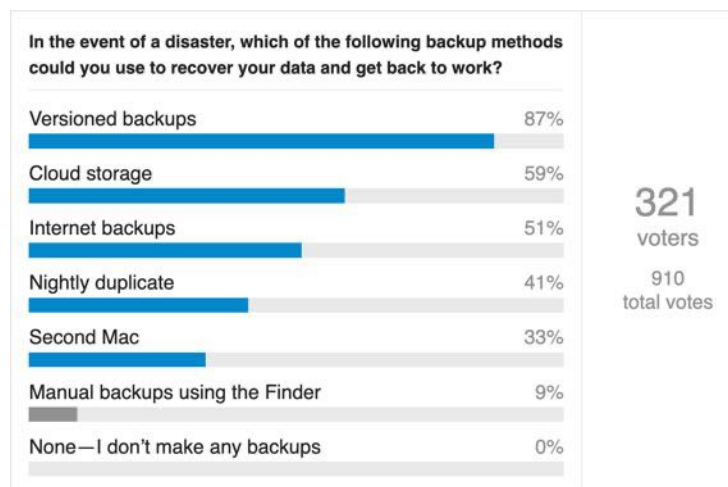Adam Engst 16 January 2025

Thoughtful, detailed coverage of everything Apple for 34 years
and the TidBITS Content Network for Apple professionals

In the event of a disaster, which of the following backup methods
could you use to recover your data and get back to work?

Method	%
Versioned backups	87%
Cloud storage	59%
Internet backups	51%
Nightly duplicate	41%
Second Mac	33%
Manual backups using the Finder	9%
None—I don't make any backups	0%

321 voters

910 total votes

In our most recent Do You Use It? poll, we asked which backup methods you could use to recover your data and get back to work. Versioned backups—made with Time Machine by most people—were by far the most common, receiving 87% of the votes, but cloud storage was also extremely popular, with 59%. Just over half of respondents (51%) rely on Internet backups, with fewer (41%) relying on regularly scheduled duplicates and 33% saying they could turn to a second Mac to get back to work. Only 9% of people said they manually copy files to external drives for backup, and I'm extremely pleased to see that no one said they ignore backups entirely. Of course, that mainly speaks to the self-selected nature of the poll respondents—TidBITS readers know that working without a backup is like tightrope walking without a net.
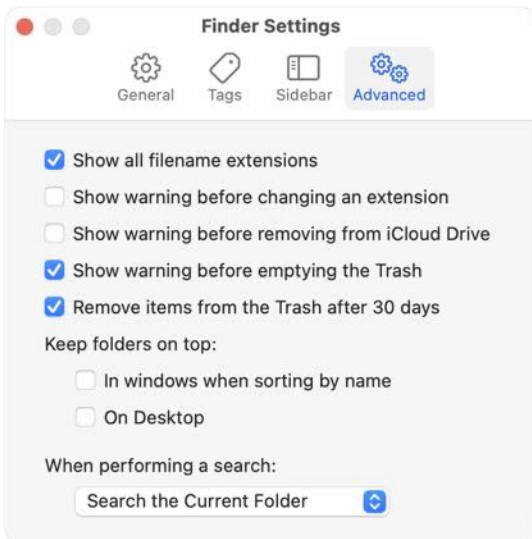
What most surprised me about the extensive discussions that followed the poll was how varied everyone's strategies were. I suspect that this is one of those areas where putting thought into developing a backup strategy is most of what's necessary for good results—the precise details can vary without significant loss of protection.

That said, I want to review each of the poll's backup methods and discuss what I learned from people's responses.

Versioned Backups

Versioned backups are essential for recovery because they maintain the contents of your drive at multiple points in time. They let you restore files when problems occur, whether from corruption, accidental overwrites, or deletions.

