TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS (TMT) SERIES - MALAYSIA

*This article is the fifth in a series exploring the Malaysian legal position with respect to various commonly asked questions in relation to the Technology, Media, and Telecommunications ("**TMT**") legal regime in Malaysia.*

In Part E of our TMT Series, we will be answering various queries pertaining to the legal regime in Malaysia insofar as it relates towards Hacking / Distributed Denial-of-Service (DDoS) attacks.

PART E: HACKING / DDoS ATTACKS

What key laws exist in terms of the criminality of hacking/DDoS attacks?

The use of technology has become widespread and crucial in various industries, including business, healthcare, and finance. With the increase in the use of technology, the risk of cybercrimes has also risen, and Malaysia is no exception to the same. Cybercrimes such as hacking and Distributed Denial of Service ("**DDoS**") attacks pose a significant threat to individuals, businesses, and governments, and it is crucial to understand the laws surrounding them. This article will discuss the key laws that exist in Malaysia in relation to these criminal activities.

Hacking is defined as the unauthorized intrusion into or control over computer network security systems for some illicit purpose. Under Section 3(1) of the Computer Crimes Act 1997 ("**CCA**"), a person shall be guilty of an offence if:

(a) they cause a computer to perform any function with the intent to secure access to any program or data held in any computer;

(b) the access they intend to secure is unauthorized; and

(c) they know that they are causing the computer to perform such a function.

The penalty for a person found guilty under Section 3 of the CCA is a fine not exceeding RM50,000 and/or imprisonment not exceeding 5 years.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584

If hacking is committed with the intention to commit an offence involving fraud or dishonesty or causes injury, as defined in the Malaysian Penal Code ("**PC**"), or to facilitate such an offence, the offender shall be guilty of an offence under Section 4 of the CCA. The penalty for an offence under Section 4 of the CCA is a fine not exceeding RM150,000 and/or imprisonment for a term not exceeding 10 years.

Persons who commit hacking offences may also be penalized under the PC and other applicable legislation for other ancillary offences, including taking movable property without consent, dishonest misappropriation of property, and identity theft.

For example, under the Copyright Act 1987 ("**CA**"), hacking is criminalized, specifically in respect of the circumvention of any technological protection measure applied to a copy of a copyrighted work that is used by the owner of the copyright in connection with the exercise of the owner's rights under the CA; and that restricts acts in respect of the owner's works which are not authorized by the owner concerned or permitted by law. Section 41(1)(h) of the CA provides that a person who circumvents or authorizes the circumvention of any of the aforementioned technological measures during the subsistence of copyright in a work or performer's right (subject to limited exceptions stipulated in the CA) shall be guilty of an offence, and attracts a penalty in the form of a fine of not exceeding RM250,000 and/or imprisonment for a term not exceeding 5 years and for any subsequent offence, to a fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years.

Persons who commit hacking offences may also be penalized under the PC and other applicable legislation for other ancillary offences, including taking movable property without consent, dishonest misappropriation of property, and identity theft.

DDoS attacks, on the other hand, involve the use of multiple systems to flood a targeted website or server with requests, making it unavailable to legitimate users. While there is no specific legislation for DDoS attacks in Malaysia, Section 233(1)(b) of the Communications and Multimedia Act 1998 ("**CMA**") provides that a person who initiates a communication using any application service, whether continuously, repeatedly, or otherwise, during which communication may or may not ensue, with or without disclosing their identity and with the intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence. A person found guilty of this offence may be liable to a fine not exceeding RM50,000 and/or imprisonment for a term not exceeding one year, and may also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584

Furthermore, under Section 431A of the PC, a person who commits mischief by cutting or injuring any electric telegraph cable, wire, line, post, instrument, or apparatus for signalling shall be punished with imprisonment for a term which may extend to 2 years and/or with a fine.

In conclusion, hacking and DDoS attacks are serious cybercrimes that can have significant consequences for individuals and organizations. Malaysia has enacted various laws to address these offences, and offenders can face fines and imprisonment if found guilty. It is crucial for individuals and businesses to be aware of these laws and take the necessary steps to protect themselves from cybercrime.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584