CYBERCRIMES IN MALAYSIA

Sitti Syamsiar Binti Muharram
Mohd. Zuhairizan Suhaimi
Markrandy Marcus

ABSTRACT

Cybercrimes are often defined as computer crimes or high-tech crimes. They are launched with the cause of harming different people's property, personal integrity, and life or stealing valuable items and information from other people. In Malaysia, different types of cybercrimes are hacking, cyber harassment, phishing, identity theft, credit card fraud, spam, cyber pornography, denial of service attacks, and virus dissemination. It was reported that around 13,000 cybercrime complaints were filed in 2019, costing about RM539 million in losses. In 2020, there were 17,000 cases reported. The number of cases grew to over 20,000 in 2021, with a total loss of RM560 million. There were 3,273 cases documented up to February 2022, amounting to RM114 million in losses. Following a sharp increase in reports of online crimes, cyber security remains one of Malaysia's top concerns. To prevent this from happening to us, we need to know how to recognize phishing, keep personal information safe, beware of public computers, use a credit card instead of a debit card, buy only from valid websites and avoid suspicious emails.

Keywords: Cybercrimes, Information Technology, Computer Safety

INTRODUCTION

Cybercrimes are often be defined as computer crimes or high-tech crimes. They are committed with the intention to harm other people's property, personal integrity, someone's life, and to steal valuable items and information from other people. Examples of cybercrimes include computer viruses, distribution of pornographic content, hacking or unauthorized access, unauthorized of computer data modification, extensive online defacing, identity theft or phishing, cyber-squatting, cyber stalking, and many others (Mohamed, 2012). It was reported that around 13,000 cybercrime complaints were filed in 2019, costing about RM539 million in losses. In 2020, there were 17,000 cases reported. The number of cases grew to over 20,000 in 2021, with a total loss of RM560 million. There were 3,273 cases documented up to February 2022, amounting to RM114 million in losses (Bernama, 2022)

Cybercrime not only causes tremendous destruction to the government and the public, but it also allows criminals to hide their identities prodigiously and technically skilled criminals engage in a series of illegal activities online. Cybercrime, in a larger meaning, is any illegal action involving the use of a computer or the internet as a tool or a target, or it can be both. (Rahman, 2019).

Most of the earliest offenders and victims of cybercrime were Americans since computers and the Internet began actively used in their country at an early stage. But by the twenty-first century, there was hardly a village on the world that had not been impacted in some manner by cybercrime (Dennis, 2019). This paper discusses the types and incidents of cybercrimes in Malaysia in the recent years, as well as how to avoid it.

TYPES OF CYBERCRIMES IN MALAYSIA

On a regular basis, a wide range of crimes are performed on the internet, some of which are intended at the computer and others against the computer users. Here are some specific examples of cybercrime:

i. Phishing

This technique involves pretending to be a legitimate company to get personal information including credit card information, login, and password combinations. The most popular phishing technique is email spoofing. In a counterfeit email, the email header is generated to create the impression as though the message were originated from one location while it was sent from another. Figure 1 below shows how the phishing process takes place:

Figure 1 Phishing Process (Goni, *et al.*, 2022)

ii. Spam

Spam e-mails have been a concern for quite some time. Spamming is the act of sending numerous copies of unsolicited mail or bulk emails to numerous recipients, such as chain letters. The greatest solution to these problems relies on categorization and filtering of spam email (Selamat, *et al.*, 2013).

iii. Hacking

Hacking is not the simple act or series of crimes that many people seem to think it is. Hacking is a set of skills. It is a comprehensive term that describes a range of actions. The illegal usage computer and system resources are known as hacking, while the act of modifying hardware and software components to accomplish their purpose other than which they were designed primarily is known as computer hacking. Therefore, those that conduct computer hacking are commonly known as the hackers (Kumar & Agarwal, 2018).

