Madware - What it is, warning signs, and how to remove and prevent it

Gridinsoft Help Center

What it is

Madware is aggressive mobile advertising. It stuffs your phone or tablet with pop-ups, full-screen ads, notification spam, and sneaky redirects. While not always outright malware, it invades privacy, slows performance, and can open the door to riskier installs.

What you may notice

- Pop-ups and full-screen ads outside of apps
- Random redirects in your browser or Play Store
- New icons or shortcuts you didn’t add
- Battery, data, and CPU usage spiking

How it sneaks in

- "Free" apps bundled with intrusive ad SDKs
- Cloned or repacked apps from third-party stores
- Overreaching permissions granted during install

Remove it now

- Uninstall the most recently added or suspicious apps.
- In Settings -> Notifications/Permissions, revoke ad-heavy access.
- Run a reputable mobile anti-malware scan and reboot.
- Clear browser cache and remove unknown profiles/VPNs.

Prevent it

- Install only from official app stores and check reviews and permissions.
- Avoid clones, cracks, and "booster" apps that demand broad access.
- Keep Android or iOS and apps updated.
- Use privacy-friendly browsers and limit ad tracking where possible.