Hook, line and sinker

Over the years Malaysians have fallen victim to slick fraudsters, with new types of schemes emerging during this movement control order period. StarMetro lists down and discusses 10 common scams in the country. >2&3
SCAMS have been around for countless years and the culprits behind them have become more creative and increasingly sneaky in their attempts to cheat people. They are more prevalent now, making the current situation even harder for Malaysians to bear.

The Federal Commercial Crime Investigation Department (CCID) investigated 14,050 cases of scams, with losses estimated at RM914m for the first six months of this year.

Some good ways to avoid being a victim in this digital age include being sceptical of everything you view, using unique passwords and enabling two-factor authentication on all accounts.

When in doubt, always check bank account details given by the suspected scammer via http://ccid.rmp.gov.my/senakmule/ or call the CCID hotline at 013-2111 222.

StarMetro has compiled a list of the 10 most common scams locally in hopes that everyone would think twice to avoid being duped into parting with their savings, but this list is by no means exhaustive.

Macau scam

The Macau scam often starts with a phone call from someone pretending to be an officer from a bank, government agency or debt collector.

The scammer will claim that the potential victim is involved in undesirable or illegal activities and then offers to help by transferring his money into a specific bank account to prevent the authorities from freezing their own accounts.

Another common modus operandi is that these fraudsters use is pretending to call from Standard Chartered or other banks, saying that the victim has not paid their credit card's outstanding bill or a loan, and threaten to have their bank account blacklisted or frozen.

Victims will be tricked into paying a certain amount via a given account within a short period of time.

These calls typically utilise "spoofing" where scammers can display any phone number on one's mobile phone screen to trick the victims into believing that the calls are coming from whatever authority the scammer claims to be.

CCID acting director Comm Datuk Saiful Azly Kamaruddin was reported saying that in the first six months of the year, a whopping 2,176 scam calls impersonating the police were detected, which led to a total loss of RM103m.

Police reports also saw a 20% increase in phone or Macau scam cases during the movement control order (MCO) period from March 18 to May 18, leading the police to urge the public to never give any personal information over the phone to strangers, and to verify such calls by going to any police station.

Kidnapping scam

Deceivers in this type of scam operate by telling their victims that their child or family member has been abducted and demanding a ransom to ensure their safe return.

They prey on parents while they are at work or out of the house, sometimes utilising realistic background noises of crying children to deceive them into quickly paying up to stop the child from being harmed.

Scammers will also use "spoofing" to disguise their phone numbers as belonging to the kidnapped family member.

A viral video of a Malaysian grandmother who kept her cool and scolded the alleged kidnapper after receiving a ransom call, was heavily circulated in 2017.

A foreign media reported that Australian police investigated eight incidents of virtual kidnapping where the scammers coerced foreign students into faking their own abductions and trick families overseas into paying ransom. This involved a total payout of about RM9.6m this year.

Postal scam

This scam has been around for many years where scammers inform their victims that their parcels or lucrative prizes are being held by Customs and that payment is required to clear the parcel for delivery.

The victims will later realise that they have been cheated when no parcel arrives.

In a recent case on July 28, the victim was said to have been called by police claiming that contraband items had been found in a parcel addressed to the victim who would face money laundering charges if they failed to make payment.

The victim ultimately lost RM1m to the scammer. In the first six months of this year alone, the CCID received 17 cases of postal scams with losses close to RM8.3m.

Love scam

This type of scam is believed to be the easiest to carry out.

Scammers pose as eligible bachelors before duping women into parting with large amounts of money.

Comm Saiful Azly said the syndicates knew exactly how to brainwash the victims once they found an easy target.

Such scams also operate by blackmailing female victims after they send nude photos of themselves to the fraudster.

MCA Public Services and Complaints Department head Datuk Seri Michael Chong was reported to have said that 90% of such cases involved women.

Those most vulnerable were usually above the age of 40, he said, adding that the scammers would usually target widows, divorcees and older single women.

He also said that educated professionals tended to be the most easily cheated.

Phishing scam

This type of fraud is operated by setting up free public hotspots to get as much personal
data as possible of victims once the victim connects to the hotspot.

It includes stealing victims’ banking information when they perform online transactions and gaining access to their email addresses or social media accounts.

