Science Translations
Established 1990
PC410.COM™
PC Updater News

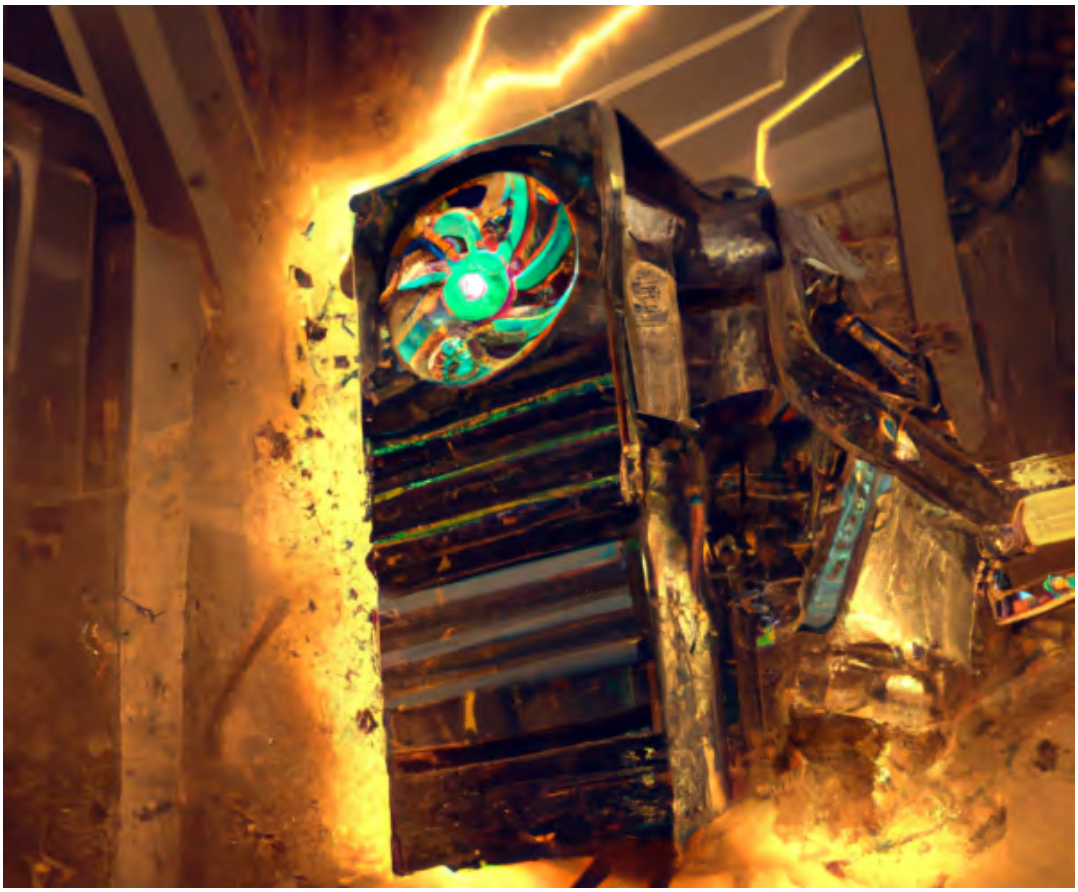

Image Backups vs Data Archives

Backups are important, right? A backup exists so that when lightning strikes your power line, and takes out your computer, you can get back all your files. Or if ransomware encrypts everything. Or you hit SAVE instead of open on your most important spreadsheet, so you've overwritten it with a blank file. Or a

former employee erased a folder, and you found out 4 months later. Or the drive in the computer is failing, but you didn't know it until now, so some or all of the files in the backup are bad.

