Mobile Security

iPhone (iOS) Options

- Use an alphanumeric base password containing numbers, letters, and special characters (not 4 or 6-digit PIN's).
- Enable biometrics.
- Enable "Stolen Device Protection" and "Find My iPhone."
- Consider enabling "iOS lockdown mode" depending on personal risk profile.

Android Options

- Use an alphanumeric base password containing numbers, letters, and special characters (not 4 or 6-digit PIN's).
- Enable biometrics.
- Only install apps from reputable sources (Google Play Store/Samsung Store); avoid sideloading unless from trusted sources.
- Consider enabling "Google's Advanced Protection", option depending on personal risk profile.

Report a crime to your local Secret Service Field Office

https://www.secretservice.gov/contact/field-offices

To learn more:

National Association of Corporate Directors
https://www.nacdonline.org/security

United States Secret Service
https://www.secretservice.gov

Additional Resources

Cybersecurity and Infrastructure Security Agency
https://www.cisa.gov

Federal Trade Commission/Identity Theft
https://identitytheft.gov

Internet Crime Complaint Center (IC3)
https://www.IC3.gov

PERSONAL CYBERSECURITY PROTECTIONS

for Corporate Directors and Executives

The United States Secret Service

in collaboration with

NACD®
Empowering Directors. Transforming Boards.

Passwords and Accounts

- Use a password manager.
- Use strong passwords unique to each site/account.
- Minimize or prevent password reuse.
- Use phishing-resistant authentication, like FIDO passkeys, or hardware-based security tokens, wherever possible. Wherever possible, disable SMS, email, or phone one time passwords (and similar authentication or account recovery options) to ensure effective protection using multifactor authentication.
- Ensure remote wipe capability (iOS/Android "Find My Device") available or corporate Mobile Device Management (MDM) solution capability.

Operational Security

- Assess your personal risk profile.
- Social Media:
  - LinkedIn, Instagram, Facebook, TikTok, X, etc.
  - Understand and inventory the information you are sharing or providing an adversary.
  - Be mindful of what you share online; personally or professionally, it could be used against you.
- Back-up critical personal information using the "3-2-1" rule:
  - 3 copies,
  - 2 different media types, and
  - 1 offsite/alternate location storage.
- Separate personal and business communications/ accounts where possible.
- Be hyper-aware and establish processes/ responses for phishing/vishing and smishing scams designed to steal confidential information.
- Shop and bank only at reputable and secure sites.
- Use reputable email providers for personal emails.
- Establish out of band processes and procedures to verify verbal commands to subordinates not conducted in person (deep fake voice impersonation defense).
- Use end-to-end encrypted communications applications, such as Signal, where appropriate and permissible.

Antivirus and Patch Management

- Enable automatic updates on:
  - Personal computers,
  - mobile devices when available, and
  - home and office devices when available.
- Major computer operating systems and software vendors provide regular patches that generally should be applied immediately.
- Ensure you either update or set to automatically update firmware for your Internet-of-Things devices within your home/office (e.g., routers, sensors, smart TVs, refrigerators, thermostats, household cameras, car, etc.).