

Offsite Backup: Benefits and Threats Unveiled

Author : Jonathan Tunn

Published: September 7, 2010, 7:14 pm

Good backup habits are essential to everyone who uses a computer with important information. It takes just a few accidental clicks of the mouse - or worse, one isolated hardware failure - and valuable data can be lost. One dilemma for backup users is often where to put their backups. Storing them on your own hard drive is obviously not the best option. Not everyone wants to split their backups into several parts using a CD or DVD burner, and an external hard drive isn't a standard fixture on many users' desks.

One solution to this problem, and a solution that can save a lot of time and effort, is offsite or remote backup. Backing up to a computer offsite means that your data will end up on a different drive or computer, which basically halves the chance of catastrophic loss. This can be especially useful for office users. If your company has several locations, backing up over a network to a computer situated elsewhere can provide a contingency in case of a power surge, fire, employee misuse or plain user error.

Offsite backup over a network:

Most backup programs support network backup, and the way to use this is simple. Local Area Networks (LAN) and Wide Area Networks (WAN) usually feature "network drives", which appear to your computer as an ordinary drive. They often have names like M:, N:, O: and so on. Depending on permissions set up by the people administrating your network, you may be able to write to certain drives but not read from them, or you may not be able to change or delete data once it's written. These are common situations, but they should not affect the way you back up.

Once you have found a suitable location for your data - your administrator will be able to help you with this - backing up can be as easy and fast as with an external drive.

Select the appropriate drive and the data you want to save and that's it. Even though a network connection is usually not as fast as a local cable, this is just a matter of waiting. Most programs allow you to set a backup timetable, which is a great way to take the effort out of backup. If you leave your computer on at night, then setting an incremental backup every second day at 2am, for example, ensures the safety of your data. A possible disadvantage here is that if your network goes down, you might not be able to get your data back for some time. Laptop users might not always be connected to the network at the scheduled backup time, defeating the purpose entirely.

Offsite backup through FTP:

Another form of offsite backup uses a File Transfer Protocol (FTP) server over the Internet. FTP is traditionally used to move large files online and can reliably transfer any files of any size.

To access data stored on an FTP server, you can use your backup program, a special FTP client or just a regular web browser. While there are two "types" of FTP server, public and private, you will almost certainly be using a private server, which requires a password to access your data. Advantages of this method include that you can view the files stored on the FTP any time you wish using any FTP client, mobile users can back up from anywhere in the world with an Internet connection, and FTP backup can be somewhat cheaper than a specialised remote backup service.

The main disadvantage inherent in this method is data security. The FTP protocol is not secure, and even a private FTP account does not ensure the security of your files; it only protects access to the FTP server. Anyone with access to your username and password has access to your data. Added to this, unless you take steps to protect it, your data will be unencrypted as it travels to the FTP server, and could possibly be intercepted. We recommend that you encrypt your files before sending them.

One option is to store your data in a standard password-protected ZIP archive. This is a quick method that allows you to extract your files on any computer using any ZIP client. There are ZIP programs that provide tighter security by applying stronger encryption algorithms, like AES or Blowfish. This increases the security of your data, but to decrypt your files you may need to use the program that encrypted and backed them up. To obtain access to a private FTP server, find a good hosting company (try searching with Google) and compare based on price and location - companies with servers based in your country will usually be faster. Beware that your Internet Service Provider (ISP) might charge you for the data you send, so you may wish to make incremental backups over FTP, which only backup what was changed since your last backup.

Specialised offsite backup:

Another form of offsite backup is the use of a special server provided by the company that makes your backup solution. They usually use their own protocols to encrypt and transfer your data, and a special program on their end to store it. You may have some issues using such services if you're behind a firewall, as some of these services use non-standard Internet Protocol (IP) ports.

Offsite backup services are usually paid for by the month, by the amount of data transferred or both. They can be quite expensive, especially if you wish to back up a lot of data, or use the service over a long period of time. As with FTP servers, you may also be charged by your ISP to send your data.

Still, offsite backup services represent a convenient method, as they'll usually be built right into backup programs that support the feature. Ensure the credentials of the company you're dealing with, as an offsite backup service is pointless if your backup company happens to shut up shop or "can't find" your data - just as your hard drive fails.