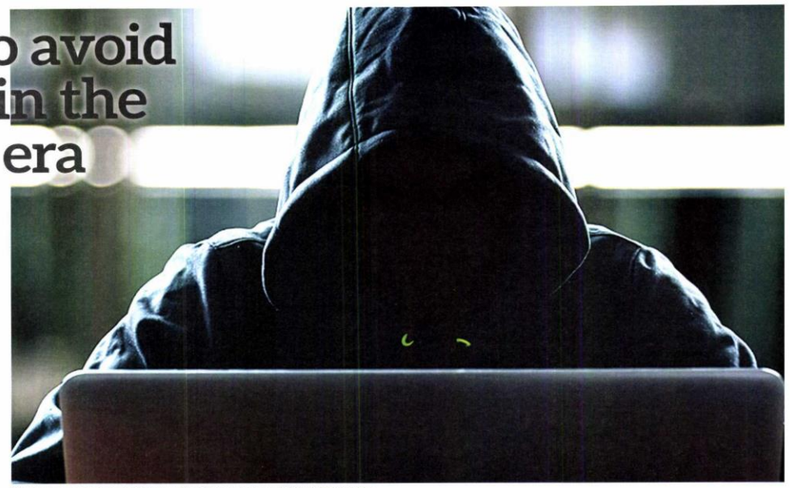
PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: How to avoid scams in the digital era
Publication/Portal: Focus Malaysia
Date: 15 June 2019

Language: English
Section: Income+
Page: 25

How to avoid scams in the digital era

- **Ensure** the company is regulated and has valid licences from authorities
- **Although** millennials are familiar with all things digital, they may be too trusting and are constantly on their smartphones connected to unsecured public networks



Many scams are operated by organised groups across different countries

By **Jo-Ey Chee**

Scams have evolved to become more sophisticated over the past few years, in tandem with advances in technology.

The digital age has only made it easier for scammers to reach millions of consumers in an instant.

Malaysians are not exempt and have increasingly suffered losses from online scams since 2017, according to news reports.

At the rate things are going, it would be quite naïve to think that you will never be at risk of being scammed.

Someone pitches to you a deal that sounds too good to be true. What will you do? Even if you had chosen to walk away, there are other types of scams that can still sneak up on you under pretences like surveys and virus.

A survey report showed that Malaysians are most susceptible to internet scams compared to neighbouring countries.

In 2017, Bukit Aman released a list of 27 companies on its radar for investment fraud. These companies, which had been monitored since 2013, were believed to have duped at least 1.7 million victims of an estimated RM4.45 bil.

Among the companies being monitored are Crude Palm Oil Investment Scheme, Highway Group Resources, Federal Reserve Chicago Bond, DBI Housing Scheme, Tok Belagak Gold Investments and Century Dynasty.

Scams are everywhere. They target everyone regardless of age, gender and background.

As financial relationships become more digital, we too become more vulnerable to online scams.

There is also the misconception that millennials are less vulnerable to scams because of their digital knowledge.

The truth is they are just as susceptible to scams as any other consumer. Social media platforms like Instagram are roaming grounds for scammers.

Despite constant reminders, financial scams are seemingly not going away anytime soon. So how do you protect yourself against them?

Those who are more willing to entertain unsolicited calls pitching investment sales ideas are at higher risk of being scammed

Who is more susceptible?

People who are more likely to fall for scams tend to be more of a risk taker. They place more focus on the potential of high returns and less on the risks.

They also overestimate their ability to back out of a suspicious offer. What they have overlooked is the possibility of being identified by scammers, who may bombard them with emails or calls once they have responded.

Those who are more willing to entertain unsolicited telephone calls and email pitching investment sales ideas are also at higher risk of being scammed.

They also do not learn from past mistakes and might pursue unconventional investment opportunities even after being scammed.

They get excited about the idea of investing in "backdoor" schemes. It is a given that they are also attracted to investment schemes that promise exaggerated returns.

On the other hand, people who are quick to delete junk mail, spam email and stop calls are less likely to fall victim.

There is no such thing as being too careful when it comes to scams. Many scams are operated by organised groups across different countries.

A robocall may appear on your caller ID as if it's coming from your area code after the origin of the call is rerouted but in fact it could be from someone overseas.

Don't be emotional

How often do we find ourselves regretting an emotionally-driven decision?

