PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Online scams- do not talk to strangers!
Publication/Portal: The Malaysian Reserve
Date: 15 December 2020

Language: English
Section: News
Page: 4

Online scams — do not talk to strangers!

Whatever identity the scammers use, if their conversation includes specific instructions over the phone, just hang up

by NUR HANANI AZMAN

IF YOU receive a phone call from someone who claims to be an official of some high-browed government department or any financial institution, and the conversation revolves around a certain amount that you owe or a non-existent debt that might have been registered under your name — just hang up.

Chances are, you are about to be scammed and if you're the gullible type, the initial call would lead you to losses worth thousands of ringgit or worse, your entire life savings.

LE Global Services Sdn Bhd CEO Fong Choong Fook said whatever identity the scammers use — police officer, bank employee, custom officer — if their conversation includes specific instructions over the phone, just hang up.

Fong, who is also a cyber security consultant, said real officers wouldn't call people randomly as they will go straight to your house and pick you up if you're on the wrong side of the law.

"If you are still in doubt after hanging up, you can just go to the official website and look for the numbers that were used, and check with the actual office.

"Relatively, awareness among Malaysians towards scam is still very low. There'd be reports on a daily basis about how people have been scammed, mainly because they put too much trust towards technology," he told *The Malaysian Reserve*.

Fong said most people are hooked into social media and other apps, especially since the introduction of the Movement Control Order (MCO), and this opens the door to many fraudsters and scammers.

In August, Deputy Home Minister Datuk Seri Ismail Mohamed Said revealed in Parliament that fraud made up the highest number of scams during the MCO period.

The government data revealed that frauds related to e-commerce were the highest between March 18 and June 30, with 2,020 cases involving losses amounting to RM12.6 million.

As of Aug 4, the cases ballooned up to 2,500 with total loss at RM17 million.

Fong said Macau Scam is still the No 1 scam in Malaysia since it has been operating for so long and the story lines used are convincing, especially involving law enforcement and financial losses.

"Macau scam is well-placed in all levels of society. That's why it is still the No 1. Love scam via social media platform is currently catching up with Macau Scam," he added.

From the email claiming you've won the latest iPhone 12 to phone calls from people claiming to be representing your bank, it is becoming increasingly difficult to keep up with the range of scenarios that are used by these fraudsters.

Unwanted messages and fake ads bombard us on a regular basis. Most of us hit ignore or delete. However, many others aren't so lucky, especially during these unprecedented times.

These are five famous scams that are happening in Malaysia. Be alert and do not fall for it!

Macau Scam

In Malaysia, Macau Scams are categorised as telecommunications fraud. Usually, the victim gets a phone call from an official-sounding person and is told he or she has outstanding loan payments or unpaid fines.

The victim panics and willingly follows the instructions of the "official", including transferring huge sums of money into another party's bank accounts, to supposedly "avoid getting into trouble".

Bernama on Nov 19 reported a total of 1,420 out of 2,676 Macau Scam cases have been charged in court between January and October, involving losses amounting to RM256 million.

Please remember to not transfer cash into other bank accounts following telephone conversations with strangers!

BigPay Scam

You could get a call or SMS (short message service) from someone pretending to be a BigPay staff member, who may mislead you into giving away important information, especially one-time password (OTP) number.

Fraudsters might go the extra mile to impersonate them by using their logos as their profile image. Some of them might call you via WhatsApp call.

Recently, @bigpaymeapp Twitter account was flooded with complaints from its users about getting a scam call saying that they won RM3,000.

"Hi there. Thank you for mentioning us here. The number which contacted you via WhatsApp is not from BigPay and neither will we reach out via WhatsApp to request for any users' personal details/OTP. Please report and block the number right away.

"As of now, there has not been a data leak/breach. These scammers are keying in mobile numbers at random to assess who has a BigPay account," it replied on Twitter.

Social Media Scam

Social media scams have become overwhelmingly popular with cyber criminals. Facebook and Instagram have made it easy for strangers to earn your trust by impersonating people or brands.

Sometimes, these fraudsters spend weeks talking with you before pulling their scam.

Scams on Instagram happen when people create fake accounts or hack into existing Instagram accounts you've followed.

According to Instagram, it can be in many types of scam. Among the usual modus operandi:

• Romance scams: Romance scammers typically send romantic messages to people they don't know, often pretending to be divorced, widowed or in distress. They'll engage in online relationships claiming to need money for flights or visas. Their goal is to gain your trust, so the conversations may continue for weeks before they ask for money. Be vigilant of engaging in such conversations with people you don't know in real life.

• Paid subscription services: Scammers will offer the sale of paid subscription services or lifetime access to these paid subscription services for a one-time payment. Avoid purchasing subscription-based services from unknown third parties since scammers won't deliver the product, or the product won't work as they claim it will.

• Phishing scam: Phishing is when someone tries to get access to your Instagram account by sending you a suspicious message or link that asks for your personal information. If they get into your account, a scammer may have access to things like your phone number or email address. They may also change your password to lock you out of your account.

Job Scam

Online scams have become a big threat and job sites have not been spared either. If a job promises high pay for little work, be leery. That's 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.

A daily reported in September that a group of 18 Malaysians were duped of RM180,025 by a man who had allegedly offered them "jobs" at a casino in Cambodia.

Online Money Lending Apps

The Personal Data Protection Department (PDPD) has opened investigation papers on six unlicensed money lending apps that are suspected of misusing personal data.

The six applications are Asialend, Dreamlend, iPayfren, iPinjaman, Helplend4u dan GoCash4u.

"All such online applications were found to have accessed and copied people's information, including personal information unrelated to loans without borrowers' consent," the statement read.

Those whose personal data have been misused by such unlicensed online money lending apps are urged to contact the PDPD enforcement division through email at *penguatkuasaan@pdp.gov.my* or the personal data protection system *(daftar.pdp.gov.my)* to assist investigations.

PDPD advises Malaysians to be more careful when applying for loans online, especially when giving downloaded apps permission to access information, to avoid personal data being misused by irresponsible parties.

In this time of great difficulty, it is important to remain vigilant so as to not be deceived by their tactics and tricks. Do not disclose your personal financial information to any suspicious parties. Do not be scammed into transferring money to unknown third-party accounts.

Please check with the bank on the unknown third-party accounts. If you receive any unsolicited telephone calls, SMS or emails, protect yourself by not responding to any such unsolicited contact.

Even Bank Negara Malaysia will never request for personal information or clarification via SMS, telephone call, email, social media or any messaging app.