

Backup 101

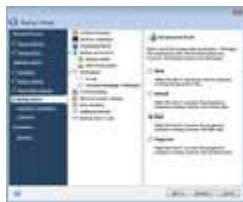
Prevent A Data Disaster

The consequences of not backing up data need no explanation. Just imagine this: You turn on your computer and nothing happens. The hard drive is gone, all the data on it is gone, and there's nothing you can do to get that data back. If that thought doesn't make you want to back up everything on your computer immediately, then nothing will.

Unfortunately, backing up data is a chore. Many **backup** programs are readily available, but they are packed with enough features to confuse anyone. Furthermore, selecting the wrong type of backup when using these types of programs can actually do more harm than good, depending on how you want to store your data.

First you need to understand the basics of backup.

Full Backups



Some backup software, such as Acronis True Image Home 2009 (\$49.99; www.acronis.com), lets you compress backups so they require less storage space.

alone. Full backups that are not modified (such as those stored on recordable DVDs) are called archives, because the files within the backup never change.

Full backups are very inefficient in terms of the time it takes to create the backup and also in terms of storage space required because so much data is copied.

In general, you make a full backup once and then use the following more efficient backup methods to keep it updated day-to-day.

When most people think of back-ups, they think of full backups, which copy everything on the hard drive. The most thorough method of performing a full backup is called drive cloning, which copies everything, including Windows files that are needed if you want to restore your computer to working order after a complete hard drive failure. Less thorough full backups simply copy all user files on the system and leave Windows system files

Incremental & Differential Backups

A major feature to look for when buying backup software is its ability to perform incremental and/or differential backups. These maintain backups of the latest versions of your files in two different ways.

Incremental backups copy only the data that has been changed since a file was last backed up, meaning incremental backup jobs complete very quickly and don't require a lot of storage space. The downside is that restoring files from an incremental backup can be a lengthy process because the backup software has to stitch multiple backups together to create the whole file.

Differential backups create a completely new copy of a file that has been changed. It takes longer to perform a differential backup because more data is copied relative to an incremental backup, but restoring data is much faster relative to an incremental backup because complete copies of backed up files are instantly available. Some software also lets you configure differential backups so that older copies of backed-up files are retained when the new copy is backed up. This is called versioning, as it lets you maintain an archive of different versions of the same file so you can easily revert to an earlier revision of a file whenever you wish.

Backup software can do far more than just make copies of your precious files. Here are some additional features to look for when comparing products.

Synchronization. Sometimes referred to as "mirror" backups, synchronization lets you maintain identical copies of files in two places (such as the local hard drive and an external backup hard drive). This is nice for files such as pictures or work documents that you edit because the latest edited version is always backed up.

Scheduling. Backup software is useless if you don't use it, so scheduling is an important feature to look for. The most basic scheduling creates automatic backups on a regular basis, such as a certain time each day, but use something more sophisticated if possible.

File filtering. It is easy yet inefficient to back up everything on your computer all of the time. File filtering allows you to select certain types of files to include or exclude in the backup. This is perfect when you are backing up files to removable storage media, such as recordable CDs that have a limited amount of storage space.

Compression and encryption.



Even simple backup software, such as the utility that comes with Windows Vista, has filtering capabilities that let you automatically back up certain types of files.

Compression is technology that compacts digital files so that they require less storage space than they would otherwise require, and it works best with files that contain text. Digital images and most digital music (such as MP3 files) are already compressed, so don't expect to use your backup software to compact them much more than they already are.

Encryption uses a key to scramble data before it is backed up, and only people who have access to the key can descramble and restore the data. It's a good idea to always use encryption when you save financial documents and other files that contain personal information.

Backup: Step-By-Step

Step 1: Plan. First, you need to determine exactly what files you want to back up, staying within the limitations of your backup media. Backing up an entire hard drive requires a hard drive of similar capacity or a stack of optical discs, such as recordable CDs or DVDs.

If you don't want to back up the entire drive, then write down the names of all the folders containing files you do want to back up and also consider using a file filter to tell the backup software to only back up certain types of files.

Schedule backups on a daily basis and flag your most important files to be backed up every time they are saved.

