Simple Security tips for hardening your Android Mobile Device

We come across news of ransomware attacks, data leaks and privacy breaches daily. Hence, it will not be surprising if we are wondering how secure our android device is. Let us first have a glimpse of basic level (general categories) of Android app vulnerabilities.

Type	Description	Negative Consequence
Incorrect Permissions	Permissions allow accessing controlled functionality such as the camera or Global Positioning System (GPS) and are requested in the program. Permissions can be implicitly granted to an app without the user's consent.	An app with too many permissions may perform unintended functions outside the scope of the app's intended functionality. If too few permissions are granted, the app will not be able to perform the functions required.
Exposed Communications	Internal communications protocols are the means by which an app passes messages internally within the device, either to itself or to other apps. External communications allow information to leave the device.	Exposed external communication (data network, Wi-Fi, Bluetooth, Near-Field Communication (NFC), *etc.*) leave information open to disclosure or man-in-the-middle attacks.
Exposed Data Storage	Files created by apps on Android can be stored in Internal Storage, External Storage, or the Keystore. Files stored in External Storage may be read and modified by all other apps with the External Storage permission.	Sensitive data can be exfiltrated or tampered by other apps, or unintentionally transferred to another system in a backup.
Potentially Dangerous Functionality	Controlled functionality that accesses system-critical resources or the user's personal information. This functionality can be invoked through API calls or hard coded into an app.	Unintended functions could be performed outside the scope of the app's functionality.
App Collusion	Two or more apps passing information to each other in order to increase the capabilities of one or both apps beyond their declared scope.	Collusion can allow apps to obtain data that was unintended such as a gaming app obtaining access to the user's contact list.

Steps to tighten up the security of the Android Phones:

1. **Google play protect feature**

   - Go to Settings > Google > Security
   - Play protect regularly checks your Apps and devices for harmful behavior and notifies for

any security risks found

- If you want to improve the security further, enable the improved harmful app detection feature

2. Use Common Sense

- Do not open any suspicious emails, links.
- Do not download apps or any other content from non-reliable sources.
- Install latest software updates available for your device.

3. Secure your DATA – Encrypt your device

- Go to Settings > Security > Encrypt phone option
- Store data on the internal storage of your device, not in external storage cards.
- Set up screen lock on your phone

Why Encrypt

Unencrypted data stored on the phone can be accessed by PC apps even if the phone is locked.

4. Secure your PRIVACY

- Lock your phone using pattern lock.
- Make the patterns invisible
- Disable smart lock as it unlocks the phone automatically in some situations.
- Create a separate user account, in case you want to hand over your phone to a friend for some work, do that by switching user accounts.
- Enable two-step verification. This will ensure control of your accounts.
- Visit Google's Security Checkup page (https://myaccount.google.com/security) to check on the devices that you are logged into.