CYBERCRIME THREAT LANDSCAPE AMID THE MOVEMENT CONTROL ORDER IN MALAYSIA

N.K. Tharshini ♣
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

Zamri Hassan
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

Faizah Haji Mas'ud
Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak

ABSTRACT

The COVID-19 pandemic has evolved rapidly and affected almost all the world's countries, creating unprecedented chaos on human lives, physical health, mental wellbeing, and the world economy. During this time, digital space has become an indispensable global means of communication, entertainment, and social interaction. However, high reliance on digital tools increases the risk of being prey to cyberattacks. In order to explore the cybercrime threat landscape, empirical research was conducted to examine the shared experiences related to cybercrime threats during the enforcement of the Movement Control Order in Malaysia. Data was collected using an online survey among 332 respondents across Malaysia. The finding stipulated that most of the respondents comprised females aged between 18 and 28 years old. The result also indicated that majority of female became victims of online phishing/malware distribution [(M = 0.58, SD = 0.13); t (113) = 2.24, p = 0.02] and online sexual harassment [(M = 0.56, SD = 0.11); t (107) = 2.38, p = 0.01]. The understanding of cybercrime experiences faced by the public during MCO is essential to help law enforcement agencies to stay vigilant on issues related to public safety and security during unprecedented conditions.

Keywords: Cybercrime; COVID-19; Malaysia; Movement Control Order; Pandemic

Received: 31 July 2020
Accepted: 27 September 2021
https://doi.org/10.33736/ijbs.4323.2021

1. INTRODUCTION

Cybercrime is a global phenomenon perpetrated using technological devices. Intensive blooming in digitalisation has led cybercrime to become one of the fastest-growing threats in the world. The agenda of the cybercriminals primarily focuses on obtaining information related to intellectual property, business and commercial strategy, customer information (e.g. contact details, banking information, payment card details), and sensitive financial information (Norton Cybercrime Report, 2010). In 2019, the Internet Organised Crime Threat Assessment (IOCTA) published by the European Union Agency for Law Enforcement Cooperation (EUROPOL) revealed that the cybercrime landscape encompasses six significant domains. These domains are online child sexual

♣ Corresponding Author: Faculty of Social Sciences and Humanities, Universiti Malaysia Sarawak (UNIMAS), 94300, Kota Samarahan, Sarawak, Malaysia; Email: stharshini@unimas.my