M

Mobile Malware: Types, Warning Signs, and Safe Removal

Mobile malware is malicious software targeting phones and tablets to steal data, abuse permissions, control accounts, commit fraud, or disrupt the device.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Common types of mobile malware
02 How infection happens
03 Warning signs
04 What to do immediately
05 Prevention
06 Source

Quick answer: Mobile malware is malicious software designed to steal data, abuse permissions, control accounts, commit financial fraud, spy on activity, display unwanted advertising, or disrupt a phone or tablet. Remove network access, preserve evidence, secure accounts from another device, and use the platform’s trusted removal or reset

process.

01 Common types of mobile malware

- **Banking Trojans** use overlays, accessibility abuse, screen capture, or remote control to steal financial access.
- **Spyware** collects messages, location, contacts, audio, photos, credentials, or activity.
- **Infostealers** target sessions, passwords, wallets, and application data.
- **Adware and madware** deliver intrusive ads, redirects, tracking, or additional unwanted software.
- **Ransomware or lockers** block access, encrypt data where possible, or demand payment.
- **Bot and proxy malware** uses the device's connectivity for spam, fraud, traffic relay, or other commands.

02 How infection happens

Common paths include deceptive apps, unofficial stores, malicious links, fake updates, configuration profiles, abused enterprise provisioning, and instructions to grant accessibility, device-administrator, notification, VPN, or screen-capture permissions. Exploits requiring no user action exist but are less common and often highly targeted; ordinary prevention advice should not assume every infection needs an obvious APK.

Android and iPhone use different distribution, permission, and system controls. On Android, Play Protect checks apps from Google Play and other sources for harmful behavior and may warn, disable, or remove them. On iPhone and iPad, review installed apps, configuration and device-management profiles, VPN settings, and platform security updates. Jailbreaking or rooting weakens important security boundaries on either platform.

03 Warning signs

Investigate mobile-security alerts, an app installed from an unexpected source, unfamiliar accessibility or administrator access, unexplained VPN or profile configuration, hidden app icons, disabled protection, repeated overlays, unknown messages, rapid battery or data use, and account logins or financial transactions you do not recognize. Performance or battery problems alone can have benign causes.

04 What to do immediately

1. Enable airplane mode and disable Wi-Fi if active spying, fraud, or command traffic is suspected.
2. Do not use the device for email, banking, password management, cryptocurrency, or recovery codes.
3. From a trusted device, change exposed passwords, revoke sessions, verify MFA and recovery methods, and contact financial providers through official channels.
4. Record alerts, suspicious apps, installation source, permissions, profiles, phone number, and incident time. Managed devices should be handled through the security team.
5. Use the platform’s trusted harmful-app scan and update mechanism. Revoke unnecessary high-impact permissions, then remove the responsible app or profile.
6. Factory-reset when privileged control, persistence, or integrity cannot be resolved. Reinstall apps manually from verified sources.

Do not restore unknown installation packages, management profiles, or an unverified full-device configuration. Account recovery remains necessary after a reset because copied credentials and sessions are not erased from the attacker.

05 Prevention

Keep the operating system and apps supported and updated. Use official stores and verified publishers, leave built-in harmful-app protection enabled, and review permissions regularly. Use a strong screen lock, unique passwords, phishing-resistant MFA where available, encrypted backups, and remote-find or erase features. Organizations should manage device compliance, work profiles, application allow-lists, and separation of work data.

06 Source

Enterprise mobile-device controls are covered in NIST SP 800-124 Revision 2. Android harmful-app scanning and removal behavior is documented in Google Play Protect Help.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com