**University Information Security Office**
University of South Carolina

# **Mobile** Security

It is time to start treating your phone and tablet like a computer.

## Tom Webb

Tom has a B.S in Information Management from the University of South Carolina. He holds various certifications including: GREM, GXPN, GCIA, GCFA, GCIH, and CISSP. He has contributed to the SANS forensic blog, the SANS Internet Storm Center and several open source projects.

He is currently the Interim CISO and Security Operations Manager for the university.

## "Phones" are vulnerable.

In today's world, most of us carry powerful computers with us everywhere we go. We typically call them "phones" or tablets. But, aren't they really much more than that? Modern mobile devices boast full Internet connectivity and often become warehouses of data, waiting to be exploited.

Many of the same threats facing traditional computers apply to mobile devices as well. Trojans, malware, and theft are all very real concerns. Combine that with the amount of private data most people carry on their device(s), you've found two very good reasons to start taking steps to increase your mobile security.

## *Try to avoid wireless hotspots.*

When you choose to connect your device to an unprotected wireless hotspot, an attacker could be able to see any unencrypted traffic. Plain text. Real time. They could capture your passwords, sensitive information, or redirect your phone to malicious websites.

You can help avoid this by utilizing one or more of the following solutions.

-Use a VPN (USC Juniper)
sslvpn.sc.edu

- Only use your phone's cell network or a private, protected wireless signal.

- Avast (SecureLine Product)

- Open DNS (Umbrella Prosumer)
https://store.opendns.com/umbrella/prosumer#login

These technologies and user practices will help ensure that no one is listening in on your private information.

## *Only install authentic software or apps.*

The Google Play Store, and many other Android App stores are known to carry "Trojan Horse" programs. These attacks can hi-jack your phone, allowing attackers to read SMS, spy on your communications, or target your contacts.

To mitigate this risk, make sure you only install apps you need. Those apps should be provided directly from a reputable software publisher.

## *Install anti-virus software.*

Since we have learned that mobile devices can become infected by Trojans and malware, we need to make sure we are running a trusted anti-virus software.

*(continued)*

UNIVERSITY OF SOUTH CAROLINA

Here are a few options:

**Android:**

- AVAST
- AVG
- TrustGo

**iOS:**

- Lookout
- Norton

These apps will constantly scan your phone, comparing it's contents to an established database of known threats. This allows you to identify bad apps and take action.

## Keep your operating system up to date.

When developers release an update for mobile operating systems, they are correcting performance issues and closing known security vulnerabilities. If your operating system is out-of-date, your phone **is** vulnerable.

**Android:** *(current version 4.4.4 - August 2014)*

- Settings → About Phone → Software Update

**iOS:** *(current version 7.1.2 - August 2014)*

- Settings → General → Software Update

## Keep an eye on privacy.

Many of the features that make mobile devices so convenient and useful could be detrimental to your privacy. Your device's location services allow mapping and navigation functions to operate. They also reveal your location. Likewise, a Bluetooth connection allows you to go hands-free. But, at what cost?

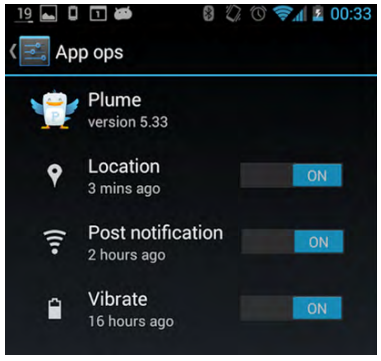
You can customize privacy settings by following these simple paths.

**iOS:**

- Settings → Privacy

**Android:**

App Ops Starter (from Play Store, Android 4.3 & newer)




## Take Charge of your security.

With the right combination of technologies, it is possible to communicate very safely from a mobile device. Secure voice calls, secure e-mail, even secure messaging is avalable. You just have to know where to find it!

**Try these technologies out for better security.**

Secure Voice Calls:

- Red Phone (Android)
- Signals (iPhone)

Personal Secure E-mail:

- Virtru

Secure E-mail attachments: (Faculty & Staff)

- Accellion *(coming soon!)*

Secure Chat:

- CryptoCat (iOS)

By using these apps to transmit your communications and data, you can have more confidence that the message is being received without being intercepted by a third party.

## Password protect your mobile device.

A passcode works just like the passwords you're accustomed to using for other devices and services. It keeps prying eyes from quickly taking control of your device and it's data.

You should always use the maximum number of digits your device allows. A standard 4-digit passcode can usually be guessed in less than 15 minutes!

**iOS**:

- Set a passcode
- Settings → Touch ID & Passcode

## Encrypt your device.

Most Android phones allow users to easily encrypt the entire device, including any external memory being used. If an encrypted device is lost or stolen, no one will be able to easily access the data it holds.

**Android:**

- Under Security
  - Encrypt Device and SD card
  - Setup Password

## Activate "Remote Wipe" features.

Another feature to protect your device and data in the event of loss or theft is the ability to remote wipe the device. With remote wipe activated, it is possible to erase all data from a device as soon as it goes missing. There is no more certain way to protect your data when you suspect a device may have have fallen into the wrong hands.

Activation and use procedures vary wildly among devices, operating systems, and service providers.

## Notes