HOW TO CHECK YOUR **ANDROID PHONE** FOR TRACKING APPS

CHECK YOUR ANDROID PHONE

Step 1: Review Installed Apps

1. Open *Settings*.
2. Tap *Apps* or *Apps & Notifications*.
3. Select *See all apps*.
4. Review for unfamiliar or suspicious apps.

Step 2: Check App Permissions

1. Go to *Settings > Privacy or Security & Privacy*.
2. Tap *Permission Manager*.
3. Check permissions for Location, Camera, Microphone, Contacts, SMS.
4. Ensure only trusted apps have access.

Step 3: Check for Device Administrators

1. Go to *Settings > Security > Device Admin Apps*.
2. Review and disable unfamiliar apps.

Step 4: Look for Hidden or Spy Apps

1. Open *Settings > Apps > See All Apps*.
2. Select *Show system apps*.
3. Look for suspiciously named apps.
4. Use trusted security apps to scan for hidden apps (Free versions of AVAST or AVG).

HOW TO REMOVE SUSPICIOUS OR TRACKING APPS

1. Go to *Settings > Apps > See All Apps*.
2. Tap the suspicious app.
3. Select Uninstall.
4. If it's a device admin: Disable via *Settings > Security > Device Admin Apps* first.
5. For stubborn apps: Restart in Safe Mode and uninstall.

HOW TO PREVENT TRACKING APPS

1. Download apps only from the Google Play Store.
2. Regularly review app permissions.
3. Install a trusted mobile security app.
4. Avoid unknown links and files.
5. Keep your OS updated.
6. Use Play Protect: *Play Store > Profile icon > Play Protect > Run scan*.

FINAL TIPS FOR ANDROID DEVICES

1. Avoid sideloading apps.
2. Use strong, unique passcodes and enable biometric security (face recognition or fingerprint reader).
3. Be cautious with public Wi-Fi
4. Consider using a VPN.
5. Monitor data usage for unusual activity