MouseTracks
Issue 10
May 2018
News from *MacOnSite*

Getting messages about Upgrading?

When should you upgrade your Operating System?

Apple now manage all updates and upgrades through the App Store, and by default this is set to inform you of when new versions of macOS (the operating system) and any applications which you have downloaded from the App Store are available. The messages can be quite persistent so it can be very tempting to accept them just to stop them being annoying. But is that the best course of action?

Updates: These are usually bug fixes and security patches and it is good idea to install them. They will change your software from, for example, macOS 10.12.1 to macOS 10.12.2. Only very occasionally do they cause a problem which is usually quickly rectified with another update.

Upgrades: These are significant new releases of application and operating system software. Updates will change your software from, for example, macOS 10.12.x to macOS 10.13.x. The operating system upgrades are the most significant as this is the software which actually runs your Mac and enables you to open applications such as Safari, Mail, Pages, Word etc, and controls everything from pictures on your desktop to network connections and printing documents. Upgrading the operating system can bring unexpected changes. Some software may no longer work or need upgrading (which might not be free), the performance of your Mac may be impeded, or in the worst case scenario, something may go badly wrong during the upgrade and your data is erased. So, before upgrading, ask yourself a couple of questions:

1. What new features in the upgrade do I actually need?
2. Is all my software and hardware (including printers and scanners) compatible with this new version?

If you decide to upgrade, make sure you have a least one full backup of your Mac before you start, and set aside plenty of time for the upgrade to install as they can sometimes take a few hours. If you have any questions or concerns, just get in touch and we can address them.

Airplane Mode in iOS 11

Apple have made a subtle but useful change to the way Airplane Mode works in iOS11 (this only applies to iPhones and and iPads which have a SIM card). Previously, when turning on Airplane mode, both the SIM card and the WiFi hardware were switched off. It was then possible to turn the wifi back on again and leave the SIM card switched off, and this complied with most airlines requirements. Now however, switching on Airplane mode ONLY turns off the SIM card, so you no longer have to go and turn the Wifi hardware back on again. A small change, but helpful.

Away from the desk…

Watching the sun set from our accommodation on the Kapiti Coast:

Getting to Grips with…Planning for a disaster

Disasters can take a number of forms: fire, flood, theft, earth quake, volcanic eruption, or visiting children/ grandchildren. The outcome is the same: you are separated from the data which runs your life, helps you earn your income, and provides memories of the past. You and your data may never be reunited again unless you plan for such an eventuality.

There are two key strategies to put in place prior to a disaster to help you recover your technological equilibrium successfully.

1. Insurance - certainly house/office contents, and probably building too. One of the biggest challenges to overcome after some disasters is finding somewhere to put your workspace so that you can get up and running again.

2. Data backup which is somewhere else, ie: off-site, as opposed to just in a different room in the same building. This is just as important for home users who store all their photographs and music on their Macs as business users who store all their financial and management data on their Macs.

I am not an insurance broker so I am only going to consider data backup.

The basic philosophy for data backup for disaster recovery is to keep a copy of the data off-site; away from your home or office. There are two common approaches to achieve this:

Backup to the cloud

All the common cloud syncing services (iCloud, DropBox, Google Drive etc) effectively also provide you with an off-site backup. iCloud is very good for your Contacts and Calendar data, and can all deal with Notes, Bookmarks, Photos and Documents. DropBox and Google Drive are also good for documents, but the caveat with all the services is that to copy your documents to the cloud, they have to be in the correct location on your Mac.

For email it can simply be a case of using IMAP instead of POP for your email protocol, and that way all your email data is stored on the mail server as well as your Mac.

Managing applications takes a little more planning as it requires all software to be purchased on-line, either from the App Store or as a download from a website. In order to be able to reinstall the applications in the event of a disaster, the account credentials (usually a username and a password) will be required and so should be stored somewhere else other than on your Mac. This also applies to your cloud storage and email service accounts. There is no point in keeping a file of this information in your DropBox folder if you can't remember your DropBox account details in order to access your account from another machine.

Cloud backup software is also an option, but tends to lead to a false sense of security as internet upload speeds are often much slower than download speeds so the backups take a long time so there may be key data missing.

Multiple Drive Backups

Backup products such as Time Machine and Carbon Copy Cloner can make a full backup of your Mac hard disk to multiple external hard disks. A common scenario is to have two external drives for backup, which get swapped at regular intervals so that one is always on-site and one is always off-site. With this approach if disaster strikes, your Mac can be completely rebuilt from the off-site backup drive.

There are a couple of caveats with this approach:

1. If you swap drives out once a month, the data on the off-site drive could be up to a month out of date in the event of a disaster.

2. Keeping a copy of all your application account credentials is still necessary as many applications (Microsoft Office being the obvious example) can detect that they have been reinstalled from a backup and will need re-authenticating.

The best approach?

Use a combination of the two. Keep a full backup off-site and frequently changed data in the cloud.

In order to ensure that you have the best approach, every so often (say once a year) your disaster recovery plan should be tested.

If you need any help working out what is best for you, just get in touch.