

5. Backups and Recovery

- [5.1 Backups](#)

5.1 Backups

Core Concepts: Protect Your Data, Have a Recovery Plan

You need backups BEFORE disaster strikes. Ransomware, hardware failure, theft, accidental deletion, fire, flood, or simple human error, any of these can wipe out years of photos, documents, and memories in seconds. The question isn't IF you'll need a backup, but when.

5.1.1. Understanding Backups

A backup is simply a copy of your files stored somewhere other than your main device. If something happens to your computer or phone, you can restore your files from the backup. The key principles:

- Automatic is better than manual
- Multiple backups are better than one
- Different locations are better than same location
- Tested backups are better than untested

The 3-2-1 Rule

This is the gold standard for backups:

- **3** copies of your data (the original plus two backups)
- **2** different types of storage (e.g., removable drive, and cloud)
- **1** copy offsite (cloud storage or at a different physical location)

Don't let perfect be the enemy of good, even one automatic backup is better than none.

Common Backup Mistakes to Avoid

- **"I'll do it manually"**: You won't. Automate it.
- **"I'll do it later"**: Do it now. Disasters don't wait.
- **"My only backup is on the same desk as my computer"**: Fire, flood, or theft takes both.
- **"I've never tested my backup"**: Hope is not a backup strategy.
- **"I sync to the cloud, that's my backup"**: Sync is not backup; if you delete something, it deletes from the cloud too. Use actual backup services.

- **"I backup my whole computer including programs":** This is overkill and wastes space, just back up your data files.
- **"I haven't checked my backup in months":** Backups fail silently. Check monthly.

Quick Start Backup Plan

If you do nothing else, do this today:

- Buy an external hard drive (at least 2TB, costs ~\$50-80)
- Enable Time Machine (Mac) or File History (Windows) to back up to that drive
- Enable iCloud Backup (iPhone) or Google Backup (Android)
- Test restore one file
- Set a calendar reminder to check backups monthly

This gives you basic protection in 30 minutes. You can add cloud backup and other layers later.

Remember: The best backup is the one that exists. A simple automatic backup you've tested beats a perfect backup plan you never implement. Start simple, then improve over time.

5.1.2. The Basics

- Enable built-in backup tools
- Know what you're backing up
- Back up your phone
- Test your backups

Enable Built-In Backup Tools

Every modern operating system has a built-in backup feature. Turn it on right now:

Windows (Windows Backup):

- Open Settings > System > Storage > Advanced storage settings > Backup options
- Connect an external hard drive (USB)
- Turn on "Back up using File History" or "Back up my files"
- Select what to back up (Documents, Pictures, Desktop, etc.)
- Set frequency (daily is most likely the right balance)

Mac (Time Machine):

- Connect an external hard drive (USB or Thunderbolt)
- Open System Settings > General > Time Machine

- Click the + button and select your external drive
- Turn on "Back Up Automatically"
- Time Machine backs up hourly, keeps daily backups for a month, and weekly backups until the drive is full

Linux (varies by distribution):

- Ubuntu: Settings > System > Backups (uses Déjà Dup)
- Connect external drive and select it as backup location
- Enable automatic backups

Know What You're Backing Up

Make sure your backup includes:

- Documents folder
- Pictures/Photos folder
- Desktop files
- Downloads folder (if you keep important files there)
- Any other folders where you store personal files

You don't need to back up:

- The operating system (you can reinstall it)
- Applications (you can reinstall them)
- Temporary files

Back Up Your Phone

Your phone probably contains more important data than your computer; photos, contacts, messages, and app data.

iPhone (iCloud Backup):

- Settings > [Your Name] > iCloud > iCloud Backup
- Turn on iCloud Backup
- It backs up automatically when connected to WiFi, plugged in, and locked
- Free tier gives 5GB - you may need to buy more storage for photos

Android (Google Backup):

- Settings > Google > Backup
- Turn on "Back up to Google Drive"
- Enable "Photos & videos" backup in Google Photos app

- Backs up over WiFi automatically
- Free tier gives 15GB shared across Gmail, Drive, and Photos

Test Your Backups

This is critical and almost everyone skips it. A backup you haven't tested is just hope, not a backup.

How to test:

- Pick a file and rename it
- Use your backup system to restore it
- View the restored file and make sure it works
- Did it work? Great! If not, troubleshoot now before you actually need it

Test your backups at least twice a year. Set a calendar reminder.

5.1.3. Better Protection

- Use encryption
- Add cloud backup
- Maintain external drive backups
- Set a backup schedule
- Backup before major changes
- Monitor your backup storage

Use Encryption

If your backups contain sensitive information, encrypt them.

Why encrypt?

- If someone steals your external drive, they can't access your files
- Cloud providers can't view your files (zero-knowledge encryption)
- Protects financial records, medical information, and personal documents

How to encrypt:

- Mac Time Machine: Enable encryption when setting up the backup drive
- Windows: Use BitLocker to encrypt the external drive (see OS Hardening section)
- Cloud services: Look for "zero-knowledge encryption" or "client-side encryption"

- Dedicated tools: Duplicati <https://duplicati.com/> or Restic <https://restic.net/> for encrypted backups

Critical: Store your encryption password somewhere safe (password manager). If you lose it, your backup is useless.

Add Cloud Backup

If you back up to a removable drive, consider adding backups to a cloud service provider. Cloud backup stores your files on servers maintained by a company, accessible from anywhere with internet. This gives you the "offsite" component of the 3-2-1 rule.

