



## Series 6 – How Do I Backup my Important Files?

Welcome back to a series of computer related articles brought to you by VistaSol Computer Solutions. Over the coming weeks we are going to be featuring articles based on the theme of 'How do I . . .?'

This week we're continuing with a new series of articles on the subject of 'How Do I backup my Data', to this end we're offering some practical advice on the whys and wherefores of backing up your data.

### Part 2 – Prepare to Protect your Data from Disaster

I mentioned last week that 'You'll only ever need a backup when you haven't got one'. This may seem to be a bit of a tongue in cheek statement, but if I were to tell you that only around 1% of our customers who come to us with a failed hard disk or complete system crash, have made a recent backup of their important data – then that should put this in perspective!

Backups are the last line of defence against hardware failure, floods or fires, damage caused by a security breach, or just accidental deletion of data. If you're not sure if you need a backup, ask yourself these questions:

- a. What would happen if you lost all your personal data?
- b. How long would it take you to recover i.e. replace the information lost?
- c. How much disruption and delay would occur as a result of this loss?

### Why make backups?

Backups protect you against such things as:

- Hardware failure. Hard Disk failure is more common than you may think.
- Accidental file deletion.
- Theft and natural disaster.
- Catastrophic virus or spyware infections - you may have to erase your hard disk and reinstall everything to rid yourself of such infections.

### Backup tips

- Plan for the worst case. Think about the worst thing that could happen to your computer data and protect against that.

- Backup all your personal data regularly e.g. once a week, or at least once a month.
- Occasionally restore some of this backed up data to make sure the backup system is working properly.
- If you're running a business, store some backups away from your business place (or 'offsite' to use the jargon) in case your backup data gets stolen or damaged along with the computer it is backing up.
- Encrypt and password-protect backups to protect your privacy.
- Don't keep backups with the computer they are backing up in case they are stolen or damaged at the same time.

## Types of Backups

There are two main types of backup activities:

### Full backup

A full backup is the starting point for all other backups and contains all the data in the folders and files that are selected to be backed up. Because the full backup stores all files and folders, frequent full backups result in faster and simpler restore operations. It would be ideal to make full backups all the time, because they are the most comprehensive and are self-contained. However, the amount of time it takes to run full backups often prevents us from using this backup type regularly. Full backups are therefore often restricted to a weekly or monthly schedule, although the increasing speed and capacity of backup media is making overnight full backups a more realistic proposition.

You should be aware however of a potential security issue with this type of backup: each full backup contains an entire copy of your data. If the backup media were to be illegally accessed, stolen or lost, the entire copy of your data could be in the hands of unauthorised persons. This is why when deciding to use a backup program to make full backups, make sure it supports encryption to protect the backed-up data.

Advantages of full backups:

1. Restore time is the fastest
2. The entire backed-up data is stored in a single file (better storage management)

Disadvantages of full backups:

1. Backing up is the slowest compared to other backup types
2. The storage space requirements are the highest (compared to incremental backup). However, considering how cheap storage devices are the moment, this is a low impact disadvantage.

Once a 'full' backup has been carried out, subsequent backups usually take the form of 'incremental' backups (see below).

## **Incremental Backups**

Incremental backups store all files changed since the last 'Full' or 'Incremental' backup. The advantage of an incremental backup is that it takes the least time to complete. The disadvantage is that during a restore operation, each increment is processed and this could result in a lengthy restore job.

Incremental backup provides a faster method of backing up data than repeatedly running full backups. During an incremental backup, only files changed since the most recent backup are included. That's where it gets its name: each backup is an increment for a previous backup.

Advantages of incremental backups:

1. It's the fastest backup type since it only backs-up changed files
2. Saves storage space compared to other types
3. Each backup increment can store a different version for a file/folder

Disadvantages for this backup type:

1. Full data restore is slow compared to other backup types (you need the first full backup and all increments made since then)
2. To restore the latest version of an individual file the increment that contains it must be found first

## **Backup Strategy**

Making your first backup often determines your strategy for future backups. For example, if your first backup takes a couple of hours to complete, any subsequent backup will probably be 'incremental' to save time. Whereas, if your first backup takes less than an hour, subsequent backups will more than likely be 'full' backups also.

## **How to backup**

If all of this seems a little daunting, don't worry there are plenty of software packages around which will automate these activities for you – and best of all, some of them are free.

Next week, we'll discuss what backup software is available, and which of these may be best suited to your needs.