PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: ANATOMY OF A SCAM
Publication/Portal: Smart Investor
Date: 1 April 2021

Language: English
Section: N/A
Page:6

FEATURE |

ANATOMY OF A **SCAM**

Scammers are quick to take advantage of consumers' financial vulnerability following the enforcement of the MCO.

By **Bernie Yeo**

The Covid-19 pandemic has significantly changed the way we work and do business. While many people have adapted to the 'new normal', countless others have lost their jobs or accepted pay cuts due to the Movement Control Order (MCO), which was enforced in March 2020 to contain the spread of the coronavirus.

The ensuing financial vulnerability – coupled with increasing dependency on technology – is something financial fraudsters were quick to catch on to and take advantage of. As a result, there has been a surge of reports about Malaysians falling victim to financial frauds, with losses amounting to millions of ringgit.

Bank Negara Malaysia defines financial fraud as an illegal act involving complicated financial transactions. It falls under civil law and is usually conducted by business professionals with specific knowledge and with criminal purpose.

For example, statistics provided by the Ombudsmen for Financial Services (OFS) have revealed that 394 disputes relating to unauthorised use of credit/debit cards and internet banking were received in 2020 – a whopping increase of 145% compared to 161 cases in 2019.

These disputes were largely related to unauthorised transactions arising from scams as well as unauthorised online transactions.

However, people working remotely from home is only one of the many factors that contribute to the increase of financial frauds and scams in Malaysia, says Ombudsman for Financial Services chief executive officer Marina Baharuddin.


Marina Baharuddin

"Working from home is only one of the many factors. There are many other contributing factors, among them age, human behaviour, fast growing techniques used by fraudsters such as phishing, mental fragility, as well as the desire for quick financial remedies by those in desperate need for money as their own livelihoods have been affected by the pandemic," she tells *Smart Investor*.

Springboard to make money

In the wake of the pandemic as well as the lockdowns imposed by many countries, attackers of all kinds sought to capitalise on people's fear about the disease. As such, most of the phishing scams related to Covid-19 have been launched by cybercriminals using the disease as a springboard to make money.

"According to Kaspersky's 'How Covid-19 Changed the Way People Work' survey, more than a quarter (27%) of the survey respondents say that they have received malicious emails related to Covid-19 while working from home," says Kaspersky General Manager (Southeast Asia) Yeo Siang Tiong.

Yeo Siang Tiong

Kaspersky's telemetry also shows that, the number of scams related to social payments increased five-fold in 2020 compared to the same period in 2019. Fraud emails of this kind, explains Yeo, offer various financial assistance, surcharges, allowances and other types of payments.

"On a larger scale, we have detected 360,000 unique malware samples every day in 2020 on average, up by 5.2% compared to the previous year. This was influenced mostly by a large growth in the number of Trojans and backdoors, a 40.5% and 23% increase, respectively," he continues.

Trojans are malicious files capable of a range of actions, including deleting data and spying, while backdoors are a specific type of Trojan that gives attackers remote control over the infected device.

Financial scams and how to avoid them

If you believe that you are impervious to financial scams, think again. Fraudsters are an ever-present threat and work around the clock to steal your personal information and exploit your weaknesses to gain access to your money and accounts.

According to OFS's Marina, one of the most common types of financial scams is phone scams. This includes Macau scams where potential victims are informed that their identity was fraudulently used for credit card applications.

In order to void the card, they are required to submit their credit card details as well as the secure password (One Time Password). Consumers are also tricked into revealing their banking credentials as well as the security password.

"In a different scenario, the scammer calls an unsuspecting victim pretending to be from a legitimate source, disguising themselves as officers from the Royal Malaysian Police (PDRM), Bank Negara Malaysia (BNM), or the Malaysian Anti-Corruption Commission (SPRM), for example, as a means to try to convince the target into divulging their card details and One Time Password (OTP)," Marina explains.

