Carney Forensics

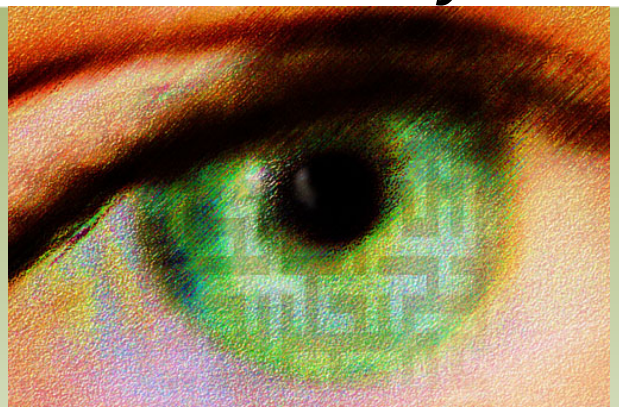
Mobile Device Cybersecurity for Family Lawyers

Minnesota CLE

Family Law Institute

March 26, 2018

John J. Carney, Esq.



Mobile Device Cybersecurity

What Are We Worried About?

Data Breaches
Privacy Breaches
Lost or Stolen Devices
Theft of IP
Viruses and Malware
Ransomware
Spyware
Advanced Exploits

Advice for Mobile Device Users

- **Don’t ever give up possession of your device!**
- Always protect your phone with passcode, PIN, pattern lock
  - Not your name
  - Not spouse’s name
  - Not dog’s name
  - Not birthday
  - Not phone number
  - Not street address
  - Not “123456”
  - Not “password”
  - Not “letmein”
  - Not “iloveyou”
- Set short time-out period for auto-lock feature in Settings

What Passcode is Strong Enough?

- For security purposes a 10 to 15 character alphanumeric passcode delivers much greater security benefit compared to a simple 4 or 6 digit numeric passcode
- iOS use of a longer, complex passcode protects against brute-force breaking of the passcode in earlier versions
- Android use of a complex passcode can help prevent recovery of device data, with exception of microSD card
- Pass Phrases are good, complex passcodes:
  - I will graduate in 2018
  - I like Dr. Pepper 1024
  - Old Man and the Sea 1952
  - 2001: A Space Odyssey

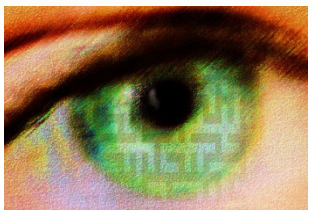
Advice for Mobile Device Users

- Encrypt mobile device handset, “a no-brainer solution”
  - Only 10% of Android, but 95% of iPhones (by default)
- Does not protect memory card, which can be removed
- Encrypt mobile device memory cards (microSD)

- Upgrade new mobile operating system version immediately
  - Google Nexus or Google Pixel bought from Google Store

- Assume at some point device will be lost, stolen, or infected
  - Download or configure “Find my Phone” app on device
  - Setup “Remote Wipe” capability

- Back up device regularly to PC, Mac, or Cloud
  - iTunes, Android Backup
  - iCloud, Lookout, other 3rd party cloud software



iPhone Settings Demo

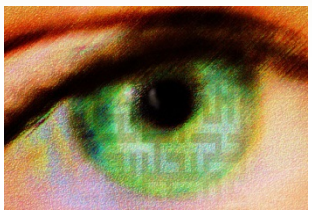
- Auto-Lock
- Complex Passcode
- Erase Data after Failed Passcode Attempts
- Find My iPhone
- Backup iPhone to iCloud
- Synchronize iPhone to iCloud
- Location Services
- Apple Pay
- Bluetooth
- Wi-Fi
- VPN App

iPhone Settings Demo (iOS 11.2)

