Best Security Practices for the Apple iPad

The popularity of mobile computing and communication devices, such as Apple's iPhone and iPad, has lead to a dramatic rise in the number of these devices on our campus, as well as in the general population. That same popularity has also made these devices very attractive for theft. In this article, we'll list some ways that you can help to secure your device in the case of loss or theft, and point out ways you can protect your data should you be unable to retrieve your mobile device.

Use a Passcode. The Apple iPad can be configured to require a passcode to allow access for use of these devices, and thus access to your information and data. Using a passcode is an excellent first line of defense against unauthorized use of your device, and protecting any sensitive information and data you may have stored on it. Basic setup is simple. On either device, go to: Settings > General > Passcode Lock. There you can use the default setup of entering 4 characters as a passcode to unlock your device. For more detailed instructions, options such as using a longer passcode, and configuring the device to wipe all data after a certain number of failed attempts entering the passcode, go to: http://support.apple.com/kb/HT4113

In the event you have lost your device, with little possibility of retrieving it, there are still options to protect your data remotely, including wiping the device. Those options are as follows:

Register your iPad, with the Casper Mobile Device Management service. This service is provided and maintained by UITS. By registering with this service, a member of the SoIC IT staff will be able to remotely lock, clear the passcode, or wipe your iPad. You will find directions for registering your device here: Securing Your iPad For Use at Indiana University).

Use Apple’s Find My iPhone, iPad, or Mac service. To use this service, you must activate and use Apple iCloud. (http://www.apple.com/icloud/) If you lose your device, and it is online anywhere, you will be able to locate it using any computer, or another iOS device. You also have other options such as setting a passcode lock remotely, or doing a remote wipe. Find out more about this service here: http://www.apple.com/icloud/ Scroll down the page to learn more about using Find My iPhone, iPad, or Mac.

Use Exchange/OWA for Remote Security. If you have, or setup an Exchange account at Indiana University, you can use this account in conjunction with Outlook Web App (OWA) to remotely access your device, and do many of the above listed functions, including a remote wipe. First, you must configure your device to use Exchange Active Sync. Detailed instructions on how to do this are listed here: http://kb.iu.edu/data/axhp.html

Once you have your device synchronized with the Exchange service, you will be able to remotely access your device using OWA. Detailed instruction for using OWA to assess, and control your device remotely are located here: http://kb.iu.edu/data/avrv.html

Likely, the best overall security would be to use a combination of the passcode lock, and one of the remote services listed here. And of course, never leave your device unattended in an insecure area, such as a lab or library for even a few minutes. It doesn't take long to put one of these devices in a pocket, or backpack. If the unfortunate should happen, then one of the remote measures listed above should be applied as soon as possible, as the longer the device is lost, the greater the chance it may still be compromised, even with the above measures against this happening installed.