iv. Cyber Bullying or Harassment

According to New Straits Times (2017), Cyber-bullying or cyber-harassment are currently regarded as one of Malaysia's top five cyberthreats. Cyber harassment is referred to harassing or disturbing someone with malevolent purpose by utilizing technological tools such as social online chat and social networking. The goal is primarily to induce the victims to be disturbed or to be angry. Examples of cyber-harassment include cyber-bullying and stalking of potential victims. There are a variety of reasons why people engage in cyber harassment. They can be done for enjoyment or as an amusement to alleviate boredom, or for personal reasons such as revenge, jealousy, rage, righteousness, and bigotry, or just to attract someone's attention. It's possible that the culprit has no reason at all and was simply in the wrong location at the wrong time when the crime was committed (Kassim, *et al.*, 2018).

v. Identity Theft

An existent person's identity is used as a target or main tool in identity theft, which is a kind of fraud or illegal behaviour, without that person knowing or approval (Koopes & Leenes, 2006). These criminal acts associated to identity theft are indeed not brand-new offences; rather, they are existing offences that have been enhanced using or theft from stolen identities (Newman & McNally, 2005). Agbaje *et al*. (2015) identified different types of identity theft, with percentages for each type displayed in Figure 2:

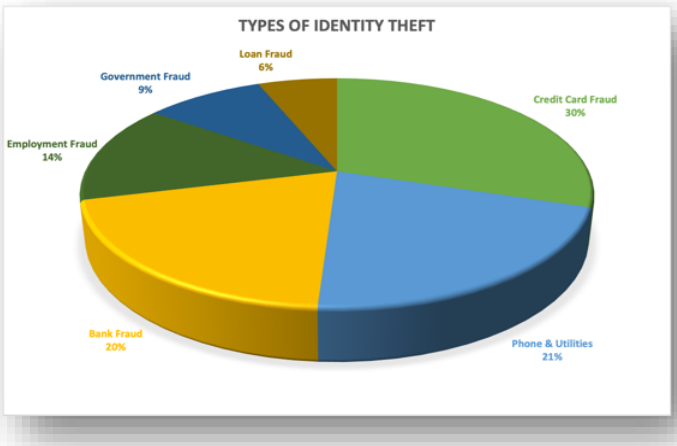

Figure 2 Types of Identity Theft (Agbaje *et al.*, 2015)

vi. Credit Card Fraud

Credit card fraud is the use of a denied, reported missing, or stolen credit card by an individual with criminal aim of gaining something of value. Using the credit card information without a real card is also another act of credit card fraud. Stealing of a person's identity to obtain a credit card is a highly risky type of credit card fraud since it frequently occurs in collaboration with identity theft. Fraudulent use of credit cards has an impact on the entire consumer credit sector. It is one of the fraud types that is growing the fastest and is also one of the hardest to discover and stop (Rose, 2019).

vii. Cyber Pornography

The act of using cyber space to make, show, distribute, import, or publish pornography or obscene materials, particularly those depicting children engaging in sexual actions with adults, is known as cyber pornography. It is a crime that is categorized as causing bodily injury. Concerns that cyber pornography contributes to include sexual abuse of children, violence against women, rape, injustice, relationship and family dysfunction, juvenile crime, prostitution, and STDs (Verma, 2012).

viii. Virus Dissemination

The spread of viruses is the process by which harmful software affixes itself to other programs and destroys the victim's system. They disrupt computers and alter or remove data, which influences the data storage. Worms and viruses are both classes of harmful software, hence they are nearly equivalent. When a virus infects one application, it automatically spreads to the others. Viruses and worms both work without the user's knowledge (Khan, 2012). Figure 3 below shows the types of viruses that exist in cybercrime world:

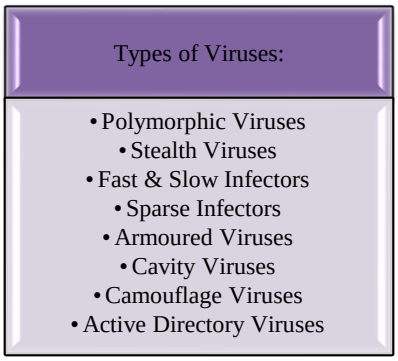

Figure 3 Types of Viruses (Khan, 2012)

ix. Denial of Service (DoS) Attack

One of the most powerful attacks a hacker can carry out is a denial-of-service attack. It has been a continuous threat to websites. It is a type of attack on a networking structure that prevents a server from serving clients. Millions of requests will be sent to make the server slow, flooding with massive packets of erroneous information and sending requests with an invalid or faked IP address. Denial-of-service attacks can be divided into different types according on how they are approached. They are Data Level, Network Level, Application Level, and Operating System Level (Elleithy *et al.*, 2006).

