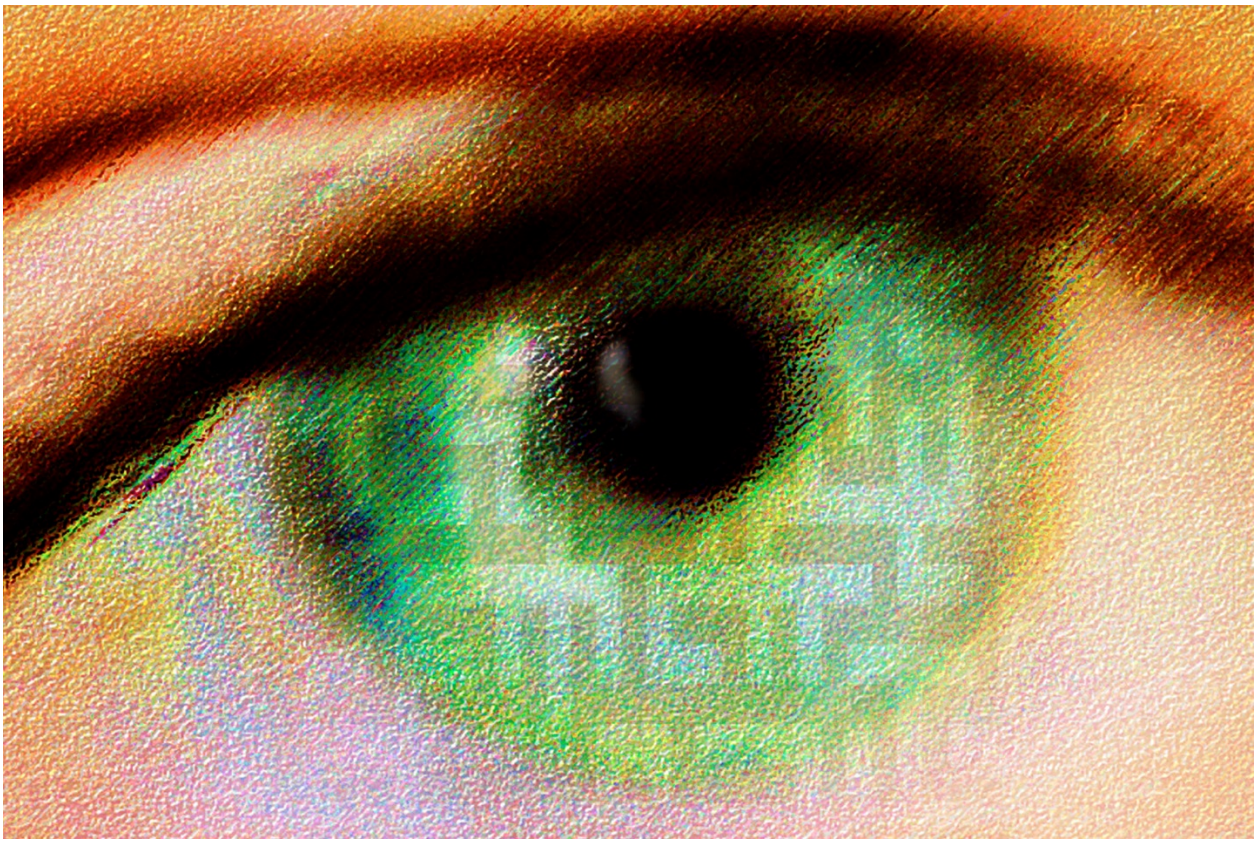

Mobile Device Cybersecurity: What Can You Do To Protect Your Smart Phone?

