This guide covers some of the basic steps you can take to begin to secure your personal iPhone or iPad. It assumes you are running iOS 10.

Note: Not all features are available in earlier versions, and some menu options may differ slightly.

Tips

Update iOS to the latest version
Apple will release updates to iOS to enable new features and address security issues. Try to install updates as soon as possible. You will be prompted when there is a new update, but you can check manually:

- Tap Settings > General > Software Update

Set a passcode
Your device will be encrypted, but only if you set a passcode, PIN or fingerprint.

- Tap Settings > Touch ID & Passcode > Turn Passcode On

You may also wish to slide off some functions in the allow access when locked section, to prevent others from using Siri to reveal data, or viewing personal notifications on the lock screen.

Set the phone to auto lock

- Tap Settings > Display & Brightness > Auto Lock > Select the time period to auto lock your device

Turn on fingerprint access
You may want to turn on Touch ID to unlock the device or approve purchases with a fingerprint.

- Tap Settings > Touch ID & Passcode > Add a Fingerprint > Follow the on-screen instructions

Enable ‘Find My iPhone/iPad’
To help in the event that your device is lost or stolen, you can enable the Find my iPhone feature.

- Tap Settings > iCloud > Find My iPhone > Slide to turn on Find my iPhone and Send Last Location

If your device is ever lost or stolen log into https://icloud.com/find to attempt to find it on the map, play a sound on the device, and turn on Lost Mode.

Backup data using iCloud or iTunes
You backup data to Apple’s iCloud storage when the device is locked, connected to Wi-Fi and power.

- Tap Settings > iCloud > Backup > Turn on iCloud backup

You can also backup a device using iTunes if you wish to keep a local backup.

- Launch iTunes > connect via USB > Trust the computer > Select the device and Backup Now
Use two-factor authentication

As passwords are at risk from being guessed or phished, you can use two-factor authentication to further secure your Apple ID. This means when you sign into a new device you will need to have something you know (your password) and something you have (your phone).

Apple's support page[^1] on two-factor authentication goes into detail on how to set this up and how it works in various scenarios.

Apps

Permissions

Check the permissions of an app before you install it, to make sure you are not sharing more data than you realise.

- For example, consider whether you wish to grant a torch app permissions to access your contacts, camera and microphone.

Change permissions

You can review app permissions under Settings > Privacy. Select a category and review all apps that have that permission. Slide off any you wish to disable.

Selling your device

If you decide to sell your iOS device, then you will need to remove the link to your iCloud account and erase the device. You will be prompted for your Apple ID and password.

To sign out from iCloud

- Tap Settings > iCloud > Sign Out > Tap Sign Out, then tap Delete from My iPhone

To erase the device

- Tap Settings > General > Reset > Erase All Content and Settings

Further information and help

The IT Service Desk are happy to help you connect your device to the University’s wireless network. Sorry, but the Service Desk does not provide hardware support, including repairs of any kind.