Android Malware Scams Targeting Seniors: Run the Safe Check

Description

Do not install an app from a message, pop-up or unofficial store.

If a suspicious APK was installed, stop using the affected phone for banking, disconnect it, contact the bank from another trusted device and make the relevant reports.

Recognise sideloading

An APK installed outside the official app store can bypass normal store review and request dangerous permissions. Do not enable install unknown apps for a strangerâ??s instructions. (Singapore Police Android malware advisory)

A compromised phone may display overlays, intercept messages or remain under remote control. Call the number on the physical bank card from another trusted device.

Situation	What changes
No app was installed	Leave the channel, block it and verify through the official organisation
APK or unknown app was installed	Disconnect the phone and use a clean device for banking contact
Banking credentials or card details were entered	Call the bank immediately and follow its containment steps
Money moved or device is controlled remotely	Report urgently and preserve transaction and app evidence

Related: recognise the separate remote-support scam sequence

Disconnect without destroying evidence

Turn off Wi-Fi and mobile data or use airplane mode, but do not immediately wipe the phone if Police or the bank may need evidence. Photograph app names and transaction alerts from a clean device where safe. (CSA SG Cyber Safe Seniors)

Change banking, email and critical account credentials from a clean device and follow each providerâ??s session-revocation steps. Do not reuse a new password on the compromised phone.

Example: A five-minute family check can cover four items: app source, accessibility permission, device-admin permission and bank transaction limit. Record the settings, not passwords.

Seek technical restoration

Back up only known personal files, scan or reset under trusted guidance, and reinstall from official stores. A deleted app icon alone does not prove the device is clean.

Remove unnecessary sideloading permission, set transaction limits and agree on a call-before-install rule. Make the check easy enough to use under pressure.

- Stop the suspicious conversation
- Disconnect the affected phone
- Use another device to call the bank
- Preserve app and transaction evidence
- Change critical credentials cleanly
- Report to Police and ScamShield as appropriate
- Restore the phone through a trusted route

Related: check suspicious numbers and links through ScamShield

Date Created
11/08/2026
Author
vanessakoh