Ultimate Backup Guide

By John Crowhurst

John The Computer Man

Table of Contents

Introduction 3

Restoring previous versions 4

Backup devices 5

How to size your backup drive 6

Treesize 6

OmniDiskSweeper 7

Backup methods 8

Manual backup 8

Automated backups 9

Back up BitLocker recovery key 11

BitLocker Recovery Key as a barcode 12

Disabling BitLocker 14

Windows 11 Home 15

Windows 10 and Windows 11 Pro 16

Backup your Web Browser 17

Backup Web Passwords 17

Backup Bookmarks/Favourites 18

Backing up social media 19

Export your Instagram account 19

Export your Facebook account 19

Export your LinkedIn account 19

Export your TikTok account 20

Export your Twitter (X) account 20

Export your YouTube account 20

Using a downloader 20

Storing passwords as barcodes 21

Two Factor Authentication 22

Using Two Factor Authentication 22

Passkeys 24

Cloud Storage 25

Cloning 26

Disk Image 27

Introduction to PARA Method 28

Conclusion and Links 29

Introduction

Backups are the most essential yet most overlooked and forgotten part of using and owning a computer and usually only when we have a disaster, we then realise how important they are to our data, whether that be the photos of loved ones; important documents or a book you have been writing.

Backups can be as simple as a copy of your important files done manually to another device, or they can be automated. However, there are online “backup” systems that aren’t really backups at all and lure you into a false sense of security, they are a “sync”.

A sync basically mirrors everything you have in a set of folders with another device, be that an external drive or Internet storage. It seems like a backup, but with one difference:

A backup is a copy of your files from the past, a sync is a current copy of your files in the present, which means if you overwrite a file with the wrong content, the sync will synchronize those changes to the file, and before you realise what you’ve done you have lost the original[1].

[1] We will cover restoring previous versions on the next page.

Restoring previous versions

It is very easy to overwrite the wrong file by accidentally saving changes over it or (in the case of Microsoft 365, autosave changes over the file you are using as a template) and need to recover the changes, often after we have closed the program.

In Windows there are previous versions saved with the file, which can be accessed by right clicking on the file and choosing Properties then clicking on the “Previous Versions” tab. It used to be possible to recover deleted files using Previous Versions, so you must now restore them from your backup.

On the Mac, you can choose “Revert To” from the File menu in most programs, which allows you to revert to the last opened, last saved or previous saved versions as well as browse the list of saved versions of that file. Note that you can recover deleted files from Time Machine backups.

Backup devices

In the past, the humble floppy disk was the method most people used to back up their files. These were replaced by CDs and later DVDs, but most modern computers lack a DVD drive these days and it is such a faff to create CDs and DVDs as storage media. These days there are a few options open to the home user and another option open to businesses that handle large amounts of data:

1. USB Stick – Often called memory sticks or flash drives, these offer an easy and compact solution for backup needs. However, they do have reliability issues over time and can be slow.
2. USB Drive – These are often called portable drives, which are just as easy as a USB stick, but are larger and that extra bulk must be considered. Older USB drives used a spinning hard drive, which had to be kept on a flat surface away from knocks to avoid damage to the heads, but modern USB drives contain a Solid-State Drive (SSD) which is immune to damage from knocks although they are prone to sudden death at the end of their life.
3. Cloud Storage – This is not a backup solution on its own, it provides an additional method of storing data. If a drive fails, or a computer is stolen the data is recoverable from Cloud Storage but if there is malware on the computer that encrypts or corrupts the data, the Cloud Storage will synchronize that data and it will also be corrupted.
4. Tape backup – This is often used in businesses that handle large amounts of data. The tape drive is basically a cassette recorder built into a desktop computer that runs software that makes it a server. Tape backup software will handle everything for you, so you insert the required backup tape, and the drive will rewind, play and record then eject the tape when required.

