Media Title : New Sarawak Tribune
Headline : Online financial fraud growing but preventable
Date : 13 March 2023
Section : News
Page : 8

Online financial fraud growing but preventable

BY NURA VALENTIANA LORNA
tribunenew2019@gmail.com

KUCHING: In just about every country in the world, financial fraud is a major issue, and Sarawak, is no exception.

Financial fraud cases have increased recently in the state, costing both individuals as well as organisations a great deal of money.

Phishing, identity theft and investment scams are just a few of the techniques fraudsters use to trick people.

Due to ignorance and blind faith in others, elderly folk in particular are especially susceptible to these scams.

In light of this growing problem, New Sarawak Tribune spoke with the head of Bank Negara Malaysia (BNM) Kuching Office Mohd Irman Mohd Din to gain insights on the issue of financial fraud in Sarawak.

Mohd Irman, who has extensive experience in the financial sector, offered valuable advice on how individuals can protect themselves against financial fraud and what steps can be taken to prevent such crimes from occurring in the future.

He imparted his expertise and knowledge on the various types of financial fraud that are common in Sarawak, the tactics used by fraudsters, and the role played by the government in preventing financial fraud.

Additionally, he said while the development of digital technology has brought about a number of advantages, it has also opened up fresh chances for scammers to prey on individuals and organisations.

Although e-commerce and online banking have made financial transactions more convenient, they have also made it simpler for fraudsters to obtain sensitive personal and financial data.

To combat financial fraud, he said BNM has been taking various measures, including strengthening regulatory frameworks, enhancing supervision and raising public awareness.

He noted that BNM has been collaborating with law enforcement agencies to investigate and prosecute scammers and has been raising public awareness on the dangers of online scams.

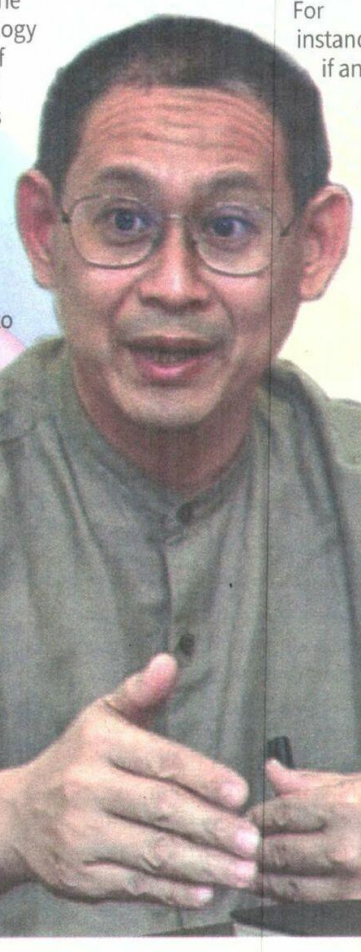
Q: What are the main scams which fall under BNM's jurisdiction?

We only focus on two main scams, which are illegal deposit-taking and illegal money services such as forex trading.

Illegal deposit-taking refers to individuals or organisations that take public funds without a licence, promising returns on the money.

It should be noted that only banks are authorised to accept deposits from the public for savings and other purposes.

The second is illegal money services such as illegal forex trading and remittances activities. For instance, if an individual wants to exchange currency with Indonesian citizens at the border, this is illegal because that individual does not have a licence for money changing services.



Q: The most prevalent fraud at the moment is the Macau Scam. Can you give a brief description of this fraud?

Most of the cases involving the Macau scam are online frauds, as frequently reported in local newspapers and social media.

Victims are contacted by criminals who pose as enforcement officers from various agencies such as the postal service, court, tax department and even the police.

They will target victims based on certain criteria that are deemed easy to attract or deceive and take advantage of them for a lot of profit in a short time.

Scammers exert emotional pressure on the victim by claiming that the victim has a criminal record, that unauthorised items or parcels have been sent or that there are outstanding debts with the bank.

To help resolve the issue, the victim is asked to make a payment of a certain amount to an individual's account.

Various techniques are used by criminals to deceive the victim to the point where they feel afraid and surrender their money or personal banking details to the criminal.

We have received information that there are victims who received calls from the police, courts and others. What is strange is that sometimes these calls are received on Sundays, which are non-working days. This is a fraudulent act.

Therefore, the public should be aware of this issue so that more people out there do not fall victim to such incidents.

Q: How do these scammers operate and determine whether a person's bank account has a sizeable sum of money?

I believe they are simply speculating, but I can only presume that these criminals are taking a chance.

As a result, they will never grow bored of calling victims every day, all day long. They also appear to be following a script when they speak.

In the past, if someone wanted to cheat another person, they would have to meet that person. But not anymore.

Blindly handing over thousands of ringgit, even reaching millions, can now be done with just a phone call.

