Media Title : The Borneo Post Sarawak
Headline : Scam alert: How oversharing leaves you vulnerable
Date : 24 July 2023
Section : Home
Page : 10

Scam alert: How oversharing leaves you vulnerable

Nina Muslim

KUALA LUMPUR: Fuelled by a global pandemic and social media, online fraud and scams are increasing and show no sign of abating, even as governments and communities step up efforts to increase awareness among the public.

According to figures given to Bernama by Bukit Aman's Malaysian Commercial Crime Investigation Department, Malaysians reported losses of RM650,329,897 to sale, loan, investment, phone and love scams in 2022, an increase from RM509,881,921.13 in 2021 and RM503,883,501.06 in 2020.

News reports recently quoted Malaysian Communications and Multimedia Commission chairman Salim Fateh Din as saying that the number of cases continues to remain high with 12,000 such cases reported between January and April this year.

A recent survey by Southeast Asian market research and data analytics firm Milieu Insight involving 2,500 respondents in five countries, including Malaysia, found that almost half of Malaysians have been scammed. The respondents were picked at random and representative of Malaysians by age, race and gender.

The July 6 survey found the most common scams Malaysians fall victim to are buying and selling scams at 39 per cent; investment scams at 36 per cent; and phishing spams, where unsolicited messages are received via email or other platforms disguised as coming from a legitimate source, at 35 per cent.

The survey also found victims shared a common belief about scams.

"The thought of 'it will not happen to me' is one of the greatest challenges ... we often underestimate the risk of falling victim to scams," said Sonia Elicia, assistant marketing director at Milieu Insight.

Experts say this belief, where only stupid, greedy and naive people would fall for a scam, makes it difficult for people to develop and practise good and safe habits online. Scams are now very sophisticated and intricate so it is not shocking if one falls for it.

All the experts Bernama talked to said they themselves fell for an online scam in some way or another. They told Bernama there are many common mistakes people make online that could leave them vulnerable.

Oversharing

About three years ago when the pandemic was at its height, Sonia received calls and text messages purportedly from the Singaporean police saying she had technically committed a crime.

They sent her documents with the Singapore police logo on them as proof. They also had her private details which made her believe she was communicating with law enforcement officials. They asked for SG$8,000 (RM27,772) to resolve the issue.

"It was so intricate that I fell for it because they understood my entire background, they knew who my family was, where they lived, that they had a puppy," she told Bernama via Zoom.

She added the scammers might have gotten her details through her social media accounts.

Experts agreed oversharing makes people vulnerable, paving the road to various scams such as Macau and love scams. What makes one popular on social media can also pose a danger to that person.

"It is possible to get everything in detail on social media if, and only if, the person overshares," said Hazwany Jamaluddin of Arus Academy, a sustainable education initiative.

For the most part, people know not to give out their personal details like bank information or addresses. However, online safety does not mean just protecting these details, it means protecting other aspects of personal life no matter how innocuous.

Online safety experts cite three main things that people are too cavalier about when online: photos, locations and personal security.

"I'm very scared of the photo thing because of the children. A lot of young parents create social media (accounts) for their kids saying they want to document their growth or journey from a baby. And they don't think it's a problem," said Kaia Tan from Security Matters, a non-governmental organisation (NGO) that trains people on online safety.

She said it is not safe to post photos of children for fear of inviting unwanted attention.

She added posting photos of young children online is a violation of their privacy which may also affect their future employment or relationships.

"They never think of their kids when they grow up. I don't want to see my naked baby photos when I grow up and I don't want people to see (those photos)," she said.

Hazwany suggested parents blur their children's faces if they still want to post their photos until the children are old enough to take charge of their social media.

She said users also need to be sure there is no private and key personal information visible in the photos, or personal details that can compromise one's safety physically or financially such as identity card number or passport number.

"If the social media account is open to the public, whoever has bad intentions will find key landmarks to find the person's home address or find key information that leads back to the personal details," warned Hazwany.

Location, personal security

Another big mistake is careless location-sharing. The experts said people must be careful when using the check-in feature on social media or enabling location-sharing in their social media settings when they post something.

"If occasionally you want to check in at some places that you think are nice, that's fine. But not like (places that are a part of your) daily routine," said Tan.