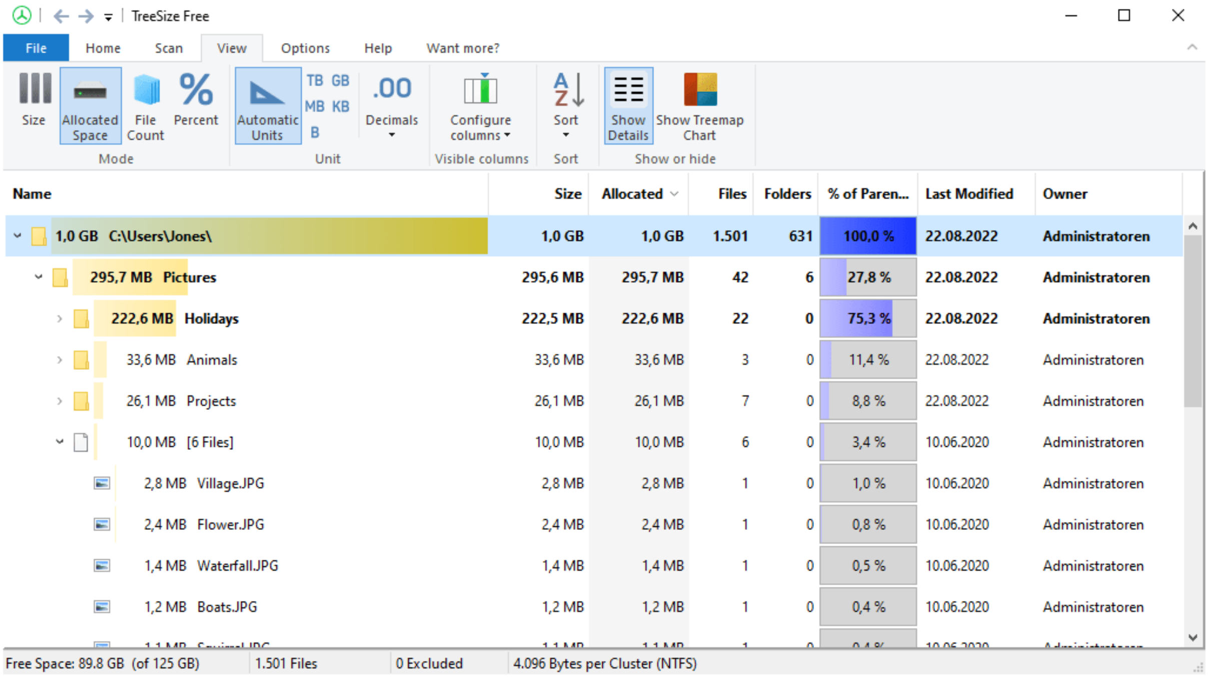
How to size your backup drive

Having an idea of what size of backup drive that you will need depends on the amount of data you have stored on your computer.

You can find out easily how much your computer is using through Treesize for Windows and OmniDiskSweeper for Mac. Links to both programs are available on the last page.

The rule of thumb is to choose a backup drive that is at least double the size of your data, so it is fine to backup 1GB with a 1TB drive. 1TB is 1000GB and 1GB is 1000MB.

