PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: 'Beware of lurking scammers'
Publication/Portal: The Borneo Post (Sabah)
Date: 9 August 2022

Language: English
Section: Home
Page: 3

'Beware of lurking scammers'

Jeremy Veno

YOUR phone rings and on the screen, it shows an 'unknown number', which you quickly answer – assuming that the call is from a friend or a family member.

However, on the other end, a male voice can be heard introducing himself as a police or a bank personnel, telling you that you were involved in a crime or your bank account had been frozen over suspicion of it being associated with money-laundering.

At this point, you can feel a chill down your spine and you start to deny everything that they claim you had committed.

After several minutes of telling you what could happen and creating that sense of urgency, the caller then starts to tone down and convinces you that there is a simple solution at hand.

Among the 'top solutions' is for you to transfer all the money in your savings account to a third-party bank account for safekeeping.

Fearing for the worst, you follow all the instructions, beginning with depositing your hard-earned savings into the stated third-party bank account.

It is only after that – and also the failed attempts in contacting back the caller – would you finally realise that you have been scammed.

This scenario depicts the classic Macau scam, which has duped thousands of Malaysians over the years and caused them to lose millions of ringgit to scammers, who are operating locally and overseas.

Ongoing problem

Despite the countless ongoing advocacy campaigns, there are still people who become victims of this scam, regardless of their age, gender, profession and income level.

According to the Malaysian Communications and Multimedia Commission (MCMC), the scammers are cunning: they are quick to adapt to the latest technology, and are skilful in psychologically manipulating the victims.

Another modus operandi is the targeted victim would receive emails or messages, out of the blue, supposedly from 'legitimate organisations' asking for sensitive information. MCMC's advice for this is 'to hang up the phone, or to not respond to the message'.

"Instead, contact the said organisation via its official line to verify the caller's identity and also the shown phone number."

In a scam call, the scammer would also ask for a person's personal details, bank account number, passwords and Transaction Authorisation Code (TAC) to facilitate money transfer.

It is also possible that the scammer may steal a person's identity to cheat other victims. Another clear indicator of a scammer at work is when they would pressure their victims to make quick decisions and then, order them to keep their conversations and money-transferring to a third-party account 'a secret'.

What to do after being scammed?

On what to do after being scammed, the victim should lodge a police report as soon as possible to facilitate prompt action and investigation.

It is highly advisable for the victim to keep any evidence of the scam such as the text messages, screenshots or recording of the conversation, so as to assist the police in their investigation.

Scam victims who have lodged reports to the MCMC, would be referred to the relevant authorities because depending on types of scam cases, they are under the jurisdiction of the different agencies such as the police, the Ministry of Domestic Trade and Consumer Affairs (KPDNHEP), the Securities Commission Malaysia (SC), or Bank Negara Malaysia (BNM).

If required, the MCMC on its part would provide technical assistance such as information and digital forensics analysis.

As a proactive step, MCMC would also reach out to the websites or the social media platform provider to delete the scammer's content such as advertisements or posts to avoid them luring in more victims.

MCMC's role

Between January 2020 and June 30 this year, MCMC had recorded a total of 5,802 complaints related to fraud/scam, which had been referred to the relevent authorities for further action.

The Commission had also, between January 2020 and May 2022, blocked a total of 1,826 fake or phishing websites – an exercise carried out under the Communications and Multimedia Act (CMA) 1998.

These websites were blocked after reports were received from the public as well as from banking institutions who are part of the Internet Banking Task Force led by BNM.

By working together with telecommunication network providers, MCMC has blocked a total of 1.6 billion calls that are suspected to be scam attempts.

At the moment, MCMC is outlining a new guideline to avoid scams via short message service (SMS), and also conducting more advocacy campaigns together with the police and other service providers.

Our personal data

It is also revealed that scammers would cast their nets wide and pick on random victims based on sets of data that they have bought from fraudulent individuals or companies.

It is also important to note that scammers are also on the prowl for the victims' personal data to gain access to their savings accounts.

"There are ways where our personal information can be collected regardless if we are aware or not," says MCMC.

Many a time, individuals are not aware that they are giving away to scammers their personal data during phone calls – in a process called 'social engineering'.

During a call, the scammer would ask questions and the victim would end up disclosing full name, home address and MYKAD number without hesitation.

A scammer can also obtain the victim's personal data through competitions run by shopping malls or any other public places, where they (participants) need to fill in their personal details.

Another method that scammers use to browse social media such as Facebook and Instagram, and collect the full names and phone numbers of users who have opted to share these details publicly.

MCMC has also revealed that there are syndicates that buy people's personal data from unscrupulous individuals, who can be just anyone – from a security guard of a housing area, or a member of the organising team of an event.

Sebenarnya.my

Sebenarnya.my is a portal set up by the MCMC to enable the public to check and verify any news or reports, as well as to provide them with the latest information about the modus operandi of scammers.

This portal is also meant to provide awareness to the public of any potential scam that could strike anyone, anywhere at any time.

A total of 370 articles have been published on Sebenarnya.my, under the column 'Waspada', as at June 30 this year.