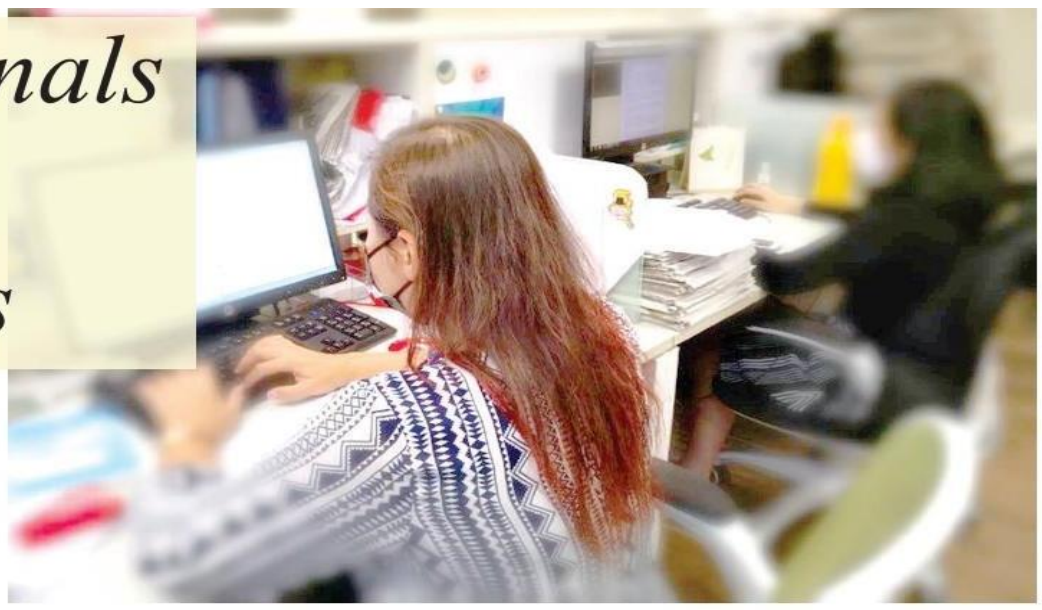
PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Even professionals fall victim to cyber criminals
Publication/Portal: Daily Express (Sabah)
Date: 20 December 2021

Language: English
Section: Local
Page: 7

Even professionals fall victim to cyber criminals



Police have warned the public to be wary of job offer scams.

■ Second of a two-part series

Sherell Jeffrey

SABAH has seen its fair share of stories about scams that have gotten national and State media attention.

One of them involved scammers offering cheap tour packages online. The last major scam involved 120 people, including around 40 Sabahans, who purchased a tour package to Turkey and Greece in 2018.

Then in 2017, Sabah police nabbed the mastermind to a firm behind the so-called project had not done any work on the site but had instead advertised it through social media and used live streaming.

The company even used live streaming to show off the project at Likas Stadium, which was packed with 2,000 people, largely Chinese and Taiwanese. They even held a Gala Dinner Award Night in Kota Kinabalu on the same night to lure victims into the scam.

In 2015, an entrepreneur's offer to give out free houses to Sabahans was described by many as "too good to be true". Even the then Sabah Tourism, Culture and Environment Minister Datuk Seri Masidi Manjun expressed doubts on the offer.

SAC Victor Sanjos, Deputy Director of the Bukit Aman Commercial Crime Investigation Department's Cyber Crime and Multimedia Division, said based on data since 2014, it is the people that provide scammers the opportunity to do so.

Professionals such as lawyers and surgeons, as well as government officials and business sector CEOs and chairmen, have all been victims.

"Are they unable to read? Do they have no idea? Are they illiterate? No, I don't believe so.

"The number one reason is that we constantly forget," he said.

According to him, the Commercial Crime Investigation Department has a system called the Commercial Trend Intelligence System that requires all investigating officers to interview cybercrime victims and ask if they have heard of cybercrime prevention methods.

"Many victims have heard of anti-cybercrime efforts. The question is, how did they become victims in the first place? When they are well aware of cybercrime, how did they become a victim?" The majority claim to have forgotten.

"Victims also have a tendency to avoid making verifications. When told to transfer money into an account, we don't check to see who owns the account."

For example, suppose you receive a call from someone purporting to be a Customs officer who informs you that a parcel addressed to you has been seized. The "officer" stated that the shipment contained money and jewellery and that a charge was required to release the item. The "officer" opens an account for you, and you deposit money into it without checking to see who it belongs to. You've been duped out of your money.

Another possibility is you receive a call from the police alleging that you have been charged with a crime. When they threaten to arrest you unless you pay, you shiver with fear.

"Scammers will constantly say, 'Don't tell anyone because we'll jail you if you do.'

"The police will not call you to say they are about to arrest you. The police will come to arrest you and take you to court as soon as possible; they will not threaten to arrest you over the phone," he said.

One of the tactics employed by Commercial Crime to combat cybercrime is to create a system where all of these accounts, known as Mule Accounts, are registered.

"We make this information available to the public, including the scammers' phone numbers." This system exists in only one country: Malaysia. Even the international community uses this service," he explains.

If the money is going to the government, he says, the account should be set up as a government account rather than an individual account like the ones used by scammers.

"Our goal is to limit the number of cybercrime cases since the money at stake is your money, not government money.

"It's money set aside for the future, or money borrowed from family and friends," he explained.

