Scientific Research Publishing

Open Journal of Political Science, 2024, 14, 166-176
https://www.scirp.org/journal/ojps
ISSN Online: 2164-0513
ISSN Print: 2164-0505

The Efficacy of the Malaysian Government's Response towards Cybercrime

Ahmad Redzuan Mohamad[1], Mohd Rizal Yaakop[2], Mohd Azmi Mohd Razif[3]

[1]Centers of Learning, History, Politics and Strategy, Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[2]Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[3]Islamic Science Institute, Universiti Sains Islam Malaysia, Nilai, Malaysia
Email: redzumark@gmail.com

How to cite this paper: Mohamad, A. R., Yaakop, M. R. & Razif, M. A. M. (2024). The Efficacy of the Malaysian Government's Response towards Cybercrime. *Open Journal of Political Science, 14,* 166-176.
https://doi.org/10.4236/ojps.2024.141010

Received: July 21, 2022
Accepted: January 28, 2024
Published: January 31, 2024

Abstract

Cybercrime is an activity that is becoming more prevalent nowadays in various countries. Today, this crime is being taken seriously by all countries because it has had a negative impact on society. In Malaysia, the forms of cyber crime we face are hacking, money laundering, phishing and cyber fraud. Cybercrime can be defined as any form of criminal behavior that uses any type of electronic device through an internet connection and involves individual or group behavior. Therefore, this article will discuss how the Malaysian government reacts in dealing with the current issue of cybercrime as well as existing cyber laws in Malaysia. This is because cybercrimes usually occur during online money transactions, food orders through applications such as Foodpanda, e-hailing orders, online money transfers, and company registration and others. Even so, with the speed of internet use that is seen to have a positive impact on society, there is no denying that there are also negative effects that need to be addressed.

Keywords

Cybercrime, Government Reactions Towards Handling Cybercrime Issues

1. Introduction

Generally, the internet comes from the word internetworking. Internetworking can be translated as a communication system between networks. Through a network of computers located around the world, two-way communication and exchange of information can be achieved in a short time (Robert H'obbes' Zakon, 1999). A very significant increase in internet usage can be seen in 2020 due

to the covid-19 pandemic that hit the country with the first case in Malaysia was reported on 25th January 2020 involving China citizens who came to Malaysia on January 23rd, 2020 (Zakon, 2003).

To curb the spread of the epidemic from becoming more serious, the government implemented the first Movement Control Order (MCO) on March 18th, 2020, followed by the second phase MCO, Conditional Movement Control Order (CMCO), Rehabilitation Movement Control Order (RMCO) and followed by the four phases latest National Recovery Plan (NRP). The MCO that was implemented give various impacts on the country. With the closure of operations of various sectors such as the economy, government departments, and education the people's movement became restricted and had to always stay at home.

The effects of the Covid-19 pandemic did not only occur in terms of the country's economy but the social aspects and styles of the population underwent significant changes. With so many workers having to work from home (WFH), as well as the education sector also running the home teaching and learning process (PdPR) this has undoubtedly contributed to the statistical increase in ICT Use and Access by individuals and households.

According to the Department of Statistics, the highest internet activities usage by Malaysians is social media. However, by 2020 services related to e-learning, e-health, e-commerce, and entertainment have increased significantly.

Despite the rapid increase in internet usage which is seen to facilitate the lives of the people in Malaysia in this pandemic era, as will be presented below in **Figure 1**, The Royal Malaysian Police revealed that a total of 4327 cybercrimes were reported in the first quarter. Meanwhile, Berita Harian reported that work from home (WFH) activities and also the high use of social media during MCO compared to usual caused many users to be targeted by cybercriminals.

2. Definitions of Cybercrime

According to Dewan Bahasa Dictionary, crime means any wrongful act under the law. Cybercrime is defined as a form of criminal conduct using any type of electronic equipment through an internet connection committed either individually or in groups. This crime is also able to cross the border from one country to another in a short period (Rahim & Manap, 2004).

Cybersecurity Malaysia states that cybercrime can be categorized into three categories. The first is where information technology systems and intellectual property are targeted for exploitation or theft and intrusion. The second is where ICT equipment is used to commit crimes. For example, home computer equipment is used to run a malicious program to break into other computers and is used to steal money, identities, and even passwords. The third category is where ICT equipment is used as a medium to commit crimes. For example, incitement, criticism, inciting disharmony, bullying, and spying (CyberSecurity Malaysia, 2020).