Another common tactic is to impersonate a close friend or colleague online to encourage the victim to click on links to phishing websites, or to download attachments that enable the criminals to access accounts and steal personal information.

While seemingly harmless, all data of the victim can be shared and used for identity theft, access bank accounts or make the victim a target of other scams when their personal information is shared with other scammers.

Global anti-cybercrime organisation Anti-Phishing Working Group (APWG) found over 165,772 phishing websites in the first quarter of this year alone and another 139,685 cases of unique phishing emails directing users to a phishing website.

Face mask scam

In light of the Covid-19 pandemic, many people were cheated when buying face masks online at very high prices.

According to the CID, during the MCO period between March 18 and June 30, there were 781 cases of face mask scams resulting in RM81.1m in losses.

The department made 204 arrests with 76 charged in court.

Consumers were easily enticed by cheap and fast orders, most of which were promoted by illegitimate suppliers.

The department advised the public to not believe the system and get duped by people claiming to have fast production.

Similar scams also exist on various e-commerce platforms for luxury goods, concert tickets and luxury beauty items such as skincare and makeup.

Savings scam

Recently, fraudsters targeted EPF contributors by offering them ways to help withdraw RM500 from Account 2 of their savings, knowing that many were desperate for money during the MCO.

Many victims were enticed by scammers who claimed to have a way to circumvent the EPF safeguards to withdraw money from their retirement savings and the common would ask to first be paid in cash of between 30% and 60% from the minimum withdrawal of RM150,000.

Some even offer personal loans using EPF savings as collateral.

The Consumers Association of Penang said if consumers were careless, they would end up poorer because of exorbitant interest rates and risk being harassed when they were unable to repay their loans.

The police have opened 393 investigation papers into EPF scams with total losses reaching RM3mil in March alone.

Investment scam

This type of scheme usually promises high returns and zero risks. Victims are usually lured into making small payouts before the culprits disappear with their life savings.

One example is the Royal Gold investment scam which led five retirees to lose a whopping RM3mil of their life savings and EPF in 2014.

The victims said the fraudulent companies often held meetings with hundreds of investors, promising that the victims were protected by insurance policies and had no risk of losing their money.

Foreign exchange trading scams are also a common modus operandi.

CID found 467 online investment scams amounting to RM52.4mil in losses this year. A total of 13 online investments websites have also been identified as scams by the police.

Malaysians are also urged to check Bank Negara’s (BNM) financial consumer watch list which shows companies and websites that are not approved or authorised under the laws and regulations administered by BNM.

Mule account scam

The syndicates behind this scheme often promise victims lucrative jobs with high returns by simply handing over their ATM card or online login and password, or in exchange for victims receiving and transferring large amounts of money to a third party account.

Online scam syndicates often use higher education students, the homeless, drug addicts and the unemployed by using their bank accounts to deposit money cheated off victims, in efforts to prevent detection of their illicit activities.

Johor police chief Comm Datuk Ayob Khan Mydin Pitchay was reported saying that 440 people were arrested between Jan 6 and May 31 this year during major operations in Johor.

The Malaysian Crime Prevention Foundation (MCFF) also advised the public not to allow their personal bank accounts to be used or handled by any other person to prevent them from being used as money laundering accounts.

TAC scam

This scheme typically occurs when scammers contact the victim claiming that they had mistakenly used the victim’s phone number and that the transaction authorisation code (TAC) details were mistakenly sent to their phone.

They will then ask the victims to share their TAC number before stealing money from their bank accounts.

On Feb 4, a man lost RM3,220 in savings to a scammer after falling for this scam.

Throughout the MCO, there was a rise in the number of TAC scams with online scammers actively coming up with new strategies to dupe victims.

Bank Negara urged the public not to share their TAC number with anyone and avoid accessing public WiFi.

They are instead asked to use their personal mobile devices whenever they access online banking or provide personal information online.

This scam has fleeced Malaysians of almost RM15mil in 2018.

(Above) A video of this grandmother scolding a scammer who attempt-
ed to extort her went viral in 2017. — Filepic

(Right) Comm Ayob Khan (right) showing seized electronics that were used to run a Macau scam operation in Johor. — Filepic

(Above) The Immigration Department’s single biggest operation in November 2019 saw 680 arrests of those running an investment and forex scam from this building. — Photo courtesy of Immigration Department.