- Display & Brightness / Auto-Lock
- Touch ID & Passcode / Change Passcode / Passcode Options
- Touch ID & Passcode / Require Passcode
- Touch ID & Passcode / Erase Data after Failed Passcode Attempts
- Accounts & Passwords / iCloud / Find My iPhone
- Accounts & Passwords / iCloud / iCloud Backup
- Accounts & Passwords / iCloud / Photos, Mail, Contacts, etc.
- Privacy / Location Services
- Privacy / Location Services / Google Maps
- Privacy / Location Services / Maps
- Wallet & Apple Pay / Apple Pay Cash
- Bluetooth
- Wi-Fi
- VPN App (NordVPN)

Advice for Mobile Device Users

- Be cognizant of what apps you install on your phone
  - Only Apple App Store, Google Play, Amazon App Store
  - Which app permissions you accept
- Turn off Wi-Fi and Bluetooth when traveling to protect against device automatically connecting to unsafe networks
- Consider mobile security software to help protect against virus, spyware, malware exploits like ransomware and drive-by download attacks:
  - Lookout
  - Trend Micro
  - Malwarebytes
  - FortiClient



Google play

Mobile Device Spyware?

- What is Spyware? What does it do?
- Telltale signs your phone may be infected with Spyware
  - Someone mysteriously knows your schedule, whereabouts?
  - Someone asked to borrow your phone?
  - Phone battery drain or warm?
  - Trouble powering phone off?
  - Flashing or unusual lights on phone?
  - Mysterious, new icon on phone's screen?
  - Significant new data charges on phone bill?
- How can users guard against Spyware?
  - Don't ever give up possession of your phone
  - Always protect your phone with complex passcode or PIN
  - Turn off Bluetooth when not in use
  - Turn off Wi-Fi
  - Turn off NFC

Mobile Device SpyWare?