Treesize

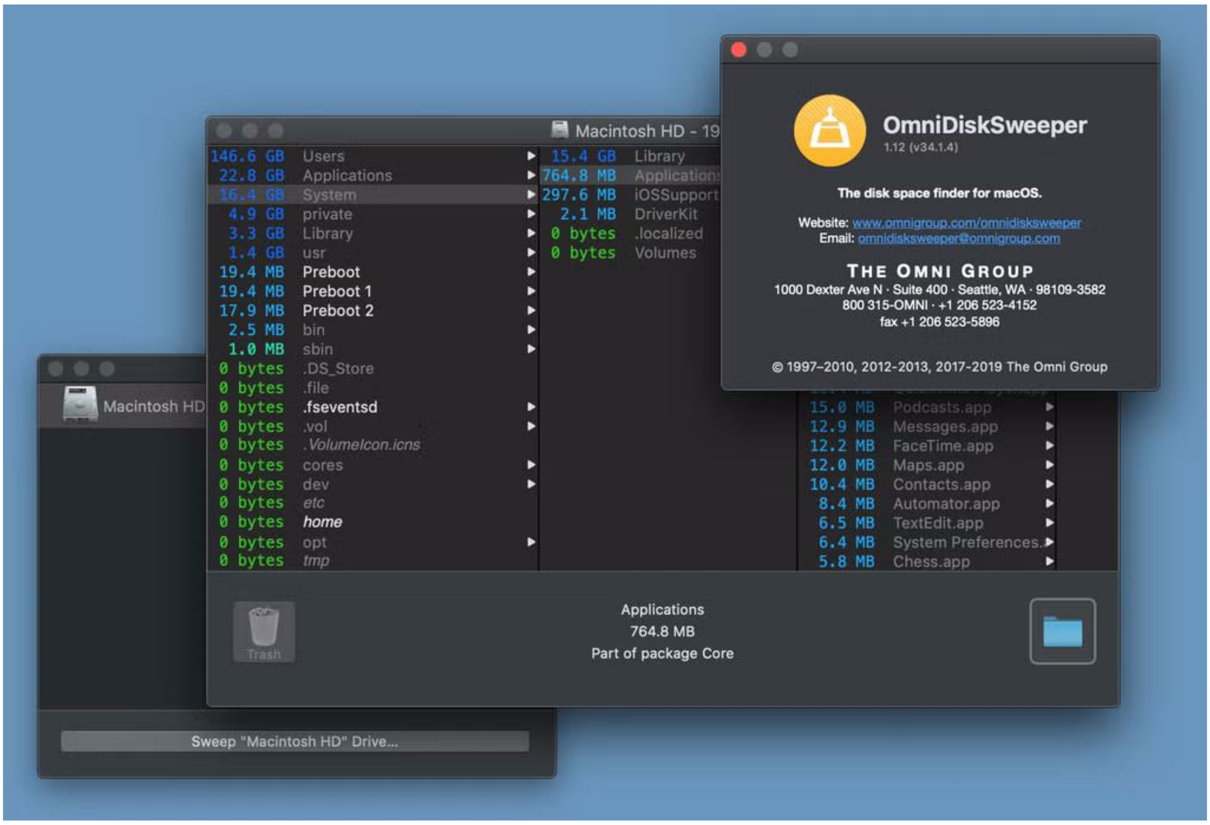


Name	Size	Allocated	Files	Folders	% of Paren...	Last Modified	Owner
1,0 GB C:\Users\Jones\	1,0 GB	1,0 GB	1.501	631	100,0 %	22.08.2022	Administratoren
295,7 MB Pictures	295,6 MB	295,7 MB	42	6	27,8 %	22.08.2022	Administratoren
222,6 MB Holidays	222,5 MB	222,6 MB	22	0	75,3 %	22.08.2022	Administratoren
33,6 MB Animals	33,6 MB	33,6 MB	3	0	11,4 %	22.08.2022	Administratoren
26,1 MB Projects	26,1 MB	26,1 MB	7	0	8,8 %	22.08.2022	Administratoren
10,0 MB [6 Files]	10,0 MB	10,0 MB	6	0	3,4 %	10.06.2020	Administratoren
2,8 MB Village.JPG	2,8 MB	2,8 MB	1	0	1,0 %	10.06.2020	Administratoren
2,4 MB Flower.JPG	2,4 MB	2,4 MB	1	0	0,8 %	10.06.2020	Administratoren
1,4 MB Waterfall.JPG	1,4 MB	1,4 MB	1	0	0,5 %	10.06.2020	Administratoren
1,2 MB Boats.JPG	1,2 MB	1,2 MB	1	0	0,4 %	10.06.2020	Administratoren
1,1 MB Squirrel.JPG	1,1 MB	1,1 MB	1	0	0,4 %	10.06.2020	Administratoren

Free Space: 89.8 GB (of 125 GB) | 1.501 Files | 0 Excluded | 4.096 Bytes per Cluster (NTFS)

On Treesize, you can see how much you are using by measuring the drive, in most cases this will be the C drive. Take the size of Users into account as that is often the area you will be backing up as the rest of the folders are either programs or system that you can ignore.

OmniDiskSweeper



Macintosh HD

Macintosh HD - 19

```
146.6 GB  Users            ▶   15.4 GB  Library
 22.8 GB  Applications     ▶  764.8 MB  Applications
 16.4 GB  System           ▶  297.6 MB  iOSSupport
  4.9 GB  private          ▶    2.1 MB  DriverKit
  3.3 GB  Library          ▶    0 bytes .localized
  1.4 GB  usr              ▶    0 bytes Volumes
 19.4 MB  Preboot          ▶
 19.4 MB  Preboot 1        ▶
 17.9 MB  Preboot 2        ▶
  2.5 MB  bin              ▶
  1.0 MB  sbin             ▶
  0 bytes .DS_Store
  0 bytes .file
  0 bytes .fseventsd       ▶
  0 bytes .vol             ▶
  0 bytes .VolumeIcon.icns
  0 bytes cores            ▶
  0 bytes dev              ▶
  0 bytes etc
  0 bytes home
  0 bytes opt              ▶
  0 bytes tmp
```

```
15.0 MB  Podcasts.app            ▶
12.9 MB  Messages.app            ▶
12.2 MB  FaceTime.app            ▶
12.0 MB  Maps.app                ▶
10.4 MB  Contacts.app            ▶
 8.4 MB  Automator.app           ▶
 6.5 MB  TextEdit.app            ▶
 6.4 MB  System Preferences.     ▶
 5.8 MB  Chess.app               ▶
```

Applications
764.8 MB
Part of package Core

OmniDiskSweeper
1.12 (v34.1.4)

The disk space finder for macOS.

