



Headline: You've Been Scammed!
Publication/Portal: Smart Investor
Date: 1 April 2021

Language: English
Section: N/A
Page: 54 & 55

MAC/APR 2021 LIFE HACKS

YOU'VE BEEN SCAMMED!

Here is some simple actionable advice that you can put into practise right away to safeguard yourself from becoming another scam statistic.

In this age of mobile phones and the Internet, we seem to be bombarded by spam calls, and our privacy is being infringed upon more and more each day.

You've probably received tonnes of WhatsApp or text messages luring you into online gambling, and a bunch of phishing emails that is clogging up your account. Technology is changing so rapidly and sadly this has empowered criminals to find new ways to tempt, cheat and steal.

The Macau Scam for example, which starts with a phone call from someone pretending to be an officer from a bank or a debt collector, has been the No.1 scam in Malaysia for the last couple of years.

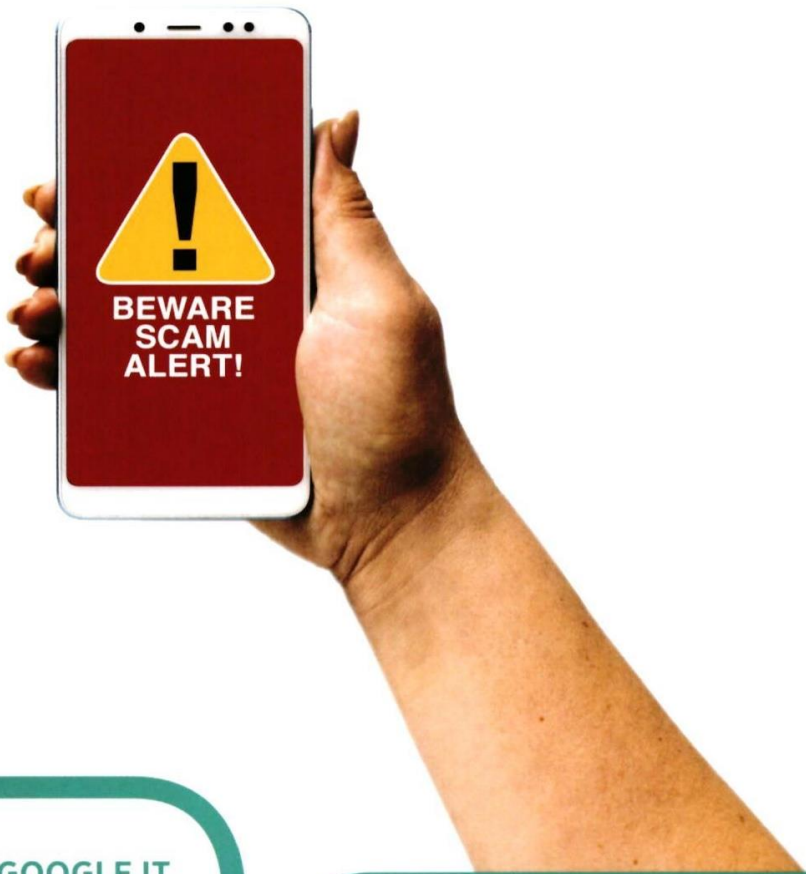
You may think that only senior citizens get duped this way, but the truth is scammers are preying on everyone. Even a manager of a banking agency lost more than RM1.97mil when tricked by a such a syndicate last May!

Why do people still fall for these tricks? Scams usually succeed because they sound like the real thing. Scammers create believable stories that convince you to give them your money or personal details.

But a key thing to remember is that scams will not work without your participation! The best way to safeguard yourself from falling prey is to start educating yourself. Here are some tips to get started:

Be alert! Scams are rampant, so keep up to date with the news on how scammers are operating. Always be on your guard when you're dealing with someone you do not know, whether it's over the phone, by email, on a social network or in person.

If you do get scammed, be sure to lodge a report with the police as well as the relevant agency (eg for cybersecurity issues, you can go to www.cybersecurity.gov.my or call 1-300-88-2999; if it's a matter related to Bank Negara, you can call 1300-88-5465 or email bnmtelelink@bnm.gov.my). Remember as many details as you can, including dates and times that calls or messages were received, and details of the key persons that you dealt with. To file a police report, you can contact the Commercial Crime Investigation Department Bukit Aman Police Station (rmp@rmp.gov.my) or go to the nearest police station.



GOOGLE IT

Check to see that who you're dealing with is a legitimate entity. Be cautious of companies that only use yahoo or Gmail etc. as email addresses. Never click on suspicious texts, pop-up windows or attachments in emails if they come from a strange source.



NEVER SHARE PERSONAL DETAILS

Keep passwords and PIN numbers in a safe place. Try memorising them and use phrases that are not common or easy to guess. Change your passwords frequently. Be very careful about how much personal information you share on social media sites; for example, children's and parent's names, or what school you studied at. Scammers can use this information to create a fake identity or to target you with a scam.



CALL BACK

If you receive a call from a bank, police station, phone company or tax department, say you'll call back. Companies that only disclose a cell phone number (or an overseas number) are often associated with fraud. Look up the contact yourself and call to check if the call was bona fide. If the person on the line tries to dissuade you from doing this, chances are it's a scam!



GET AN APP

There are various apps that can help you identify potential fraudsters, such as Truecaller, a smartphone application that has features of caller-identification and call-blocking. Choose a credible antivirus for your computer too, one that has basic security solutions but is also capable of protecting against hacker attacks and fraud.