Media Title : The Star
Headline : ' I watched them take control of my phone remotely'
Date : 10 August 2026
Section : Nation
Page : 6


Don't install apps under pressure
Scammers persuade users to download malicious software
Viral anti-corruption blitz is fake, say cops
Expert: Grasslands is best option to curb human-elephant conflict

'I watched them take control of my phone remotely'

PETALING JAYA: A routine phone call can quickly turn into a financial nightmare when unsuspecting victims lose control of their smartphones to scammers.

Confidential information and other personal details will then be manipulated by these fraudsters, causing financial and emotional distress to the victims.

For a Shah Alam resident who wished to be known only as Lim, the scam started with a phone call from a "bank officer", warning him about suspicious transactions.

The caller instructed him to download an application, purportedly to verify his identity and secure his account.

Thinking he was following a security procedure, Lim installed the application and granted the requested authorisation.

"After installing it, it seemed that someone had taken control of my phone.

"I could see apps opening by themselves, but I could not control what was happening," said the 42-year-old.

Within minutes, the scammers had gained access to his banking application and made several transactions.

Lim claimed that he lost about RM7,800 from his account before he managed to disconnect the phone from the Internet and contacted the bank.

"I always thought scams happened because people clicked suspicious links.

"I never expected that scammers could take over my phone while I was still holding it.

"By the time you realise it is the work of a scammer, it is too late, as you have probably already suffered financial losses," he said.

Another victim, who wished to be known as Tan, 56, from Ipoh, said she was contacted through WhatsApp on July 1.

The caller informed her that she had won a RM3,000 prize and was offered a choice between shopping vouchers or cash credited to her e-wallet.

Tan said she opted for a cash reward, and the call was subsequently transferred to a "manager", who sounded like a foreigner.

"I just followed his instruction to claim the reward.

"He then took control of my phone screen and kept directing me from one site to another without giving me time to think," she said.

Tan said she then contacted the platform's customer service through the app, activated the kill switch and lodged a police report within an hour.

She also said the official complaint submitted through the app, together with screenshots and supporting documents, later disappeared from her phone.

Tan claimed that RM4,500 was charged to her pay-later account while another RM6,000 was withdrawn through the platform's loan facility, bringing her total losses to RM10,500.

"The RM6,000 purported loan was converted into a 24-month repayment plan, requiring a monthly instalment of over RM300.

"The sum of RM4,500 was transferred to an entity listed as 'Lucky Boy Trading', although I had not purchased any items," she said.

A victim from Subang, who identified himself as Ravi, 35, said scammers posing as delivery company employees convinced him to install an application to reschedule a parcel.

After granting the application access to his phone, he noticed that messages and notifications were appearing and disappearing without his involvement.

"I thought I was only following instructions to receive a parcel. I never expected them to be able to take control of my phone."