Website: www.omnigroup.com/omnidisksweeper
Email: omnidisksweeper@omnigroup.com

THE OMNI GROUP
1000 Dexter Ave N · Suite 400 · Seattle, WA · 98109-3582
800 315-OMNI · +1 206 523-4152
fax +1 206 523-5896

© 1997–2010, 2012-2013, 2017-2019 The Omni Group

Like Treesize, OmniDiskSweeper sorts your data by size with the largest first and you need to look at the size of Users. Choose a drive that is at least double the size of Users.

Backup methods

Manual backup

A manual backup is the simplest, but most laborious way to backup files.

On Windows you need to open **File Explorer** (which is the yellow folder on the bottom bar) and connect your USB stick or USB drive to your computer. Select the file or folder you wish to backup, then right click and click on "show more options" then choose Send to, and the drive letter of your USB stick or drive will appear as an option.

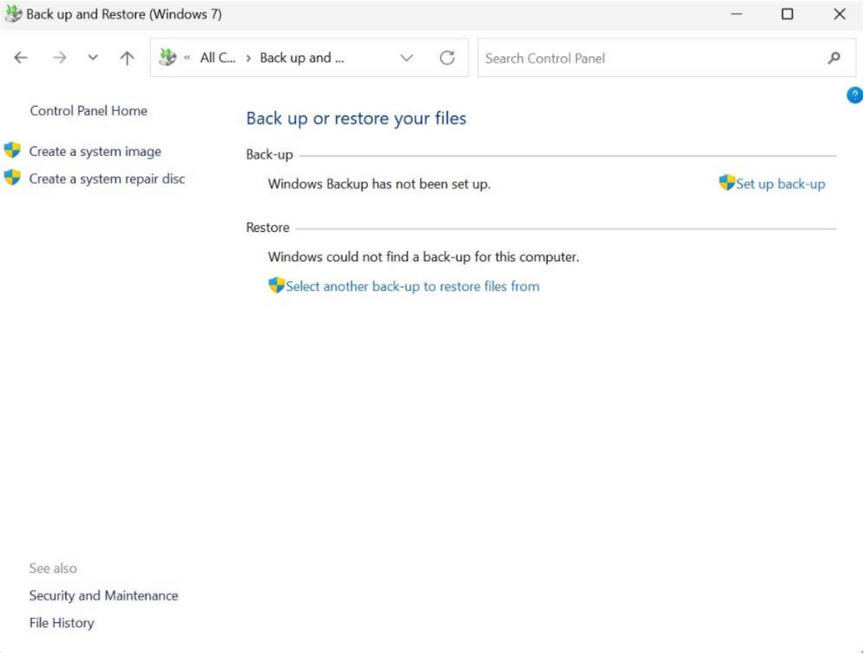
On Mac you will need to use **Finder**, so click on the smiley face in the dock. Plug in the USB stick or drive[2] into your computer, then drag the files or folders over to the new icon created on the desktop. When you finish copying your files and folders, drag this icon into the trash can to eject.

[2] If these do not appear, go to Finder Settings (from the Finder menu, choose Settings or Preferences, then sidebar and check both Hard drives and External drives) and then they will appear on the desktop and on the sidebar of Finder windows.

Automated backups

You can create an automated backup in two ways in Windows:

The old way, that Microsoft calls **Backup and Restore (Windows 7)** and that performs a full backup to external media. A full backup involves the complete creation of all the files and folders that exist on a computer, it effectively creates duplicate copies of your data on the external media. It is the most time-consuming backup process but is the quickest to restore. This can be found in Control Panel.