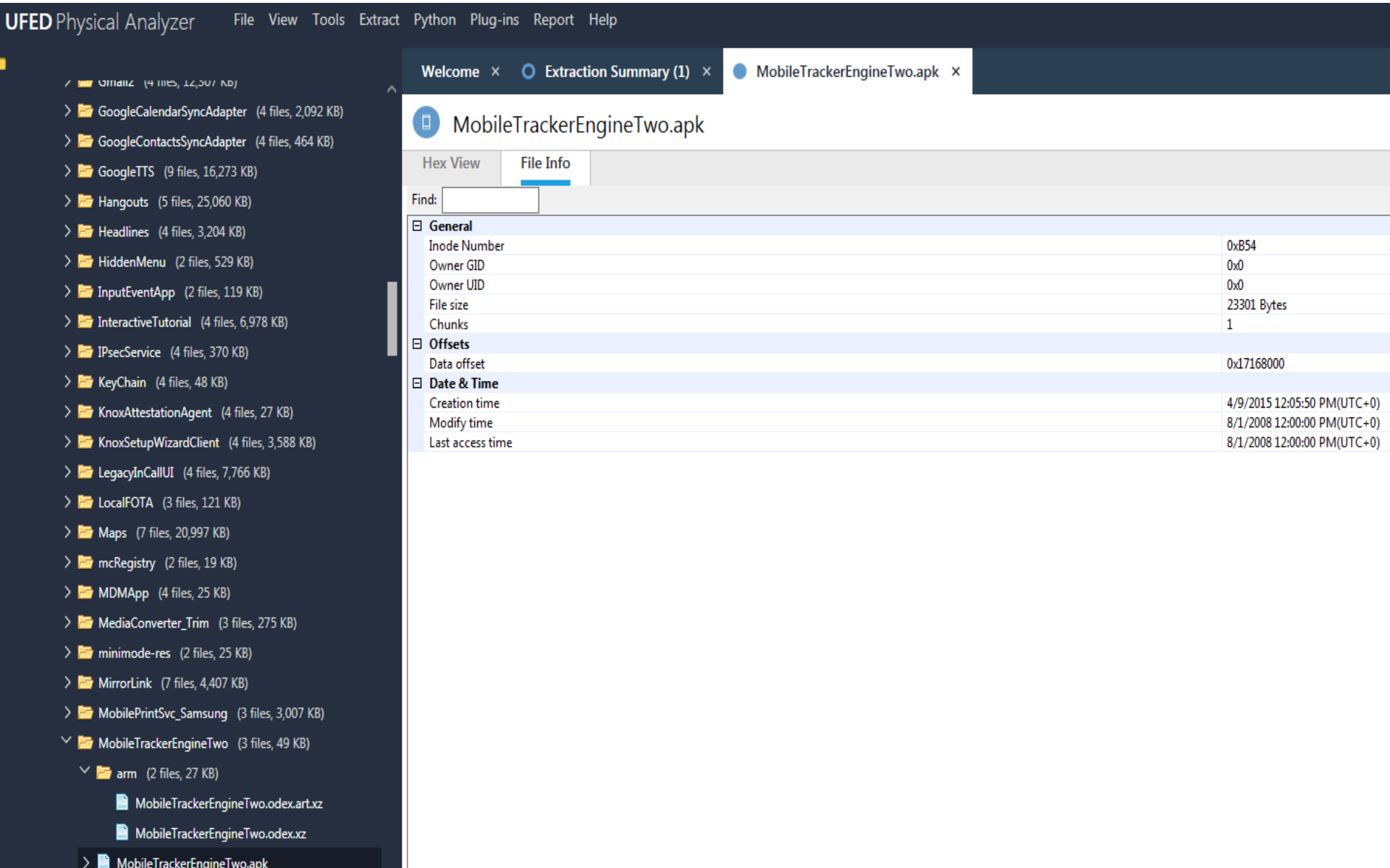
Extraction Report

Samsung SM-G900P Galaxy S5

Infected Files (3)

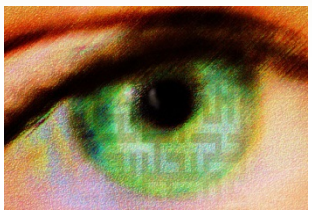
#	File Info		Additional file info		Malware Information	Malware Type	Deleted
1	Name: Path: SHA256:	MobileTrackerEngineTwo.apk system (ExtX)/Root/app/MobileTrackerEngineTwo/MobileTrackerEngineTwo.apk	Size (bytes): Created: Modified: Accessed: Source file	23301 4/9/2015 7:05:50 AM(UTC-5) 8/1/2008 7:00:00 AM(UTC-5) 8/1/2008 7:00:00 AM(UTC-5) system (ExtX)/Root/app/MobileTrackerEngineTwo/MobileTrackerEngineTwo.apk : 0 / 0x0 (Size: 23301 bytes)	Android.Monitor.MobileTrack.B	Virus	Intact
2	Name: Path: SHA256:	base.apk userdata (ExtX)/Root/app/com.fgol.HungrySharkEvolution-1/base.apk	Size (bytes): Created: Modified: Accessed: Source file	22607544 7/1/2015 7:30:16 PM(UTC-5) 7/1/2015 7:32:46 PM(UTC-5) 7/1/2015 7:30:16 PM(UTC-5) userdata (ExtX)/Root/app/com.fgol.HungrySharkEvolution-1/base.apk : 0 / 0x0 (Size: 22607544 bytes)	Android.Riskware.Agent.gXALP	App	Intact

Mobile Device SpyWare?



Categories of Cyber Attacks

- Phishing – social engineering tricks designed make user divulge personal information
- Spear Phishing – highly effective because it's targeted and personal
- SMiShing – mobile attacks using SMS
- QRishing – attacks using Quick Response (QR) codes
- Clickjacking – tricks a user into performing undesired actions by clicking on a concealed link
- Trojan or Malicious apps
- Worms – self-replicating exploits
- Man-in-the-Middle Attacks



Anatomy of Mobile Attack

VIAFORENSICS

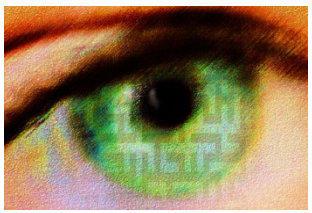
Evolution of Mobile Attacks

- Mobile platforms have been compromised repeatedly
- Quantity and value of information stored and transacted on mobile devices is rapidly increasing
- Attacks follow the money
- Experts anticipate growth in both broad (phishing) and targeted (spear phishing) attacks on mobile
- Reality Check
  - It’s about the DATA
  - Mobile data is handled by apps
  - Ergo, it’s about the APPS
  - **App Security is Mobile Security**