Ideally, deletions shouldn't require going to your backups. To make recovering deleted files and folders even easier, use Finder > Settings > Advanced to turn on "Remove items from the Trash after 30 days" and don't empty the Trash manually unless you really need the space. That way, you always have a month to pull a deleted item out of the Trash.)
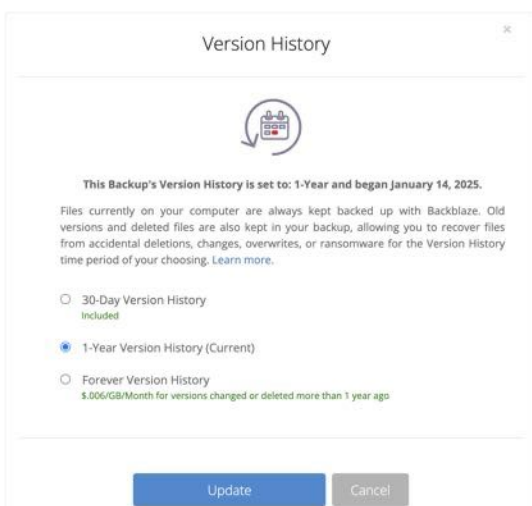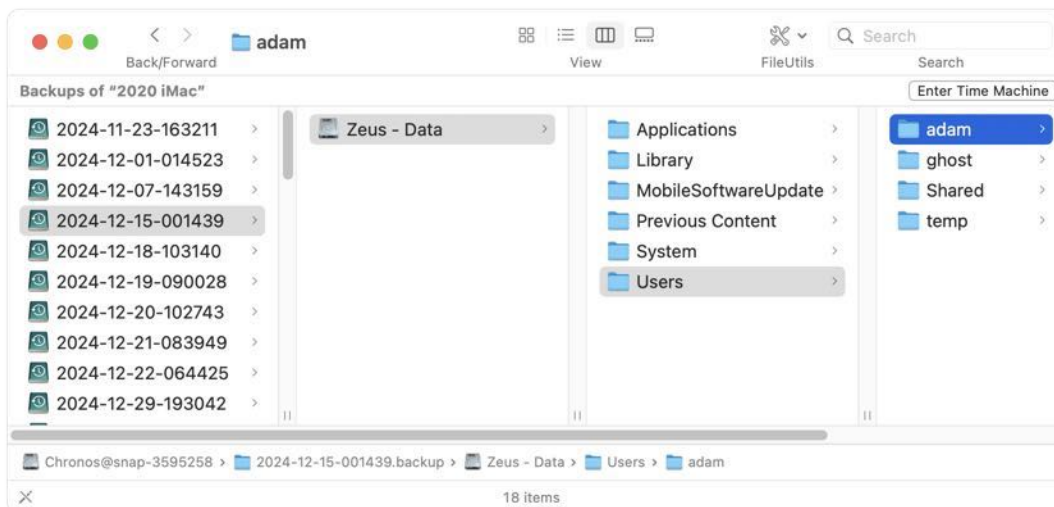
The canonical versioned backup app is Apple's Time Machine, which makes a backup every hour, automatically pruning the hourly backups after 24 hours and the daily backups after a week—it keeps weekly backups for all previous months. The oldest backups are deleted when space is needed, but Time Machine always keeps the latest version.

Some people don't trust Time Machine because of bad experiences in the past, but it's worth keeping in mind that Apple has radically changed how Time Machine works under the hood over the years, so what was true a decade ago no longer is today. What hasn't changed is Time Machine's tremendously funky interface for finding and restoring files. Happily, thanks to Time Machine's use of snapshots, you can now navigate through your backups in the Finder. Choose the backup you want, and you'll find all the data on your drive from that date.
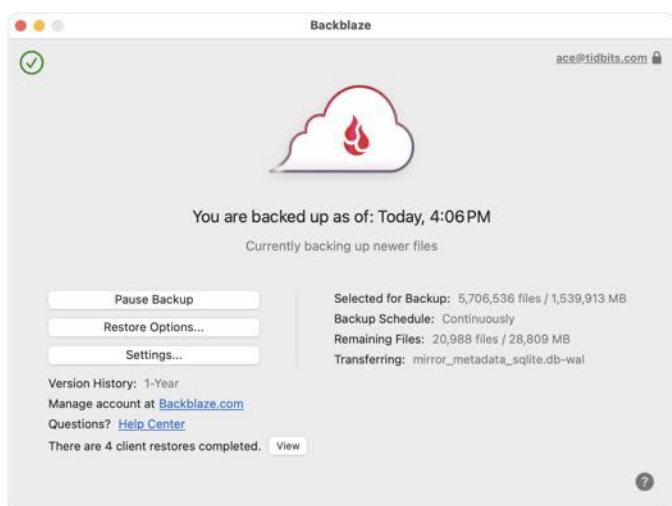

Other apps also provide versioned backups. Apps that can make local versioned backups include Carbon Copy Cloner (which has evolved beyond the duplicates implied by its name) and Retrospect. The cloud backup apps Arq and Backblaze also provide versioned backups. In October 2023, Backblaze increased its free version history from 30 days to 1 year, but you must choose it explicitly—I just remembered to update mine (see "Backblaze Raises Prices, Makes Extended Version History Standard," 25 August 2023).