Back up and Restore (Windows 7)

Back up or restore your files

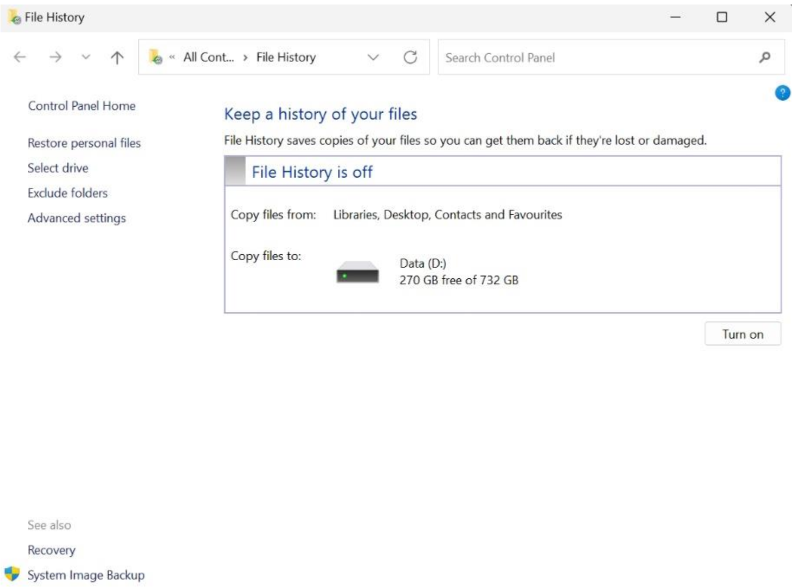
Back-up

Windows Backup has not been set up.

Restore

Windows could not find a back-up for this computer.

The new way is called **File History**, which creates a full backup of your data, then takes snapshots of every file that gets changed. This is considerably faster than the old way, but it can fill external media as there is no easy method to remove the history of these files from the backup once enabled. Search for File History in Settings.



File History

Keep a history of your files

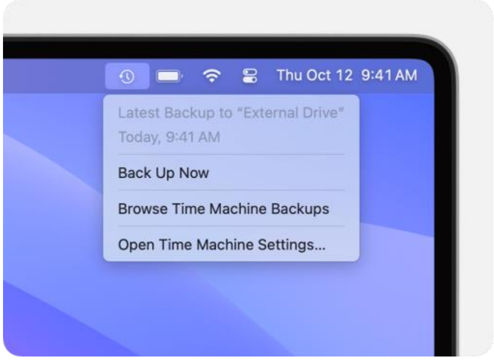
File History saves copies of your files so you can get them back if they're lost or damaged.

File History is off

Copy files from: Libraries, Desktop, Contacts and Favourites

Copy files to: Data (D:) 270 GB free of 732 GB

On the Mac there is **Time Machine**, which performs a full backup then takes incremental backups every hour for the past 24 hours, daily backups for the past month and weekly backups for all previous months and then older backups are automatically deleted when the backup drive is full. It is recommended that the external media be at least double the storage available to the Mac. So, if you have 1TB of storage, you need 2TB for Time Machine. Time Machine also keeps a backup on the Mac for up to 24 hours.

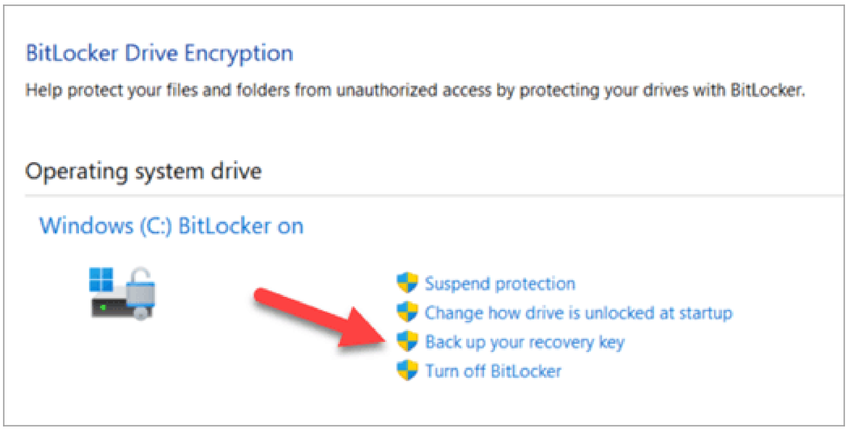

Thu Oct 12 9:41 AM
Latest Backup to "External Drive"
Today, 9:41 AM
Back Up Now
Browse Time Machine Backups
Open Time Machine Settings...

Apple has a useful guide on Time Machine here: https://support.apple.com/en-gb/104984

Back up BitLocker recovery key

Microsoft in recent years has been enabling BitLocker encryption on Windows, this means your data is encrypted. BitLocker encrypts your data using a password and recovery key. If you forget the password, you can use the recovery key to access your data. If you have lost both and you have a problem with your computer, your data is unrecoverable.

