CSIR CYBER SECURITY AWARENESS

Beware and Stay Safe from **Cyber Attacks**

Mobile Security

Mobile security refers to safeguarding mobile devices and their data from unauthorized access, malware, phishing, and other cyber threats. It includes updating software, using strong authentication, avoiding malicious apps, and ensuring secure communication to protect sensitive information and maintain device integrity. Regularly backing up data and enabling remote wipe features are also essential for enhanced protection.

Do's

- ✓ Keep the mobile OS and latest Antivirus updated with the latest patches.
- ✓ Download apps only from official app stores (Google Play/Apple Store).
- ✓ Check app popularity and user reviews before downloading.
- ✓ Note down the IMEI number and keep it offline for emergencies.
- ✓ Use auto-lock with passcode or security patterns. Enable Mobile Tracking for lost/stolen devices. Take regular offline backups of your data.
- ✓ Scan files with antivirus software before transferring to your mobile.

Don'ts

- ✗ Do not root or jailbreak your mobile device. Avoid enabling Wi-Fi, GPS, Bluetooth, or NFC unless necessary.
- ✗ Do not accept unknown Bluetooth/file sharing requests.
- ✗ Avoid apps requesting unnecessary permissions (e.g., GPS for a calculator).
- ✗ Do not open suspicious links from SMS or social media. Disable automatic downloads on your phone.
- ✗ Avoid apps with bad reputations or low user bases.
- ✗ Do not store sensitive data without securing it on your phone.

FOR REPORTING SECURITY INCIDENTS: incident@csir.res.in