Mobile Security Checklist

Initial set-up and configuration:

- Apply all software updates from a trusted network (office, etc.).
- Back-up all data to on offline storage device (spare SD card, USB drive, etc.)
- Turn on phone encryption (including SD card) and establish access PIN
- Turn off Bluetooth, NFC, Location services, build habit of turning on as needed
- Set USB Connectivity to Charge Only
- Uninstall or Disable and turn off mobile-data on all non-critical apps
- Don't use personal pictures as background or screen savers
- Sanitize Owner Info on screen lock
- Ensure that “install applications from unknown sources” is disabled
- Disable voice search and voice typing (“OK Google” et al).
- Uninstall Facebook applications and others (use website via browser)
- Turn off spell checker, voice typing, fast-fill, alt keyboards
- Disable auto-complete, pre-load, and suggested search in browser
- Disable print services
- Install, configure the following applications:
- https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain
    - Establish a PGP key for your phone in OpenKeyChain, upload public key.
    - Install PGP software on your home/office laptop/desktop. Create, upload key.
    - Download public key for home/office to OpenKeyChain.
    - Test encrypting a file on phone and decrypting on home/office machine.
- https://play.google.com/store/apps/details?id=net.osmand&hl=en_US
    - If have SD card, configure to use SD storage
    - Download commonly used countries and regions for offline use (if SD card, do whole world)
- https://play.google.com/store/apps/details?id=com.google.android.apps.translate
    - If have SD card, configure to use SD storage
    - Download commonly used languages for offline use (if SD card, download all available)
- https://play.google.com/store/apps/details?id=com.microsoft.translator
    - If have SD card, configure to use SD storage
    - Download commonly used languages for offline use (if SD card, download all available)
- https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
    - Download to a secondary device that is left in secure storage
    - Enable MFT (two-factor auth) on all critical accounts where able. Record key on both devices.
- https://play.google.com/store/apps/details?id=com.simplemobiletools.filemanager

- https://play.google.com/store/apps/details?id=com.termux
  - Initialize storage by starting it and typing “termux-setup-storage” at command line
  - Update system by typing “apt update && apt upgrade” at command line
- https://play.google.com/store/apps/details?id=eu.faircode.netguard
  - Purchase in-app NetGuard Pro feature “View blocked traffic log”
  - Configure NetGuard to “Show user apps” and “Show system apps”,
  - Individually block both wifi and mobile data for ALL apps.
  - Then deselect the critical constant use apps.
  - Build habit of enabling other apps data access as needed.

Your phone should now be configured to block most network traffic by default and be readily used offline in foreign countries. Reboot your phone and double-check your settings and functionality. The NetGuard firewall should be running after reboot.

Before travel departure:

- Apply all software updates from a trusted network (office, etc.).
- Back-up all data to on offline storage device (spare SD card, USB drive, etc.)
- Change all passwords on accounts from alternate terminal (laptop, desktop, etc.)
- Purge any unneeded applications, data, or accounts from device
- Evaluate risk vs. needs of trip (environment, duration, operational needs, etc.)
- If needs allow, set-up secondary device for travel use with cut-out accounts
- Download maps, languages, and pre-brief materials for destination
- Lock down additional configuration options
  - disable wifi, mobile data, auto-time, google back-ups, purge SIM, etc.

Operational use:

- Ideally use a burner, or alternate phone with local SIM for daily needs.
  - ! Use primary device offline as lookup/reference device.
- Keep wifi disabled.
  - ! If wifi is needed, lockdown all traffic in NetGuard except single app.
- If need to move data from trusted device to other devices, use HW write protect USB drive.
  - ! Enable HW write protect switch before inserting into untrusted systems.
- When need to go dark or when devices are powered off, store in RF shield sack.
- Never plug trusted device into external USB sources, for power or data transfer.
  - ! Use charging data blocker, vendor charger, provided battery pack, or USB drive.