CAPACITY ENHANCEMENT GUIDE

Mobile Device Cybersecurity Checklist for Consumers

November 2021

OVERVIEW

Mobile devices are an integral part of our daily lives. There are an estimated 294 million smartphone users in the United States, making these devices an attractive target for cybercriminals.[1] Threats range from mere annoyances (spam messages) to severe (loss of personal information, credentials, or money). Listed below are simple cyber hygiene steps consumers can take to improve the cybersecurity of their mobile devices.

Audience and Scope

The measures described in this guidance focus on various easy-to-implement steps all mobile device users can take to improve the cybersecurity of their mobile devices. **Note:** for additional guidance tailored for—but not limited to—mobile devices security for federal users, see the National Security Agency publication Mobile Device Best Practices.

KEEP UP TO DATE

- ☐ **Update platform.** Enable automatic operating system updates to enhance privacy/security and fix flaws.
- ☐ **Update apps.** Enable automatic app updates to ensure you are using the most current security technologies.

USE STRONG AUTHENTICATION

- ☐ **Enable device authentication.** Set strong login passwords/PINs and use biometric authentication.
- ☐ **Enable two-factor authentication.** Enable two-factor authentication for apps or websites that support it.

PRACTICE GOOD APP SECURITY

- ☐ **Use curated app stores.** Disable third-party app stores, which can be vectors for the spread of malware.
- ☐ **Delete unneeded apps.** Periodically review and delete apps that are unused or no longer needed.
- ☐ **Minimize PII in all apps.** Limit personally identifiable information (PII) stored in apps.
- ☐ **Grant least-privilege access to all apps.** Set the privileges on your installed apps to minimize access to PII.
- ☐ **Review location settings.** Only allow an app to access your location when the app is in use.

PROTECT NETWORK COMMUNICATIONS

- ☐ **Disable unneeded network radios (BT, NFC, Wi-Fi, GPS).** Every connection is a potential point of attack.
- ☐ **Avoid public Wi-Fi.** Cybercriminals can use public Wi-Fi networks, which are often unsecured, for attacks.

PROTECT THE DEVICE

- ☐ **Install security software.** Security software (e.g., mobile threat defense) protects against malware.
- ☐ **Use only trusted chargers and cables.** A malicious charger or PC can load malware onto smartphones that may circumvent protections and take control of them. A phone infected with malware can also pose a threat to external systems such as personal computers.
- ☐ **Enable lost device function.** Configure settings to automatically wipe the device's data after a certain number of incorrect login attempts (e.g., 10), and enable the option to remotely wipe the device.

BEWARE OF PHISHING ATTEMPTS

- ☐ **Protect against phishing attacks by:**
  - Checking an email's legitimacy before opening an attachment or a link.
  - Not clicking on links in emails in your junk or spam folders.

[1] Estimated number of smartphone users in the United States from 2018 to 2025. Statista.