Android "10" List

As a phone owner, you must have a base understanding of what you are getting into when it comes to phones. As a smartphone user, here are ten things that you must know how to do on your journey to becoming a responsible smartphone user.

**** RESTART YOUR PHONE DAILY and DISABLE BLUETOOTH, WIFI, & NFC when not in use. ****

1. Disable Location Services
   - **Settings > Location >>** Disable all for best security
     - ALT: > Location Services >> Disable Accuracy, History, Sharing, Both Scanning
     - ALT: > App Permissions >> Remove Apps with “All the Time” & “While in use”
2. Restrict App Permissions to the bare minimum
   - **Settings > Security & Privacy > Privacy > Permission Manager**
     - Review each permission and remove all except critical apps
3. Remove known Wi-Fi access point history
   - **Settings > Wi-Fi > Tri-Dots > Advanced > Manage Networks**
     - Remove all stored Wi-Fi not required.
4. Privacy from Google Settings:
   - **Settings > Security & Privacy > Privacy > Other Privacy Settings**
     - Android System Intelligence: Cannot be disabled. Clear history monthly
     - Ads: Delete Advertising ID. If you see “Get new Advertising ID” Your good.
     - Usage & Diagnostics: Turn off
     - Activity Controls: Turn off All things.
5. Enable Secure Folder
   - **Settings > Security & Privacy > Secure Folder**
     - Enable with a different pin or password than device.
     - Use the + to add apps. These are copies and can use different accounts.
     - Apps in here are separated from the rest of the tablet and protected.
6. Enable Biometric logon
   - **Settings > Lock Screen > Screen Lock >>** Set PIN (min 8 digits), face, and fingerprint
     - Enabling this prevents someone observing your pin in public
7. Enable Private DNS
   - **Settings > Connections > More Connections > Private DNS > Private DNS Host**
     - Use 1dot1dot1dot1.cloudflare-dns.com OR dns.google
8. Use a VPN (All the Time)
9. Use a password manager, and don’t store passwords in the native phone
10. Disable Special Access Permissions (Samsung Line)
    - **Settings > Apps > Tridots > Special Access > Usage data Access**
      - Disable ALL Apps
    - **Settings > Apps > Tridots > Special Access > Wi-Fi Control**
      - Disable ALL Apps
    - **Settings > Apps > Tridots > Special Access > All File Access**
      - Disable Apps you have downloaded and do not deem critical.

Apple "10" List

As an iPhone user, you are already on your way to having a secure digital life. The iPhone has many natural security features, but it's a good idea to ensure you know how to do the following at a minimum.

**** RESTART YOUR PHONE DAILY and DISABLE BLUETOOTH & WIFI when not in use. ****

As a user of technology, you are obligated to know how to do the following:

1) Keep your iPhone iOS up to date
   ⇒ **Settings > General > Software Update**
2) Activate the "find my iPhone" feature (Optional)
   ⇒ **Settings > Tap your name > Find My > [Turn On & disable share location]**
3) Disable AD-ID and app tracking
   ⇒ **Settings > Privacy & Security > Apple Advertising > Personalized Ads Greyed out**
4) Manage or Disable Location Services
   ⇒ **Settings > Privacy & Security > Location Services:**
   ∗ Set all apps to "Never" or "When Shared" and go from there.
   ∗ System Services > DISABLE Everything except Find My and Status Bar Icon.
   ∗ Significant Locations > Clear History and Disable.
5) Set phone "self-destruct" (wipe after 10 failed passwords)
   ⇒ **Settings > Face ID & Passcode > Erase Data (at bottom)**
   ∗ While here disable all options in Allow access when locked.
   ∗ FaceID is a great way to protect from public observance of your passcode!
6) Use "Safety Check" & App Privacy Report to audit your data.
   ⇒ **Settings > Privacy & Security > Safety Check**
   ∗ Emergency Reset is good for a potential breach or hack of your accounts.
   ∗ Manage Sharing and Access is good to know who can see what.
   ⇒ **Settings > Privacy & Security > App Privacy Report**
   ∗ Turn on and come back in a couple days.
   ∗ This report will tell you what apps are accessing what sensors and your data.
7) Avoid public Wi-Fi and remove stored Wi-Fi
   ⇒ **Settings > Wi-Fi > Edit (Upper Right)** >> Remove all unneeded Wi-Fi.
8) Disable Siri on the iPhone lock screen
   ⇒ **Settings > Siri & Search > Disable Siri** >> This will make a number of things not work
   ∗ Car Play will not work. At a minimum **disable** "Hey Siri" & Allow while locked
9) Revoke app permissions for the camera, microphone, etc.
   ⇒ **Settings > Privacy and Security** >> For Microphone, Camera, Health...
   ∗ For each one Review the green and make grey what is NOT needed.
   ∗ Disable Research Sensor & Usage Data (Don't give up your data!)
10) Setup Domain Naming Service (DNS) >> Install NextDNS or Cloudflare App

Bonus Actions:

- Enable Advanced Data Protection
- Enable Security Keys with Apple >> (Requires 2 x Security Keys)