PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: When it is too good to be true
Publication/Portal: The Star
Date: 25 July 2022

Language: English
Section: Business / Bizbytes
Page: 5

Money & You

When it is too good to be true

Scammers are finding new ways to cheat the gullible

By B.K. SIDHU
bksidhu@thestar.com.my

ALMOST every day we read or hear about someone losing money to scammers.

Cybercriminals are steps ahead as they continously find new ways to steal your data and money.

Of late, there has been a rise in recruitment ads offering part-time jobs in so called "reputable" companies and the paypacket for a day's work is RM500 to RM1,000.

Getting paid RM500 or RM1,000 for a day's work is big money and certainly many would be tempted.

But, before you take the leap, ask yourself, can this be true?

Then there is the Wangiri scam making its rounds. Most telecom providers have warned their users of this scam.

This is a phone scam where the fraudsters try to extract money from potential victims by calling from unknown international numbers, a report said.

It added that scammers make many short duration calls to trick the users into calling back to a premium rate number and the fraudsters are hoping you will call back.

If you do, you will be charged a lot of money while being on the call.

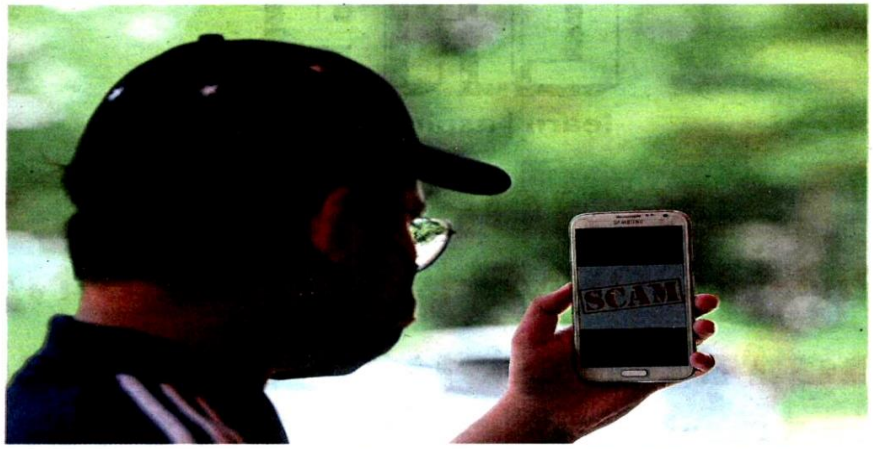
What you will be listening to is usually a pre-recorded message or tone designed to keep you connected for some time.

It was reported that Wangiri originated in Japan. It means "one ring and cut".' It is a fraud that affects millions of users globally.

Wangiri is said to be one of the top five fraud methods used by scammers around the world.

The report said it is a significant financial risk for phone companies and end users, who lose billions each year to such scams.

Check Point Software Technologies Ltd said more than half of the world's population, or 4.62 billion people, use social media, which has become part of their daily lives.



Tricks of the trade: The Wangiri scam is a phone call fraud method that affects millions globally.

While these platforms can be fun and a great way to share experiences with friends, they also present a potentially dangerous cyber security risk, it said.

It highlighted four major risk factors that everyone should bear in mind to stay safe while using social media.

Firstly, don't share your personal information. Use different passwords to minimise damage if you are a victim of an attack.

Secondly, watch out for unsolicited password reset emails. By clicking on them, cybercriminals can get access to your entire account. Avoid it at all costs.

Thirdly, cybercriminals often use links to redirect users to malicious sites, it said. These links can come in the form of innocent looking emails or SMS.

Don't click on them. Instead, use your usual browser to check for any messages.

Check Point said another trick attackers use to steal your data is to change a URL to make it look like the genuine article. Check the URLs by making sure that the website has an SSL security certificate. If so, you will see the letter "s" in the address bar and it reads: *https://*.

"Thanks to technology, any confidential information sent between two systems is protected and this prevents cyber criminals from being able to access the data being transferred, including information that could be considered personal," it said.

Scams come in many ways, be it via phishing emails, social media, SMS, WhatsApps messages and so on. However, there are also scammers just ready to pounce on you when you post items for sale on social media sites.

Recently, Wahida (not her real name) posted the sale of her second-hand cooker on a social media platform. The mistake she made was she posted her mobile number.

Within minutes of posting, she was inundated with WhatsApp messages from people wanting to buy the cooker. She thought it was her lucky day.

Ironically, none of the interested buyers wanted to negotiate on the price. They were more than willing to pay her immediately and arrange pick-up the next day. They just wanted her bank account details.

What she noticed was that the pattern of questioning was similar and some of the numbers were not locally registered.

There are many other scams and a popular one is when you get a message saying you have used your credit card and the transaction is a big amount.

It is natural to panic if you did not make such a purchase. The obvious thing one will do in this situation is to call the number provided in the message, only to realise it is not your credit card or bank number.

No doubt a phone is a necessity in this day and age. But it also exposes us to a lot of dangers. Be on the alert and avoid giving out your personal and bank details to anyone.