



Headline: Scammers have a field day with more people on the internet

Publication/Portal: Focus Malaysia (online)

Date: 15 April 2020

Language: English

Section: -

Page: -

Scammers have a field day with more people on the internet

ASIDE from pummelling the economy, it appears that the Covid-19 situation has spawned a series of scams that come in varying forms.

Just yesterday, AirAsia Group warned the public of a scam on Facebook that linked its founder and group CEO Tan Sri Tony Fernandes' name to a fictitious foundation offering opportunities to assist in projects in exchange for its membership.

People are spending more time online during the movement control order (MCO) period and are becoming more exposed to these social media scams.

Other examples include the face mask sales scam that promises delivery of the limited product to victims on Facebook and Instagram as well as chat apps like WhatsApp and WeChat only to pull off a disappearing act once payment is made.

There are also scammers who try to lure people into giving out their personal details by offering assistance in withdrawing EPF savings on social media platforms. Under i-Lestari Withdrawal programme, EPF members can withdraw a maximum of RM500 a month for 12 months from May 1.

According to Bukit Aman Commercial Crimes Investigation Department (CCID) director Commissioner Datuk Seri Mohd Zakaria Ahmad, scammers are using new tactics to trick victims. He said a new *modus operandi* was found following six police reports filed in April.

Zakaria said scammers would tell victims to download a beta testing app on their handphone and then ask them to click on a link that led to a fake Bank Negara page. They were then told to fill in their particulars in an online form, including bank details.

The scammers will then withdraw the money from the victim's account before instructing the victim to delete the form. He said six such cases were reported, with losses estimated at around RM295,350.

When asked if scammers become more active during a crisis situation, Federation of Malaysian Consumers Associations (Fomca) CEO Datuk Dr Paul Selvaraj said scams have always been on the rise regardless of the situation.

“These scams are structured according to current themes that struck people’s emotions but generally there have always been a lot of scams. People are also spending a lot of time on the internet these days.

“The government has given an assurance that face masks are available but not a lot of places have them, hence the panic. People should purchase these on legitimate websites, not on Facebook,” Paul said.

According to him, what we need to do is keep educating people on the matter especially during this crisis situation as people are worried and vulnerable.

“Check on official sites if you have any doubt and all these bodies have their own official sites. Check on SSM (Companies Commission of Malaysia) to make sure that the company you’re dealing with is legitimate.

“Prevention is difficult because oftentimes it’s a hit-and-run situation whereby the perpetrator is long gone before you realise it’s a scam and the age of the internet is making it easy for them to hide. Local authorities should work with consumer organisations to educate the public and build awareness as the best protection is self-protection,” said Paul.

According to Wong & Partners financial services partner Wong Sue Wan, there are a number of pointers to keep in mind. First, recognise that scams exist and be vigilant. If an offer is too good to be true, it probably is and to consider falling back on service providers or sellers you are familiar with.

Secondly, keep your devices and passwords secure, including reviewing the privacy and security settings on your social media networks. And lastly, be wary of any request for payment or access to your personal details.

Although these are not exhaustive, Wong said they serve as a good reminder when receiving communications on a deal that is too good to pass up.

“In the unfortunate circumstance that money has been lost or personal information has been provided to a scammer, there may be no recourse. But certain steps should nevertheless be taken to limit the damage.

“There is no one size fits all in terms of action to take, and would vary depending on the circumstances. For example, contacting your financial institution to request a halt to the transaction; changing your password if your device or account has been hacked or infected with malware; and lodging a report with the relevant authorities which may be able to trace the perpetrator,” says Wong.

Scams target everyone — regardless of age, background or income level. It preys on a person who may have let down his/her guard and when he/she least suspects it (eg, by making the “offer”

or the communication seem just like what one would expect to receive from the sender or regulator).

“It is not necessarily more prevalent at this juncture, but the chances of it being identified now or coming across a scam now may be higher because the public is spending more time on certain websites or devices,” explained Wong. — April 14, 2020