App User Security Stats

Apps Installed on Average Mobile Device: 320
Permissions Requested by Android Apps: 20 (average)
Apps Send Data to Ad Networks: 50%

Devices Don’t Have a Passcode: 43%
Android Devices Have USB Debugging Mode Enabled: 18%
Android Devices Allow Installation of Unverified Apps: 43%
Devices are Rooted: 9%
Unique IP Addresses Connected to Everyday: 160
Wi-Fi Access Points Connected to Everyday: 2 (average)
Mobile Devices Connect to Unsecured Wi-Fi Each Month: HALF



Analysis from 140M mobile security data points uploaded daily from 180 countries

2016 Mobile Security Report

NowSecure™

Android Settings Demo

- Screen Timeout (Auto-Lock)
- Secure Startup
- Screen Lock Type
- Secure Lock Settings
- Unknown Sources
- Other Security Settings (Encrypt)
- USB Debugging Mode
- Google Security & Backup
- Lookout App (Security & Theft)
- Malwarebytes App
- Location Services

- NFC & Bluetooth
- Mobile Hotspot
- Wi-Fi
- VPN App
- App Permissions

Android Settings Demo (7.0)

- Display / Screen Timeout (Auto-Lock)
- Lock Screen & Security / Secure Startup
- Lock Screen & Security / Screen Lock Type
- Lock Screen & Security / Secure Lock Settings
- Lock Screen & Security / Unknown Sources
- Lock Screen & Security / Other Security Settings (Encrypt Device)
- Developer Options / USB Debugging Mode (About Phone / Build # 7X)
- Google / Sign-in & Security
- Backup and Reset
- Lookout App (Security, Theft, Backup)
- Malwarebytes App
- Location or Google / Location
- NFC and Payment
- Bluetooth
- Mobile Hotspot & Tethering
- Wi-Fi
- VPN App (NordVPN)
- Apps / Application Manager / <Pick App> / Permissions

Mobile App Security

NowSecure Tested 400K Mobile Apps:

24.7% of Android Apps Have One or More High Risk Security or Privacy Flaws

10.8% of All Apps Leak Sensitive Data over Network

12.3% leak IMEIs (International Mobile Equipment Identity)

5% leak MAC Addresses (Ethernet and Wi-Fi)

2016 Mobile Security Report

NowSecure™

Mobile App Security

NowSecure Tested 400K Mobile Apps:

App Categories Having at Least One High Risk Vulnerability

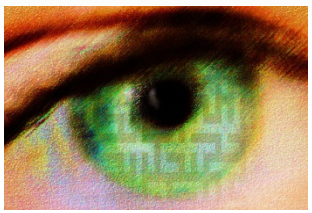
- Business: 27.6%
- Social: 30.5% (4.7% More Likely to Leak E-mail Address)

Financial App Insecurities

- 16.9% Have at Least One High Risk Vulnerability
- 4.2% Leak Sensitive Data

Game App Insecurities

- 32.8% Leak Sensitive Data



2016 Mobile Security Report

NowSecure™

Secure Text Messaging Apps

- Signal (Open Whisper Systems)
  - No-charge, open source app that employs end-to-end encryption
  - Send encrypted group, text, picture, and video messages
  - Encrypted phone conversations between Signal users
  - All you need to use Signal is your phone number
  - Supports iPhone and Android
  - Minimal user data retained
  - Electronic Frontier Foundation Score: 7 out of 7
  - Wired articles in 2016 and 2017

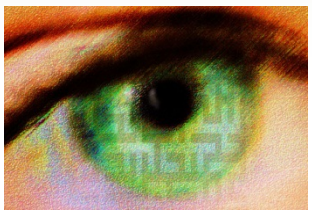
Attachment A

Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis

Secure Text Messaging Apps

- WhatsApp (Facebook)
  - Provides end-to-end encrypted messaging on iPhone & Android
  - Uses Facebook privacy policy and data sharing giving Facebook access to WhatsApp phone numbers and usage data
  - Unencrypted backups and no key change notification by default