Cybercrime has evolved tremendously. Before this, cybercrime was only li-

mited to the physical environment such as causing loss or damage to equipment, data, and information to software or computer processing equipment through virus attacks and intrusions (Abdullah, 2003). Now with the sophistication of technology, today cybercrime has involved any form of crime that occurs through cyberspace and involves computer devices (Manap & Jamal, 2003).

3. Types of Cybercrime in Malaysia

As reported by Cyber Security Malaysia, statistics show that a total of 8226 cases involving cybercrime occurred from January 2021 to September 2021. Among the most reported cases were fraud cases of 5899 cases, followed by intrusion of 1198 cases.

The following are some of the most common types of cybercrime in Malaysia.

3.1. Phishing

Phishing is a form of cyberattack where it creates a website that looks legitimate and convincing but tries to steal personal and sensitive data (Paraschiv et al., 2021). There are 2 types of these phishing websites, firstly for financial theft, and secondly, spoofing i.e. imitating legitimate websites for identity theft and spread of malware (Chen et al., 2020). In most cases, the victim will receive an email or message that seems convincing from the bank or service provider. Tricked victims will enter confidential information such as revealing passwords or personal information to criminals.

3.2. Hacking

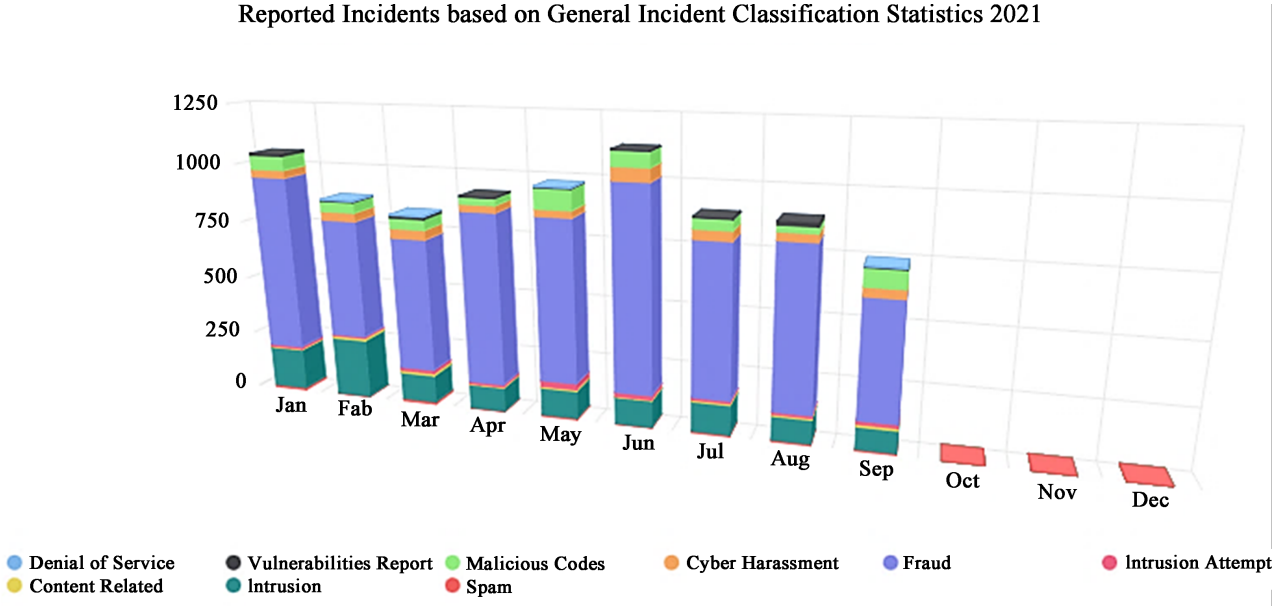
Hacking means any activity or access that occurs in a computer system without the permission or knowledge of the computer owner (Yar, 2006). A computer hacker is usually someone who knows computers and computer programming. Hackers will usually change the security system of a computer by trying to steal or copy the information contained in a computer, modify or damage the system of a computer. Aside from that, some hackers are just hacking for fun and to show off their skills.

