# Why back-up?

Backing up is the copying and archiving of computer data so it can retrieve it if something happens to the original. Years of work can disappear in an instant as a result of theft, carelessness, confiscation, or breakage, so it is extremely important to have an up-to-date backup and a well-tested means of restoring it.

Creating an effective backup policy can be tricky for a few reasons:

* The need to store original data and backups in different physical locations;
* The importance of keeping backups confidential;
* The challenge of coordinating among different people who share information with one another using their own portable storage devices.

In addition to backup and file-recovery tactics, this lesson addresses two specific tools, Cobian Backup and Recuva.

# Identifying and organising your information

The first step to formulating a backup policy is to figure out where all your personal and work information is currently located. This may include the following:

* Email may be stored on the provider's mail server, on your own computer, or both.
* Documents, address books, or chat histories on the computers you use, which may be in the office or at home.
* Information may also be stored on USB sticks, portable hard drives, or CDs.
* Contacts and important text messages on your mobile phone.
* Your website may contain important information or collection of work.
* Don't forget your non-digital information, such as paper notebooks, diaries and letters.

Next, you need to work out which of these files are 'master copies,' and which are duplicates. The master copy is generally the most up-to-date version of a file and is the one you will want to back-up.

You should make a table of all the information types you identified above and for each of them note:

* Whether that information is master copy or duplicate;
* The device or devices they are stored on;
* The physical location that the device is usually kept.

This table will help you see which of your information (or master copies) is only in one location and therefore vulnerable.

# Your backup strategy

To back up all of the data types listed above, you will need a combination of software and processes. Basically, you need to make sure that each data type is stored in at least two separate locations.

* **Electronic documents** - Create a full backup of the documents on your computer using a program like Cobian Backup, which is described in more detail below. Store the backup on something portable so that you can take it home or to some other safe location. External hard drives, CD/DVDs or USB memory sticks are possible choices. Because this category of data often contains the most sensitive information, it is important to protect your electronic document backups using encryption. You can learn how to do this in the [Protecting Files lesson](umbrella://lesson/protecting-files) and in the [TrueCrypt Guide](umbrella://lesson/truecrypt).
* **Program databases** - If you use a calendar application or an electronic address book, for example, you will need to find the folder in which these programs store their data. Once you have determined the location of your program databases, you can back them up in the same way as electronic documents.
* **Email** - Rather than accessing your email only through a web browser, install an email client like Thunderbird and configure it to work with your account. The [Thunderbird](umbrella://lesson/thunderbird) Guide explains in detail how to do this. Also most webmail services will provide instructions on how to use such programs and, often, how to import your email addresses into them. If you choose to move your old email messages to your computer so they are not stored on the server for security reasons, make sure that you include them in the backup of electronic documents described above.
* **Mobile phone contents** - To back up the phone numbers and text messages on your mobile phone, you can connect it to your computer using the appropriate software, which is generally available from the website of the company that manufactured your phone. You may need to buy a special USB cable to do this.
* **Printed documents** - Where possible, you should scan all of your important papers, then back them up along with your other electronic documents, as discussed above.

# Storage devices

Before you can back up your data, you must decide what kind of storage device you will use.

* **USB sticks or external hard drives** ? These are inexpensive, offer large capacity, and are easy to overwrite numerous times. USB sticks often have a lifetime of approximately ten years, with external hard drives lasting longer.
* **CDs** ? CDs store around 700 Megabytes (MB) of data. You will need a CD burner and blank discs. If you want to erase a CD and update the files stored on it, you will need to have a CD-RW burner and rewritable CDs. All major operating systems, including Windows XP, now include built-in software that can write CDs and CD-RWs. These discs may begin to deteriorate after five or ten years.
* **DVDs** - DVDs store up to 4.7 Gigabytes (GB) of data. They work much like CDs but require slightly more expensive DVD or DVD-RW burner, and appropriate discs. As with a CD, the data written on a normal DVD will eventually begin to fade.
* **Remote server** - A well-maintained network backup server may have almost unlimited capacity, but the speed and stability of your own Internet connection will determine whether or not this is a realistic option. Keep in mind that running a backup server in your own office, while faster than copying information over the Internet, violates the requirement that you keep a copy of your important data in two different physical locations. There are free storage services on the Internet, as well, but you should very carefully consider the risks of putting your information online and you should always encrypt your backups before uploading them to servers run by organisations or individuals whom you do not know and trust.

# Backup Software

Cobian Backup is a user-friendly tool that can be set to run automatically, at regularly scheduled times, and to include only files that have changed since your last backup. It can also compress backups to make them smaller. You can learn how to install and run it in our [Cobian Backup](umbrella://lesson/cobian-backup) Guide.

When using these backup tools, there are a few things you can do to help your backup system work smoothly:

* Organise the files on your computer. Try to move all of the folders that contain electronic documents you intend to back up into a single location, such as inside the My Documents folder.
* If you use software that stores its data in an application database, you should first determine the location of that database. If it is not in a convenient location, see if the program will allow you to choose a new location for its database. If it does, you can put it in the same folder as your electronic documents.
* Create a regular schedule to perform your backup.
* Try to establish procedures for all of the staff in your office who do not already have a reliable, secure backup policy. Help your colleagues understand the importance of this issue.
* Make sure to test the process of recovering data from your backup. Remember that, in the end, it is the restore procedure, not the backup procedure, which you really care about!

Once you have backed up your information or created a back-up process, you need to figure out a safe place to store it. Remember, this needs to be a different location to the one where the original information is! (i.e. if backing up your office files, the usb stick you use should not be kept in the office)

When you delete a file in on your computer, it usually disappears from view, but its contents actually remain. Even after you empty the Recycle Bin, information from the files you deleted can usually still be found on the hard drive. See the Deleting lesson to learn more about this. Occasionally, if you accidentally delete an important file or folder, this security vulnerability can work to your advantage. There are several programs that can restore access to recently-deleted files, including a tool called [Recuva - File Recovery](umbrella://lesson/recuva), which you can learn how to use in our tool guide.

It is important that you do as little as possible with your computer between deleting a file and attempting to restore it. The longer you use your computer before attempting to restore the file, the less likely it is that you will succeed. This also means that you should use the portable version of Recuva instead of installing it after deleting an important file. (Or better ? install it before anything happens!)

While it might sound like a lot of work to implement the policies and learn the tools described in this chapter, maintaining your backup strategy, once you have a system in place, is much easier than setting it up for the first time. And, given that backup may be the single most important aspect of data security, you can rest assured that going through this process is well worth the effort.

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Protecting Files lesson](umbrella://lesson/protecting-files)
* [Deleting Lesson](umbrella://lesson/safely-deleting)
* [TrueCrypt Tool Guide](umbrella://lesson/truecrpyt)
* [Thunderbird Tool Guide](umbrella://lesson/thunderbird)
* [Cobian Backup Tool Guide](umbrella://lesson/cobian-backup)
* [Recuva ? File Recovery Tool Guide](umbrella://lesson/recuva)

### FURTHER READING

* [Security in a Box - Chapter 6, Backing up](https://securityinabox.org/chapter-6)