Wait. That's not all the same disaster, and the same recovery plan won't cover all that. Different disasters need different backups, and having a set covers more options. Here are basic types, and why businesses need them all:

- **Image backups:** That's a full copy of the C: drive, all of Windows with the boot files, software, and the documents of all the users. It's what I need to restore a dead drive on the same computer, or to pull out the documents and data for a new computer. Image backups are usually created as a single large compressed file per backup.
- Data Backups: That's documents, spreadsheets, pictures, scans of paper files, license keys and installation links or downloads for paid software, employee records, all preferably in multiple copies by date, and readable without the original computer. These backups are either a large file per day, or separate files.
- **Data Archives:** Same as data backups, justoffline and kept longer, to cover more issues. These are disconnected from power and networks, or use a cloud backup service with an 'immutable' feature. Archives should be separate files, because you usually don't go into the archives for entire drives, but usually go looking for an older version of a specific file.

So for those risks above, different types apply.

- **Lightning:** Takes out the computer, usually not drives, but backup drives are usually also no longer usable. A new computer is likely, so offline data backups are needed, not an image backup.
- **Ransomware:** Encrypts all the data, some settings, sets traps to re-infect. Sometimes sits quietly for months, so that ransomware gets into the backup sets, and then finally encrypts. Data backups usually cover this risk, but the archives may be needed.
- **Overwrote a document:** Overwritten files don't show up in the Recycle Bin, so daily or continuous backups can recover the most-recent version. Usually, when I get this call, we pull out the prior week's version from the data backup.
- **Sabotage and Deletion Errors:** These aren't generally found right away, so data archives are needed.
- **Failing drives:** The most-recent data backup may also be corrupt. I have frequently had to rely on the second-newest image backup to restore data after a drive failure.

3-2-1 Backups

This is why I emphasize having two kinds of backups. It's the 3-2-1 rule again.

There should be three copies of every important file.

- The work file on your server or in your Docs folder
- A local backup copy on a Network-Attached drive or a USB backup drive.
- A cloud backup copy, or an air-gapped copy on a disconnected USB drive. Or set your cloud backups to keep files longer. Backblaze has options to keep backups a year, or forever, but the standard is only 30 days. (Call for help turning that option on.) Most other cloud backups also have longer-term options.

Are the Backups Backing Up?

Combo disasters are the most difficult to recover from: Ransomware when the cloud backups have stopped. Windows boot-failures triggered by drive errors. Any two-fer, basically.

The best defense against these complex issues is to monitor the backups. Check that they're running, at least once a month. Look at the results, and see if the backup files are present and dated correctly and that the backup drive isn't full, dead, or missing. Look in Windows Update History to see if Windows updates are running, and check if the drives test as good, and under 80% of capacity. It takes around 10 minutes each month once you've done it a few times. Nothing beats actually looking at the system to see if everything is happening as expected. It's what you don't expect that can cause the most damage.

*Monthly backup monitoring is available as a service. Call 410-871-2877 for a backup review if in doubt.

Phishy Movie or Web Site?

As always, look before you click. Starting this month, Google is selling domain names which end in .zip and .mov. So here's what to watch out for in scam emails. Something in a phish email that looks like a compressed ZIP file may actually be a link to a web page. The same applies to .mov, which we would normally expect to be a movie file, not a web page. Luckily, we're not used to seeing .mov files in emails; they're too large to send that way.

That last chunk of the domain, that part that lies just before the first single slash in a page address is called a TLD, for top level domain. Examples: .com, .net, .org, .co.us, .co.uk. You can look them up to see for what or from where they're used, here:
https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

As always, look at links before following them, by floating the mouse over the link without clicking. While a .com could be anywhere, .com domains cost money, and some of the international domains that are heavily used as disposable targets in spam are both free and worthless in business. And there are other risks: Many targets are commonly placed in hidden folders on hacked websites of legit companies.

The rule remains: When an email arrives, from an unknown sender, there should be a reason to click a link that is NOT the usual FUD trio of Fear, Uncertainty,or Doubt. They're selling something, maybe legit, maybe a phish, and it's not for your benefit to click, it's for theirs.

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

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