MALAYSIAN INSTITUTE
OF ACCOUNTANTS

8 APRIL 2020

To All Members

WARNING ON CYBER THREATS AND CYBERATTACKS USING THE COVID-19 TROJAN HORSE

Following the COVID-19 outbreak, the National Cyber Security Agency (NACSA) – Malaysia's lead agency for cyber security matters - has observed a rise in several scams and malware activities employing the COVID-19 theme to lure victims to give out personal information and install malicious apps.

These latest cyberattack campaigns include Business Email Compromise, Malware, Ransomware and phone scams, believed to be organised by Advanced Persistent Threat (APT) actors and organised crime groups leveraging on the COVID-19 crisis. The impacts of such cyberattacks include, but are not limited to, loss of information, service disruption, information exposure and financial loss.

According to NACSA, multinational cyber security and defence company Trend Micro has reported that several malicious domains containing the word "corona" as part of the domain name have been identified. Furthermore, NACSA notes that the National Cyber Coordination and Command Centre (NC4) has also identified several malicious email subjects, attachments and malicious URLs that use the word "COVID-19" and "coronavirus" in their phishing lures.

Stay Safe, Practice Good Cyber Hygiene

To counter these rising cyberthreats, NC4, NACSA, and National Security Council (NSC) would like to remind everyone to be vigilant and to observe good cyber hygiene practices while working from home during the period of the Movement Control Order (MCO) from 18 March to 15 April 2020. A full list of malicious domains, email subjects and hashes, as well as the list of NASCA's recommendations are available here.

The Institute advices all members to observe these recommendations as cybersecurity is imperative to ensuring digital safety and national security. In addition, the Institute also cautions members to be vigilant when using virtual meeting applications which does not have strong privacy and security protection.

The Institute will continue to closely monitor and maintain close communication with the national cybersecurity agencies as well as the Government, regulators and our stakeholders, and will notify members of any future developments.

#STAYHOME #STAYSAFE #ACCOUNTABILITY #INTEGRITY

Thank you.

Dr Nurmazilah Dato' Mahzan
Chief Executive Officer