April 1, 2021 @ 5:17pm
LETTER: The Federation of Malaysian Consumers Associations (Fomca) and the National Consumer Complaints Centre (NCCC) would like to alert Malaysian consumers on sudden spike of scams related complaints and be cautious and remain alert to scams. Scammers are becoming increasingly more sophisticated with their tactics and are hoping that you let your guard down. We urge consumers not to provide their personal, banking or any details to strangers who have approached them though phone calls. Fomca been receiving approximately 450 complaints and enquiries related to scam since January 2021. Based on our observation, these scammers take advantage of the vulnerable consumers and surprisingly some of the victims are highly educated. It is becoming more difficult to know and differentiate between a scam and a legitimate business. Fomca also would like to urge all relevant authorities to be more active and play their role in curbing these unscrupulous activities. Many consumers are still not aware about scamming activities. The Communications and Multimedia Ministry and the Malaysian Communications and Multimedia Commission (MCMC) should play an important role to educate consumers by using their channels to reach out to the public at large. The Domestic Trade and Consumer Affairs Ministry also need to publish and update frequently all scam related cases in their website so that consumers would be able to get information relating to scams. Enforcement agencies also must charge these culprits and increase fines and jail terms for these offences. Scammers are constantly trying to steal consumers' personal data using fake emails, websites, phone calls, and even text messages. They use a variety of ways to try to trick people into providing personal information, bank account numbers, and other valuable information such as credit card numbers. In many cases, their goal is to steal money from you. Below are some terms used for different online scams and how they work, so consumers can protect themselves and evade from falling into the trap. 1. How do scammer contact their victims? Phishing is a term for scams commonly used when a criminal uses email to ask you to provide personal financial information. The sender pretends to be from a bank, a retail store, other service provider or government agency and makes the email appear legitimate. Criminals often try

to threaten, even frighten people by stating "you're a victim of fraud" or some other crime related offence message to trick you into providing information without thinking. They also may sound that you need to intervene quickly as to avoid from being charged in court of slapped with big fines. Do not ever succumb to it. Smishing is similar to phishing, but instead of using email, the criminal uses text messaging to reach you. Same idea, they pretend they are from an organisation you might know and trust such as a commercial bank or the Inland Revenue Department (LHDN) and try to get your personal information. Do not fall victim to it. Vishing, similar to phishing and smishing, is when scammers use phone services such as a live phone call, a "voice activated machine," or a voicemail to try to trick you into providing personal information by sounding like a legitimate business or government official. 2. What are the different types of scams? A. Government impostor scams are when fraudsters pretend to be an employee of the LHDN or other government agency, sometimes even using the names of real people. Remember, LHDN does not send unsolicited correspondence asking for money or sensitive personal information, and they never threaten you. Also, no government agency will ever demand that you pay by online transfer or immediately. LHDN would never contact you asking for personal details, such as bank account information, credit and debit card numbers, social security numbers, or passwords. B. Fake person scams happen when a fraudster hacks into someone's email account and sends out fake emails to friends and relatives, perhaps claiming that the real account owner is stranded abroad and might need your credit card information to return home. If you receive such an email, make sure you contact the sender through other means before sending any money or personal information. C. Love scammers normally take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get the victims to provide money, gifts or personal details. A love scam is not easy to detect as the perpetrators do not rush in to and they can woe their na&#65533;e victim by promising them many things. With most people chatting online and finding their partners through online dating sites, it is difficult to distinguish a genuine person from a scammer. D. Secret or mystery shopper employment scams involves fake advertisements for job opportunities that claim to be "hiring" people to work from home. As the potential new "employee," you might receive an official cheque as a starting bonus, and are asked to cover the cost of "account activation." The scammer hopes to receive these funds before the official cheque clears and you realise you have been scammed. If a job promises high salary for little work, be wary. That is a common sign of a job scam. Some other key signs of a fraudulent job advertisement include request for money remittance prior to any

job interview or confirmation of job offer before any face-to-face job interview. 3. How can I avoid scams? Be suspicious if someone contacts you unexpectedly online and asks for your personal information. It does not matter how legitimate the email or website may look. Only open emails, respond to text messages, voice mails, or callers that are from people or organisations you know, and even then, be cautious if they look questionable. If you think an email, text message, or pop-up box might be legitimate, you should still verify it before providing personal information. If you want to check something out, independently contact the supposed source probably a bank or organisation by using an email address or telephone number that you know is valid, such as from their website or a bank statement. Be especially wary of emails or websites that have typos or other obvious mistakes. Before making online payments to the sellers, please check the bank account number or phone number of the seller through the "Semak Mule" application created by the police to identify if the account holder is a scammer. Consumers can log on to the website at https://ccid.rmp.gov.my/semakmule/ To avoid falling prey to scammer in the future, it is better for us as consumers to equip ourselves with all the knowledge to avoid these scams. BASKARAN SITHAMPARAM Senior Manager NCCC / Fomca &#65533; Source: https://www.nst.com.my/opinion/letters/2021/04/678783/consumer-alert-%E2%80%93-scam-cases-are-rising