**Mobile Device Security**

**ITA is pleased to provide this information update as part of our commitment to support your information assurance efforts.**

**Background:** As the rate of mobile device adoption continues to spike and the sophistication of these devices advances, smartphone security is becoming increasingly important. As business information and personal information move from the PC onto handheld devices, users are becoming more efficient road warriors. Unfortunately, smartphones are also introducing a great risk to the IT equation. The more capable these devices are of helping users access and manipulate data, the more capable they are of being used by hackers to do the same. Utilizing the following tips can help increase your level of protection.

**-Turn On Encryption:** Always be careful and have a level of paranoia about what happens to your sensitive information. Lock down your devices and take security seriously just as you would for any PC.

-**Require Authentication:** A survey released by Credent Technologies in September 2009 found that in just a six month period more than 31,000 New Yorkers left behind mobile devices in a taxicab. Mobile devices are too easy to lose not to use proper authentication. And yet, most users don't use the password function on their devices.

**-Utilize Remote Wipe Capabilities:** Remote wipe enables you to remotely erase all of the data stored on your phone. It's an important security feature widely available on smartphones, either by default or as an application you can (and should) install.

**-Third-Party Applications:** Smartphones are vulnerable because they are essentially miniature computing platforms that can accept any nature of third-party applications. Limit the installation of unsigned third-party applications to prevent the "bad guys" from requisitioning control of your devices.

**-Be careful with Wi-Fi and Bluetooth:** Disable Wi-Fi and Bluetooth when you're outdoors. These functions are easy to exploit for sending malicious code or viruses. It's also possible that sensitive information could be intercepted by a sniffer (software that can intercept data passing over a digital network) when these functions are enabled. The safest places to use these functions are at home or at trusted locations.

**ESS-P delivers monthly information assurance awareness updates as a customer service from ITA.**

Respectfully,
ITA Information Assurance
NIPR: ITAIA@conus.army.mil; SIPR: ITAIA@hqda-s.army.smil.mil

Reference: AR 25-2, Para. 2-8(g)
Classification: UNCLASSIFIED
Caveats: NONE

Creating Connections