Another common type of financial scam is internet banking scams, among them Transactional Authorisation Code (TAC) scams. These occur when fraudsters log onto the victim's internet banking account illegally, and then contacts the victim on the pretext that they wrongly registered the victim's hand phone with the bank.

This explains the request for TAC being sent to the victim's hand phone. The unsuspecting victim reveals the TAC which enables the fraudster to perform fund transfers from the victim's account.

"Consumers receive calls or text messages informing them that they had won an e-wallet lucky draw prize. The fraudster would leverage on the e-wallet lucky draw, shopping e-wallet prizes as well as Government e-wallet or cash incentive programmes as an opportunity to dupe and entice victims to click on the link displayed on the text message/online apps.

"The victims are then required to disclose their bank account details to the fraudster in order to redeem the prize," Marina continues.

Fraudsters are also known to use mobile banking apps for such activities where they trick the victim into revealing their banking credentials and the TAC to transfer money from the victim's account to a third-party account and/or to top-up their e-wallet accounts.

Some of the banking mobile app requires only one OTP to bind the device to the apps which then allows all subsequent

Under the Financial Ombudsman Scheme, OFS only accepts disputes related to direct financial losses from unauthorised transactions through designated payment instruments or payment channels such as internet banking, mobile banking, or automated teller machine (ATM), or unauthorised use of a cheque that fall within RM25,000.

"Financial fraud is defined by BNM as an illegal act involving complicated financial transactions. It falls under civil law and is usually conducted by business professionals with specific knowledge and with criminal purpose."

CYBER SCAMS: WHAT ARE THEY

- **Phishing email** appears in your email inbox — usually with a request to follow a link, send a payment, reply with private info, or open an attachment. The sender's email might be tailored to closely resemble a valid one and may contain info that feels personal to you;
- **Domain spoofing** is a popular way an email phisher might mimic valid email addresses. These scams take a real company's domain (ex: @america.com) and modify it. You might engage with an address like "@americas.com" and fall victim to the scheme;
- **Voice phishing (vishing)** scammers call you and impersonate a valid person or company to deceive you. They might redirect you from an automated message and mask their phone number. Vishers will try to keep you on the phone and urge you to take action;
- **SMS phishing (smishing)** similarly to vishing, this scheme will imitate a valid organisation, using urgency in a short text message to fool you. In the message, you'll usually find a link or a phone number they want you to use. Mobile messaging services are also at risk of this;
- **Social media phishing** involves criminals using posts or direct messages to persuade you into a trap. Some are blatant like free giveaways or sketchy "official" organisation pages with an urgent request. Others might impersonate your friends or build a relationship with you long-term before 'attacking' to seal the deal;
- **Clone phishing** duplicates a real message that was sent previously, with legitimate attachments and links replaced with malicious ones. This appears in email but may also show up in other means like fake social media accounts and text messages.

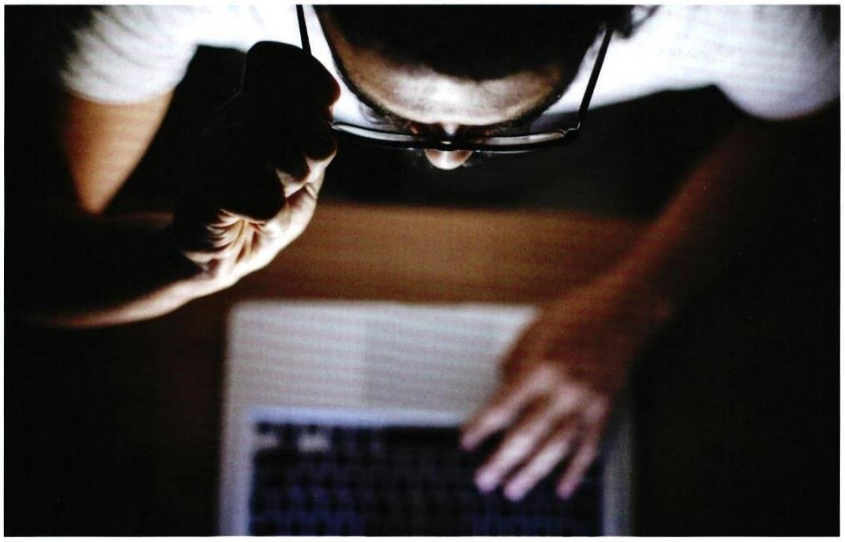
In addition, here are other types of phishing you should be aware of:

