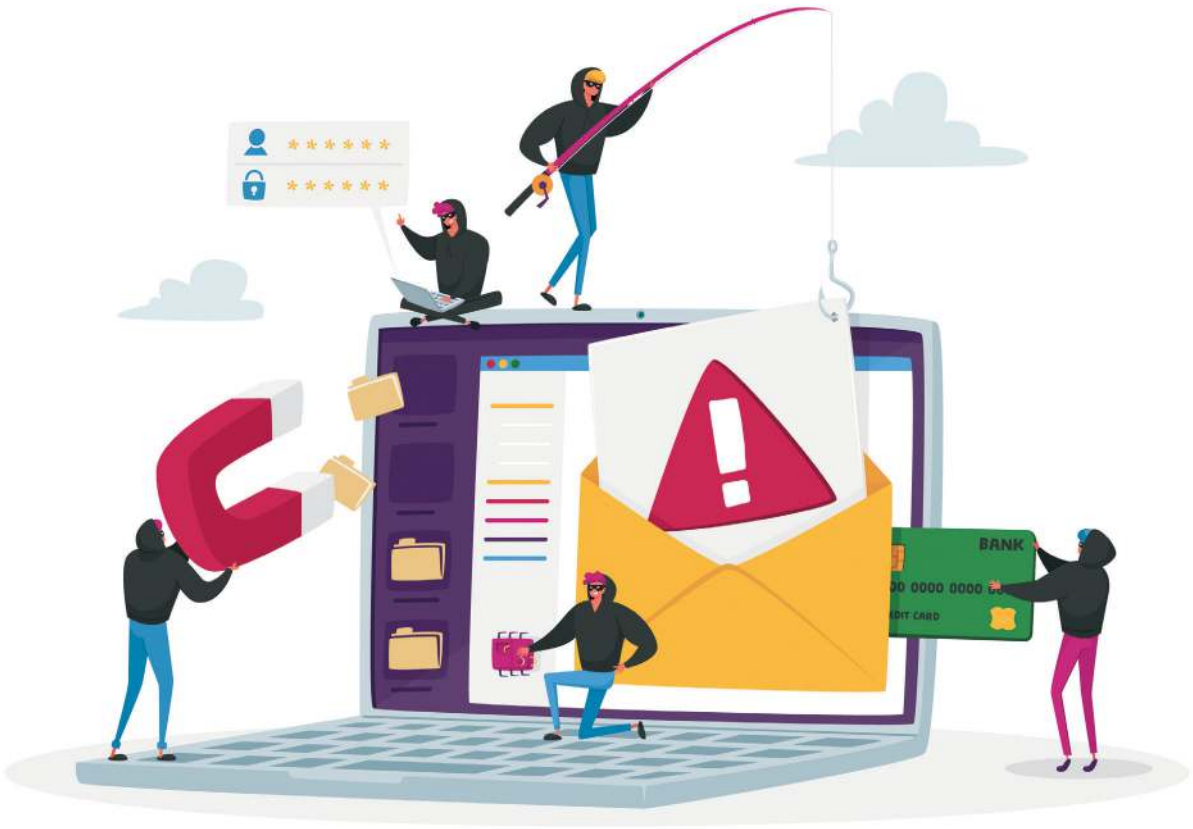

AVOIDING INVESTMENT SCAMS

What you should look out for and how to not fall for these malicious schemes.

By CW Yap

The economic impact brought on by Covid-19 has led many people into financial distress. Those looking for quick gains could easily fall into investment schemes that take advantage of their desperation and fears. Some of the victims might use all of their life savings or even obtain bank loans to participate in such schemes.

For the perpetrators, their goal is simple: profit from the plight of their victims. While the stealing of private information and hard-earned savings are not new, such investment schemes are regularly updated and amended so as to portray a look and feel of legitimacy.

