

CYBER SECURITY AND YOU

May 2019

QUICK TIP

While there are many choices of backups, there are a couple of helpful rules to use.

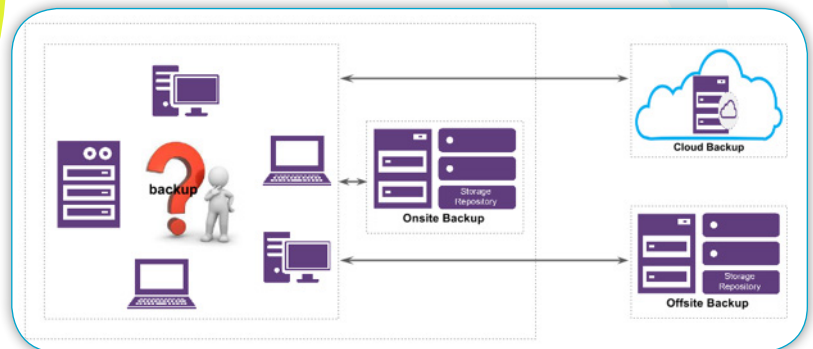
You should always have two different backups: one online and the other offline; one onsite and the other offsite.

Make sure you backup everything you deem important.

The most important rule: It should run automatically and alert you, should it fail.

WHAT YOU NEED TO KNOW ABOUT BACKUPS

The first thing you need to know is why backups are important: ransomware, viruses, storage failures, house fires, flooding, theft, and little johnny who wanted to install a new game, so he deletes your “unimportant files” to clear off enough space. **It really does not matter why your data is unreachable; what matters is that you can get it back.**



There are online and offline backups, on-site and off-site, real-time and scheduled backups.

Online vs. offline: An online backup is always accessible, like syncing to the cloud. An offline backup is like a tape backup that you have to access before you can restore anything. Before you say online backups are better, realize that if you happen to get ransomware or a virus, it is likely to infect your backups as well as your computer; unless your backup is offline and inaccessible.

On-site vs. off-site is as simple as it seems. An onsite backup isn't very helpful if your house burns down, but a total restore from a cloud takes much longer from the cloud. That's why you need both.

Real time backups mean you are safe almost as soon as the data appears, but are you backing up the infection before you realize you were infected? The scheduled backup will normally allow you to pick a point in time prior to the infection occurring.

The object is to find a balance of all of the above. There is no magic bullet for backup, but every person needs to ask themselves “how do I recover if” my home burns, my hard drive fails, I get Ransomware, my cloud vendor goes out of business, etc. If you are happy with the answers to those questions, then you have a good backup solution.

WHAT DOES LASERS DO FOR BACKUPS?

At LASERS, we have a backup solution that incorporates all of the above mentioned methods.

What we do **NOT** backup are your local drives (usually C:\), so please store your important data in a location that is protected, like a network share or your home drive (H:\).

As always, your IT Department is happy to answer any questions you have.