3.3. Scammer (Love Scam and Macau Scam)

Love scam or love conspiracy is a form of cybercrime. It happens by targeting women especially professional women by having a love affair. This crime occurs when the perpetrator pretends to initiate a love affair with the victim and then will deceive the victim into giving a sum of money to them (Whitty & Buchanan, 2012).

According to the Royal Malaysian Police, the modus operandi of this syndicate is to try to get acquainted with the victim through email and social media to deceive the victim. Usually, victims who are lonely and do not have a life partner will be easily deceived (Ismail, 2023).

Meanwhile, according to PDRM, the Macau scam was masterminded by locals



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Denial of Service	1	2	3	1	3	0	1	2	3	0	0	0	16
Vulnerabilities Report	8	5	12	4	6	3	3	13	3	0	0	0	57
Malicious Codes	58	44	42	29	83	64	44	25	76	0	0	0	465
Cyber Harassment	35	37	40	29	30	55	41	34	35	0	0	0	336
Fraud	746	502	566	726	689	861	639	680	490	0	0	0	5899
Intrusion Attempt	11	10	16	12	24	18	8	12	12	0	0	0	124
Content Ralated	2	11	10	6	9	5	8	7	12	0	0	0	70
Intrusion	178	252	119	100	116	112	126	101	94	0	0	0	1198
Spam	10	4	11	5	8	4	7	6	6	0	0	0	61
	1049	867	819	912	968	1122	878	880	731	0	0	0	8226

Figure 1. Cybercrime reports categorically from January to September 2021.

and foreigners who would deceive the victims by contacting them by phone whether offering lucky draws, posing as government officials or banking staff, cheating on kidnappings, and trying to demand ransom (Awani, 2021; Aminnuraliff, 2022).

3.4. Identity Theft

Identity theft is an act that occurs when an individual uses another individual's sensitive and confidential information to commit a crime. The confidential information may contain the individual's name, date of birth, address, and financial information. The convenience of internet technology is now an opportunity

for criminals to obtain other people's confidential information easily. Victims are usually unaware that their identities are being used to commit unlawful crimes. Users should be careful when filling out and providing confidential information to any untrustworthy websites.

3.5. Harassment or Cyberbullying

Harassment or cyberbullying happens when a group of individuals tries to threaten, embarrass and commit defamatory or personal attacks on other individuals using electronic information and communication devices such as email, blogs, and mobile phones using the internet.

Types of cyberbullying that often occur are sending disturbing and threatening messages, abusing screen names or impersonating others, extending and disseminating inappropriate photos and comments to others (Farhana, 2016). Victims of cyberbullying can become depressed to the point of suicide. Cyberbullying is therefore categorized as a criminal act and can be prosecuted.

Based on the description that has been given, there are five types of cyber crime in Malaysia. That is phishing, hacking, Scams (Love Scam and Macau Scam), identity theft and harassment or cyber bullying. Crime and cybercrime have become a growing problem in our society, even with the existence of the national criminal justice system. All of these cybercrimes have been categorized according to specific cases and classifications based on national laws.

4. Malaysian Government Reaction in Addressing the Issue of Cybercrime in Malaysia.

Like other countries, Malaysia is also experiencing difficulties in tackling cybercrime cases. Cybercrime unlike other traditional crimes is very difficult to identify and track the perpetrators. This is because the crimes committed are online and are not explicitly related to any geographic location (Jahankhani et al., 2014).

Besides that, the main issue is that the criminal is hard to catch because of a lack of technology, laws, and cyber analysis. Apart from that, the main reason why criminals are difficult to catch is due to the lack of sophisticated technology, effective laws, and cyber analysts. Malaysian Vice-Chairman of Prevention, Tan Sri Lee Lam Thye suggested six steps that the government should take to tackle the problem of cybercrime so that it does not threaten national security.

First, the government needs to strengthen cyber security infrastructure facilities and regulate the communication and multimedia ecosystem in the country. Second, the government should strengthen the security of the country's cyberspace and increase the level of awareness of the people to use multimedia devices ethically. Third, by diversifying cyber security awareness programs as one of the awareness programs on internet use and the dangers of cybercrime threats to society. Next, appointing new cyber security professionals who are charismatic and competitive can upgrade the efficiency of existing cyber security guards. Finally, governments need to act swiftly and efficiently in ad-

dressing current and future cyber threats by taking a more comprehensive and holistic approach (Jahankhani et al., 2014; Harian, 2020).

