PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: 57 fraud calls and text messages as of June this year
Publication/Portal: The Star
Date: 12 August 2018

Language: English
Section: Focus
Page: 16

57 fraud calls and text messages as of June this year

YOU have probably experienced it, or know someone who has.

A person pretends to be from a bank and calls you to settle an outstanding payment.

In the process, the person asks for some financial information or credit card details.

Or, you receive a text message saying that you won a contest. But to collect your prize money, you will have to divulge personal information.

Using such methods, scammers have found ways to deceive their victims into transferring large sums of money, or gaining access to sensitive information.

It's not unheard of, and despite numerous reports of it, fraud calls and messages are still persistent today.

Because they can be so convincing, many still fall victim to such tactics.

As of June this year, 57 cases of spam calls and text messages were received by CyberSecurity Malaysia (CSM).

In 2017, the cases totalled to 88, with most or 76 cases being spam calls and WhatsApp messages.

Twelve of them were fraudulent SMS messages.

CSM chief executive officer Datuk Dr Amirudin Abdul Wahab says cybercriminals have up the ante in such cyberscams.

"The technology used to deceive victims is constantly changing and it can be difficult to trace it back to the source," he says.

And despite warnings by banking institutions and media reports, the public still lacks awareness on cybersecurity.

The usual tactics employed by spam callers involves using a caller ID spoof, so that the call appears as though it is from a real bank.

The fraudster would already have details of the victim like their full name, IC number and address.

The victim would be informed that the purpose of the call is to collect outstanding payment for purchase of goods or services charged to their credit card.

"When the victim denies having such a credit card or performing the transaction, he or she will be asked to contact Bank Negara Malaysia (BNM) for verification.

"The victim calls the number given and will be greeted with an automated attendant which identifies the call to BNM, and is subsequently transferred to a person claiming to be from the central bank," says Dr Amirudin.

The fraudster then obtains details from the victim such as credit card and banking information to conduct illegal transactions..

"They may also trick the victim into performing transfers such as through an ATM machine to a designated account given by the scammer to avoid legal action for the supposed outstanding payment," he adds.

Another common modus operandi is to convince the victim that he or she has won a contest.

The recipient will be requested to go the nearest ATM machine to register for online banking on the pretext the prize money will be transferred online.

The scammer guides the victim on steps to register. In the process, the scammer's mobile number is also registered to receive the transaction authorisation code (TAC).

"After registration is complete, the fraudster has the victim's personal information and can siphon funds from his or her account," Dr Amirudin explains.

To avoid being a victim, he urges the public to ignore such calls or hang up immediately.

"Verify the claims through your bank's official channels.

"If you come across such calls, change your password or PIN of all online accounts that may have been compromised," he advises.

Victims should also lodge a police report for further investigation.

Those who wish to report cybersecurity incidents can also contact the CSM through its Cyber999 Help Centre at 1-300-88-2999 (office hours) or its 24-hour emergency hotline 019-266 5850. For more information, log on to *www.mycert.org.my*