Internet or Offsite Backups

I was excessively concise in the wording of this poll answer, labeling it just "Internet backups," but where I was going with that is the need for a backup somewhere other than in the immediate vicinity of your Mac. Some sort of offsite backup is essential to protect from theft, fires, tornadoes, and numerous other disasters that will affect both your Mac and any backup stored with it.

Historically, offsite backups required schlepping hard drives to another location, a process that is only as reliable as the person doing the transport. Another issue with physical offsite backups is that the destination location often isn't all that far away— storing a drive at your neighbor's house won't have helped if you live in Pacific Palisades. Plus, hard drive reliability isn't improved by moving them around repeatedly.

That's why I've become a big fan of Internet backup services like Backblaze. Before Backblaze, I relied on CrashPlan, which unfortunately discontinued its consumer-level services in 2018—see "CrashPlan for Home Ends Today," 22 October 2018. There are others, like IDrive and Carbonite, but I haven't used them.

Some people don't like having another subscription fee, lack sufficient Internet bandwidth to back up a lot of data effectively, or are uncomfortable with storing their data in the cloud. If that's true for you, you're likely back to moving drives around.

Storing backups in a safe might seem like a reasonable alternative and would likely protect against theft as long as the safe is secure. However, not all "fireproof" safes are appropriate—ratings matter. You want at least a Class 150 or Class 125 safe, which is rated to keep the internal temperature below 150º (sufficient for magnetic media) or 125º (safe for optical media). Safes are also rated for how long they can keep the temperature below that level—although house fires can last several hours, it's uncommon for the area around a safe to burn hot for more than 20 minutes before the fire moves on. Although wildfires burn much hotter and last longer, the safes are tested at higher temperatures than standard house fires. Don't forget to look for water resistance—firefighters will be dousing the area with a lot of water.

Regularly Scheduled Duplicates

Although versioned backups generally provide a relatively quick way of accessing just the latest version of backed-up files, a duplicate is a more intuitive form of backup—it's an exact copy of the selected files at the time of the backup. Duplicates don't protect against file corruption or deletion because as soon as you update the duplicate, those changes are reflected in the backup copy.

However, duplicates are useful for restoring files quickly with familiar Finder actions rather than having to muck around in the weird Time Machine interface or use another app. They also work well with Migration Assistant for restoring data after erasing a drive or setting up a new Mac. (Migration Assistant also supports Time Machine, but not proprietary backup formats.) In addition, it is possible to make bootable duplicates that can, in some situations, be used to boot a Mac so you can get back to work as quickly as possible after some types of internal drive failure.

This answer in the poll was also poorly titled "Nightly duplicate." I hadn't anticipated that some people would make weekly or monthly duplicates, particularly bootable ones. They're not perturbed that their duplicates are almost always outdated because they could get more recent files back from regular Time Machine backups or cloud storage. That's true, but it seems to introduce unnecessary complexity over a nightly schedule.

A few people make duplicates manually, which is a fine addition to an automated backup strategy but not something to rely on solely. One of the cardinal rules of backup is that it's best to remove the human element to the extent possible. If you have to remember to initiate a backup manually, Murphy's Law states that you will forget or be too busy right before the event that causes you to need your backup.

In terms of software, the main players are Carbon Copy Cloner, ChronoSync, and SuperDuper. All three are fine apps and will do a good job of making duplicates. Carbon Copy Cloner has additional versioned backup capabilities, ChronoSync offers more synchronization options, and SuperDuper is the easiest and most focused on duplicates.

Cloud Storage

I need to emphasize that putting your files in cloud storage is not a backup. Here's why: A backup, by definition, must be separate and independent from your working files. If you accidentally delete or corrupt a file in your cloud storage folder, that change immediately syncs to all your devices—there's no way to recover the original. So when I use iCloud's Desktop & Documents folder syncing feature to make files available on my iMac and MacBook Air, I may have a copy of each file on each Mac, but any changes I make to one of those copies are immediately reflected on the other

machine. Versioned backups are designed to eliminate this concern, and even duplicates only reflect such changes when they're updated.

However, cloud storage can play a huge role in getting back to work quickly after a disaster because all those files live in the cloud as well as on any synced devices. If you store much of what you do in folders synced by Dropbox, Google Drive, or iCloud Drive, as soon as you reconnect to your account from a reinvigorated Mac or new Mac, all your files immediately become accessible. You can even get to them from an iPhone or iPad. That also applies to Web apps like Google Docs, where data is never stored locally.