People should educate themselves about the investments they are considering. Perhaps, start with being mindful about content and marketing scams. Here are some useful tips that help with identifying new scammer methods:

TREND #1: MARKETING GURU SCAMS

Have you ever received advertising or sponsored content in social media that features the following:

- A young man in an 'expensive' two-piece suit with fancy watches and supercars
- Seasoned businessmen casually showed off their recently earned millions

Both are professionally produced with the goal of enticing unsuspecting audiences. These videos and infographics feature phrases like "Learn from the best!", "Get rich fast – here's how!", and – to address the new normal, "Overcome these challenges like a winner!"

Ironically, the main source of income for all these self-declared big return-earners is the very snake oil they sell as their bona fide formula for success. While this foul tactic may seem

easy-to-spot, it has already established a long-standing following from easy-to-scam victims.

To attract potential targets, they show-off prospective opportunities and offer more content with a discount. Once convinced, the audience is then pulled into a deeper scam.

Here are some tips to consider when you come across such materials:

- Look out for the promises that sound too good to be true
- Check the backgrounds of high-rollers who promote this and how they sell their materials
- Report these scams to social network administrators and email providers

TREND #2: CRYPTOCURRENCY SCAMS

Coming in close second is another trend-jacking attempt – cyber scams that try to look legitimate. This is now commonplace in the cryptocurrency sector and have snared plenty of victims. With bitcoin, ethereum, and meme-coins, like dogecoin, being widely promoted as financial safehouses, especially when top blockchain currencies have reinforced value against the US dollar and euro, many jumped onboard. What is worse is that they do it without any due diligence.

These people are easy targets to con with half-truths. Those who run fake blockchain token exchanges may even use edited images of figureheads such as Elon Musk or Jack Ma, to project how these billionaires are "promoting" cryptocurrency. Examples of messages include "Earn big on cryptocurrency!" or "Elon Musk is investing in cryptocurrency – Join now!"

The best thing anyone can do when seeing such content is:

- Read up and research everything using trustworthy news sources
- Register and learn with platforms that are approved by the Securities Commission Malaysia

"It is no secret that your private information is no longer confidential thanks to various global data thefts and accidental leaks."

- Always refer to real facts that global regulators and banking authorities have produced or are using as they are paid to do the proper research and provide the results for free – those with malicious goals are asking targeted victims to pay for their fly-by-night content.

Side-tip: Always keep your digital wallets close and use a secure password with additional layers of protection such as PIN numbers or secondary questions to ensure no one can access it.

TREND #3: VIRAL FAKE NEWS THAT CAN PHISH AND USE BEHAVIOURAL TRACKING

It is no secret that your private information is no longer confidential thanks to various global data thefts and accidental leaks. The dark web is full of ongoing transactions whereby personal data is traded like a busy wet market. With such data easily brokered, scammers can dig up private details as well as activities and behaviour that can be exploited.

The usual tactics include calls from various government agencies or banks that sound and feel real. Attempts on data theft includes asking for personal identification, details on secret questions and answers, and even PINs and passwords. They even act as victims as part of the ploy to ask for passcodes that are sent to targeted victims by mistake.

Another trick is to create and share fake news that has malicious code attached to it. This is then used to track the person who shared the content and from what device. Such attack strategies generally obtain user profiles that have been sold on the dark web and with records of additional information, such as the social networks that they are active in.

For those who believe they are targeted, the critical things to do are:

- Check and make sure to only use alpha-numeric with symbols for passwords and turn on two factor authentication (2FA) to ensure hackers cannot easily access any private data
- Be mindful of content, calls, and messages from numbers that are not listed in your phonebook, and always double check with real news sources if the content is real
- Always be weary when strange requests for personal data are made – the better response is to check with official channels to clarify if such attempts are genuine

BEING MINDFULLY AWARE

While all these tips are aplenty everywhere, why are there still many victims of cyber-crime? Businesses must be proactive about cyber-security plans and be consistently updated. That includes reinforcing best practices and monitoring upcoming security trends and threats.

Always do the following before making an investment decision:

- While this is not the most definitive guide, it is a good reminder to always ask if a winning formula sounds like it is "too good to be true".
- Verify purported facts with proper authorities and regulators. SI