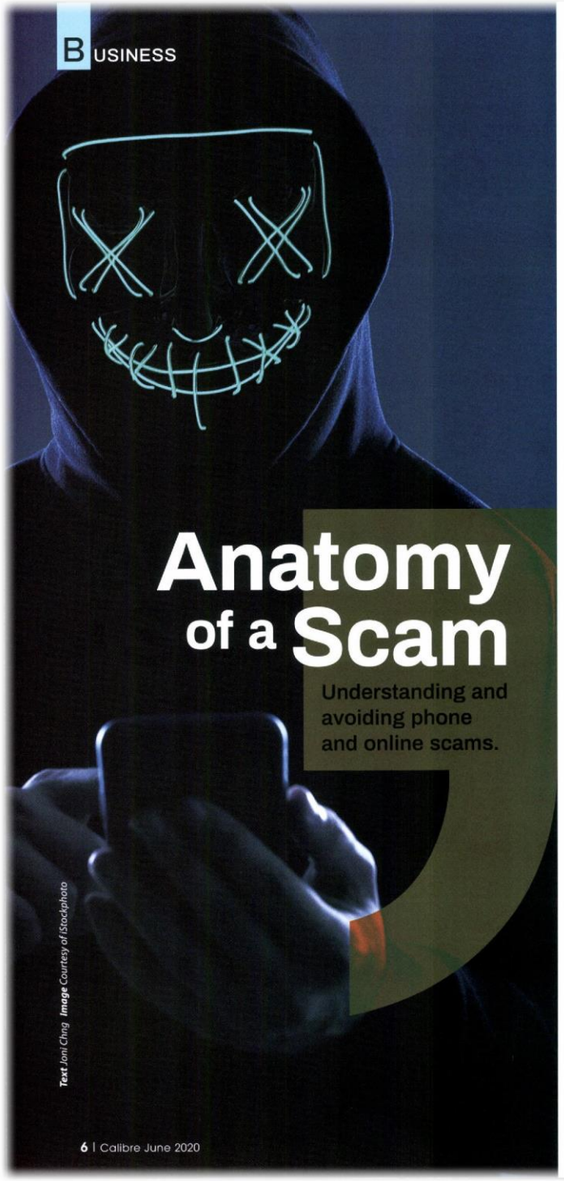
PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Anatomy of a scam
Publication/Portal: Calibre Magazine
Date: 1 June 2020

Language: English
Section: N/A
Page: 6



You got a call from an unfamiliar number. The person on the line claimed to be a police officer, informing you that you are wanted for money laundering. They recently arrested a suspect who named you as an accomplice.

Panic kicks in. This must be a mistake; you must have been a victim of identity theft. Somehow, your personal information had been compromised and now you are being framed. The 'officer' then offers to help you out of the mess and clear your name; all you have to do is follow a few steps to aid in their investigation. Distraught and wanting the matter to be over with, you agree to cooperate. Plus, the caller comes across as an authoritative, compassionate, and helpful person.

You are instructed to transfer a sum of money into a bank account set up by the police to allow for investigation, with the assurance that it would all be returned when it's over. You complied, and then you don't hear back from them again. That's when it hits: You have just been scammed.

According to the Bukit Aman Commercial Crime Investigation Department (CCID), there were about RM6.2 billion in losses suffered by victims of commercial crimes, from phone scams to non-existent loan cases from January to December last year.

DECODING THE SCAMMERS' MODUS OPERANDI

Let's look at three of the most common phone and online scams, and why they work:

Macau scam – The scammer would pose as an authority figure, usually a police officer, bank officer or government official over the phone. The victim would be told they have some kind of criminal conviction against them. There are also cases of callers pretending to be a representative of a telecommunications company, calling to claim a long outstanding bill or face legal action. They may claim to have kidnapped your family member and demand ransom, or told the victim they have lottery winnings to claim. The ultimate aim is to get the victim into a heightened emotional state, so they can be talked into revealing personal banking information or handing over money.

Love scam – Sometimes known as parcel scam, scammers usually connect with their targets via social media or dating sites and apps. They would befriend or romance their target. Once a relationship and trust is established, the scammer would entice the victim with promise of gifts in the mail. An accomplice would then contact the victim, posing as a government officer or courier staff, claiming the package has been detained by authorities for inspection. The victim is required to pay money to have the parcel released.

Another favourite tactic of love scammers is to tug at the victim's heartstrings with sob stories of unexpected financial troubles, such as being diagnosed with an illness or their home was burglarised, to convince the victim to send them monetary aid. If the victim ever requests to meet in person, expect the scammer to be a no-show.

Bogus offers – With the world battling the COVID-19 pandemic, the CCID said early April that there have been a total 556 cases of scams involving the sale of face masks over various social media and online platforms in Malaysia, with losses amounting to RM4.2 million.

The majority of these cases occurred during the Movement Control Order (MCO) that started on 18 March. Bulk quantities of masks were up for sale, but once payment was made, the goods were not delivered and the seller could not be reached anymore.

Sales of non-existent goods, financial products and services, bogus job opportunities and investment schemes are some of the oldest scams in the book. Unfortunately, technology has made it easier for scammers to operate.

WHAT CAN YOU DO TO PROTECT YOURSELF?

At the heart of all scams is emotional manipulation. The typical game plan is to get the potential victim at their most emotionally vulnerable state, where one's good judgment would be clouded. Here are a few ways to protect yourself from becoming a victim:

Stay calm and trust yourself – You know for a fact you did not commit the offense the stranger on the phone is accusing you of, but scammers would try to intimidate and gaslight you into doubting yourself. They would try to create a sense of urgency, in hopes that you would buckle under pressure and do what they want. Don't hesitate to hang up and call the real cops.

Don't let your heart rule your head – Never, under any circumstance, should you send money to someone you've never met on the basis of a relationship that developed exclusively online. Likewise, say no to any gifts they offer to send you, even if it's in the name of love and friendship.

Take control of your digital life – Ideally, you should stick to buying things online from legitimate outlets with a secure payment system on their website. Look out for official announcements and only install apps from official service providers, for example, Google Play or Apple App Store. When it comes to emails and mobile phones, never click on unverified links in emails or text messages and do not open untrusted attachments. Always verify the legitimacy of sources before responding to any emails, text message or voice calls asking for personal or sensitive information.

Stay informed and be aware – Scammers may get crafty with their tactics, but an informed target will always be their worst nightmare. The CCID infoline (013-2111-222) or cybercrime alert Facebook page (https://www.facebook.com/CyberCrimeAlertRMP) are excellent resources for staying current.