T2021_19 Importance of Backing Up Your Data (24th November 2021)

What is data back-up

Backing up is the process of storing data on a secondary medium (file, hard drive, external hard drive, memory card, flash drive or cloud). Depending on the volume of data to be backed up, each medium used for backup may differ.

The purpose of having alternative storage for backup files is to eliminate data loss from the primary storage medium in the event of a failed hard drive, a cyber-attack on the workstation or network, or if storage volume becomes full and must be overridden to create more storage, not to mention the impact of natural disasters that can destroy records.

What does backing up a device mean?

Backing up a device can mean a variety of things, and depending on the device, you may need to be very specific when mapping out this process. Sometimes this simply means backing up specific mobile settings and functions, or options and data settings for a PC.

It can also simply mean, making a copy of everything from a particular device, as opposed to a few files or folders. This process is very common for all forms of mobile devices and laptops. Due to the sheer number of files, backing up a desktop PC is often a bit more involved. The primary concern with smartphones is frequently the vast collection of priceless photographs they contain.

Where should backups be stored?

One of the most significant backup stumbling blocks is determining where to save the files that are being copied. This can be done in triplicate: on the current device hard drive, on an external hard drive, and on a local network server. The files can be saved in the cloud as well. This can cause some hiccups depending on several factors:

- The security practices of the cloud storage system you may be considering.
- The type of encryption to use before uploading files to a secondary storage platform.
- One must take note, if the files to back up are work-related, the person in charge of the backing up of data must have a business approved storage/backup solution.

This is because having files in a randomly selected service of your choice can have a disastrous consequence if sensitive files are hacked or leaked.

Type of backup strategy to implement

The reliable starting point for most businesses is to have a 3-2-1 backup strategy.

- Employer/employees should have three copies of their data.
- Have two copies of data on-site but on different devices.
- One remote copy for the event of natural disaster (fire, flood, hurricane, or earthquake).

The local copies of your data will give you easy and immediate, redundant access to your data when you need it. The remote copies can act as an insurance policy, in the case of a natural disaster occurring.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- The importance of backing up (12 of November 20211). Retrieved from Malwarebytes.

  https://blog.malwarebytes.com/101/2021/11/the-importance-of-backing-up/

- The importance of backing up (no date). Retrieved from Norton.

  https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html