# I'm an IT expert. Here are the 6 most common backup mistakes people make


## Summary

The article describes six common backup mistakes people make and suggests ways to avoid them. The article emphasizes the importance of having multiple backups in different locations, performing regular backups, and using automated backup software.


## Table of Contents



Avoid these pitfalls when backing up your data!

By Dominic Bayley Australian Editor, PCWorld Sep 25, 2025 6:00 am PDT

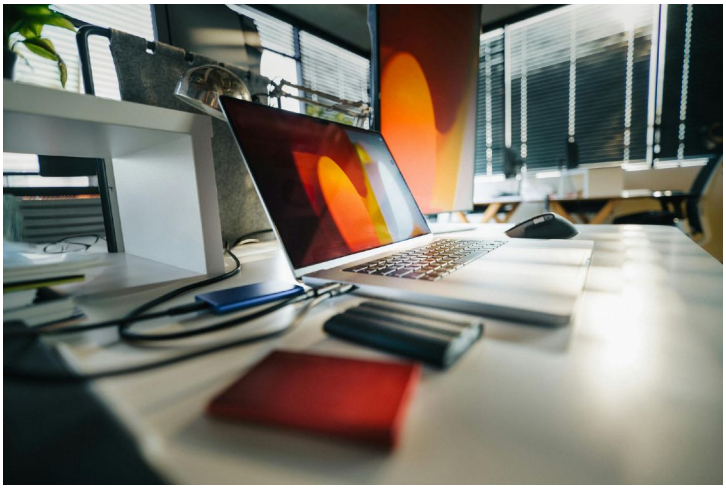


Image: Pexels: Jakob Zerdzicki

Backing up your files can be a lifesaver when data gets corrupted, or in the case of total drive failure. But it must be done right. Too often I hear stories of well-meaning people trying to back up their data only to still lose that data because they've made mistakes along the way. Here are the main backup pitfalls you want to avoid, and some suggestions for what to do instead.

## 1. Storing backups in one place

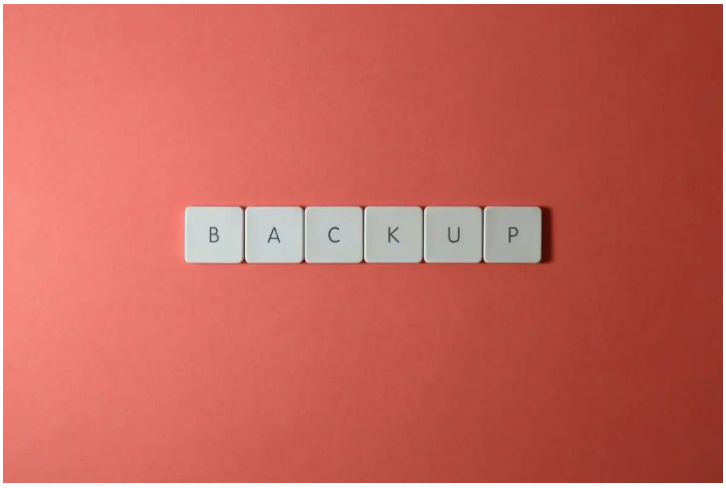
Backing up to just one drive or flash drive means that if anything happens to that one backup, which is not a stretch to imagine, you've lost all your data.

Instead of having a single point of failure, you need to have more backups. When deciding how many copies of the data to back up I recommend you go by the 3-2-1

rule. That is, have 3 copies of your data, two on different media types, and one offsite in another secure location like in the cloud.

See our roundups of the best Windows backup software and best online backup services to help you with your backup plan.

## 2. Infrequently backing up




Pexels: MIguel A Padrinan

Backing up sporadically or only occasionally means you stand to lose any data that you've accumulated since your last backup. The thing about PC errors and drive failures is that they can be quite random, you never know when they're going to happen. So, you need to always be prepared for the worst.

Instead of haphazardly backing up data, perform regular daily or weekly (if you work with less data) backups, i.e. create a defined schedule for your backups. Some backup software / services even often real-time backup to ensure that there's no gap in data preservation.

## 3. Backing up data manually

Let's face it, manually backing up data takes time and effort and we're less likely to want to do it if we're short on time or feeling lazy. That's why I suggest having an automatic backup active, either via cloud services or backup software. You can schedule it to run during off hours when it won't interfere with your regular activities.

Automating the process will mean you don't have to worry about doing it yourself and your data will still be backed up no matter how you feel or how much time you have to spare.

## 4. Forgetting about security

Pexels: Arina Krasnikova

It's one thing to back up your data frequently, it's another thing to ensure that the data is safe and isn't stolen or accessed without authorization. To prevent that, it's important that the software and cloud services you're using encrypts your data and that you have a data decryption key available.

If possible, also use multifactor authentication

(MFA) to access the data when it's stored online. This will provide an extra layer of security should hackers attempt to gain access.

## 5. Overwriting old backups

Having a recent backup that works means your data is safe, but every time you back up your data you risk the data becoming corrupted. That's why you should never overwrite an older intact version, you could lose that data forever.

Versioning is a better way to ensure you never lose a copy of your data. This involves keeping several versions of your data at any given time, a newer version alongside older versions. If you're using cloud services or backup software, you'll want to ensure they offer versioning too.

## 6. Not testing backups

Too often I hear people saying they've backed up their data, only to later discover that the backup was corrupted and can't be restored. To prevent that happening you need to ensure that your backups actually work. One way to do this is by opening a few files after a backup to test it immediately, or by periodically opening files and/or performing a full test recovery to check that you can actually restore the files from a backup when required.

Doing so will give you peace of mind that your data is safe and that if the worst happens, you still have a working backup to restore from.

…

Author: Dominic Bayley, Australian Editor, PCWorld

Based in Australia, Dominic Bayley is a hardcore tech enthusiast. His PCWorld focus is on PC gaming hardware: laptops, mice, headsets and keyboards.