Check List

John J. Carney, Esq.
Carney Forensics
www.carneyforensics.com

TABLE OF CONTENTS

Maintain Physical Control of Your Device at All Times

Use Strong, Complex Pass Phrases
- A long, ten to fifteen character alphanumeric password is best
- Four or six digit password is not enough
- Four or five words and/or numbers separated by spaces are good pass phrases
- Movies, songs, book titles, etc. are easy to remember

Use Automatic Lock Settings
- Set "auto-lock" for a short period of time (30 seconds or less)
- Set device lock after reasonable number of failed unlock attempts (10 to 15)

Disable Wi-Fi, Bluetooth, and NFC Settings When Not in Use
- Do not connect to unsafe devices around you
- Connect to Wi-Fi at work or home and Bluetooth in automobile, etc.

Eliminate Use of Public Wi-Fi Hotspots
- Disable Wi-Fi setting at Starbucks, hotels, etc.
- Use personal hotspot (service provider's 3G/4G) on your smart phone instead
- Consider Virtual Private Network (VPN) third party service on your smart phone

Protect Home Wi-Fi
- Use WPA2 authentication key on your home router
- Update your home router firmware regularly
- Consider Virtual Private Network (VPN) third party service for your home router

Encrypt Your Mobile Device
- Encrypt your Android smart phone and microSD card
- Connect your Android smart phone to power when you encrypt it
- Your iPhone is encrypted already by default

Use and Regularly Test Mobile Device Tools for Loss or Theft
- Enable remote location, ring, lock, and erase services for lost mobile device
- Use Find My iPhone app on iCloud account for your iPhone
- Use Android Device Manager on Google account for your Android phone
- Consider third party mobile apps like Lookout, Cerberus, etc.

Upgrade and Patch Mobile Device Operating Systems
- Upgrade to new operating system version immediately
- Connect your mobile device to power during upgrade and use safe Wi-Fi signal

Choose and Install Mobile Malware Protection
- Eliminate viruses, spyware, and exploits like ransomware, etc.
- Protect against drive-by download attacks for safe surfing
- Consider Trend Micro, Kaspersky, Lookout, etc. for iPhone
- Consider Malwarebytes, Kaspersky, Trend Micro, Lookout, etc. for Android

Beware Mobile Social Engineering Scams

Be alert for clickjacking attacks that trick user into clicking on harmful link or attachment
Be alert for personalized, spear phishing attacks in your web mail or e-mail apps
Be alert for SMiShing attacks ("SMS phishing") in your text messages

Do Not Jailbreak Your iPhone or Root Your Android

Compromises vendor security controls and weakens the security of your mobile device
Do not enable "USB debugging" or "Stay awake" settings on your Android
Do not enable "Unknown sources" setting on your Android

Choose and Install Password Manager

It creates long passwords, automatically logs in, reduces password reuse, has scorecard
Consider third party options like Dashlane, LastPass, eWallet, etc.

Enable Two-Factor Authentication (2FA)

It is a second, time-based password for secure access to web accounts and mobile apps
Use Google Authenticator or Authy app on smart phone to get time-based passwords

Backup Your Mobile Device

Check your iCloud settings on your iPhone to backup to the cloud
Check your Google settings on your iPhone or Android to backup to the cloud
Consider backing up your Android to the cloud with third party Android apps (Lookout, Titanium, Helium, MyBackup, SMS Backup, etc.)
Backup your iPhone to your Windows PC or your MacBook with Apple's iTunes

Mobile App Store Validity

Only download apps from Apple App Store for your iPhone
Only download apps from Google Play Store or Amazon Appstore for your Android

Install Secure (Encrypted) Mobile Messaging Apps

Consider Signal, WhatsApp, and Google Allo
Consider TigerText for HIPAA compliant needs

Be Aware of Mobile Obfuscation

Spoliation by wiping phone remotely or resetting to factory conditions in settings
Spoliation by using third party "cleaner" apps
Use of hidden, password protected apps with vaults to hide documents, photos, or apps
Use of decoy apps which appear to do one thing while designed to do something else

Other Resources

Check the U.S. FCC's "Smartphone Security Checker" for iPhone, Android, Windows Phone, and BlackBerry