Secure your data clouds before storing any data

by Julia Ann

There was a time when one could just upload a file to the cloud and never worry about their security at all. It is no longer that safe anymore and we have to take measures to improve this insecurity otherwise we are prone to losing confidential data that may cost us a lot.

The measures taken by some cloud service providers]

The only proven security for your data is use of encryption. The encryption should always be used before the data is even uploaded to the cloud.

For the Dropbox and Sydive as well as the likes, one can use an add-on so as to encrypt the data before it is uploaded. The use of Safe Monk or the Boxcryptor enables an encrypted folder to be added before you can upload your files. This is also done for other services that may be using the WebDAV standard.

If you want a server that does not use an add-on, Dropbox and the likes have to be dropped completely. The Spideroak whose Hive service is known as the Zero-knowledge data backup is a great security tool since it does not even store your password and deletes it once you log out.

The Bittorrent Sync is a p2p file sharing one and works the opposite of Spideroak. It has no 3rd party file management systems or the central server. Therefore data is transmitted between the devices.

Note: The use of the devices is prone to physical damage and risk of data loss.

Cloud service providers and their security degrees

The Dropbox and Google are the giant physical cloud servers that are usually used by most people for personal and even public data. However they are not secure at all.

The Microsoft Skydive and the Apples I cloud are other servers that provide cloud services to the public and are encrypted to improve its security. However, the hackers have beaten them in their own game.

The Network Attached Servers are personal cloud service providers, whereby unlike the Dropbox and others, they use the external hard drives that are connected to a person's Wi-Fi network hence they can transmit the data stored whenever a person connects to it. Examples of such are the LaCie cloud box and the Seagate Central drives. Sometimes they are not referred to as the cloud services because of their nature.

The cloud locker is another one but more secure than the NAS since one has more control over the files stored.

The Tonido and the Pocket cloud do not use the hard drives are can be remotely access the home computer. These tend to be more secure since there is no sharing of a password and the data is accessed from a device to another rather than the insecure from a device to the cloud then to another device.

The pocket cloud wholly relies on the Google log in for security.

The general security measures for cloud use

- The major one is to understand the type of cloud service you are using. Norton contact can be of great help.
- Choose a good master password.
- Choose a cloud password that is unique from all the others you use
- Do not share your password with someone you don't trust
- Always have a backup for your data.

Author: Julia is an Avid Blogger from Manchester, UK with 5+ years of experience in blogging. She is interested to learn new things. As of now she is focusing on Sky Contact Number which provides information regarding digital satellite TV and radio service.