Continues next page

Scams from 'Macau' and 'Chicago'

THE most rampant investment scams in Malaysia are:

• Macau scams: These are categorised as telecommunication fraud. The scam works in various ways – either via a phone call to "lucky draw winners," ransom demands for purported kidnapping, and spoofing, where the syndicate members pose as police personnel, Bank Negara officials, or even bank officers.

A victim is usually contacted by an individual posing as a police or bank officer informing the victim that he or she is wanted for a criminal offence such as money laundering or funding terrorism. This scare tactic is used so that the victim becomes desperate and will immediately transfer money into the fraudsters' account to erase his record immediately. Don't panic if you receive such calls. Instead call Bank Negara or your bank and do not call any number given to you by the caller.

• Mecca Investment Scam: Here, a syndicate lures individuals into investing in hotel rooms in Mecca. The investment for each room is RM3,500 and is touted as "shariah-compliant". Investors are promised profits of up to 360% a year. The scam is also known as Mecca Fund Global.

• Federal Reserve Chicago Bond Scam: This is a fraudulent investment scheme which operates under the name "Federal Reserve Chicago Bond". It promises very high returns on investments. It is estimated that some 7,600 individuals have fallen victim to it and have lost about RM90 mil.

Scammers play on target's emotions

From previous page

Scammers have a way of targeting certain victims and know how to evoke a certain emotional reaction from their intended victims.

Emotions cloud our judgment. So, always make sure that you have your emotions under control and be conscious of your emotions.

Always seek opinion from people you know and trust. Although millennials are familiar with all things digital, they may be too trusting.

They are constantly on their smartphones connected to unsecured public networks. They also tend to do more financial transactions over the phone that involve giving away personal banking details like passwords everyday.

Avoid logging into financial records, accessing bank accounts and making purchases online when using public Wi-Fi.

How to avoid scams?

Adopting a preventative mindset helps you stay away from scammers lurking online and offline.

Believing that you aren't likely to be scammed will only put you at greater risk than others.

Do not let others use your bank account even if it's your close friends or relatives. There have been cases where people unknowingly allow others access to their bank accounts which were then used for illegal activities.

Freelancer Ellyn Yeo had a close brush with scammers. "I was contacted one day by my bank asking if I had booked any hotel room using my card overseas.

"I checked and my card was in my wallet. After I told them that I did not perform any such transaction, the bank cancelled my card and gave me a new one," she shares.

Always be cautious when it comes to sensitive financial information and never reveal your PIN to anyone via unsolicited phone calls, text or email.

It goes without saying that you should also never click on links provided in emails even if it appears to be from your bank or other reputable organisations.

If you receive calls from people claiming to be from Bank Negara Malaysia (BNM) asking for your credit or debit card or banking details, end the call immediately.

Get-rich-quick schemes

Beware of get-rich-quick schemes and internet investment schemes that sound too good to be true.

If you want to invest, please ensure the company is regulated and has valid licences from the authorities such as BNM, Securities Commission and the Ministry of Domestic Trade and Consumer Affairs.

BNM updates a list of unauthorised companies and websites which you can refer to.

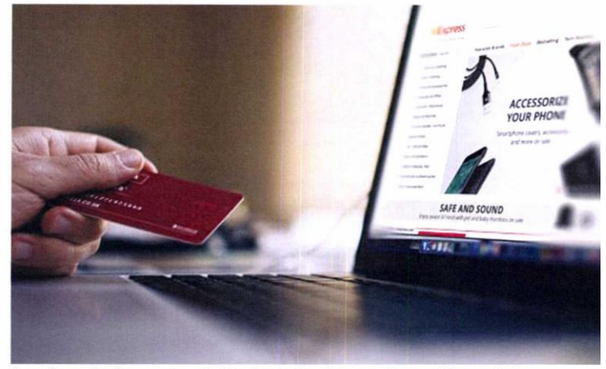
Be wary of any investment opportunity on the internet that is not in writing. Should you choose to invest, remember to keep copies of the investment and all communications.

One of the biggest red flags of suspicious investment schemes is a promise of high and guaranteed returns.

There is no such thing as guaranteed returns in investment. If you are getting consistent returns at 15% to 20%, you should be alert.

Lack of financial awareness also plays a role as to why consumers continue to become victims.

Make sure you do your due diligence as an investor and that you understand how the schemes work. Do not put all your money into one investment scheme.



Do not forgo safety for convenience. Avoid performing financial transactions on public networks

Business owner Lee Chee Chong says: "I was once approached to participate in investment activities that promise guaranteed returns at unusually high rates within a few months.

