Media Title : The Star
Headline : Scams are like viruses, say experts
Date : 30 December 2023
Section : Nation
Page : 4

Scams are like viruses, say experts

'Users need to arm and protect themselves'

By TEH ATHIRA YUSOF
and CHARLES RAMENDRAN
newsdesk@thestar.com.my

PETALING JAYA: Despite consistent media coverage, including many a front-page story in newspapers, Malaysians continue to keep getting duped by scammers in ever increasing numbers.

It is time for people to arm themselves against this tide with knowledge, preventive measures and common sense, say cybersecurity experts.

Universiti Tunku Abdul Rahman Centre for Media and Communication Research chairman Dr Sharon Wilson said as long as people use a device or gadget linked to the Internet, they are exposed to scam syndicates.

"Vulnerability to online scams can vary based on factors like Internet usage patterns, awareness, and demographics.

"Individuals of all ages should stay informed on online security practices to reduce the risk of falling victim to scams," she said.

As of Nov 30, the reported losses via online crime in the country this year had reached more than RM177mil.

Of these, 8,213 reports were lodged with the authorities while 529 bank accounts – holding a combined value of nearly RM66mil – were frozen.

According to an Ipsos Malaysia survey, more than 50% of victims in the country did not seek help from the authorities after being scammed.

Wilson said there are several types of scam tactics that can be used to target the different age groups.

"Perhaps Gen Z may be vulnerable to job scams and parcel scams, while senior citizens may be vulnerable to investment scams – but no one is spared," she added.

Universiti Kebangsaan Malaysia's (UKM) Cyber Protection and Governance (CPG) Lab head Prof Dr Zarina Shukur said the people who are most at risk of getting scammed are the ones who often rely on technology for their financial transactions.

"Other people who are vulnerable to fraud are those who remain ignorant of the news and awareness raised by authorities on scam syndicates and their ways," she said.

"There are also people in desperate need of financial assistance, causing them to be involved with these activities without much thought on the repercussions."

On ways to prevent getting scammed, Wilson advised users to question and verify any incoming requests for personal information and identify those seeking sensitive information.

Users should check the legitimacy of websites by checking the URL or weblink for spelling errors or unusual domain names, she said.

"Be cautious of emails or messages asking for personal or financial information, especially if they create a sense of urgency. Use trusted platforms and be cautious when making online transactions.

"If shopping online, ensure that the seller does not lure you out of the official shopping platform.

"Call up family members and friends to check if they had made a phone call or text message requesting financial help," she said.

Wilson added that for an extra layer of security, create complex passwords, avoid using the same password across multiple accounts, don't store these passwords on the phone or any technological device, and enable two-factor authentication.

"Keep your operating system, antivirus, and other software up to date to patch vulnerabilities. Regularly back up important data to protect against ransomware attacks.

"Use a secure and password-protected WiFi connection to prevent unauthorised access and avoid public WiFi, including plugging your phone into a public portal using a charging cable," she said.

Wilson said social media users should regularly review and adjust the privacy settings on their accounts.

"Be financially literate. The public must also stay informed about common online scams and tactics to recognise potential threats," she added.

UKM's Prof Zarina said that there are ways to overcome fraud by creating a personal banking policy.

"Firstly, do not trust any schemes that are too good to be true. With a personal policy, you can separate your bank accounts for specific online use.

"For example, do not use your main bank account for online shopping. Instead, have another bank account specific for shopping purposes.

"For those with a main account profile, stick to one specific device for online banking – it could be the computer desktop at home," she said when contacted.

Wilson stressed that it is crucial to alert authorities of scamming incidents because it helps law enforcement understand the scope of the issue, investigate patterns, and take necessary action.

"Increased reporting can lead to better awareness, prevention, and prosecution of scammers, ultimately protecting more peo-

The seven types of scams commonly used to target Malaysians

Ecommerce Scam (most prevalent type in the country)

> Scammers entice victims with offers of low prices for costly goods on ecommerce websites and social media platforms. Victims often left with fake items or nothing.

> Target: Online shoppers.

> What to do: Make purchases from reputable ecommerce merchants and do not be drawn to unrealistic offers.

Macau Scam

> Scammers will randomly make phone calls to potential victims and disguise themselves as government officials and other trusted officials such as bank officers demanding victims transfer money into mule bank accounts provided by the scammers 'for investigation purposes'.

> Target: The elderly, especially retirees, but anyone with a bank account with large funds are vulnerable.

> What-to-do: Hang up the phone upon receiving such calls, do not entertain the caller.

Investment Scam

> Potential victims are enticed with high returns such as doubling investments within 24 hours or less. Victims who sign up initially receive profits to encourage them to top up their investments until they are unable to top up their investments.

> Target: Gullible individuals with large savings and unfamiliar with financial investments.

> What-to-do: Stay away from investments that are unregulated by Bank Negara. If the returns on the investment are too good to be true, they probably are.

Job Scam

> Scammers offer high-paying salaries or commissions either for illegal or non-existent jobs locally or overseas.

> Target: Young, gullible and desperate job seekers.

> What-to-do: Avoid responding to unverified job offers on social media platforms, email and those that impose a fee for applicants.

Loan Scam

> Loans are often advertised on social media platforms with very low interest rates, guaranteed approval and no supporting documents required.

> Target: Social media users and small loan seekers.

> What-to-do: Avoid responding to emails and online loan offers by unverified sources and unlicensed moneylenders.

Love Scam

> Love scammers befriend and mesmerise their victims with romance and promises of marriage. Once trust is built, love scammers seek money from their victims.

> Target: Both men and women who desperately seek romance and relationships.

> What-to-do: Be wary and suspicious of unknown individuals who make contact through social media platforms offering friendship and later seek financial help.

Parcel Scam

> Scammers impersonating postal employees or Customs Department officials or the police scare potential victims claiming a parcel addressed to them was found with illegal content.

> Target: Online shoppers, individuals in a relationship with love scammers.

> What to do: Hang up any phone call which claims a parcel with illegal content is addressed to you. If in doubt, contact the police. Do not accept unknown cash-on-delivery parcels.

The Star graphics

ple from falling victim to such activities.

"Scams are like viruses. Treat them as such.

"Take preventive measures. Discuss it with your family and friends, be alert, be smart," she said.