



March 7, 2008

Backing Up Your Files, Before Its Too Late!

Sean Sweeney

In my line of work, I've heard the horror stories of losing important data more times than I care to count. I've been cussed out in person and over the phone by people who lost their data due to their own stupidity, or hardware failure. In their fit of rage they tend to always place blame on the computer repairman or tech support. Sometimes it is financial data, a novel somebody had spent 2 years writing, all of their family photos, and sometimes it is just little things like music files or even pornography collections. I've literally heard it all.

Call me cold hearted, but in each of these situations the person spends at least 5 or 10 minutes shouting at me about how important that data was to them, and why it was so important to them. My response? Again, call me cold hearted if you will, but I usually answer with this phrase, "It couldn't have been that important, or you would have backed it up." When it comes down to it, it is true. The problem is that most people don't realize how volatile the information is on their harddrives, combined with the fact that most people don't know how to back it up.

Sometimes people think they are backing up their files, only to find out when the time comes that the media they thought had their backups was either blank or didn't contain the right files. So knowing how to backup files is also important.

Rule #1: Don't trust the harddrive!

A harddrive on your PC is a bad place to trust important data to be stored safely. There are several reasons why:

- **Harddrive failure:** A harddrive is a mechanical device and subject to failure. Period. Current statistics show a harddrive being the most likely component in your computer to fail. The good news about that is that drives are cheap, easy to replace, and are very compatible between different computers so finding one that works with yours is easy. The bad news is losing what is stored on the drive.
- **Accidental erasing:** This is the most common issue I see. Most people accidentally erase something important or somebody else who uses the computer erases the information not realizing what it was.
- **Viruses and Spyware:** Some viruses actually purposely corrupt data, but this is not very common. What is common is that it may cause your system not to boot correctly and make it difficult or impossible for you to access your data. Often a complete hard-drive wipe and re-install of the operating system is required to correct it, usually causing you to lose all of your files. If the data is very important, you can pay somebody to retrieve it, but don't expect it to be cheap.
- **Theft:** Yes - people steal computers all the time. Many unfortunate souls have returned home or to their office to find the computer gone, along with a fortune in valuable data that was stored there.

Rule #2: Don't wait until you think there is a threat.

Putting it off until you feel there is a reason to back it up is not a good idea. Most of the above mentioned problems are not problems that creep up on you. It usually happens instantaneously and once it does, it's too late. If you have any files at all on your computer that you would be upset about if they were lost, the time to

start backing them up is NOW! In fact, it is accurate to say that losing your data isn't a question of if, rather of when.

Rule #3: Pick a backup medium that is reliable.

- Don't use another harddrive, especially one that is connected to the same computer as the main drive. Although this is better than nothing, most of the problems such as virus, theft, and accidental erasure will just as likely affect both drives.
- Don't use cheap CDs or DVDs. Believe it or not, in the last few years CD and DVD media have become temporary storage. Most manufacturers make claims of impressive storage life, but in reality I wouldn't put any data on an optical disc that you would want to read next month, much less next year. The discs have just become extremely unreliable. DVD-RAM and the re-writeable media such as CD-RW and DVD-RW actually may be more robust for long term storage, as ironic as that sounds. This is because they do not employ dyes. One of the main problem of data loss on optical media is that the dye fades over time and becomes unreadable. The re-writable media such as DVD-RAM and the RW media actually use a crystalline material.
- Don't use floppy disks. Although most peoples data won't even fit on a floppy these days, the floppy disk media has become extremely unreliable the last few years as the market for them has declined and manufacturers are trying to cut costs.
- Don't use zip disks or other proprietary formats. If your computer is stolen or damaged, it may be difficult to find another drive to read the disks in. Not only that, but most of these types of formats have proven to be unreliable.
- Don't assume because it is stored in your email or other online facility that it is safe.

What is recommended?

I tend to recommend protecting your data from two fronts. Primarily, use one of the options below as a your first line of defense. Follow that up with introducing a remote backup solution as your secondary. Important data should be protected twice. Consider that you only use one of the options below to return home or the office to find that your systems and removal backup both destroyed by a flood, fire or energy surge.