"Since it was recommended by a close acquaintance, I decided to give it a try out of curiosity. Of course, I ended up with nothing and even lost the few thousand ringgit I invested."

Based on a survey report, 67% of Malaysians use debit cards for cashless transactions. It also reveals that online banking is the favoured choice of making payments.

Our lives are also increasingly revolving around our mobile phones and app-based services like e-hailing and online shopping.

Suffice to say, digital wallets and online financial services seem to be the future.

Security and fraud concerns

Malaysians cite security and fraud concerns as the major hindrance to using mobile wallets. According to news reports, some 50% of them are wary of potential security issues that come with using this mode of payment.

As financial relationships become more digital, fraud cases involving the use of payment networks and data theft have also increased.

When using public Wi-Fi, there is always the risk of exposing personal information to scammers. As such, use your credit card only when you are connected to secure internet services and on trusted websites or apps.

Do not forgo safety for convenience. Avoid performing financial transactions on public computers and networks. Protect the sensitive information stored on your computer by installing antivirus, firewall and spyware protection.

Remember to turn on the auto-updating feature to make sure the software is always up-to-date.

Read the website's privacy rules before supplying sensitive information like passwords. Make sure the website uses encryption. Check if there is a lock icon on the left of the web address. This is to ensure that the information you're entering is encrypted and protected from cybercriminals.

Be wary of people who approach you on social media and messaging apps offering financial organisations even if they claim to be from a reputable organisation. You can always do your own research or contact the company directly via its official website to confirm.

You can also download mobile applications that help block spam calls and messages to avoid falling for scams.

Different types of scams

Illegal Internet Investment Scheme
How it's done?
- Operators of illegal internet investment schemes lure unsuspecting victims to make on-line investments or receive investment advice online, by offering investment opportunities above a market rate of return and will claim that their schemes are at zero or very low risk.
- When questioned, most illegal operators will either claim to be foreign operators that do not require licences from Malaysian regulators to operate their business, or claim that they already have the appropriate licence from relevant authorities/regulators.
- Unsuspecting victims of these schemes would be enticed as operators will pay them high returns at the initial stage and this is used as a tactic to lure and recruit new investors.

Illegal Foreign Exchange Trading Scheme
How it's done?
- Illegal operators usually operate on a small scale and claim they can provide remittance services efficiently, without the need for any documents or identification. By engaging in these transactions, customers run the risk of being cheated and their funds may never reach its intended destination.
- Illegal operators usually target job seekers by placing attractive advertisements to lure prospective employees to join the company, after which they use them to solicit for new investments.
- Illegal operators usually portray a professional and reputable image, a high-tech office layout and advanced IT facilities, such as a LCD screens displaying movements in exchange rates to provide the impression that a legitimate and real business is being conducted. These facilities are merely a false front.

Unauthorised Withdrawals
How it's done?
- In most cases, victims of unauthorised withdrawals had received an unidentified SMS (from fraudster) to inform them that they have won a cash prize.
- To claim the promised cash prize, the victim is informed that they have to open an internet banking account.
- The victim then contacts the fraudster and the fraudster will provide a step-by-step guide on how to register and activate their internet banking account using the ATM terminal.
- At point of registration at the ATM terminal, the victim will be given an internet banking personal identification number (PIN). The fraudster will ask the victim for this PIN and use it to create an internet banking account for the victim.

Unauthorised Use of Credit/Debit Card
How it's done?
- Victim receives SMS or telephone call: Requesting victim to confirm a credit card transaction for the purchase of goods or services purportedly charged to the victim's credit card.
- When victim calls the telephone number provided in the SMS, the fraudsters identify themselves as agents of a commercial bank, and again, ask the victim to confirm whether the credit card transaction had taken place.
- When victim informs the fraudster that he has no such credit card or transaction, the fraudster will advise victim to lodge a report with BNM's "Unit Kad Kredit Palsu", or with the commercial bank's "credit card management department". The fraudster will provide the victim with the telephone number for the "Unit Kad Kredit Palsu".

Misuse of BNM & Senior Officers' Names and Positions
How to Protect Yourself?
- If someone claiming to be from Bank Negara Malaysia calls you and talk you into joining any investment schemes or suspected fraudulent activities, you should end the call immediately;
- You may also verify the claim or identity of the said 'Bank Negara Malaysia officer' by calling the bank directly.
- Be sceptical - Bank Negara Malaysia officer will never call you to promote any 'too good to be true' investment schemes; and
- In case an arrangement has been made, keep copies of all the communication records and documentation.

Source: Bank Negara Malaysia