SANS MGT-438

Ten Security Tips
Erik Couture

10 iPhone/iPad Security Tips

1. Use a Passcode Lock – The simplest and most effective way to reduce the risk to your iDevice is to set a good Passcode. Turn on the Passcode lock, (*Settings → General → Passcode Lock*), and avoid the most common passcodes (http://amitay.us/blog/files/most_common_iphone_passcodes.php). Use the Erase Data function to wipe your iPhone after no more then 10 failed attempts. If you forget your own PIN, you can always restore your device from iTunes.

2. Turn on Auto-Lock – A Passcode lock is of little use if it doesn't take effect reasonably quickly. Set your device to Auto-Lock in no more than a couple minutes; should your device be stolen this will maximize the chances that the device will lock out before the thief has much of a chance to do damage. Set the Auto-Lock timeout by clicking on *Settings → General → Auto-Lock* and selecting the appropriate time period.

3. Practice safe Wi-Fi – It is commonly known that Wi-Fi security is broken at worst and questionable at best. Nevertheless, the high cost of cellular data makes using available Wi-Fi hotspots tempting for most users. Prefer WPA-encrypted hotspots to WEP, and either over unsecure Wi-Fi. If you have to use un-trusted internet hotspots, avoid using ones with common names such as 'linksys', 'dlink' or 'Free WiFi', as these are quite possibly maintained by a hacker who would gain full visibility of your traffic. Ensure you prevent your phone from jumping onto any nearby Wi-Fi hotspot by forcing it to ask you before joining a network. (*Settings → Wi-Fi → Ask to Join Networks)*. Ideally, turn off Wi-Fi altogether if you're not actively using it, this will minimize your risk exposure, and save battery to boot! (*Settings → Wi-Fi → Off)*.

4. Connect to your email securely – Email often contains some of our most important personal and financial data. However, it is often transmitted completely unencrypted and readable to anyone who cares to sniff it out. Send mail securely with your iDevice by configuring your Mail client to communicate with the server using SSL. Go to *Settings → Mail, Contacts →* Your account *→ Advanced,* then set the SSL option to *On*. If your organization uses an Exchange email server, talk to your administrator to ensure your device is configured securely.

5. Browse the web securely – Even when taking care connecting to the web via Wi-Fi, it is simple for hackers to eavesdrop on your traffic if they are also logged in to the same access point. Even if you're using a WPA2 connection, a hacker who has the password (for example in a coffee shop) is effectively on the same network as you. This permits him/her to perform a variety of attacks on your iDevice including intercepting traffic and stealing your passwords. Make use of a Virtual Private Network (VPN) whenever you are on an untrusted hotspot. A VPN creates a secure tunnel for your traffic to the internet via a trusted gateway server and will prevent any attempts to eavesdrop. See http://support.apple.com/kb/ht1424 , http://www.witopia.net, and http://hotspotshield.com for tips and examples.

6. Back up and Encrypt – Backing up alone isn't technically a security measure, but having a current backup can certainly help you recover from a security breach of device loss with minimal downtime. When backing up your device in iTunes, however, ensure you check the "Encrypt Backups" box so your device's information is protected should your

computer be lost or compromised. On iOS 4.0 and later, your data is encrypted as well while at rest on the iDevice.

7. Set up remote wipe – Assuming your iDevice has been updated to iOS 4.2 or later, you have the ability to securely erase all data from your iPhone remotely, should your phone be lost or stolen. To enable and use this functionality, simply set up the Find My iPhone service (www.apple.com/iphone/find-my-iphone-setup) and you will gain the ability to wipe your phone, change the passcode lock or display a message remotely from any web browser. There's even an 'App for That', which helps you locate your lost iPhone from your iPad.

8. Update iOS and Apps – Sync your device with iTunes on a regular basis and update to the latest version of iOS when it is available. In iOS 5, being released in Fall 2011, the process of updating the operating system promises to be simplified as it will be possible over Wi-Fi, with no PC or Mac sync required. Ensure you keep your apps up to date by checking the App Store for updates and applying them regularly. Not only will this provide you with the latest and greatest features for your apps, but it will ensure any known security holes are patched.

9. Jailbreaking – Jailbreaking, the process of unlocking the phone to allow the installation of non-Apple-approved software, has gained popularity recently due to tools that make it simple for any user to accomplish. Jailbreaking, by default, opens up administrator access to your phone to remote users with a default password. This is not malware, but a function of the jailbreaking process. Left unsecured, this can open up your phone to running other, undesired, non-Approved software such as malware, and to remote exploitation. Change your root password immediately (Google "*change iPhone root password*" for instructions) and install non-approved applications at your own risk, with the understanding that they may very well be stealing your data or performing some other nefarious act.

10. Change your SIM Pin – The SIM card in your iOS device identifies you to the network for service and billing purposes but also stores personal information such as contacts and text messages. It is prudent for any GSM phone user to secure his/her SIM card using a PIN number. This is not the same PIN as the phone's auto-lock, as it locks not the phone but the ability to use the SIM in another phone, [would meaning be clearer if comma was removed] should you lose the SIM. To set the PIN, enter *Settings → Phone → SIM PIN → ON*, and enter a code.