CYBERCRIMES IN MALAYSIA

The Malaysian Communications and Multimedia Commission (MCMC) through the Network Security Centre (NSC) handled a total of 2,520 network security incidents throughout 2020. The category with the highest number of incidents handled was Website Defacement with 1,467 incidents, followed by Phishing with 576 incidents. The breakdown of the incidents is as shown in Figure 4:

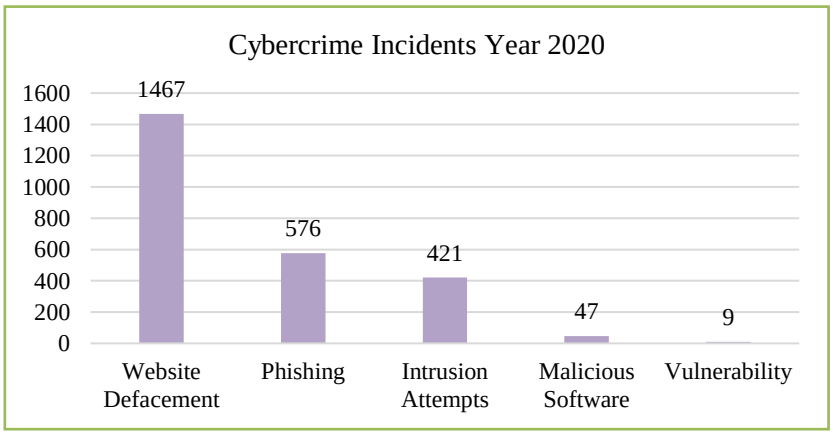

Figure 4 Cybercrime Incidents Year 2020

Source: MCMC Annual Report 2020

The Bernama news portal also reported that, around 13,000 cybercrime complaints were registered in 2019, costing RM539 million losses. In 2020, there were 17,000 cases reported. The number of cases grew to over 20,000 last year, with a total loss of RM560 million. There were 3,273 cases documented up to February of this year, amounting RM114 million in losses.

WAYS TO AVOID CYBERCRIMES

Cybercriminals can be repelled by precautionary measures including passwords, firewalls, encryption, and other security policies and practices. Cybercrime detection is a necessary last defense for protection, or at the very least to help in loss minimization as preventive methods are not always successful (Smith *et al*., 2016). Table 1 shows the various ways to avoid cybercrime from occur:

Table 1: Ways to Avoid Cybercrimes

No		
1	***Know How to Recognize Phishing***	Most often, any bank will never send an email to inform their client whether their account has been hacked and therefore demanding for sensitive information such as the TAC number or password. Everyone must never share their password to anyone because these are clearly phishing scams.
2	***Keep Personal Information Safe***	Do not include the year of your birth in the full date of your birth on Facebook. Consider the security queries your bank and other secure locations might ask you, such as "name of favorite pet" and "first school you attended."
3	***Beware of Public Computers***	Don't use public computers to access your accounts or personal information since they may have software that collects keystrokes and captures your passwords and account numbers.
4	***Use Credit Card instead of Debit Cards***	With a credit card, you have much greater liability protection than a debit card in the event of fraud when making online purchases.
5	***Purchase only from Reputable Websites***	Remember to look for "https" in the Web URL because it is quite easy to set up a fake online store or a store that appears to sell goods, but their intention is just to collect credit card information.
6	***Check Bank Accounts & Reports Regularly***	Some experts suggest keeping a daily eye on your credit card and bank account activity. This is to ensure that there is no unusual or suspicious transaction using your credit card and in your bank account activity.
7	***Avoid Suspicious Emails***	Do not click on links in strange emails, even if they appear to be from friends. Infections from viruses and malware communicated over email are the most frequent cyber risk of identity theft. Remember on how many emails claimed to be from friends whose email accounts have been hacked you have received in the past 12 months.

