IT Security - Protecting your Mac OS X device

This guide covers some of the basic steps you can take to begin to secure your personal Mac. It assumes you are running Mac OS X 10.10 and above.

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

Tips

Have a backup

You should always have an up-to-date backup of important files, as data can be lost through hardware failure, theft of your Mac or file corruption. A backup means that your files are stored in two separate places. For example on your Mac and on an external USB drive.

Your University H: drive

Every student and staff member has access to their own H: drive storage space – it is fast, reliable, secure, and backed up nightly. Backups are retained for 30 days, but we may be able to restore previous versions of files that you accidentally modified or deleted, or that were otherwise damaged going back two months. Information about your H: drive is available in Toolkit – just search for H drive.

Time Machine

You can use Time Machine[1] to back up your Mac to an external USB drive. Normally, this is offered when you first plug in an external hard drive. Select **use as backup disk** on the external drive you want to use.

If you are not prompted to enable TimeMachine click **Apple menu (top left)** >**System Preferences** > **Time Machine**. Select **Backup Disk** and then select an external hard drive you wish to use as a backup drive.

Once you set up Time Machine, it will take hourly backups automatically for the last 24 hours, daily backups for the past month, and weekly backups for all previous months. It will remove the oldest backup when the drive is full.

Update Mac OS

Apple will release updates to enable new features and address security issues. Try to install these as soon as they are available.

- Click **Apple menu** > **System Preferences** > **Software Update**[2]
- Click **Update Now** to install the latest updates for the currently installed version
- Click **Upgrade Now** to install a major new version

Enable password prompts

Rather than launching straight into the desktop, you should have a logon password to protect your device in the event it is lost or stolen.

- Click **Apple menu** > **System Preferences** > **Users & Groups** > **Login Options** > Click the **padlock icon** to unlock it, then enter an **administrator name and password**. Click **Automatic login**, then **Off**

---

[1] https://support.apple.com/en-gb/HT201250
[2] https://support.apple.com/en-gb/HT201541

- To prompt for a password after waking from sleep: **Apple menu** > **System Preferences** > **Security & Privacy** > **General**. Turn on **Require password to wake this computer from sleep or screen saver**

Turn on disk encryption

Apples disk encryption is called FileVault[3]. You can use FileVault to ensure you data is not readable in the event your Mac is lost or stolen.

Check the status of FileVault

- Go to **Apple menu** > **System Preferences** > **Security & Privacy** > Click **FileVault** tab > If FileVault is not enabled, click **padlock icon**, enter **administrator name and password**, click **turn on FileVault**

Turn on the firewall

A firewall will control any incoming connections to your Mac from an external source.

Check the firewall status

- Go to **Apple menu** > **System Preferences** > **Security & Privacy** > Click **Firewall** tab > If Firewall is not enabled, click **padlock icon**, enter **administrator name and password** and click **turn on firewall**

Review privacy permissions

You can give applications permission to access information, for example your location. It is a good idea to review privacy permissions to make sure you are happy with the permissions you have granted.

- **Apple menu** > **System Preferences** > **Security & Privacy** > Click the **Privacy** tab > Select a category such as **Location** and review all apps that have that permission

Review sharing settings

There are various ways to share data using your Mac, such as allowing file sharing, screen sharing or remote logins.

You can review Sharing settings under **Apple menu** > **System Preferences** > **Sharing**. Look for services that are ticked **On**. Untick any that you want to switch off.

If you want to switch a sharing service on, select it and review the detailed settings so that you understand the data you are sharing.

Enable 'Find My Mac'

To help in the event your device is lost or stolen you can enable the Find my Mac feature.

- Click **Apple menu** > **System Preferences** > **Apple ID** > **iCloud** > Log into your iCloud account and turn on **Find My Mac** > You will also need to enable **Location Services**

- If your Mac is ever lost or stolen, log into iCloud Find to attempt to locate it on the map, play a sound on the device, or lock and erase the Mac[4].

Run an Anti-Virus

Although Macs run an anti-malware product called Xprotect and experience fewer malware threats than Windows devices, they are not immune to viruses.

---

[3] https://support.apple.com/en-gb/HT204837
[4] https://support.apple.com/en-gb/HT210515

You can install a freeware Anti-Virus package to scan your Mac and any USB drives. Two example products free for Mac personal users are Sophos and BitDefender

Make sure you update your anti-virus product and run scans regularly.

Use complex and unique passwords

It is a good idea to use complex passwords and have a unique password per website. You can use a personal password manager to help you.

iCloud keychain

Apple's iCloud keychain[5] syncs your passwords across all of your Apple devices. You can choose to store your passwords on each device, or on the cloud.

Other password managers

Other password managers are available, such as KeePass, LastPass and 1Password. Some are free and some may have a small annual charge.

Selling your Mac

If you decide to sell your Mac, then you will need to remove the link to your iTunes/iCloud account as well as erasing and reinstalling OS X.

To sign out from iTunes

- Open i**Tunes** > click the top **menu bar** > **Account** > **Authorisations** > **Deauthorize this computer**

Sign out of iCloud

- **Apple Menu** > **System Preferences** > **Apple ID** > **iCloud** > deselect the **Find My Mac** checkbox

- **Apple Menu** > **System Preferences** > **Apple ID** > **iCloud** > **Sign out**

Erase and reinstall OS X

- See Apple's fact sheet[6]

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.

---

[5] https://support.apple.com/en-gb/HT204085
[6] https://support.apple.com/en-gb/HT204904