Good cloud backup options:

General purpose cloud storage:

- Google Drive: 15GB free, integrates with Android
- iCloud: 5GB free, seamless with Apple devices
- OneDrive: 5GB free, integrates with Windows
- Dropbox: 2GB free, works on all platforms

Dedicated backup services (recommended):

- Backblaze: Unlimited backup for one computer, ~\$9/month
- Carbonite: Similar to Backblaze, ~\$6-24/month depending on plan
- IDrive: 5GB free, affordable paid tiers

Why dedicated backup services are better:

- They back up everything automatically, not just selected folders
- They keep versions of files (so you can restore an older version)
- They're designed for recovery, not just storage
- They run continuously in the background

Maintain Your External Drive Backup

If you're using an external hard drive for backups:

- Keep it plugged in so backups run automatically (but see ransomware note below)
- Check monthly that backups are actually running; look at the backup software to see the last backup date
- Replace the drive every 3-5 years, hard drives don't last forever

Ransomware consideration: Some ransomware can encrypt external drives that are connected. To protect against this:

- Have at least one backup that's disconnected or in the cloud
- Or rotate two external drives, use one for a month, then swap it out and store it somewhere safe such as a fireproof safe

Set a Backup Schedule

Different types of data need different backup frequencies:

- **Critical work documents:** Back up hourly or immediately (real-time cloud sync)
- **Photos and personal files:** Back up daily
- **Phone:** Back up daily (automatic when charging overnight)
- **System settings:** Back up weekly or after major changes

Most backup software handles this automatically once you set it up.

Back Up Before Major Changes

Always create a backup before:

- Installing a major OS update
- Upgrading to a new computer or phone
- Installing new hardware (especially hard drives)
- Major software installations that might affect system files
- Disk repairs or reformatting

Monitor Your Backup Storage

Check regularly that you have enough space:

- External drives: Should be at least 2x the size of what you're backing up
- Cloud storage: Watch for "storage almost full" warnings
- If you run out of space, backups may stop silently; check occasionally that new files are being backed up

5.1.4. Extra Credit

- Own your cloud data

- Implement true offsite backup
- Create a disaster recovery plan

Own Your Cloud Data

When you use cloud services like Google Drive, iCloud, or Dropbox, your data lives on someone else's computer. For most situations this is fine, it's convenient and reliable, but you give up some control. The company can change terms, raise prices, close accounts, or potentially access your files. If you want more control over your cloud storage, you can create your own personal cloud.

What "owning your cloud" means:

- Your files live on hardware or at least infrastructure you control
- You can access them from anywhere, just like commercial cloud services
- No storage limits except the size of your drives
- Complete privacy, no company can access your files
- Local cloud options have no monthly fee after additional purchase price

Basic options for personal cloud storage:

Network Attached Storage (NAS) - A NAS is essentially a specialized computer with hard drives that sits on your home network and provides storage to all your devices.

Beginner-friendly NAS options:

- Synology DiskStation (DS220+, DS224+): Easy to set up, excellent software, great for beginners. ~\$200-300 plus drives.
- QNAP: Similar to Synology, good interface. ~\$150-400 plus drives.
- Western Digital My Cloud: Simplest option, plug-and-play. ~\$150-300 with drives included.

What you can do with a NAS:

- Automatic backup from all your computers and phones
- Access files from anywhere via mobile apps or web browser
- Stream photos, videos, and music to your devices
- Share files with family members
- Create your own personal Dropbox/Google Drive replacement

How difficult is it?

- Setup: 1-2 hours following the manufacturer's setup wizard
- Ongoing maintenance: Minimal, mostly software updates
- Technical skill needed: If you can set up a WiFi router, you can set up a NAS

Considerations:

- Initial cost: \$300-600 depending on capacity
- Your internet upload speed matters: If your home internet has slow upload speeds, accessing files remotely will be slow
- You're responsible for drive failures: Buy drives rated for NAS use (WD Red, Seagate IronWolf) and set up RAID for redundancy
- Power outages: Your NAS is at home, so if your power goes out, you can't access it remotely
- Still need offsite backup: A NAS at home doesn't protect against fire, flood, or theft - you still need an offsite backup (cloud service or physical offsite drive)

This gives you speed, control, and protection.

Bottom line:

Owning your cloud data isn't for everyone, but if you:

- Have lots of data and don't want ongoing monthly fees
- Want complete control over your files
- Are comfortable with basic tech setup
- Have good home internet

then a personal NAS can be a great long-term investment. Otherwise, commercial cloud services are perfectly fine and often more reliable for non-technical users.

Implement True Offsite Backup

For maximum protection, keep a backup in a completely different physical location:

Options:

- Cloud backup (already covered in Better Protection)
- External drive stored in a fire-proof safe, a bank safe deposit box, or at a friend or family member's house (swap drives monthly)

Offsite backups protect against fire, flood, theft, and natural disasters that could destroy both your computer and local backups.

Create a Disaster Recovery Plan

Document your backup system so you (or someone helping you) can recover:

What to document:

- What backup services you use

- Where external drives are stored
- Login credentials for cloud services (stored in password manager)
- Encryption passwords (stored in password manager)
- Step-by-step instructions for restoring from each backup type
- Who to call for help (tech-savvy friend or family member)

Keep this documentation in your password manager and print a copy for your emergency kit.