10 Ways to keep your Data safe in Cloud Environment

Suman Nanda , Posted on June 6, 2016, filed in: Information Technology

A "cloud" in the technological sense, can be defined as a huge online place for storing and accessing data and program files in the internet, instead of your computer hardware- like local disk. When we talk about storing and accessing data, our first concern is how secure is our data, how much can we rely on the cloud environment. Cloud environment is as safe as data stored in an individual data server.

Cloud is the latest trend in technology and most of us store all data in cloud housed in Dropbox, Google Drive. Generally, people assume that all the data stores in cloud is safe, but it is not true. There are ways beyond our control in which our data could be hacked. However, following some small measures and with very little effort, we could prevent uninvited access to your information. Given below are 10 ways in which data in cloud environment be secured.

Smart Passwords and Security Questions keep data Secure

It is an unspoken rule to choose a unique password for your account. A password that cannot be guessed easily even if someone know few facts about the target. It can be made a complex one by using various numerals, symbols uppercase letters that would make it even more difficult to guess in the very first place.

Coming to the part of security questions, it is advised not to use answers that are available online, instead try creating one yourself. Ofcourse, the security questions remains the same but try giving some inappropriate or absurd answer to the security question, something that no one would ever guess.

Encrypting files helps in Securing Data

Using encryption software will mix up information and make it impossible for any other person without a decryption password to read it.

It requires a little bit effort from the user atleast for memorizing passwords for different services that offer encryption as major feature.This is the best idea for securing your data in cloud environment. This includes searching, paying and using third party encryption software for data.

Boosting Data Security through Two-factor Authentication

This means in addition with username and password, an additional security measure is added. Every time a user logs in, a unique code is sent to a device the user has.

A simple example is every time we create an account in google an SMS is sent to registered mobile phone along with the app, sometimes it is designed purposely for the purpose like in case of some banks.

Sometimes it might be quite irritating to always look into another device while logging it, also it might become a hassle in case if the device is not available or couldn't be accessed. Yet it is a very effective method to secure data even when someone already has your password.

Backing up Information is a must in Securing Data

It's so strange to see how cloud has become so popular that now we are actually discussing about backing up data stored. Everything we have in cloud is not important, some things are very important to us, while some may not seem so important.

So it's wise to create a backup for all the data that we are going to use in the future.This can be easily done by storing data in some external hard drives, a very cheap and useful method of backing up the data.

Another method that can be used is approaching third party cloud services that have been precisely designed for backing up data. So basically there are very simple and effective ways for backing up and you have no excuse not to use one.

Securing Sensitive Details on Public Systems like Internet Cafes

Internet provides limitless online storage to the users which is actually a great relief and brilliant platform to store data, but it also has its own consequences. It is not wise to just leave all the unwanted information as it is.

It is not useful to you doesn't mean that it cannot be used by any unwanted user.Like messages with information about your credit card details, personal information, banking details etc should be deleted as soon it has been used. In case if these messages or files need to be included then *ad infinitium* but don't forget to have their back up before deleting them.

Play smart to keep your Data Safe

Never be too sure for anything and always be cautious about the stuff you are doing online. Like, using antivirus software to prevent your system from malwares that may allow intruders to access your personal details.

Always lock your Wi-Fi with a unique password, you can also considering not broadcasting it. Never go through suspicious e-mail messages, not even from the companies with which you are associated. In case if you end up on a site that looks suspicious and has a domain .ru just leave.

Check the Cloud Service Vendor as a Trust of Security

The most basic level is choosing your cloud service provider. This level makes all the difference of securing and protecting data. The best way of choosing a cloud service provider is always opting for a reputable provider, the one who will offer high class leading security for their cloud solutions.

If you want to store your data in private servers then always opt for a trusted host.Never think of just trusting any service vendor, or go through the very first vendor you come across. Take some time to check the clod service vendor's credentials. Take interest in the security protocols they use and also verify their details.

Purchase cloud services with that provide high standards of security:

Unlike all other business processes cloud security has various sanctioned standards that need to be fulfilled. These standards to assure your cloud service providers meet consists of ISO27001, ISAE3402/SSAE16 and CSA STAR. This is the first cloud security program that was recognized internationally.

Pay attention while logging in increases security:

Just using unique password, security questions or two way authenticator does not ensure complete protection. Sometimes we log in from a device and forget to log out, or use other's devices to log in to our account.

Always pay attention to the device you are using while logging in your account, there may be intruders nearby waiting for a small mistake that might help them hack your account.

Regular updates and remote purging to keep data safe:

As the security measures are being improvised, the hackers are coming up with new methods of getting into our personal information. It was estimated that approximately 200,000 malicious programs and viruses are discovered everyday, the report itself makes one question how safe is our data in the internet.

Although it is a time consuming process that demands some extra effort but keeping updated software, upgrading system might be the simple and easy way to protect against unwanted attention or threats. Alongwith online security software it also includes operating systems and protocols as well.

It won't be wrong to say that your data is always at risk remote hacking and physical theft or data being accessed by unauthorized components. One way to minimize these risks is by remote formatting software by permitting you to delete some important data as soon as your data is stolen or missing. Now a day producers of the mainstream device gives the option of remote data wiping.

Conclusion

Finally just like all the other things cloud environment comes with some consequences of data risk, but by these simple measures might come to your rescue and help you secure your data. It's better to take some precautionary measure within the time rather than regretting later when your data has been hacked or lost.