Following are the actions that the government has taken to address security threats and cybercrime in Malaysia:

4.1. Awareness Campaigns and Advertisements

To tackle cybercrime, the first thing that should be done is to provide awareness to the community on how cybercrime can pose a threat to the lives of victims. Various campaigns through print and digital media need to be done more aggressively so that consumers are more aware and take an informed attitude related to cybercrime.

4.1.1. Cybercrime Prevention Awareness Campaign by the Ministry of Communications and Multimedia (MCMM)

In 2019, a cyber prevention awareness campaign was organized by MCMM. The objective of this campaign is to provide education and raise public awareness related to telecommunication crime.

The cyber prevention awareness campaign also targets retirees, the middle class, career women, high school students as well as higher education and college students. Apart from that, MCMM also cooperates with the media, the Royal Malaysian Police, various agencies and departments under MCMM such as the information department, MCMM broadcasting, and involves non-governmental organizations (NGOs) and the involvement of community leaders.

A total of 3 campaign terms have been used to make this campaign a success, namely CYBERCRIME, CALL FRAUD, AND LOVE SCAM, and use 2 hashtags for promotional purposes and to warn the community such as ***#ScamAlert*** and ***#JanganTerpedaya***.

Apart from that, to ensure that these campaigns and promotions are effective and successful in raising public awareness, a working committee on the promotion and publicity of cyber awareness and prevention campaigns has been established. This ensures that promotion and publicity are done more aggressively and more effectively.

A total of 11 interview slots in electronic media such as TV and radio were conducted. In addition to announcements, posters and pamphlets were also made. All this is necessary to ensure that the various announcements related to the cunning tactics used by cybercriminals can be understood and taken seriously by the community.

4.1.2. CyberSafe Program (Cyber Safety Awareness for Everyone)

The CyberSafe program is an initiative from cyber security Malaysia that aims to cultivate public knowledge related to cyber security and internet security awareness to create a positive internet usage culture among Malaysians.

The word CyberSafe is a short form of Cyber Security Awareness for Everyone whose mission is to provide various knowledge and information about cyber awareness to the community.

The word CyberSafe has been taken from the acronym Cyber Security Awareness for Everyone which has a mission to provide a wide range of knowledge, information, and resources related to cyber security to the community. This is to ensure that every layer of society has a positive and safe experience while surfing the internet.

Various information and internet safety tips can be found on their website https://www.cybersafe.my/en/ which is suitable for all walks of life such as children, teenagers, parents, and organizations. There is a variety of information, articles, cyber tips, and various posters available on the website to educate users to be wise related to cybercrimes that occur today.

4.1.3. The *#TakNakScam* Campaign Launched by the Ministry of Domestic Trade and Consumer Affairs (KPDNHEP)

The *#TakNakScam* campaign launched in June 2021 aimed to raise consumer awareness on online fraud and cybercrime which showed an increasing trend during the MCO. It also educates the public to identify, review and report fraudulent tactics used by scammers (Hariah Metro, 2021; Amri, 2022).

The campaign was also conducted in collaboration with various related agencies such as the Royal Malaysian Police (RMP), Cybersecurity Malaysia, the Malaysian Communications and Multimedia Commission (MCMC), and the Securities Commission Malaysia (SC).

The campaign calls on Malaysians to remember 3 simple steps which are "Identify, Check and Report" so that the public remains vigilant in identifying, confirming financial fraud.

The term **Identify** in this campaign means consumers should be careful and vigilant while considering whether someone is a scammer or not. If consumers feel like dealing with a scammer, they can avoid becoming a victim. Second, when consumers suspect an individual is suspicious, they need to **check** with the authorities through official channels. Finally, **report** any criminal activity that occurs to the authorities.

Throughout the campaign, educational videos, guides, and tips to identify, deal with, and report activities related to cybercrime were shared comprehensively in various channels online and offline as well as to each agency that cooperated to make this campaign a success. Even the CCID Fraud Action Center has been in operation since 15th February 2021.

4.2. Establishment of Cyber Security Related Organizations

The Malaysian government is very serious about curbing and preventing any crime related to cybercrime. Therefore, the government has established Cyber Security Malaysia under the agency of the Ministry of Science and Technology (MOSTI) (Jayabalan et al., 2014).