- Allo (Google)
  - Uses “Signal Protocol” to provide end-to-end encrypted messaging in “incognito” mode
  - Uses a darker background, but is not the default mode



Advanced Security Solutions

- Password Management
  - Generate safe passwords, auto login, safely share passwords
  - Scorecards to reduce password reuse and easily change
  - Cross platform support for Windows, OS X, iOS, Android
  - Products like Dashlane, LastPass, RoboForm, eWallet, etc.

- Two-Factor Authentication (2FA)
  - Second, time-based token for access to web accounts & apps
  - Google, iCloud, Amazon, Banks, Credit Cards, Investing, etc.
  - Obtain 2FA token from mobile apps
    - Google Authenticator
    - Twilio Authy

Advanced Security Solutions

- Virtual Private Networks (VPN)
  - Service provides access to secure, encrypted network
  - Solves unsecured Wi-Fi Access Point connection problem
  - Avoid free offerings and choose service carefully
  - Consider log retention policy, performance, ease of installation
  - NordVPN supports six connected devices at once

- Mobile Device Management (MDM)

  - Central management and control of mobile devices
  - SMBs may like Google Apps or Microsoft Exchange ActiveSync for limited, low-cost capabilities
  - Enterprises may invest in industrial strength offerings like JAMF, AirWatch, MobileIron, Good Technology

Smartphone Security Checker

FCC Smartphone Security Checker

This tool is designed to help the many smartphone owners who aren't protected against mobile security threats. To use this tool, choose your mobile operating system below and then follow the 10 customized steps to secure your mobile device. More about the Smartphone Security Checker.

Select Your Mobile Operating System

- Android
- Apple iOS
- BlackBerry
- Windows Phone

Generate Your Checker

Also available, a general smartphone security checklist (PDF).

Visit the HealthIT.gov Mobile Security Guide for 10 steps you can take to protect and secure health information when using your mobile device.

Consumers using smartphones, tablets and other mobile devices as "mobile wallets" to pay for goods and services should check out the FCC Consumer Guide on Mobile Wallet Services Protection for tips on protecting devices, mobile wallet services and applications, and associated data from theft and cyber attacks.

Smartphone Security Checker

Ten Steps to Smartphone Security for Android

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. It is important to protect your smartphone just like you protect your computer as mobile cybersecurity threats are growing. Mobile security tips can help you reduce the risk of exposure to mobile security threats.

STOP | THINK CONNECT

1. **Set PINs and passwords**. To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defense in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.). You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.
2. **Do not modify your smartphone's security settings**. Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.
3. **Backup and secure your data**. You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.
4. **Only install apps from trusted sources**. Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

Consult Check List for Tips

Mobile Device Cybersecurity for Family Lawyers

Check List

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

TABLE OF CONTENTS

A. Maintain Physical Control
B. Strong, Complex Pass Phrases
C. Automatic Lock Settings
D. Disable Wi-Fi, Bluetooth, and NFC Settings
E. Public Wi-Fi Hotspots
F. Protect Home Wi-Fi
G. Mobile Device Encryption
H. Mobile Device Tools for Loss or Theft
I. Mobile Device Operating Systems
J. Mobile Malware Protection
K. Mobile Social Engineering Scams
L. No iPhone Jailbreak or Android Root
M. Password Manager
N. Two-Factor Authentication
O. Mobile Device Backup
P. Mobile App Store Validity
Q. Secure Mobile Messaging Apps
R. Mobile Obfuscation
S. Other Resources

Questions & Answers

Carney Forensics

"Digital Evidence is Everywhere"

Cell Phones / Smart Phones

Smart Tablets

Computer Forensics

GPS Devices

Social Media / Email

Sign up for our Newsletter!!

www.carneyforensics.com

Carney Forensics