Media Title : The Star
Headline : Don't install apps under pressure
Date : 10 August 2026
Section : Nation
Page : 6

Don't install apps under pressure

Scammers persuade users to download malicious software

By KHOO JIAN TENG
khoo.jianteng@thestar.com.my

YOUR RIGHT to know

PETALING JAYA: As smartphones become central to banking and daily life, scammers are finding increasingly sophisticated ways to seize control of the devices and the accounts within.

Universiti Sains Malaysia Cybersecurity Research Centre director Prof Dr Selvakumar Manickam said criminals were now turning to remote-access tools and malicious applications to bypass conventional scam safeguards.

He said victims could be persuaded to install apps such as AnyDesk or TeamViewer or malicious Android Package Kit (APK) files disguised as legitimate banking, delivery or other services.

Once installed and given permissions such as accessibility access, scammers could potentially view and operate the victim's phone, including banking applications.

"An unsolicited caller asking the victim to download an app to 'resolve' an issue, a request to enable accessibility, SMS or 'install unknown apps' permissions, or being asked to remain on a call while installing something, should raise alarm bells," he said when contacted.

Unexpected battery drain or unusual phone behaviour after installing an application, particularly one downloaded outside authorised sources, are also warning signs.

Selvakumar said scammers were increasingly exploiting psychology rather than simply trying to defeat technical security measures.

"They may create a sense of urgency by claiming a bank account has been frozen, a police matter needs to be resolved or an unpaid bill requires immediate action.

"Generative AI is also making scams more convincing with criminals able to produce polished phishing messages in local languages and clone voices to impersonate family members, bank officers or government officials," he said.

Beyond screen control, malware can quietly intercept SMS messages and push notifications, including one-time passwords and two-factor authentication codes, before forwarding them to scammers.

Some newer malware could also identify a victim's SIM card and mobile carrier before subscribing them to premium services through mobile billing systems.

"Fake cellular base stations have also been detected locally, allowing criminals to send fraudulent SMS messages while bypassing some telco-level filtering," he added.

Selvakumar said the affected phone should subsequently be reset after important data has been backed up or checked by a trusted technician.

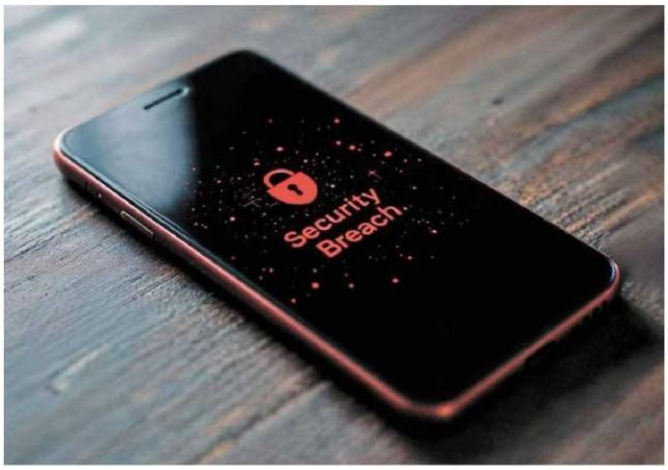
"The lesson is simple – never allow urgency or fear to override basic security precautions," he said.

Cybersecurity expert Fong Choong Fook said social engineering remained one of the biggest threats despite growing public awareness.

"Don't install any unknown or suspicious software. Have good practices such as not clicking on links from strangers or SMS," he said.

Fong added that scammers impersonating bank employees, law enforcement officers and government officials could now use AI-generated voice and video to make their identities appear more convincing.

"Users should avoid public WiFi where possible as compromised networks could expose devices to additional risks."



Compromised: Scammers are finding more sophisticated ways to bypass safeguards, such as malicious apps disguised as legitimate services. — Pic from magnific.com