Backup 101 - Rev 4 Jan 2021

By Phil Davis
January 5, 2021 (Revision 4)

I'm sure that you have heard this advice before — Back up your computer! This simply means that you should make a copy of all the data on your computer. The reason for this is simple. Lots of things can happen that result in data loss – no one is immune, so you should be prepared. Some of these are our fault; some are out of our control. If you plan and make smart choices, backups should not be a burden. If you have nothing worth saving on your computer, then stop reading and go do something else. But if you have any nagging worries, then you might want to read further.

Start planning your backup strategy by understanding the threats and the tools available for mitigating them. Think about your tolerance for the risks and make a plan that meets your needs.

Level 1: Human Error - The most common reason for data loss.

- **Threat** - Loss of data in individual files or folders. This can be caused by accidental deletion of files or folders, accidentally reformatting the system drive or operator errors.
- **Tools** to mitigate the threat:
  - **CMD + Z** Undo. Your first line of defense. Memorize this!
  - **CMD + S** Save your work often, then use **File > Revert** to restore locally-stored versions of your documents. This action works like Time Machine, but for a single file stored on your computer.
- **Software:** Use the Mac Time Machine app to automatically save versions of files and folders on an external drive. Incremental backups allow you to go back in time and fully recover an earlier version of a file or folder you changed or accidentally deleted.
- **Hardware;** An external USB Drive at least 2x the size of your internal storage. (Western Digital, Seagate, OWC)

Level 2: Hardware/Software Failure - It can and does happen.

- **Threat** - Irretrievable loss of large amounts of data, loss of applications & settings, or an utterly non-working computer. This can be caused by a system drive failure, operating system or application file corruption, physically damaging your computer or a myriad of other local catastrophes.
- **Tools** to mitigate the threat:
  - Create clone backups on external drives. A clone backup contains an exact copy of everything on your internal drive. Most of the clone backup software can configure the

backup so it is not only a copy, but is “bootable” – this means you can start and run your computer from the external drive. It will be slow, but in a disaster, you won’t care! Be aware that the clone will be a copy of everything at the time you make the clone. If you delete a file or folder, it may be deleted from the backup too, unless you have configured the software to archive deleted files.

- **Software:** Bootable clone software. (CarbonCopyCloner, Chronosync, Superduper)
- **Hardware:** An external USB Drive at least the size of your internal storage. (Western Digital, Seagate, OWC)

Level 3: Catastrophic failure - Think of this as an insurance policy, like homeowners insurance.

- **Threat** - Loss of computer, loss of data, loss of local backups drives. This may be the result of a natural disaster, fire, theft, ransomware attack, or other large-scale catastrophic events.
- **Tools** to mitigate the threat: You need an off-site backup in case of theft or disaster (fire, flood, etc). If someone breaks into your home and takes your computer, they will probably grab any hard drives they see. If your home burns down, is flooded, or gets wiped out by a tornado or hurricane, both your computer and your backup drives are going to be lost.
    - Offsite data storage using two external drives that you regularly exchange. You can also store a second clone backup at the house of a friend or relative. Remember, you will have to update the clone periodically so that the files will be reasonably current.
    - Offsite data storage using cloud backup services. Cloud backup services require you to create an account, download and install their app, and let it run. They often offer a free trial period of at least a couple weeks (which is good since it will take a while for your files to upload anyway). After that, it’s a matter of leaving your computer turned on until the initial upload is completed.
- **Cloud Backup**
    - A cloud backup service subscription. (Backblaze, Arq Cloud Backup, Carbonite)
- **Off-site Backup Using Swapped Drives**
    - **Software;** Bootable clone software.(CarbonCopyCloner, Chronosync, Superduper)
    - **Hardware:** Two external USB Drives at least the size of your internal storage. (Western Digital, Seagate, OWC)

Seven Things to Consider

1. Create a Plan for addressing backups and implement it. Avoid procrastination!
2. Backups should be automatic. You don’t want to rely upon your memory to make a backup. Use software that allows you to set a schedule and forget about it.
3. Keep external drives plugged in and configure the software to backup automatically on a regular schedule.

4. Backup drives can fail, so you might want to back up to more than one drive or have multiple drives you can rotate. Sure, one backup is better than nothing, but if that drive fails, and it will fail at some point, you no longer have a backup.
5. You should test backups regularly. If your backup drive fails, you won't know until it's too late unless you test it regularly. Boot from your bootable clone occasionally. Check your incremental backup every so often to see if you can view and restore earlier versions of files.
6. Make sure you know how to contact your off-site backup services if you need to recover your data. Phone numbers, email addresses, and login credentials are essential.
7. Keep your backup software updated.

Recommendation: Adopt a 3-Prong Approach

This approach will provide a strategy that should protect you for the inevitable day when you make a stupid mistake, your hard drive dies, or disaster strikes.

1. Make an incremental backup – to guard against individual file loss and operator error;
2. Make one or more bootable clones – to guard against local system and computer loss;
3. Maintain an off-site backup – to guard against catastrophic failures.

How to Use Disk Utility to Format an External Drive

Before you use a new external drive, use the Mac Disk Utility app to erase and format it. The reformat will ensure that the drive is ready for use on your Mac. I recommend doing this even if you buy a drive claiming to be for the Mac.

1. Plug the drive into a USB port on your computer.
2. Select **Disk Utility** from the Utilities window (or launch it with Launchpad).
3. Select the external disk from the sidebar. **Make sure** that you haven't selected the internal drive, usually called Macintosh HD.
4. Click the **Erase** button, then complete these items:
5. **Name:** Enter a name that you want the volume to have after you erase it, such as **Backup 1**.
6. **Format:** APFS
7. Click **Erase** to begin erasing and reformatting.
8. When done, quit Disk Utility.

Note: If you want to format a drive so that you can read it on both Mac and PC, you must use a PC format (FAT, ExFAT, or NTFS). **Do not use these formats for backing up a Mac**.

Frequently Asked Questions

What About Using Dropbox, iCloud, Google Drive, and Other Cloud Storage?

When you create a Dropbox account, you have a local folder on your computer that is synced with a folder on the Dropbox server. When you connect to the internet, saving a file to your local Dropbox folder uploads it to the server folder. If you have Dropbox installed on all your computers and mobile devices, changes to the files and folders will be synchronized.

iCloud functions the same way and has the advantage of synchronizing your data between all connected devices. iCloud is native to the Mac but it can be installed on Windows PCs. Other cloud storage choices, include Google Drive, Amazon Cloud, and OneDrive.

Do I need a separate hard drive for my clone and incremental backups?

No, but with one crucial caveat. All hard drives die, and that includes your backup drives. If you use one drive for both backups and that drive has a hardware failure, you will have lost both of your backups. Don't put all your eggs in one basket.

Should I use a secure USB drive for off-site storage of critical files?

If you decide to store your most critical data off-line somewhere, you may want to consider a high-capacity USB drive. A USB drive can make this process quick and easy, but they are not very secure. All someone needs to do is plug the USB into any computer, and they will have access to your files. This is where secure USB drives are useful; they have built-in security features to prevent unauthorized access to the sensitive information on your USB drive.

What About Creating Archives?

When you have files you may never need again, but can't bear to part with, you may want to archive them by saving to an external drive. Some people with extensive collections of photos, videos, or music find that storing these files as archives on external drives is a good solution. However, your archive drives are not the same as your backup drives. The archive drives must be backed up too because they are susceptible to hardware failure, theft, and the other problems that could cause data loss.