CONCLUSION

Cybersecurity continues to be one of Malaysia's top concerns following a dramatic rise in reports of online crimes. The Covid-19 pandemic has boosted the usage of digital technology in Malaysia, which has led to an increase in criminality and heightened security concerns. Everyone is at risk, even though not everyone is a victim of cybercrime. Computers are used to commit numerous types of crimes, including those that don't always occur in front of a computer. Therefore, this paper hopes to give insights and significant contributions to the respective users, be it to individual or companies on how to protect themselves from becoming the victim of cybercrime.

References

Agbaje, M. O, Awodele O., & Ogbonna, A. C. (2015). Applications of digital watermarking to cyber security (Cyber watermarking). *Proceedings of Informing Science & IT Education Conference (InSITE) 2015*, (pp. 1 – 11).

Dennis, M. A. (2019). Cybercrime. *Encyclopedia Britannica*. Retrieved May 26, 2022, from https://www.britannica.com/topic/cybercrime

Elleithy, K. M., Blagovic, D., Cheng, W. & Sideleau, P. (2006). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Journal of Systemics, Cybernetics and Informatics*, **3:** 66 – 71.

Goni, O., Ali, M. H., Showrov., Alam, M. M. & Shameem, M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, **1 (2)**: 29 – 39.

Hassan, K. H., Abdelhameed, A., & Ismail, N. (2018). Modern Means of Collecting Evidence in Criminal Investigations: Implications on the Privacy of Accused Persons in Malaysia. *International Journal of Asian Social Science*, **8 (7)**: 332 – 345.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 149–164.

Kassim, S. R. M., Zakaria, W. Z. A., Maksom, F. & Abdullah, K. (2018). Cyber Harassment Trends Analysis: a Malaysia Case Study. *International Journal of Engineering & Technology*: ***7*(4.15)**: 109 – 112.
Khan, I. (2012). An introduction to computer viruses: problems and solutions. *Library Hi Tech News*, ***29* (7)**: 8 – 12.
Koops, B. J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. *Datenschutz Und Datensicherheit - DuD*, **30 (9)**, 553 – 556.
Kumar, S. & Agarwal, D. (2018). Hacking Attacks, Methods, Techniques and Their Protection Measures. *International Journal of Advance Research in Computer Science and Management*, **4 (4)**: 2353 – 2358.
Malaysian Communications and Multimedia Commission (MCMC). (2020). *Annual Report 2020*. https://www.mcmc.gov.my/skmmgovmy/media/General/MCMC-Annual-Report-2020_HiRes_Pages.pdf
Mohamed, D. (2012). Investigating Cybercrimes Under the Malaysian Cyberlaws and the Criminal Procedure Code: Issues and Challenges. *Malaysian Law Journal*, **6**: 1 – 10.
Rahman, R. (2019). *Cybercrime Cases In A Decade: The Malaysian Experience*. Independently published.
Rashid, H. F. (2017, May 6). Cyberbullying Among Top Five Online Threats. *New Straits Times*.
Rashid, I. M. A., Yusoff, W. S., Ibrahim, S., Ramlan, S. N. & Samah, I. H. A. (2020). Investigating Cybercrimes in Malaysia: The Importance Of E-Commerce Security To Eliminate Fraud And Security. *European Journal of Molecular & Clinical Medicine*, **7 (8**): 1342 – 1346.
Ross, D. E. (2019, January 8). *Credit Card Fraud*. *Encyclopedia Britannica*.
Selamat, A., Nguyen, N. T., & Haron, H. (2013). *Intelligent Information and Database Systems* (Vol. 7802). Springer Publishing.
Verma, A. (2012). Cyber pornography in India and its implication on cybercafé operators. *Computer Law & Security Review*, **28 (1)**: 69 – 76.

Sitti Syamsiar Binti Muharram
Faculty of Accountancy
Universiti Teknologi MARA Cawangan Sabah
Kampus Kota Kinabalu
Email: sitti219@uitm.edu.my

Mohd. Zuhairizan Suhaimi
Faculty of Accountancy
Universiti Teknologi MARA Cawangan Sabah
Kampus Kota Kinabalu
Email: mzus91@gmail.com

Markrandy Marcus
Faculty of Accountancy
Universiti Teknologi MARA Cawangan Sabah
Kampus Kota Kinabalu
Email: markrandymarcus@gmail.com