I would like to emphasise that these scammers are the most spirited and resilient, and they never give up on convincing victims to fall into their trap.

Q: These days, many people are victims of internet frauds due to the development of technology. Could you just explain this further?

Online scams such as love scams, Macau scams, non-existing financing, impersonation of government agencies, and others are various methods used by criminals in carrying out their activities.

Online fraud by scammers is recorded to occur every day, and this crime does not spare any segment of society, including professionals and those in rural areas who also become victims of these very cunning syndicates.

In the past, scammers used to send links via email that would lead to bank websites that looked similar but were actually different.

For example, they would change a few letters in Maybank's name to "Mybank" in order to deceive victims and give them confidence to enter their username and password on the fake website.

However, scammers now use a new fraud tactic known as the Android Malware Scam that uses an Android Package Kit (APK) file to run their operations.

An APK file application, which one can voluntarily download, can be hacked via a link.

Because of this, it frequently occurs that one's phone is taken advantage of, especially when they visit particular websites, such as pornographic websites, where there are many alluring ads that direct to the download of APK files.

Q: How does the APK scam work and how can it be avoided?

APK scams work by tricking victims into downloading and installing a malicious APK file on their mobile device, usually through social media such as Facebook and Telegram.

The scammers create an app that appears legitimate and enticing to the victim, such as a game or a tool for improving phone performance.

Once the victim downloads and installs the APK, the app requests permission to access various features and information on the phone, such as contacts, photos and location data.

The victim grants these permissions, thinking they are necessary for the app to function properly.

However, the app is actually a tool for the scammers to steal the victim's personal information and use it for fraudulent purposes. This can include accessing bank accounts.

With this method, the scammer will add their own phone number as a favourite in the banking application, allowing them to gain the One-Time Password (OTP) and then preventing the victim from knowing if there is any transaction made.

APK scams can also be used to distribute malware that can take control of the victim's device and the scammers even read personal messages of the victim.

To avoid falling victim to an APK scam, it is important to only download apps from trusted sources, such as the official app store for your device.

Additionally, carefully review the permissions requested by the app before granting access to any information or features on your device.

Q: Nowadays, we often hear about illegal moneylenders or Ah Longs who use applications for registration and take advantage of the information of the victims. Can you explain how they work?

Legal moneylenders actually come under the Ministry of Housing and Local Government (KPKT), and in Sarawak, they come under the jurisdiction of the Resident's Office.

However, there are also illegal moneylenders, commonly known as loan sharks or Ah Longs who operate without a licence from KPKT or the Resident's Office, and they offer easy, quick and guarantor-free loans.

They are unlicensed lenders and are considered criminals. Don't let yourself or your family become victims of Ah Long threats.

Licensed moneylenders can only operate from approved addresses or offices, and they must display their licence in a prominent location on the premises.

For unregistered moneylenders, their latest tactic is to ask borrowers to download an APK file application for payment instead of meeting in person or going to a bank to deposit money.

When a borrower downloads the APK file provided by the Ah Long, the Ah Long can access the list of registered or not registered borrower and obtain their pictures and information.

The loan application will request permission to access data on the borrower's mobile phone, and Ah Long will use the borrower's personal information, such as pictures, videos, and contacts, to harass or threaten the borrower or their contacts.

Therefore, never download applications from sources other than Google Play or the Apple App Store.

Q: What does BNM advise victims of financial fraud to do when a case occurs?

I would like to remind the public, especially victims of scams, to immediately report any incidents of fraud to the National Scam Response Centre (NSRC) via the hotline at 997.

Victims who contact the NSRC within 24 hours may have a chance to recover the money that was stolen by the scammers.

If the victim contacts the NSRC within 24 hours of the incident, BNM can take immediate action to stop the outflow of funds from the system.

After contacting the NSRC, the victim should go to the nearest police station to file a report.

Then, the report should be taken to the bank concerned. Therefore, it is highly recommended for the victim to contact the NSRC as soon as possible so that immediate action can be taken.

Q: Given the increasing concern over cases of fraud, what is your call to the public regarding this crime?

To strengthen the cybersecurity of financial users during online activities and personal financial management, the concept of 3S — Spot, Stop and Share — should be practised to protect the public from financial fraud.

Furthermore, awareness about online fraud is crucial, and the public needs to be vigilant in detecting its modus operandi through media reports and share information with acquaintances and family members regardless of whether they live in urban, rural or remote areas.

They should also refrain from sharing any personal information with outsiders.

We must eradicate this crime to prevent further harm to many parties.

Financial fraud is a complex problem that requires a multifaceted approach to combat.

As such, through collaboration between regulatory agencies, law enforcement, media agencies and the public, Sarawak can work towards reducing the incidence of financial fraud and safeguard the financial well-being of its citizens.

HEAD of Bank Negara Malaysia (BNM) Kuching Office Mohd Irman Mohd Din.