

Media Title : New Straits Times
Headline : Ways to detect scams
Date : 16 January 2023
Section : LIFE & TIMES
Page : 16



Ways to detect scams

WITH the increased number of cyber-attacks in 2022, Malaysians should be more vigilant against cyber threats by scammers.

One of the tactics that Malaysians should keep an eye out for is scam calls; something often used by scammers to obtain information and personal data.

This indicates that many still fall for scammers' trickery despite the warnings of police and other authorities.

SOME OF THE LATEST SCAMS IN 2023 INCLUDE:

- **Cryptocurrency scams**
Despite cryptocurrency being the new trend for storing currency in a digital wallet, scammers have their eyes on opportunities that arise. Some cryptocurrency scams include Bitcoin investment schemes, fake cryptocurrency exchanges, or social media cryptocurrency giveaway scams.

If it's too easy, it's probably a scam.

- **Phishing in the metaverse**
Another foreign topic that has started to dominate the scamming scheme is phishing in the metaverse. Scammers pretending to be a Metaverse team would request users' data (such as usernames, passwords, etc). If the metaverse victims fall for the trick, attackers would have access to the users' metaverse accounts and manage more scam services.

- **Phone Scams**
Their latest endeavour is to impersonate victims' relatives, banks, couriers, and renowned companies, among others, and frighten or lure them into giving their personal information for their gain. If their attempt in embedding fear becomes unsuccessful, scammers will lure you into trusting them instead.

HANDLING SCAM CALLS
Several people have had firsthand experience with scammers' pathetic attempts.

Riz Iskandar, 42, often receives Inland Revenue Board (IRB) scam calls that will direct him to an automated responder whenever he picks them up. It will then instruct him to key in his identification details, at which by then, he would hang up right away.

"Organisations won't simply ask for your identification information. A structured process to verify customers or introduction must be strictly abided by any operator," Riz said.

Halida Hapim, 28, would get scam calls from various parties such as banks, foundations, IRB etc.

She explained that relevant parties would not reach out via calls or to update customer's details via their website.

"Some scammers would call during lunch breaks and ask for details such as identification or bank number. Since it is private information, it shouldn't be shared easily unless for formal documentation purposes," Halida said.

Halida added that normally, she'd hang up on scam calls immediately, but Riz likes to play along until the scammers hang up themselves.

"I just go with the flow so that they will be the ones to hang up instead. I would usually ignore or end any unknown or unidentified numbers coming into my phone," he added.

DETECTING SCAM CALLS
Using observational skills alone is not enough. The public has to take measures to secure their accounts and safety.

For instance, the Truecaller app does wonders for detecting a 'scam' number. It is a caller ID and spam-blocking app that unveils the identity of incoming calls.

It also collects global records of numbers as well as blocks unknown or foreign numbers.

For Android users, you can go for ScamShield.

It is a call-blocking and scam-detection app that can filter scam messages and call numbers used in illegal activities, which consequently prevents them from contacting us.

Bots
By Hanum Afandi

*Be wary of scam calls.
PICTURE BY FREEPIN*