Four police products to prevent cybercrime

- Mule Account which can be accessed via the Internet to verify bank accounts https://semakmule.rmp.gov.my/#
- Commercial Crime Investigation Department (CCID) Scam Response Centre that can be contacted via 03-2610 1559/1599
- CCID Info Line 013 211 122 (WhatsApp only)
- Cyber Crime Caller that can be accessed via the Royal Malaysian Police website

The CCID Scam Response Centre, according to Victor, exclusively accepts calls from the general population.

"It's a fraudster if the CCID Scam Response Centre (03-2610 1559/1599) calls you out of the blue. Because our centre will never make a public call," he said.

"Reach out to these four products when you receive calls and are unsure since these four products will save you from becoming the next cybercrime victim."

"Some may argue that the only thing lost is money, not life. I've met a few people that believe this. But they don't realise that this is money accumulated over many years of hard labour, and it's all gone in an instant."

How do scammers obtain our personal information? How do they know our names and even handphone numbers in the first place?

Information shared online will remain online despite being removed, according to Suhaila Jaffar, Director (Regulatory) of Sabah MCMC.

"When we publish a photo to the Internet, we realise it may not be particularly appropriate, so we erase it.

"However, we have no idea how many people have already screenshot or downloaded the material in that five minutes.

"We can get our information from a variety of places. Perhaps we could write our names and phone numbers on a shopping receipt in order to win a prize. This data is worth a lot of money. Data is a valuable commodity. This is why the Personal Data Protection Act was enacted.

"Let's suppose we sign up for a service and the provider states that your information will not be shared with third parties.

"But it all boils down to the service provider's honesty. People sell this data because it is valuable, it is marketed nowadays, and it is difficult to control.

"I believe it all ultimately comes down to the data handler's integrity," she explained.

Because data is everywhere, the question of how MCMC can discover these data is rather complex. What we can do is support the work of the police.

"At the MCMC, we emphasise the need of improving and strengthen self-regulation. It is up to us to be wise, responsible, and ethical online users.

"If something seems too good to be true, it most likely is. Take, for example, an RM5,000 iPhone that is being sold for RM1,000.

"This can't possibly be true. As a result, be wary of advertisements that seem too good to be true.

"Second, we must exercise extreme caution when interacting with others online since anyone can be anyone on the internet.

"We don't know if they claim to be a famous artist, but they can always use a different photo.

"This occurs frequently, and MCMC receives similar concerns. Nowadays, it is quite common.

"This is why, among other things, MCMC conducts advocacy programmes such as our Klik Dengan Bijak campaign. Our purpose is to empower the community by providing them with the knowledge they need to self-regulate."

Mohammed Tonarusli, a senior executive of Bank Negara Sabah, said scammers can get phone number from Facebook, for example. "There is a wealth of information available."

He said when we browse pornographic websites, for example, our information can be collected by scammers.

"Scammers will utilise popular websites to collect information by infecting them with a virus that will detect online user information from such websites.

"Be cautious when visiting such websites. If you see an advertisement that keeps showing up to get your attention, your information will be copied and pasted directly to the fraudster once you click on the pop-up," he said.

Another way to prevent becoming a victim of a hoax is to be cautious when receiving calls from any agency, including family members.

"I know a friend who was duped by a member of his own family, possibly owing to financial concerns."

Scammers can be found almost anywhere. Don't just give out your information. Don't just answer the phone and disclose your details when someone asks who you are.

"Don't panic if you get a call from the 'police', because you'll start revealing information if you do." He advised, "You must think clearly and wisely."

Whatever the scammer accomplishes, Victor points out, he or she will only be able to complete the cycle if there is one thing missing: a bank account.

"You must be cautious to interrupt the loop, and you must never disclose your account to anyone without first validating it.

"However, some con artists are astute, and they will double-check the account on the police Mule Account before handing it on to their victim."

As a result, we urge Malaysians to not become complicit in scams by disclosing their account numbers to them.

"If we discover that your account was used for a fraudulent transaction, we will add it to the Mule Account list and notify the bank to cancel it.

"Many such accounts belonging to government employees as well as those from the commercial sector have been blocked.

"After seeing that their accounts have been designated as a Mule Account," he continued, "some of them would come to the police pleading for their accounts to be unblocked."

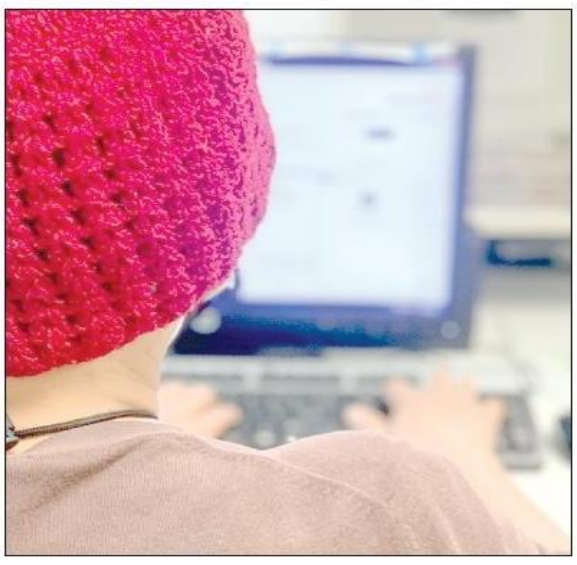
Daily Express

Home / Sabah News

Sandakan woman loses RM50k in 'love scam'

Published on: Monday, October 28, 2019
By Winnie Kasmir

In 2019, a woman in Sandakan lost RM50,000 in love scam.



Scammers will feign romantic intentions to get victims to send money under false pretences.