- USB Flash Drive: Right now for consumers with files up to a couple gigs of personal files, this is the best option. They are nearly indestructible, and the data retention seems highly reliable. They are also very inexpensive. Be sure to remove the flash drive from your PC.
- If you are going to use optical media, use the expensive ones. They even make "gold archival" quality CD and DVD media that cost about 3 times what a regular disc costs, but have much better life expectancies. Also DVD-RAM is a good, although commonly overlooked medium.
- If you have a lot of data, it might be worth looking into a more high-end backup solution such as DLT or LTO tape drives.

Rule #4: Pick a good location.

It makes sense that if it is important enough to back up, then it should be stored in a safe place. Your backup data could start deteriorating as soon as you finish writing it if your not careful. Unfortunately, this is often overlooked and consumers find out the hard way. All backup media is extremely susceptible to their storage environment. Remember, the life expectancy stated on media packaging is best case scenario and under controlled circumstances only. Any deviation from the optimum storage environment can seriously decrease that life expectancy. Don't be fooled by marketing when it comes to your important data.

- Don't trust a standard fire-safe! They are good for storing papers, but if your house catches on fire, don't expect things like CDs and floppy disks to work afterwards as they will melt. Paper can survive much hotter temperatures when direct exposure to flame is not an issue. Now, it is okay to use a safe, in fact, not a bad idea at all. Just understand that few safes that are available through standard means will protect your data from a fire.
- Don't store optical media where it is exposed to light - any light at all. Of course, you shouldn't be using optical media at all, but the more it lays out in the light, the less life it will have. Sunlight can wipe such a disc

in a few hours.

- Cool and dry! Almost all forms of media hold up better in a place that is cool and dry. So the attic or the trunk of your car is not a good place, and neither is the bathroom or kitchen.
- Dust free! The current tolerance on most drives is 1-2 microinches (1 millionth of an inch.) Comparatively, a speck of dust is 4-8 microinches and a human hair is 10 microinches. Contaminants of this size can cause serious data damage.
- Don't keep it with the computer. If the computer is stolen, the media might be too.
- Use an online storage service like Fortress Data Vaulting as a secondary option. If something should happen to your local copy then you always have your remote backup to fallback on.

How to get started.

If you have never backed up your computer before, then you may not know where to start. Let me first start by saying it isn't really necessary or even that useful to backup the whole computer. Generally speaking, you just need to backup your personal files. Here are some tips to help you get started.

- Don't worry about trying to backup and account for everything in one day. You'll always miss something. Unless there is some dire emergency, backup anything you can think of and keep using your computer. As you perform each task over the next several days ask yourself, "Do I have this backed up?" You will likely continue to discover items that you use occasionally that are not backed up.
- Don't worry about backing up software applications. It isn't practical and often it isn't even possible. Just make sure you have the original installation disk or some other way to re-install that program, should your harddrive get wiped. For example, if you use Microsoft Word to write a book, don't worry about backing up Microsoft Word the program, just make sure you backup the .DOC file that your book is stored in. That way when the time comes, you can just re-install Word from the original Word CD and then copy your .doc file back from the backup you made.
- From this moment on, try to keep your data more organized and consolidated into one folder. For example, your "My Documents" folder is a good place to start. Then when it is time to backup things, you only need worry about copying that one folder. Try to avoid keeping things on your desktop or in other locations on your harddrive.
- Email - Some people are concerned about backing up their email folders. If you are using a web-based email system such as Yahoo, Hotmail, Gmail, etc.. Forget it. There is no easy way to do this. If you are using a local email client such as Outlook Express or Outlook, it is possible to back it up but would require an entire document to explain how to do this. Do a quick search on the web and you'll find a few good solutions.

How to use Windows Explorer

So how do you actually copy files? If you are inexperienced in copying files, here is an easy way to do it. Open your "My Documents" icon which will either be on your desktop or in your start menu. Find the files you want to copy. Now don't do anything with them yet. Just resize the window with your mouse so that the window is only half as big as your screen. Then move it over to the left. Next, open the drive where your backups are going to go. For example, if you are using a USB flash drive, open the "My Computer" icon on your desktop or in your start menu. Look for the drive which will be your USB drive, then open it. Now resize it so that it fits half your screen and move it over to the right. Now your screen should look similar to the picture you see above.

Now copy the files you want by using the right-button on your mouse and dragging the item from the folder on the left and releasing on the folder to the right. It should pop up and ask you if you want to copy here or move here. Just pick copy. It is that easy. If you want to do more than one file you can hold down you shift key or control key while you click each item, then drag them all at once.

For using CD and DVD media, you'll have to follow the instructions for the specific mastering software that came with your drive.