Securing Your Android Phone
Tip Sheet

Shoestring NETWORKS

Security for mobile devices follows a best practices model. Although it is impossible to be 100% secured, it is possible to follow best security guidelines and achieve good, reliable mobile security.

Below are our recommended best practices for securing your Android devices.

Securing Android [based on Android firmware 5.0.2]

1. Enable device screen-lock. [Settings:Lock Screen]
2. Enable device encryption. [Settings:Security]
3. Only install apps from trusted sources such as the official Google Play store.
4. Be sure Google's "App Verification" is turned on: https://support.google.com/nexus/answer/2812853?hl=en
5. Install a good mobile security app such as Sophos Antivirus or Avast Mobile Security.
6. Always have the most current Android updates installed.
7. Turn off Wi-fi and Bluetooth when not in use. Avoid unsecured Wi-fi.
8. Make sure backup is turned on. Go to "Settings", then "Backup & reset" and check the "Back up my data" option to turn on auto-backup. Also select the "Automatic Restore" option.
9. Android Device Manager can help locate a lost device, or be used to enable remote wipe: https://www.google.com/android/devicemanager
10. Turn on 2-Step Verification on your Google account: https://goo.gl/5rJCyF
11. Be cautious enabling location services. Turn off when not needed.
12. Do not open any links from untrusted sources. If an unknown number (SMS/Texting) or email address sends you a link, do not open the link.
13. Use VPN (virtual private networking) when traveling or connecting to public networks.
14. Be cautious with all downloads.

Depending on the carrier and Android firmware version, recommendations mentioned above may or may not be available or may be located under a different option.

These recommendations are just that, recommendations. It is possible that what is recommended now may change in the future as the mobile environment changes.