- **Search engine results phishing** uses methods to get a fraudulent webpage to appear in search results before a legitimate one. It is also known as SEO phishing or SEM phishing. If you don't look carefully, you may click on the malicious page instead of the real one;
- **Angler phishing** impersonates a customer service representative for a real company to trick you out of information. On social media, a fake help account spots your "@mentions" to a company's social handle to respond with a fake support message;
- **BEC (business email compromise)** involves various means of breaching a company's communications circle to get high-value info. This can include CEO impersonation or pretending a vendor with a fake invoice to initiate activities like wire transfers; and
- **Cryptocurrency phishing** targets those with cryptocurrency wallets. Instead of using long-term means to mine cryptocurrency themselves, these criminals try to steal from those that already have these funds.

transfers or payments without any OTP. The transaction alerts will be sent to the new device and not to the registered mobile phone.

To avoid falling victim to scams, Kaspersky's Yeo suggests a few basic measures to always take with your emails and other communications:

- Think thoroughly before handing over sensitive information. When you get an alert from your bank or other major institution, never click the link in the email. Instead, open your browser window and type the address directly into the URL field so you can ensure the site is real.
- Never trust alarming messages. Most reputable companies will not request personally identifiable information or account details via email or even through phone calls. This includes your bank, insurance company, and any company you do business with. If you ever receive an email asking for any type of account information, delete it immediately and call the company to confirm that your account is OK.
- Do not open attachments in suspicious or strange emails, especially Word, Excel, PowerPoint or PDF attachments.
- Avoid clicking embedded links in emails at all times, because these can be seeded with malware. Be cautious when receiving messages from vendors or third parties; never click on embedded URLs in the original message. Instead, visit the site directly by typing in the correct URL address to verify the request, and review the vendor's contact policies and procedures for requesting information.
- Keep your software and operating system up to date. Windows OS products are often targets of phishing and other malicious attacks, so be sure you're secure and up to



date. This is especially the case for those still running anything older than Windows 10.

Creating awareness

As of late, BNM and the Securities Commission Malaysia (SC) have been upping their game by actively cautioning people to be careful of scams, but this has not stopped people from losing their nest-eggs to fraudsters.

This therefore begs the question: what else is there to be done?

OFS's Marina believes that institutions, consumer associations, and media platforms such as television and radio, have an important role to play in creating awareness about scams. As it turns out, social media is an excellent platform to spread scam awareness due to its vast popularity surge during the MCO period.

"Perhaps more publicity about scams can be made through programmes such as 'Scam alert week'. OFS is also doing its part by sharing articles and scam alerts on our website and social media pages," she opines.

However, despite the best efforts taken by the authorities and media in creating awareness, people are still falling victim to cybercriminals every day.

"Scammers nowadays are very sophisticated, and the current pandemic situation, in addition to the spreading of misinformation and scare tactics, work well to their advantage. Therefore, it is imperative that consumers should always be more vigilant."

"Scammers nowadays are very sophisticated, and the current pandemic situation, in addition to the spreading of misinformation and scare tactics, work well to their advantage. Therefore, it is imperative that consumers should always be more vigilant."

As to what consumers should do after realising that they have been scammed or have shared their banking credentials or transferred money to someone whom they do not know, Marina's advice is for them to immediately contact their bank.

