15 APR 2021
FEDERATION of Malaysian Consumers Associations (Fomca) and the National Consumer Complaints Centre (NCCC) would like to alert Malaysian consumers on the sudden spike of scam-related complaints. Scammers are becoming more sophisticated with their tactics and are hoping consumers would let their guard down. Consumers are urged not to provide their personal, banking or any details to strangers. Fomca has been receiving around 450 complaints and enquiries related to scams since January. Based on Fomca&#65533;s observation, the scammers take advantage of 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 would also like to urge the relevant authorities to be proactive and play their role in curbing unscrupulous activities. Many consumers are still not aware of scamming activities. The Communications and Multimedia Ministry and Malaysian Communications Multimedia Commission should play an important role to educate consumers through their channels. The Domestic Trade and Consumer Affairs Ministry also needs to frequently publish and update all scam-related cases on their website so consumers will be well informed. Enforcement agencies must also charge these culprits, and increase fines and jail terms for these offences. Scammers are constantly trying to steal consumers&#65533; personal data using fake emails, websites, phone calls and even text messages by using various ways to trick people into providing personal information like bank account numbers and other valuable information, such as credit card numbers. Here are some terms used for different online scams and how they work, so consumers can protect themselves and avoid falling into
the trap. How do scammers contact their victims? Phishing is a term for scams commonly used when a criminal uses emails to ask for personal financial information. The sender pretends to be from a bank, a retail store, other service providers or government agency, and makes the email appear legitimate. Criminals often threaten and even frighten people by stating &#65533;you&#65533;re a victim of fraud&#65533; or some other

crime-related offence to trick them into providing the information. They may also infer that the victims need to act quickly to avoid being charged in court or slapped with big fines. Smishing is similar to phishing but instead of using emails, the scammer uses text messages. They pretend they are from an organisation the victims may know and trust, such as a commercial bank or the Inland Revenue Board (IRB), to get personal information. 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 trick victims into providing personal information by sounding like a legitimate business or government official. Different types of scams Government impostor scams are when fraudsters pretend to be an employee of the IRB or other government agency, sometimes using the names of real people. The IRB does not send unsolicited correspondence asking for money or personal information, and they never use threats. Also, no government agency will demand payment by online transfer or immediately. The IRB will not contact persons asking for personal details, such as bank account information, credit and debit card numbers, social security numbers or passwords. Fake person scams happen when a fraudster hacks into a person&#65533;s email account and sends out fake emails to friends and relatives, claiming that the real account owner is stranded abroad and may need the victim&#65533;s credit card information for the related person to return home. In such a case, contact the sender through other means before sending any money or personal information. 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 take their time to woo the victims, promising them many things. With most people chatting online and finding partners through online dating sites, it is difficult to distinguish a genuine person from a scammer. Secret or mystery shopper employment scams involve fake advertisements for job opportunities that claim to be &#65533;hiring&#65533; people to work
from home. As a potential new &#65533;employee&#65533;, the victim may receive an official cheque as a starting bonus and be asked to cover the cost of &#65533;account activation&#65533;. The scammer hopes to receive these funds before the official cheque clears and

the victim realises too late that he has been scammed. Be wary if a job promises high salary for little work. This is a common sign of a job scam. Some other key signs of fraudulent job advertisements include request for money remittance prior to a job interview or confirmation of job offer before a face-to-face interview. How to avoid scams Be suspicious if a person contacts you unexpectedly online and asks for your personal information. It does not matter how legitimate the email or website looks. Open only emails, respond to text messages, voice mails or callers that are from people or organisations you know. If you think an email, text message or pop-up box may be legitimate, verify it before providing your personal information. Contact the supposed source, probably a bank or organisation, via email or valid telephone number, such as from their website or bank statement. Be wary of emails or websites that have typos or other obvious mistakes. Check bank account numbers or phone numbers of sellers through the &#65533;Semak Mule&#65533; application (https://ccid.rmp.gov.my/semakmule/) created by police to identify if the account holders are scammers before making online payments. Equip yourselves with all the knowledge to avoid falling prey to scammers. Baskaran Sithamparam and Nur Asyikin Aminuddin are senior managers of Fomca and NCCC, respectively. Comment: letters@thesundaily.com &#65533; Source: https://www.thesundaily.my/opinion/scammers-using-more-sophisticated-tactics-FY7742878