Securing Your iPhone 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 iOS devices.

Securing iOS

1. Turn on the passcode feature. [Settings:Touch ID & Passcode]
2. Turn off "Allow Access When Locked". [Settings:Touch ID & Passcode]
3. Turn on "Erase Data". [Settings:Touch ID & Passcode]
4. Turn on 2-Step Verification (2FA) for iCloud and Apple ID. (https://goo.gl/o42wMy)
5. Turn off "Ask to Join Networks". Avoid using unsecured Wi-Fi. [Settings:Wi-Fi]
6. Turn off Wi-Fi when not in use. [Settings:Wi-Fi]
7. Keep the device updated. [Settings:General:Software Update]
8. Turn on "Auto-Lock". [Settings:General:Auto-Lock]
9. Check Privacy Settings. [Settings:Privacy]
10. Turn off Bluetooth when not in use. [Settings:Bluetooth]
11. Turn on iCloud backup. [Settings:iCloud:Backup].
12. Be cautious enabling location services. Turn off when not needed. [Settings:Privacy]
13. 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.
14. Use VPN (virtual private networking) when traveling or connecting to public networks.
15. Be cautious with all downloads. Only download from the official Apple Store.

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

Be sure to do a cloud backup of your device before making these changes, as this will allow you to get back to the pre-recommended environment if needed.