Science Translations
Established 1990
PC410.COM™
PC Updater News

Resolved: 3-2-1 Backup

Start the new year with a resolution: Your files need two backups, one local and one online. Far too many computer users are far too confident that their computers won’t fail, lightning won’t strike, phishers won’t hack, and that they won’t delete their own files by accident. Of course, we know better, right? It’s just the top reason I get calls to restore a single important file.

The basic rules of backup are:

- **System backups**, also known as **Image backups**, are for replacing the entire contents of the drive, after hardware failures or Windows boot errors or ransomware. Do these backups once a month on business computers, maybe less often on home systems, depending on use.
- **Data backups** copy your stuff. Documents, pictures, shortcuts, logins,

spreadsheets, all the important stuff. Run data backups at least weekly for business computers or nightly on business servers.

3-2-1 Backup

3 Copies
2 Media Types
1 Offsite
lobe

©2019, PC410.com, All Rights Reserved.

The standard for backups is the 3-2-1 rule. There should be:

- Three copies of all your documents (photos, spreadsheets, etc).
- Two different types of storage devices (SSD, hard drive, DVD)
- One copy goes off site. (cloud, or take a copy home)
- Multiple versions of each file are kept.

Combining these rules results in this basic setup. (More layers will apply for bigger systems and offices.)

- One copy, the original of each file, is on the internal drive of the computer.
- One copy is on a local drive in the same office or home, on an external hard drive.
- One copy goes to cloud backup, unchangeable after upload, and old versions are kept by date.

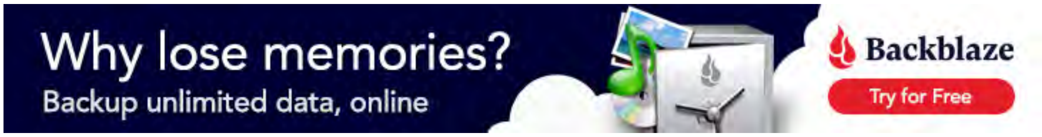
Where to Backup?

The local copy of files is easy. Small offices and home offices should use USB hard drives or network-attached (NAS) drives. While I would prefer a drive that’s locked up elsewhere when not in use, most computer users won’t remember to do manual backups; schedules and automation are required.

As for software, home offices can use Aomei Backupper, free edition, to create an image backup or to create a data synchronization task on an external drive. (Call me for assistance.) For larger offices, there are more complex products that can do more.

Cloud Backup

Remember that a cloud backup is generally just for data files. You can’t restore a computer with it; it is just documents and photos, not software. And documents change more over short periods of time than software, so cloud backup is usually set to daily or continuous backup. Which cloud? The best available right now continues to be Backlaze, with unlimited storage; they keep each file version for a year, because not every file error is found immediately. Here’s a coupon link that includes a 30-day free trial:



If you’re already using another product, probably Carbonite, continue to do that. But keep in mind that DropBox and Google Drive are not backups. They’re file sharing services that are very convenient for sharing files with other users, or with your mobile devices. They don’t keep file versions over time, so they have no protection against ransomware or accidental file deletion. They’ll happily synchronize file overwrites and deletions to the cloud. Use a cloud backup that keeps multiple copies of files by date; do not use file sharing services as backups.

Windows Backup

Microsoft has been pushing Windows Backup very, very aggressively with popup notifications in Windows. Careful. If you are on the monthly or yearly subscription for Microsoft Office, then as a Microsoft 365 customer, you have a large block of included storage for files, and for those users ONLY, Windows Backup may be useful. However, for everyone else, a free Microsoft account gets you only 5 Gb of data storage, enough for absolutely nobody, and when it fills, it breaks, badly, instead of offering to sell you a paid upgrade to a plan with more storage.

My standard recommendation is to just say no to Windows Backup if you aren't all-in on the Microsoft 365 system. Even if you are a MS365 user, keep in mind that if you are subject to encryption compliance requirements for PCI (credit cards), HIPAA (medical), or Sarbanes-Oxley (corporate), you need to use an online cloud product that offers encryption before uploading, which is NOT available in Windows backup or any file-sharing service. (Backblaze and Carbonite can encrypt before upload.)

What isn't Protected?

Only running one backup? Here's what's missing.

- Cloud backup only: No protection against full-drive losses like lightning, Windows boot issues, drives encrypted by ransomware, physical theft, hardware failure, or destruction. I can restore your data on a new Windows installation, but without your software.
- Image backup only: No protection for newer files since the last timed backup to the external drive. I can restore the system to how it was as of the date of the last backup.
- Cloud sync only, like using an online file sync product for your backup: I can restore the last version of each file stored onto a new Windows install. If that last backup was encrypted by ransomware, older versions are not available, and no restore is possible.

Plan Ahead

3-2-1 Backup has been the standard backup method for many years now. Three copies, two kinds of backup device, one file set offline, covers all the issues. Check what's missing and be ready for nearly any issue.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735