources, and setting strong passwords to reduce the risk of cybercrime victimisation. While most prevention efforts recommend victims alter their "risky habit", it is equally important in finding a way to deter cybercriminals from committing these transgressions as well.

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

Conflict of Interest
There is no conflict of interest regarding the publication and authorship of this research.

References
Broadhurst, R., Ball, M., & Jiang, C. (2020). *Availability of COVID-19 related products on TOR darknet markets*. Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/sb24_availability_of_covid-19_related_products_on_tor_darknet_markets.pdf

Checkpoint Risk Intelligence. (2020). *Threat intelligence bulletin*. https://research.checkpoint.com/2020/27th-april-threat-intelligence-bulletin/

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1277. https://doi. org/10.4102/sajim.v23i1.1277

Cook, A. (2020). *COVID-19: Companies and verticals at risk for cyberattacks*. https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/

Daily Express. (2020). *Online 'sextortion' cases increase during MCO.* http://www.dailyexpress.com.my/news/151450/online-sextortion-cases-increase-during-mco/

EUROPOL. (2020). *Catching the virus; cybercrime, disinformation, and the COVID-19 pandemic.* https://www.europol.europa.eu/cms/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

Hansson, S., Orru, K., Torpan, S., Bäck, A., Kazemekaityte, A., Meyer, S. F., Ludvigsen, J., Savadori, L., Galvagni, A., & Pigrée, A. (2021). COVID-19 information disorder: Six types of harmful information during the pandemic in Europe. *Journal of Risk Research*, *24*(4), 380-393. 10.1080/13669877.2020.1871058

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid covid-19: the initial results from a natural experiment. *American Journal of Criminal Justice*, *45*, 546-562. https://doi.org/10.1007/s12103-020-09534-4

Jatmiko, M.I ., Syukron, M., & Mekarsari, Y. (2020). COVID-19, harassment and social media: A study of gender-based violence facilitated by technology during the pandemic. *The Journal of Society and Media*, *4*(2), 319-347. 10.26740/jsm.v4n2.p319-347

Jeyasingam, J. S. K. (2020). *COVID-19 laws: Examining the legal implications on the maxim generalia specialibus nonderogant.*

https://www.zicolaw.com/resources/alerts/covid-19-laws-examining-the-legal-implications-on-the-maxim-generalia-specialibus-non-derogant/

Ketchell, M. (2019). *Inside the Mind of the Online Scammer*. https://theconversation.com/inside-the-mind-of-the-online-scammer-127471

Kranenbarg, M. W., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behaviour*, *40*(1), 40-55. 10.1080/01639625.2017.1411030

Malaysiakini. (2020). *Internet can be a boon during MCO but beware of hackers.* https://www.malaysiakini.com/news/519528/

Maras, M. H. (2019). *Internet luring of female victims*. Encyclopaedia of Women & Crime. John Wiley & Sons Inc.

Marganski, A. J. (2019). *Cyberstalking*. Encyclopaedia of Women & Crime. John Wiley & Sons Inc.

Mitchell, K. J., Ybarra, M. L., & Korchmaros, J. D. (2014). Sexual harassment among adolescents of different sexual orientations and gender identities. *Child Abuse Neglect*, *38*, 280-295. 10.1016/j.chiabu.2013.09.008

Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, *39*(2), 245-258. https://doi.org/10.1177/0894439319865518

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information System*, *29*(3), 1-16. https://doi.org/10.1080/0960085X.2020.1771222

National Cyber Security Agency. (2020). *Advisory on cyber threat using COVID-19 outbreak as theme*. https://www.nacsa.gov.my/alert2.php

National Institute of Communicable Diseases. (2021). *Latest confirmed cases of COVID-19 in South Africa.* https://www.nicd.ac.za/37362-2/

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231-245. https://doi.org/10.1007/s11896-019-09334-5

Palmer, D. (2020). *DDoS attacks are getting more powerful as attackers change tactics*. https://www.zdnet.com/article/ddos-attacks-are-getting-more-powerful-as-attackers-change-tactics/

Payne, B., May, D. C., & Hadzhidimova, L. (2018). America's most wanted criminals: Comparing cybercriminals and traditional criminals. *Criminal Justice Studies*, *32*(1), 1-15. 10.1080/1478601X.2018.1532420

Pew Research Center. (2014). *Online harassment*. https://www.pewresearch.org/internet/2014/10/22/online-harassment/

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), 247. https://doi.org/10.1002/itl2.247

Quade, P. (2020). *A deep dive into the universe of cybersecurity.* https://www.weforum.org/agenda/2020/05/extract-the-digital-big-bang/

Reynolds, J. (2020). *9 reasons digital fraud is on the rise.* https://www.securitymagazine.com/articles/93912-reasons-digital-fraud-is-on-the-rise

Soo, K., Ainsaar, M., & Kalmus, V. (2012). Behind the curtains of e-state: Determinants of online sexual harassment among Estonian children. *Studies of Transition States and Societies*, *4*(2), 35-48. http://publications.tlu.ee/index.php/stss/article/view/95

TechWire Asia. (2020). *Cybersecurity is top concern, as online threats mount in Malaysia by 82.5%*. https://techwireasia.com/2020/04/cybersecurity-is-top-concern-as-online-threats-mount-in-malaysia-by-82-5/

Tharshini, N. K., Hassan, Z., & Mas'ud, H. F. (2020). Cybercrime experience during the Movement Control Order questionnaire. RST/SWK-001182-2020 (LY2020005571). Universiti Malaysia Sarawak.

Tharshini, N. K., Hassan, Z., & Haji Mas'ud, F. (2021). Cybercrime threat landscape amid the Movement Control Order in Malaysia. *International Journal of Business and Society*, *22*(3), 1589-1601. https://doi.org/10.33736/ijbs.4323.2021

The International Criminal Police Organization (Interpol). (2020). *Financial crime*. https://www.interpol.int/en/Crimes/Financial-crime

The New Straits Times. (2020). *Cybercrime in Penang shoots up 441.7 per cent since MCO*. https://www.nst.com.my/news/crime-courts/2020/05/594436/cybercrime-penang-shoots-4417-cent-mco

The Star. (2020). *Cybersecurity cases rise by 82.5%.* https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

The Star. (2020). *MCO sees uptick in e-commerce scams.* https://www.thestar.com.my/news/nation/2020/08/17/mco-sees-uptick-in-e-commerce-scams

The Star. (2020). *Zahidi: Cybercrime complaints spiked more than 90% during MCO*. https://www.thestar.com.my/tech/tech-news/2020/07/03/zahidi-cybercrime-complaints-spiked-more-than-90-during-mco

The Star. (2021). *Saifuddin: More cybercrime reported during pandemic*. https://www.thestar.com.my/tech/tech-news/2021/06/03/saifuddin-more-cybercrime-reported-during-pandemic