Whatever you decide, don't back up files to a different folder on the same hard drive where the originals are stored. Drive failure is a major cause of data loss, so the whole point is to store backups separately from the hard drive.



You can display hidden file extensions by adjusting a simple folder option in Windows.

Step 2: See if it worked.

After performing a backup, use Windows to access the backup media and check to make sure all of your files are there. If you created an encrypted archive, check the documentation that came with your backup software to see what the file extension for that archive is and then check the backup media to see if a file with that extension exists. (See below for more about file extensions.)

Step 3: Restore test data. We recommend backing up a test file using the method you plan to use for all of your other backups. Delete the original copy of the test file and then use the instructions that came with your backup software to restore the test file using the backup copy. Take notes as you go so you can refer to them in the future when you really need to perform a backup.

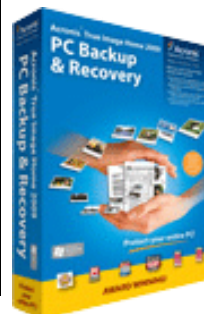
An Ounce Of Prevention

The main idea is to back up early and back up often. Even if you are forced to use backup software that doesn't have a lot of features or have to resort to making individual copies of your files, it is imperative to do so on a regular basis and in a place other than the drive where the original files are stored.

If this seems like too much of a chore, just think about the scenario laid out in the beginning of this article.

"You turn on your computer and nothing happens. The hard drive is gone, all the data on it is gone, and there's nothing you can do to get that data back."

You can't survive without your data, and your data can't survive without you.



Acronis True Image Home 2009



CMS BounceBack Pro or BounceBack Ultimate

Call or email for a Backup Step-by-Step Plan and Estimate.

The Backup List

There are certain types of critical files and folders to include in all of your backup plans, and file extensions indicate what types of files they are. For example, plain text files all have the file extension .TXT, while Microsoft Word documents often have the extension .DOC. Microsoft Word 2007 has the extension .DOCX.

Here is a list of typical file extensions and what type of file they are associated with.



WORK DOCUMENTS

.TXT, .PDF, .RTF, .DOC, .XLS, .PPT, .DOCX, .DOCM, .DOTX, .DOTM, .XLSX, .XLSM, .XLTX, .XLTM, .XLAM, .PPTX, .PPTM, .POTX, .POTM, .PPAM, .MDB



PICTURES

.JPG, .JPEG, .BMP, .GIF, .TIF



VIDEO

.MOV, .AVI, .MP4, .MPG, .WMV, .ASF, .SWF, .RM



MUSIC

.MP3, .WMA, .AAC, .M4P, .M4A, .OGG, .MIDI, .WAV



EMAIL

.PST, .DBX, .MBX



FINANCIAL RECORDS

.MNY, .QTX, .QPH, .QEL, .QDF



Saving Your PC Assets

Seven Steps to Surviving a Data Disaster.

1. Recognize a very real danger.

Your life is on your computer—photos, e-mails, music, tax returns, documents, and so much more. But did you know that, every year, **43%** of computer users lose irreplaceable files? And that over 300,000 laptops are stolen annually?

These are staggering statistics. And made more urgent by the dangers around every corner—a hard drive crash, theft, power surge, natural disaster, or accidental deletion.

2. Back up your files.

How do you avoid the nightmare of losing irreplaceable files? It's simple: Back them up.

3. Find a solution that backs up files automatically and continuously.

4. Don't settle for a partial (or expensive) backup solution.

Don't let any of your files go unprotected. You need to back up all your irreplaceable files—with unlimited backup—without spending a fortune every time your backup needs increase.

5. In the event you do lose files, make sure restoration is quick and easy.

Restoring files doesn't have to be an ordeal that's lengthy and confusing. After all, how inclined will you be to use a backup solution if retrieving files is painful?

6. Make sure your files are secure.

What's the point of backing up your files if some hacker can gain access to your data? Fact is, if your data is somehow compromised, you really haven't survived a PC disaster.

7. Give yourself a break—with a backup solution that's easy to set up.

Some users get discouraged from backing up, because installation of the backup system is difficult. Or at least they perceive it as difficult—and get scared away.