ACCOUNTING BULLETIN

Faculty of Accountancy

UiTM Kedah

2019

Vol. 2

KOD JALUR / BARCODE

eISSN 2637-0646

Cybercrime

Wan Nailah Abdullah & Roshima Said
Faculty of Accountancy, UiTM Kedah

Corresponding author: w.nailah@kedah.uitm.edu.my

Cybercrime has been an issue which impacts the lives of many people around the world. Cybercrime is a crime which, a) is directed at computers or other devices (for instance, computer hacking), and b) where computers or other devices are integral to the offence (for instance, identity theft, online fraud, and the distribution of child exploitation material) (Australian Cyber Security Centre, 2016). Some of the most typical types of cybercrime include online scams and fraud, hacking, identity theft, attacks on computer systems, as well as prohibited and illegal online content. Cybercrime is illegal because its effects can be extremely upsetting for victims, and may go way beyond merely being due to financial reasons. The crime may cause its victims to find themselves being powerless as the result of their privacy being violated. As the modern economic reliance on technology grows, the cost and incidence of cybercrime is expected to increase in many parts of the world.

In lack of a single universal definition, law enforcement has generally made a distinction between two main types of cybercrime. First, the advanced cybercrime, which consists of sophisticated attacks against computer hardware and software; and second, the cyber-enabled crimes, in which many traditional crimes such as financial crimes, crime against children, and even street crimes, which have taken a new turn with the advent of the Internet. The recent decades have seen new trends in cybercrime emerging all the time, resulting in an estimated cost of billions of ringgit to the global economy. Unlike in the past, where cybercrime was committed mainly by individuals or small groups, nowadays, the economies are facing highly complex cybercriminal networks which gather individuals from across the world in real time to commit crimes on an unprecedented scale (Interpol, 2016). Such a situation invites criminal organisations to increasingly turn to the Internet to accommodate their malfeasant activities and thus, maximise their illegal profit in the shortest time. The crimes themselves are not necessarily new. They could be fraud, illegal gambling, theft, or sale of fake medicines, yet they are evolving together with the increasing opportunities facilitated online and for such reasons, are becoming more widespread and damaging.

Here are three simple tips on how to prevent being a cybercrime victim (Stop Think Connect, 2019):

1) Maintain a clean machine by always updating the software and operating system on computers and mobile devices;

2) When in doubt about an attachment or a link, stop and think before acting. Links in email, instant message, and online posts are common ways for cybercriminals to attack computers.

3) Use stronger authentication especially for accounts with sensitive information like emails or bank accounts.

References

Australian cyber security center (ACSC) (2016). 2016 Threat report. News released. Retrieved December 14, 2016 from https://www.acsc.gov.au/news.html.

International criminal police investigation (Interpol) (2016). Cybercrime. Retrieved June 26, 2016 from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

Stop think connect (2019). How to recognize & prevent cybercrime. Retrieved October 15, 2019 from https://www.dhs.gov/sites/default/files/publications/Week3TipCard-%20508%20compliant_0.pdf