IPAD2 – SECURITY GUIDELINES

1. Implement Safari browser security depending on your needs:

   Some of these features existed in the original iPad but there have been a few tweaks for the iPad 2.

   **Safari > Autofill** – Remove all autofill to not store any names and passwords. This may be overkill for some users but if you share your iPad 2 with many different people it is a good idea.
   **Safari > Fraud Warning On** – Enables alerting for potentially fraudulent sites (false alarms are quite common).
   **Safari > Block Pop Ups** – You could experiment with this setting to see how disruptive it is but generally we’d only recommend doing this in the highest security setup where browsing is not a big requirement.
   **Safari > Turn Java Script off** – Not recommended as it breaks a lot of web functionality.

   Like many other devices web surfing and email attachments pose the greatest threats. For continued security of your device exercise good judgment when visiting sites or opening attachments. To check the actual destination of a link examine it by prior to clicking through.

2. **Set the Auto-Lock feature** to automatically lock your iPad 2 after a designated amount of inactivity. You should choose your auto lock time setting based on your normal usage but 30 minutes should work fine for most people.
   
   *Go to General > Auto lock* choose amount of time (30-60 min is recommended)

3. **Disable Bluetooth** if you are not going to use it. If Bluetooth is active it is another potential vulnerability source so if you are not using it shut it off. This is a minor security point but always a good practice to disable unneeded services.
   *Go to General > Bluetooth, turn Bluetooth off*

4. **Don’t use public networks**

Recommended Security Software

HidePad: [http://www.hidepad.com/?hop=sgnsecure](http://www.hidepad.com/?hop=sgnsecure)