Basic Steps to Secure Your iPad or iPhone

These instructions apply to both iPhones and iPads. The term, ‘device’ will mean either of these devices in these instructions. If your device is receiving PHI or other sensitive data in emails, or such data exists on the device for any reason, it should be secured by following these instructions.

1. Select Settings.
   a. Under the General tab, set the Passcode Lock to ‘ON’.
   b. Turn the Simple Passcode to ‘OFF’. This will require you to enter a complex passcode, which must be at least eight characters and include letters, numbers and at least one special character. One letter must be capitalized for extra security.
   c. Set the Require Passcode setting to the minimum time you can live with. This setting will lock your device after non-use for the amount of time you set. You will be required to input the passcode to access all device functions when this time limit is reached. Remember when choosing a timeframe that if the device is lost or stolen, the person in possession of it will have access to all features if it is not locked.
   d. Set Erase Data to ‘ON’. When this feature is selected, all data on the device is erased when the user fails to enter the correct passcode ten times in succession. It provides a significant heightened security to the device. After the five incorrect tries, the device begins locking the device for longer periods of time. On the ninth and tenth incorrect tries, the device is locked for one hour per incorrect attempt. It is on the eleventh incorrect attempt that the device is rooted, wiped and reset to factory settings. Warnings are issued all along the way after the fifth attempt so a valid user has plenty of time to remember or find their passcode.
   e. NOTE: The Passcode Lock should not be confused with the Auto-Lock feature. The Auto-lock feature simply requires a finger swipe to open the keyboard for access. If it is used in conjunction with the Password Lock, it requires a passcode entry after time set in 1.c, but its purpose other than this is simply to prevent the touch screen from inadvertent use.

2. Return to Settings.
   a. Set Restrictions to ‘ON’. You are required to set up a Restrictions Passcode, which is a four digit number.
   b. Set Installing Apps and Deleting Apps to ‘OFF’. Anyone wanting to perform either of these functions, including you, will now have to turn off the Restrictions setting before performing these functions. The primary purpose of turning the delete setting off from a security perspective is that it will not allow anyone to delete the Find iPhone app, which you’ll be instructed to install next, or to turn off the Location Services setting for Find My iPhone.
   c. You are also given ten attempts to enter this code correctly before the device is wiped if you have Erase Data set to ‘ON’.
   d. Return to the main menu.

3. Download and install the Find iPhone app from the App Store. This is a free application from Apple. It allows you to find your iPhone or iPad on a map from any other Apple device if your device is lost or stolen. It allows you to send a message of your choosing to the device, send an alarm that sounds for two minutes, remotely lock your device, and even remotely wipe your device of all data if you’re sure the device cannot be
reclaimed. (The remote device does have to be connected via a phone signal or WiFi to perform these functions.) This app provides an important security feature for a lost device.

4. Go to Settings, General, Restrictions, Location.
   a. Select ‘Allow Changes’ if this setting is not already selected.
   b. Set ‘Location Services’ to ‘ON’. You can then determine for which stalled apps you want to use this feature. You may not want to select if for all applications.
   c. Set it to ‘ON’ for Find My iPhone.
   d. Return to the Location setting.
   e. Select “Don’t Allow Changes”. This will prevent someone from turning Location Services off in the event your device is lost or stolen, thereby preventing you or law enforcement from finding it.

5. Request the VPN (Virtual Private Network), profile from DTS and install it on your device. Turn this feature on whenever using a non-secure public network. It creates a secure connection from your device to the state’s network via the internet.

6. Request the UWDN profile from DTS and install it on your device. When operating in a state building that provides wireless access, always select UWDN as your Wi-Fi network of choice. It is a secure network.

Setting these basic features will greatly increase the security on your device. Although they may cause you some inconvenience in your daily usage, they provide assurance if the device is lost or stolen that it cannot be used or any data accessed. Do not forget any of the passcodes you’ve created. If you do, the device must be reset and you will lose any data you have stored. Sensitive information should not be stored long term on mobile devices at all, whether it is in emails, downloaded documents or in applications. Sensitive data should be transferred to a more secure permanent location and deleted from the mobile device as soon as possible.