For some people, in some situations, cloud storage and Web apps let Macs act like the "thin clients" of yesteryear, providing an excellent local interface to apps and data hosted elsewhere on the network. I've heard of people who seldom back up their secondary Macs—usually a laptop—because everything they need is online. If something happened to the Mac's drive, they would just reinstall macOS and log in to their cloud storage accounts.

Also, some cloud storage systems offer limited version history, enabling you to access previous versions of a file. Again, this is not the same as a versioned backup system, but it can help you get back to work more quickly.

Second Mac

The next option in the poll involves having a second Mac available to get back to work more quickly. It's important to remember that we don't make backups for the sake of having backups; we make them so we can recover from setbacks. Many problems are minor, like an accidentally deleted file, and even more serious corruption can be addressed by erasing the drive, reinstalling macOS, and restoring files.

But what if your Mac is stolen, destroyed, or damaged badly enough that you must send it to Apple for repair? A backup of your data is necessary here, but it's not sufficient on its own—you need another Mac. For anyone whose livelihood would be impacted by doing no work for a few days, having a second Mac available is critical. It probably doesn't have to be as powerful as your main Mac, so using a laptop that supplements a desktop or keeping an older Mac around are good options. You can also use someone else's Mac, possibly by using a bootable duplicate to have it act like yours, or by creating another user account and accessing your data from your backup or cloud storage accounts.

Another temporary workaround for those close to an Apple Store involves buying a new Mac with the understanding that you'll return it within 14 days. Apple Store employees often recommend this approach when you bring a Mac in for repair.

Manual Backups in the Finder

As with manually created duplicates, backing up files by dragging them to an external SSD, hard drive, or USB flash drive is a fine way to give yourself a little more peace of mind. It never hurts to have an extra copy of your dissertation, novel, or other important document on another drive. (Well, except for the security risks if the drive isn't adequately secured and managed.)

However, such manual backups must be in addition to an automated backup strategy. Again, you don't want to put yourself in a situation where you could fail to make a backup when it is most necessary. Automation can ensure these critical tasks aren't missed due to forgetfulness or busyness.

Evaluating Your Backup Strategy

[EDITOR'S NOTE: Emphasis mine]

Ultimately, as I noted above, **backups are about getting back to work after something goes wrong.** As you think about your current backup strategy, it's worth asking yourself some questions:

- **How quickly do you need to get back to work after a disaster?** The more important this is, the more focus you will want to put on being able to use a second Mac with access to the same data. A bootable duplicate may also be helpful, but it's essential to perform some dry runs to ensure everything works from the duplicate as needed.

- **Could you recover from your house burning down or all your gear being stolen or destroyed?** The chances of such an existential disaster are low, but unless you use an Internet backup service or maintain offsite backups, you could lose everything.

- **To what extent is your backup strategy automated?** If any aspect of it requires manual activation (connecting a drive, triggering a backup, moving a drive offsite), what's the risk of failing to perform that task?

- **How much are you willing to spend on backups?** You'll need a backup drive at minimum, and an Internet backup service subscription would also be beneficial. Hard drives are cheaper than SSDs but slower, louder, and less reliable.

- **Is your backup strategy itself resilient?** Drives fail, software has bugs, and people make mistakes. An advantage of a multi-faceted backup strategy is that the diversity of hardware and software makes you less vulnerable to any single point of failure.

- **Have you tested your backups to make sure you can restore data from them?** At a minimum, try restoring a few important files from each type of backup you maintain. For bootable duplicates, ensure they can actually boot your Mac, perform adequately, and provide access to critical apps. (Note that a bootable duplicate on a hard drive is too slow to be usable for real work—an SSD is required.)

The answers to these questions should help you build or refine a backup strategy to ensure that it provides the level of protection you need. Be realistic—I hear a lot of "Oh, I'm retired, so I don't need to back up seriously anymore," which is just as self-defeating as, "Oh, I'm not interesting, so hackers wouldn't pay attention to me." Bad things happen, and most people would be devastated at losing all their photos or overwhelmed by having to recreate their financial records. I just helped an elderly friend who was distraught about her Quicken data disappearing; happily, she had merely confused Quicken by renaming her data file, so we didn't have to resort to her backup.

A thoughtful backup strategy delivers peace of mind while requiring relatively little in terms of cost or ongoing maintenance.