iOS MOBILE SCAN CHECKLIST

ALL THINGS SECURED

Periodic Scan (Quarterly or Annually):

□	Do a full scan of the phone using reputable software like Certo Software
□	Review installed apps and remove unused or unfamiliar ones
□	Make sure the OS is updated and set to "Automatic Updates - ON"
□	Review all subscriptions (App Store —> Account —> Subscriptions)
□	Review all camera and microphone permissions (Privacy & Security settings)
□	Do a Safety Check (Privacy & Security —> Safety Check)
□	Turn off unnecessary location data (Privacy & Security —> Location Services)
□	Check 2FA Setup for Apple ID (Apple ID —> Sign-In & Security)
□	Check for unknown VPN configurations (Settings —> VPN)
□	Ensure the Personal Hotspot setting is turned off
□	Turn on Advanced Data Protection (watch this tutorial)
□	Turn on Stolen Device Protection (Settings —> FaceID & Passcode)

If You Believe Your Device is Compromised:

- □ Start by turning off all WiFi & Network connections
- □ Check for unknown devices (Settings —> Apple ID —> scroll down)
- □ Change all important passwords (if possible, from another device)
- □ Set up new 2FA for Apple ID & other accounts (watch this tutorial)
- □ Turn on Lockdown Mode (watch this tutorial)
- □ Consider changing to new SIM or eSIM service (good eSIM options)
- □ Turn off all Share My Location options (Apple ID —> Find My)

Tips for Greater Security & Privacy

- When possible, it’s best to use 2-factor authentication (2FA) that is based on an authenticator app or a security key. SMS text has been shown time and again to be vulnerable to attack.

- If you don’t trust Apple or Google anymore, there are open source mobile operating systems such as Graphene OS that allow you to "flash" certain mobile devices and use a de-Googled phone.

- If you need to use a SIM-enabled phone at times but don’t want it constantly broadcasting your location and system data to your mobile provider, there is a solution known as a Faraday Bag in which you can put your phone and block all incoming and outgoing signals.

- Instead of having one phone number that you give out to every person and company, there is value in purchasing a virtual phone number that allows you to have a "throwaway" number in addition to the number that actually rings your device.

- DO NOT use the same 4- or 6-digit code that unlocks your phone for every other numeric passcode. Come up with one passcode for your phone and a separate one for everything else.

- Did you know that you can purchase a data-only eSIM? It’s still possible for mobile providers to track you with this eSIM, but you eliminate certain threat vectors without access to unencrypted phone and SMS text. This isn’t the most convenient option, but it might be one to consider for some people.