Use iPad safely

iPad is a secure computing device. The combination of hardware and software security makes it a safer device than a PC or Mac, especially if proper security steps are applied.

iPad is a secure computing device. The combination of hardware and software security makes it a safer device than a PC or Mac, especially if proper security steps are applied.

So far, there has been no remote attack on the iPad, the biggest safety risk is the loss of the device. Therefore, the first step is to ensure that the device's data is safe in case the device is lost or stolen.

Encryption and encryption

All iPads are manufactured with powerful built-in hardware encryption, but you need to enable this feature. The simple way to do this is to set a passcode for the iPad. As soon as the password is set, your data will be automatically encrypted. To activate a password, select **Settings** -> **General** -> **Passcode Lock** and enter a 4-digit code twice.

If you want to be more secure, you may not select the **Simple Passcode** option on the same page; At that time you can use longer code. When still on that page, you should also set **Require Passcode** (need to enter the password) no longer than 15 minutes and click **Erase Data** . (Technically, the iPad device will delete the decryption key, not actually delete the data, but doing so is faster and equally effective).

All modern iOS devices are also manufactured with a second encryption layer, called **Data Protection** . While the basic encryption feature is activated by opening passwords that protect all data on the device (including your applications), this feature can be resolved by intervention. jailbreak (jailbreak). **Data Protection** encrypts your email content and attachments; This feature cannot be unlocked even if the password has been solved by jailbreak. **Data Protection is** also provided for programmers using in the application, but few exploit this feature. (Currently, there is no jailbreak tool for iPad 2, so basic encryption is still safe; but this situation probably won't last long.)

Advanced encryption

To make the iPad's built-in security features more robust, you can use the iPhone Configuration Utility.
Designed to help businesses manage iOS devices, this utility provides an additional set of security features and settings for businesses, as well as individual users.
To use, select **Configuration Profile** -> **New** , and select **Passcode** from the displayed list. In the following **Passcode** frame, you have all kinds of options; The settings here will control your iPad. At least you can specify a minimum length for encryption.

To enable these password settings, you will also have to fill in some information on the **General** tab, especially the Profile name and identifier. If this is the only device you use, you can select **Always** in the **Security** drop-down box. (This way allows you to remove the profile when you want). If you configure the iPad for other users, you can choose **Never** or **With Authorization** (and then provide a password) so that this person cannot change the settings if you do not allow it.

Profile settings are easy to do: Click **Share** to email **profile** to your iPad. On this tablet, open **Mail** , find the letter, click on the attachment, and select **Install** . You can also export *profiles* to a file that can be downloaded and installed with the iPad Safari browser.

Enable remote wipe

Removing remote is an important security tool that allows you to delete data on lost iPads if and when this device connects to the Internet. If you have a *MobileMe* account, you can set up this account by activating the *Find My iPad feature* in **Settings** -> **Mail** , **Contacts** , **Calendars** -> **MobileMe** . Business users who connect to a Microsoft Exchange server (or other Exchange servers such as Kerio Connect) can delete their device with **Exchange ActiveSync** support. This is done on the server, not on your device, so you must do this with your IT administrator.

Remote wipe function only works if there is a network connection. That's why some companies only buy iPad 3G with data contracts.

Good safety habits

Please note the settings. In addition, there are many things you can do when used daily to make your iPad safer. One thing to do is make sure your network connections are as safe as possible. The best way is to use **VPN** virtual private network.

Another way is to use a secure connection for email. Microsoft Exchange servers encrypt data by default. If you use an IMAP or POP3 server, and it supports SSL, you can select **Settings** -> **Mail** , **Contacts** , **Calendars** -> your account -> **Advanced** on the iPad and enable this feature.

Although *Data Protection* encrypts your email attachments, when you send this document to an application like *Pages* , it is only protected by the iPad's basic encryption feature. If you really care about those documents, you can use a special security email server tool like Good for Enterprise and a free companion iPad app. Good tool blocks email attachments (and files downloaded from its secure browser) within the application, meaning you can read these documents, without correcting them. .

If you lose your iPad, one of the first things you should do is change your password on every service, like Dropbox or iDisk, that you connect to.

Finally, you should use the Password Pro application. This application helps you to have good coding habits (a complex password for each website), it syncs with your Mac and other devices over the Internet or with DropBox, and it stores recordings Security notes and other information such as passwords. The application also has an embedded browser of its own to log in to the site without having to copy-and-paste your account information.