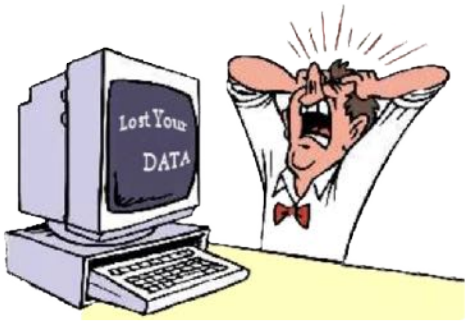
Protecting Your Files - Understanding Backup Strategies

Are you Keeping Your Digital Files Safe?



Backing up your data files (photographs, documents, etc) is probably the most forgotten important concern that you should have. Hard drives go bad, often when you least expect them to and even at times when they are still fairly new. Files can become corrupted. You need to have a good backup strategy that is consistent and regular or you will quickly learn the heart breaking feeling of losing precious data.

There is a general "rule of thumb" to consider a 3-2-1 backup strategy.

3 Copies of Your Files

2 Local Storage Media Devices

1 Copy Off Site (Cloud Drives)

#1) Store 3 copies of your files

#2) Two copies are are kept on local storage devices

Storage Device #1: Your computer hard drive is of course the first location where your files are stored.

- How old is your hard drive? More than a couple of years? You are flirting with losing all your data. Hard drives can last for many years, or a month even on a brand new computer.
- Even though your computer seems to be running well, small sectors of your hard drive can be failing, which mean that files are becoming corrupted.
- Don't tempt fate and lose your files by keeping them only on your computer!!

Storage Device #2:

USB Hard Drives: These are typically small, portable devices that have become fairly inexpensive over time.

- It's not unusual to find a 1 terabyte drive for about $60. USB Drives are now exceeding 4-6 terabytes in size. One

terabyte equals one thousand gigabytes, and can hold an impressive amount of data. These drives are durable and dependable, but remember that they too can crash, so at some point, you may want to swap out that drive for another.

Solid State Drives (SSDs): These are small "diskless", all digital data drives without any spinning platters to go bad.

- These are now becoming more common and coming down in price.
- They are quick in transferring files, small and portable.
- A one terabyte SSD will run a little over $100.
- They are supposed to "last a lifetime", but what that actually means at this point is still unknown.

DVD & BluRay Disks: Old technology and should NOT be considered as a backup medium.

USB Flash Drives: Old technology and should NOT be considered as a backup medium.

#3) One copy of your files should be kept "off site":

- At least one copy of your backup needs to be kept off site or in a location other than in your home. Think about it. What if you have a home disaster like a fire, flood, or a burglary! All your data, computers, backup drives, etc are gone. How SAD! (:
- "Cloud Drives" are one way to keep your files safe in a location other than your home.
- Another off-site option is to use a backup service that will send copies of your files to be stored at a hosted server site should you ever need to record from a hard drive failure
- Another option that you might consider is do your weekly backups onto an external USB drive and have a family member store the backup at their home. While a good option in theory, it can be difficult to remember to update that backup on a weekly basis.

Protecting Your Files - Understanding Backup Strategies
Are you Keeping Your Digital Files Safe?

Additional Things to Think About:

#1) Application Software Becomes Obsolete

- Many of us have used word processors like Microsoft Word, WordPerfect, Apple Pages or other proprietary software. They are great tools to help us put our memories and thoughts to "paper" or a digital file. Realize however that each software application will save your files in their own proprietary format. This means that one program may or may not be able to open your file created in a different software program.
- Years ago, WordStar was one of the highest regarded and most utilized word processing programs in the world, at least until Microsoft developed their Microsoft Word program. If you had saved files in the WordStar format back years ago, you are now out of luck in being able to open those files. What a tragedy if those files were histories that you had spent a long time creating.
- Interestingly, even the early versions of Microsoft Word file formats can no longer be opened by current versions of this software. It is becoming more difficult for other software programs to open WordPerfect files, a program that once was a common program out there. What happens when your operating system updates and no longer runs WordPerfect? What happens if the software company no longer keeps the software current? How will you open your digital files in the future?
- It is probably best practice at this point to save your file in RTF (or Rich Text Format) which is a standard file format that can be opened across many different programs. You will lose some of the ability to maintain more special formatting options, but for most written histories, without fancy tables, inserted graphics, etc, works out fine. In addition to saving your document as a RTF, also export it to a PDF (or Portable Document Format), which is an industry standard file type. This file type is not however meant to be editable, only viewed. I have had some old Word 95/98 data files that can no longer be opened in the current Word program. Not a good thing if they were histories, journals, or such. Microsoft Word has gone to a non-proprietary XML format that even open-source software like LibreOffice can open.
- Another option would be to save your files in your program's standard file format, especially if you are using Microsoft Word type format. Then also export your file as a PDF to maintain a 2nd file type.
- As you save files and no longer really view them over time, reassess whether those important files need to be converted to a newer file format in case you need to edit the file.

#2) Think about the type of backups you are creating

- There is a good article about the different types of backups used today found HERE.

- Periodically create a new "Full Backup Set". Even the different types of backups can "potentially" lose pieces of your data files. Retire your current backup set, placing it into a new folder labeled something like "20200318 - My archived backup set". This would tell you that the file backup set was archived on 18 March 2020. Keep this backup set on a USB hard drive that is not constantly being used, and stored in a fireproof box somewhere safe. You could also keep a copy in the "cloud" as well.
- Avoid backup software that packages all your data backups into one package. The old "Microsoft Backup" back in earlier versions of Windows did this. Once they moved on to a new version of Windows, all those packaged backups could no longer be accessed as the backup software became obsolete. The best software just keeps all of your files in a readable folder system like the original files.

#3) Think about using "Cloud Drives"

- There are many different providers that will gladly "host" or store your data for you. Some examples of these include Microsoft OneDrive, Dropbox, GoogleDrive, Apple iCloud, and others, each offering you varying amounts of free and paid storage. Each company has their own pricing structure, so do shop around.
- A nice thing about using the "cloud drive" is that your files are constantly kept synchronized between your desktop, laptop, tablet, and the cloud drive. Making changes to a file on your desktop will automatically cause any changes to that file to be changed on the cloud drive, and then on to your other attached devices as well.
- One of the concerns about cloud drives has been security. Your files are encrypted on the hosting cloud site, but the encryption is only as good as your username and password!! A strong password will keep you safe, unless you've written it down on a piece of paper that someone somehow gets access to. Should the hosting sites computers go down, you still have your "local" copies on your devices. However, realize that these server farms or hosting sites, are constantly maintained and with redundant backups themselves.
- Besides a strong password, also use "Two Factor Authentication". This typically entails the host service sending you a text or email with a code that you must enter when you try to log into your hosted cloud drive.
- Though cloud drives can be considered a good method of keeping your files off site, they are NOT a true backup. There are other services, like BackBlaze, iDrive, Carbonite, Mozy, and many others that will continuously back up your files to off site storage. They generally run about $60 per year, and most allow unlimited backup sizes. The backup process continuously happens in the background. Realize however that if you have upwards of 200-300 gigabytes of off-site backup, that when it comes down to restoring all those backup files onto a new hard drive, that it could take a week or two

until all the files are restored!! Some companies will make a copy of the files from their server onto a USB drive and mail you this drive to restore all your files.