Godfather Android Malware - What it is, warning signs, and how to remove and prevent it

Gridinsoft Help Center

What it is

Godfather is an Android banking trojan that overlays fake login screens on top of real banking and crypto apps to steal credentials, SMS codes, and seed phrases. It can also read notifications and intercept 2FA to drain accounts. Technical details and removal tips: see our Godfather on Android - overview for defenders.

What you may notice

- Banking or wallet apps show odd pop-ups or ask for extra permissions
- Unexpected SMS verification prompts or missing 2FA texts
- New accessibility service enabled that you didn’t turn on
- Battery and data usage spike without a clear reason

How it gets in

- Fake app updates and clones in third-party stores
- Malicious links in SMS, email, or messaging apps
- "Security" or "system" apps pushing for Accessibility or Notification access

Remove it now - quick steps

- Disconnect from the internet - turn on airplane mode.
- Open Settings -> Apps and uninstall suspicious or newly added apps.
- In Settings -> Security -> Device admin apps and Accessibility, disable unknown entries.
- Install and run a reputable mobile anti-malware, then reboot and scan again.
- From a clean device, change passwords for banking, email, and crypto - move funds to new wallets with fresh seed phrases.

Prevent it

- Install apps only from Google Play - avoid third-party stores and APKs.
- Be cautious with links - especially those prompting urgent "bank updates."
- Review permissions regularly - revoke Accessibility and Notification access for apps that shouldn’t need it.
- Turn on Play Protect, keep Android and apps updated, and use MFA with an authenticator app

or security key.