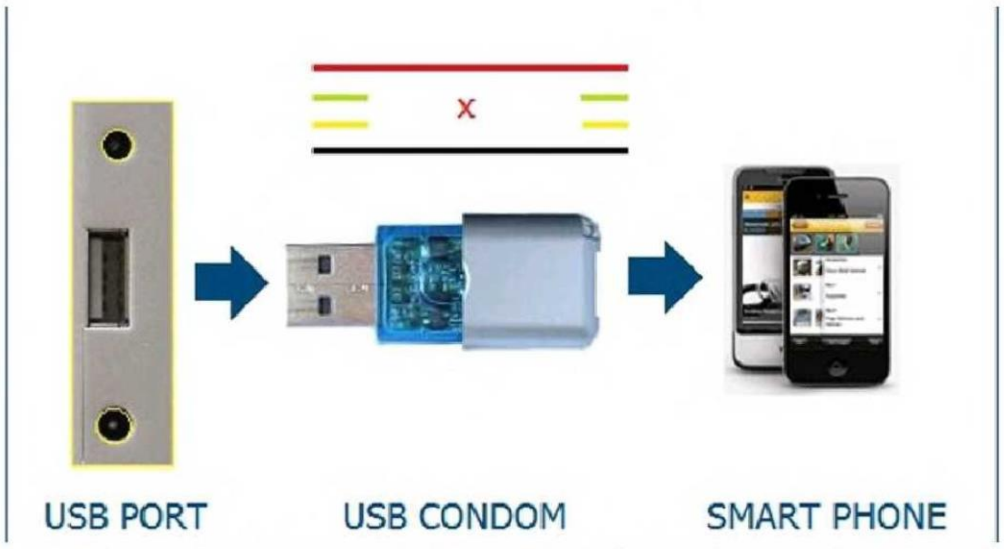
"Like I actually saw some people post 'back at home' and they even check in at their building, telling people (they're) staying there," she added.

The danger is that if users check in often enough at the same places at the same time, people with bad intentions can use it to track them down and cause problems such as in stalking cases.

Tan, who is the founder of Security Matters, also said certain events such as funerals and wakes may cause people to forget about security. Rather than posting publicly the address of the funeral or wake venue, which may be a residence, she suggested inviting people privately or in person.

However, this does not mean no one should ever post anything that shows locations.

Security Matters director of operations Ivan Lai told Bernama many social media users, especially the younger generation, like to share locations when travelling or trying out a new restaurant or hanging out.



People need to use a USB condom when plugging into any public port, like at the airport or a cafe, to recharge their phone battery, says one expert.

"If they want to post their location, they can do it after they leave the place (to be safe)," he said.

He advised users to turn off location-sharing for the app or to use a virtual private networt to mask a person's location.

The experts acknowledge that turning off locations can be a hassle when so many apps such as banking and e-hailing apps recommend location-sharing. But they pointed out that any tech that offers convenience can also put people at risk.

Sharing locations, usually hangouts, is also part of the oversharing that provides scammers and bad actors with plenty of information that can be used against a person.

Hazwany, who also co-founded the cybersecurity NGO Hack/Hackers Kuala Lumpur, described the process as a type of profiling. She said it is relatively easy to profile a person because humans are creatures of habit.

"So whenever we go to certain places, it gives out information for profiling. That profiling will always list back to personal identification such as what community (you belong to), where you hang out, what car you use, who you hang out with," she said, adding that people should be careful who they interact with on social media.

Tips for protection

By now, most people should already be aware that they must not click on suspicious links. Nevertheless, it still happens, according to the Milieu Insight survey.

Sonia said they found that in Malaysia a lot of scams happen by luring victims into phony websites that take their money and sell them nothing. They are also lured into providing personal information that is used for purposes of identity theft or tricked into clicking on links and downloading malware.

"Chief among these are surveys or contests that request personal information, and catfishing in which the scammer poses as someone they are not and befriends the victim intending to take money, personal information or other valuables," she said via email.

She added the top platforms or ways Malaysians get scammed are through social media sites like Facebook and TikTok, usually involving identity theft.

On top of that, the survey discovered one in four Malaysians, mostly older people, were not confident they could identify fake numbers or websites.

There are ways to protect oneself and clean up one's online habits. To identify scam calls, the online safety experts recommend using caller ID apps such as Whoscall and Truecaller. The free versions of both apps collect phone numbers that have been identified as scam numbers and warn users if someone uses the number.

The experts stressed the importance of encryption, which is a process of converting data into code, and being aware of what platforms have it.

WhatsApp and Signal are end-to-end encrypted which means no one other than the sender or receiver can see the message. Emails are usually encrypted from server to server, which means although the company can see the message, no one can see it if intercepted. For end-to-end encrypted email service, experts recommend Proton Mail.

They also said everyone should turn on their two-factor authentication for their social media accounts, keep their software updated and stop using the same password across all accounts.

Since strong passwords can be difficult to remember, Ivan suggested mixing languages to create easy-to-remember but difficult-to-guess passwords such as "Saya suka Kway Teow."

He added if anyone is worried whether their password or data has been compromised, they can check on the HaveIBeenPwned website.

Ivan also said people need to use a USB condom when plugging into any public port, like at the airport or a cafe, to recharge their phone battery.

"Those (ports) can transfer data so you don't know what bad guys do with the port. The ports can install malware in your phone," he said.

One other recommendation the experts gave was to 'be paranoid', saying that was the best way to be as secure as possible online.

"You may think you have everything under control but you don't," said Sonia.

Online safety experts cite three main things that people are too cavalier about when online: photos, locations and personal security. – Photo via www.kaspersky.com