Cyber security Malaysia then established the Malaysia Emergency Response Team (MyCERT) in 1997 which serves as a reference center in Malaysia related to computer security cases. MyCert serves as an internet community ref-

erence for dealing with computer security incidents and cyber prevention methods.

MyCERT is also responsible for providing assistance and handling incidents related to cyber harassment and threats, collecting information data related to cyber threats obtained from victims of cyber fraud, receiving complaints and reports related to computer security, identifying types of incidents, and providing solutions related to reported cases.

4.3. Legal Provisions Relating to Cybercrime

Given the various threats related to cybercrime due to the rapid growth of information technology, Malaysia is no exception in enacting cyber acts and laws to protect and safeguard the country's sovereignty and harmony. Among the relevant acts created are:

4.3.1. Computer Crimes Act 1997 (Section 3, Computer Crimes Act)

The Computer Crimes Act 1997 was approved in Parliament in March 1997 and came into force on June 30th, 2000. Its main purpose is related to offenses and crime of misuse of computers to commit crimes. This act describes any unauthorized access or alteration of programs and data contained in a computer without permission can be found wrong and punishable.

Parts of this act deals with crimes that involve unauthorized or illegal access to computer data and its misuse. The Act also applies to certain crimes such as phishing and identity theft. However, the act does not provide any provision on cyber espionage (Bidin et al., 2015; Jayabalan et al., 2014).

4.3.2. Communication and Multimedia Act (1998)

The Act is designed to monitor all activities and content of communication and multimedia service providers in Malaysia and enable a smooth concentration in the communications and multimedia industry. Among the activities and services regulated under the act include traditional broadcasting, telecommunications, and online services. The Act also states that there is no provision for internet censorship.

4.3.3. Digital Signature Act 1997

The digital signature act was enacted on October 1st, 1998 which aims to regulate the use of digital signatures in Malaysia. This is to ensure security on legal issues related to electronic transactions and verification of the use of digital signatures through certificates issued by licensed Local Authorities. It also provides rules on intermediaries acting as certification authorities and digital signature recognition (Anderson & Closen, 1999).

4.3.4. Telemedicine Act 1997

The Telemedicine Act 1997 was enacted for the regulation and control of telemedicine practice and matters connected therewith. It was enacted to facilitate and enable the application of telemedicine to rural areas. Medical officers can

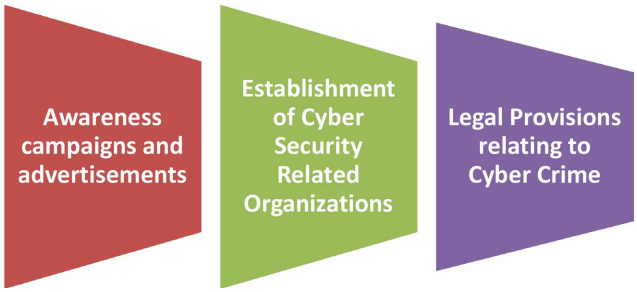


Figure 2. Research finding of the study obtained to addressing the issue of cybercrime in Malaysia.

now treat and deliver health-related information remotely through communication technology, such as shown in **Figure 2**. It allows medical practitioners to use existing information and communication technology to treat patients after the patient has given such consent.

Putrajaya Hospital is one of the first government hospitals to adopt an electronic approach. The integrated hospital information system allows patients' file referral cases to be done wherever patients receive and seek treatment.

The persons who can practice telemedicine are a fully registered medical practitioner who holds a valid practicing certificate or a medical practitioner registered or licensed outside Malaysia and holds a certificate to practice telemedicine issued by the Council and practice telemedicine from outside Malaysia through a fully registered medical practitioner who holds a valid practicing certificate to practice telemedicine.

Here are the research findings of the study obtained to addressing the issue of cybercrime in Malaysia.

5. Conclusion

Cybercrime is a new millennial crime that gives many new challenges especially to the workforce in cybercrime convictions. All parties should play their respective roles and work together to curb the spread of this cybercrime and cyber threat.

The best action should start from the individual himself by practicing good ethics while surfing the internet. Other than that, always be sensitive and aware of cyber security by being a wise consumer.

