Sufyaan's Website

sufyaan.me/backups

Taking Proper Backups

27 July 2023

Category: Technology

Taking backups is crucial in every single context. There is simply no situation where the lack of backups was beneficial. Such situations are always detrimental to people. Backups are also important for businesses, especially ones which are responsible for the lives of people, like hospitals.

Taking backups prevents data loss due to software or hardware errors. Even accidents have a minimal impact if you have a backup. It allows businesses to keep growing instead of being worried about recovering crucial client data. For public services like hospitals, being hit with ransomware is an extremely difficult moment. If the ransom is not paid immediately, it can result in loss of human lives. This is why you either have backups or lose money.

Losing precious memories hurts. Backups prevent this gut-wrenching scenario from ever occurring. With many spectacular backup solutions being free or cheap, there is absolutely no reason to take backups. If you work with new computers and devices regularly, then taking backups makes it easy to migrate and install multiple instances on new devices. This is especially easy with Linux systems due to the simple dotfile method. It also provides version control. If you have old versions of documents and files, it is easy to refer to previous examples for future work.

If there is one thing that people love about backups, it is the peace of mind you get knowing that you have an extremely low chance of losing your important data.

It does not matter if you are a normal person or a massive business; you should spend time and money to back up your data properly.

3-2-1 Backup Rule

The 3-2-1 backup rule is a rule that many people recommend following to remember to take proper backups. Here is the meaning of each of the numbers:

1. **Three Copies**: The "3" in the rule means that you should at least three copies of your data. This includes your original data, so you should have at least your original data along with two other copies. The advantage of having these many copies is that it is the perfect balance of simplicity and redundancy.
2. **Two Different Media**: The "2" in the rule means that you should have your backups on at least two different media types. This may include physical (external SSD, NAS) and digital (server you own, cloud storage) backups.
3. **One Off-site Copy**: The "1" in the rule means that you should have at least one off-site copy. Off-site in this case means somewhere other than your main home or regular backup methods. This can be an encrypted external hard drive that you leave at your relative's house, for example.

It is important to note that these rules are not a plan for everyone, and are instead meant as a base for your backup plans. The least important data that you own should at least be backed up using the base 3-2-1 backup plan.

Using Invasive Services (Drive, OneDrive, iCloud)

When it comes to using Big Tech's invasive services, you have to be extremely careful since they do not respect your privacy at all. At the bare minimum, you should be encrypting the files you upload if they are even of a little importance to you.

A popular program for file and drive encryption is VeraCrypt. To learn how to use it in detail, watch this video. The overall process goes like this:

1. Create a new encrypted file specifying the password and other details like total space.
2. **Save the password somewhere safe to not forget it.**
3. Unlock the file using your password.
4. Copy all your important files to it.
5. Unmount the file
6. Upload it wherever you want

This makes it difficult to easily access your files from your phone or another device, but it is totally worth it for your privacy.

Using Paid Services (Backblaze, Mega)

Services like Mega allow you to pay for more storage, just like Drive, OneDrive or Dropbox. There are privacy concerns with the latter three, however. ProtonDrive is also a good option, but it has had some controversy due to the privacy concerns of ProtonMail. However, I am comfortable recommending it.

BackBlaze is a backup program that is under the MIT licence. It works really well for most of their customers, so I am comfortable recommending it.

Using Owned Services (servers, syncing)

When you are using services you own, you have to make sure that you verify the integrity of your files. File corruption can happen on every platform, but it is much better to verify your files on your server since there may be issues with your setup that causes file corruption.

It is also important to keep a separate drive or storage medium on your services if possible. If anything happens to your main system, it becomes really easy to just wipe the system and install a new one, knowing that your data is safe.

You can also use sync services like Syncthing for small files that you need synced within all of your devices. I use it to sync my password manager and personal notes. It is encrypted and open-source software and works extremely fast. It is so fast that by the time I save a file and open my phone, the file is already updated. This prevents conflicts.

Taking Offline Backups

If you are taking offline backups, you should be careful with encrypting your data if you need it. You should first assess whether you need encryption or not. If you live in an area with a lot of robberies, encrypt it, as a robber who is smart enough may steal your drive.

Make sure to get an external hard drive or SSD from a reputable company like Western Digital or Samsung.

By buying a product from a reputable company, you get a reliable product that lasts a long time.

Maintaining Backups

While it is important to back up your data, it is also important to maintain your backups. At the end of every month, check your backups to see if your files are still intact. If a specific backup medium keeps showing corruption in files, move it to another drive immediately, since they can fail at any time.

Conclusion

While it is important to take backups, it is also important to make sure you are taking them properly. Follow the 3-2-1 backup rule. If you are using invasive services, encrypt all of your files before uploading them using

a trusted piece of software like VeraCrypt.

Try to use services that you own as much as possible, to be completely independent. Make sure to have offline backups.