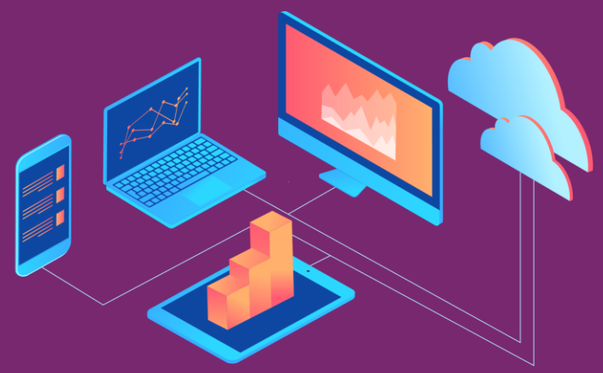
National Cyber Security Centre

Backing up your data

Most of us at some point have been unable to access important data, whether it's work documents, photos, videos, contact details or other personal information. This infographic explains why you should make backups, and the types of backup techniques available.



What is a backup?

A backup is a copy of your important data that's stored in a separate safe location, usually on the internet (known as cloud storage), or on removable media (such as USB stick, SD card, or external hard drive).

Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup.

Most backup solutions allow you to chose what data is backed up, whether that's just documents, photos and other files, or the entire contents of your phone/computer (including the apps and programs you use).

You should back up **anything** that you value. That is, anything that would inconvenience you (for whatever reason) if you could no longer access it.

Backups are not just for recovering lost, erased, or inaccessible data. If you have a new device or computer, you can use backups to transfer your existing files, apps and settings across.

Backing up using cloud storage

If you use cloud storage, a backup of your data is securely stored on the internet.

Most cloud storage solutions provide an amount of storage space for free. This might be sufficient to save all your important files.

You can create cloud-based backups automatically, which means you're more likely to have an up-to-date copy of your data.

Cloud storage requires a reliable internet connection, so is not be suitable if yours is slow, unreliable, or metered.

Protect your cloud accounts (and access to your backups) by using strong passwords and turning on two-factor authentication (2FA).

Backing up using removable media

You can back up your data to an external hard drive, a USB stick or thumb drive, an SD card or DVD/CD-R discs.

Removable media backups can hold large amounts of data, which may be beyond the capacity of cloud storage options.

Disconnect removable media when not in use. Ransomware (and other types of malware) can move to attached media, which means your backup would also be infected.

Protect your backup with a strong password in case the media is lost or stolen. Someone who has the media can't access your data unless they know the password.

Restoring backups

Once you've made your backup, it's important to check that it contains all your important data.

Check that your cloud storage contains photos you have taken recently, or any new files or folders you have recently created.

If you have data that is 'irreplaceable' (such as photos and videos of family members), then consider keeping a copy in the cloud and also on removable media, so you can always access it.

Recovering files deleted in error

Recovering files is quicker than restoring an entire backup if you only need to recover (for example) a few photos.

Look for the 'recycle bin' and 'file history' features and make sure they are turned on. A recycle bin gives you some time to recover deleted files in case a file or folder is accidently deleted.

'File history' (or 'snapshots') gives you an option to restore a file to a previous version, in case you need to undo a change.