The public also needs to be educated and take a caring attitude regarding internet crime. Educational institutions from primary school to higher education should always expose and educate students about the ethics of internet use. This is because young people like this are very easily influenced by bad influences while using the internet and causing them to easily become victims. As the saying goes, "strike the iron while it's hot".

Apart from enacting relevant laws and acts, the government should also strengthen multilateral relations with other countries to address the threat of cybercrime and make consumers feel safe and protected while surfing the inter-

net from any cybercrime threat.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Aminnuraliff, M. (2022, May 22). *Jenayah Macau Scam di Selangor membimbangkan*. Sinar Harian. https://www.sinarharian.com.my/article/203494/berita/semasa/jenayah-macau-scam-di-selangor-membimbangkan

Amri, S. A. K. (2022, August 4). *Kempen #TakNakScam raih 2.3 juta capaian.* Harian Metro. https://www.hmetro.com.my/mutakhir/2022/08/868357/kempen-taknakscam-raih-23-juta-capaian

Rahim, A. A., & Manap, N. A. (2004). *Jenayah Berkaitan Dengan Komputer: Perspektif Undang-Undang Malaysia*. Dewan Bahasa dan Pustaka, 56.

Bidin, A. B., et al. (2015). Intipan Siber: Jenayah Baru dalam Masyarakat Kontemporari. *Jurnal Islam dan Masyarakat Kontemporari, 11,* 12-25.

Awani, A. (2021). *Macau Scam: All You Need to Know.* https://www.astroawani.com/berita-malaysia/macau-scam-all-you-need-know-263044

Harian, B. (2020). *Enam Langkah 'Lawan' Jenayah Siber.* https://www.bharian.com.my/berita/nasional/2020/05/692956/enam-langkah-lawan-jenayah-siber

Chen, W. L., Guo, X. F., et al. (2020). Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20),* Yokohama, 7 January 2021, 4506. https://www.ijcai.org/proceedings/2020/0621.pdf

CyberSecurity Malaysia (2020). *Cybersecurity Incidents and Trends in Malaysia.* Vol. 1. https://www.cybersecurity.my/data/content_files/46/2222.pdf

Farhana (2016, April 1). *Cyberbullying*. PORTAL MyHEALTH. http://www.myhealth.gov.my/en/cyberbullying-2/

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime Classification and Characteristics. In: B. Akhgar, A. Staniforth, & F. Bosco, Eds., *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149-164), Syngress. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Hariah Metro (2021). *Kempen #TakNakScam Tingkat Kesedaran Penipuan Jenayah Siber*. https://www.hmetro.com.my/mutakhir/2021/07/731239/kempen-taknakscam-tingkat-kesedaran-penipuan-jenayah-siber

Ismail, A. I. (2023, February 24). *Love Scam sasar mangsa kesunyian*. Sinar Harian. https://www.sinarharian.com.my/article/246957/berita/semasa/love-scam-sasar-mangsa-kesunyian

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

Anderson, J. C., & Closen, M. L. (1999). Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority, 17 J. Marshall J. Computer & Info. L. 833. *Journal of Computer & Informa-*

tion Law, 17, Article 5.

Yar, M. (2006). *Cybercrime and Society*. SAGE Publications.

Whitty, M. T. and Buchanan, T. (2012). The Online Romance Scam: A Serious Cybercrime. *Cyberpsychology, Behavior, and Social Networking, 15,* 181-183. https://doi.org/10.1089/cyber.2011.0352

Manap, N. A., Jamal, J. (2003). Jenayah Komputer: Perbandingan Menurut Akta Jenayah Komputer 1997 dan Prinsip Undang-Undang Jenayah Islam. *Jurnal Undang-undang dan Masyarakat, 7,* 16.

Robert H'obbes' Zakon. (1999). *Hobbes's Internet Timeline.* https://www.zakon.org/robert/internet/timeline/

Abdullah, R. H. (2003). *Teknologi Maklumat dan Penggunaannya.* Prentice Hall/Pearson Malaysia Sdn Bhd, 116.

Paraschiv, D., Toade, L., et al. (2021). Internet Fraud and Phishing Attacks—A European Perspective. *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption*, Foggia, 3-5 June 2021, 394-400. https://doi.org/10.24818/BASIQ/2021/07/051

Zakon, R. H. (2003). *Hobbes' Internet Timeline: The Definitive ARPAnet & Internet History*. https://www.zakon.org/robert/internet/timeline/