"This is to enable the bank to block the account and to prevent further transactions. A police report must also be lodged as soon as possible, and remember to keep all relevant information and evidence such as text messages and documents related to the scam incident," Marina

There has been an increase in the number cases of companies and individuals which appropriate the Bursa Malaysia name and corporate logo to lend credibility to their unauthorised investment schemes. These are often marketed as attractive opportunities that promise high returns, with potential investors required to click on false websites and scam phone numbers.

Needless to say, it is imperative that individuals only invest with licensed parties only, a point that Bursa Malaysia is only too keen to point out. The company also does not engage third party agents to represent them. Anyone that receives unsolicited communications or comes into contact with agents purporting to represent Bursa Malaysia should contact 03-2732 0067 or email bursa2u@bursamalaysia.com to authenticate this content.

CORPORATE FRAUD

By Crowe Malaysia

Fraud can severely impact an organisation, causing not only financial repercussions but also irreparable reputational damage. As businesses grow bigger, the span of control lengthens and the supervision of staff becomes more tenuous.

Fraud is usually committed in small amounts initially but which grow larger over a period of time. If this fraud is not nipped in the bud, it will gradually grow to strangle the host e.g. cashflow shortages, strangulated balance sheets, poor operating results, etc.

Loopholes and lack of control in a company's system, temptation on the perpetrator due to personal needs or lack of limits on the authority of employees to transact on behalf of the company can give rise to opportunities for fraud to take place in an organisation.

Some of the common types of fraud in a company include:

1. Financial reporting fraud, occurs when companies manipulate their financial statements to show a false financial position and financial results of the company like increasing the profit and net asset position of the company.
2. Conflict of interest. This will render the decision maker not making a sound and independent judgment in the interest of the company that he is acting for. An example of this is a company director who sells his private loss making company to his own listed company.
3. Falsification of documents to hide losses, inflate costs through false invoices, or embezzle money from the company through cheque tampering and false expense claims.
4. Misappropriation of assets. Fraud of this nature can occur due to lax internal controls, lack of supervision of staff and insufficient management oversight.
5. Bribes received by staff from suppliers are like a cancer. It will slowly eat into the profits of a company as costs rise due to unseen costs being charged to the company. Bribery is an issue that has to be eradicated for a company to be run efficiently and profitably.
6. Concealment of assets such as objects and property that can be valued in money can be deliberately kept out of sight of the authorities or contending parties, especially in situations when the defending party is facing claims or undergoing bankruptcy proceedings.

With the rise of online and Internet banking, fraud can especially happen in the areas of procurement and bank transactions. Controls therefore need to be especially robust in these areas and may take the form of setting of limits of authority, for example, cheque signatories, oversight of all staff's work, proper segregation of duties, robust physical controls over the assets of the company, implementation of a standard of corporate behaviour, and use of internal audit function.

SENIOR VULNERABILITY?

A 2017 survey conducted among chartered financial planners (CFP) by the International Organization for Securities Commission (IOSCO), which represents over 150 countries' securities regulators, including Malaysia, found that 70% of them believed that seniors are at greater risk of losing money to fraud or being taken advantage of through unsuitable advice or products. Seniors were defined as those in their retirement age, or close to it.

Common reasons for seniors finding themselves victims of financial fraud included "blind" trust in their advisers or family members, a lack of both technical and financial education, aggressive sales tactics, and pressure from family and peers to commit to certain investments.

These included get rich quick schemes that promised lucrative returns with little or no risk, which could be structured as pyramid schemes, Ponzi schemes, or more simple methods like telephone or email scams.

CFPs from around the world responded to the survey, suggesting that the view of the elderly being more susceptible to financial fraud isn't just restricted to Malaysia alone, and that it is part of a wider global issue that needs to be addressed.

explains, adding that it is generally very difficult to recover the monies transferred as the transactions are done within seconds.

"Consumers who are not satisfied with the outcome after filing a complaint with their bank on their financial losses can approach OFS," she concludes. SI