You can back up your recovery key by searching for BitLocker from the Start menu, you will need to click on Manage BitLocker in Control Panel to open this screen. Choose Backup your recovery key. You have a few options including saving to your Microsoft Account, downloading and printing your BitLocker recovery key.


BitLocker Drive Encryption

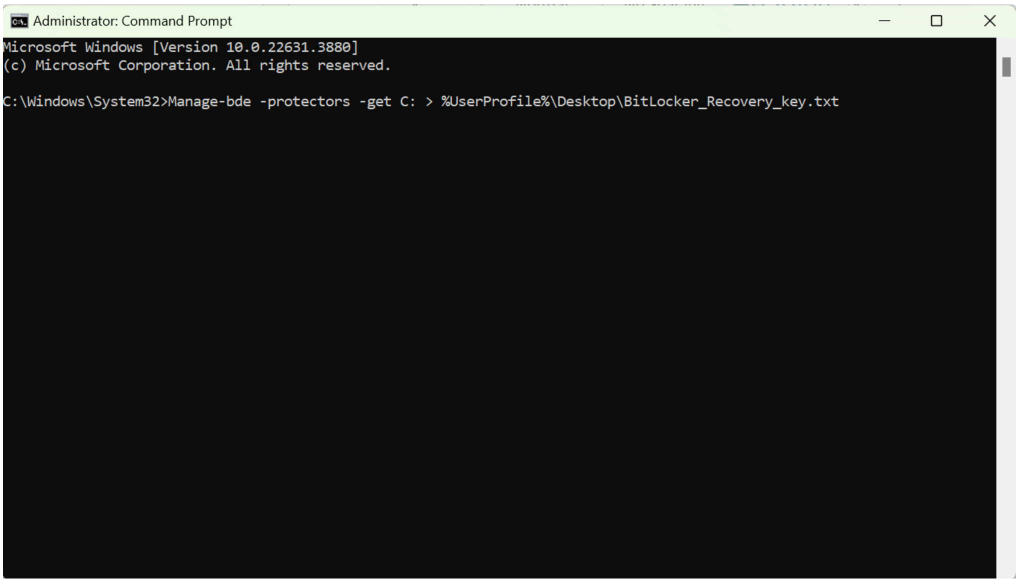
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker on

- Suspend protection
- Change how drive is unlocked at startup
- Back up your recovery key
- Turn off BitLocker

You can also extract the key using Command Prompt with the manage-bde command:



```
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>Manage-bde -protectors -get C: > %UserProfile%\Desktop\BitLocker_Recovery_key.txt
```

Now your BitLocker recovery key will be located on your desktop.

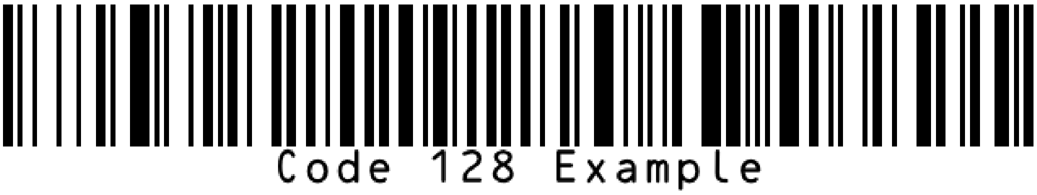
BitLocker Recovery Key as a barcode

Barcodes are symbols designed to work rapidly with computers, and since barcode readers pretend to be keyboards, they enter exactly what the barcode reads into the computer. The BitLocker Recovery Key is not exactly designed to be human readable itself, so printing it as a barcode will help hugely in entering it when you need to.

You can buy pocket barcode readers for less than £30 and they plug into the USB port for both charging and use.

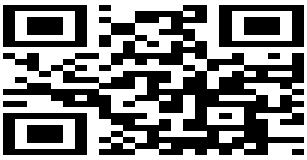
You can use an online site such as Barcode Factory to generate a Code 128 barcode which will store the BitLocker Recovery Key as this will enable you to label the barcode with a human readable message. This can be printed out and stuck on the side of your computer for ease of use, and since the shape is rectangular, it makes it a better choice for the side of your computer, or at the back where nobody will see it.

Code 128 is known as a 1-dimensional barcode, since it is a series of black and white lines that can be read with a CCD or laser barcode reader.



Example of a Code 128 barcode

An alternative is the QR Code* which is a 2-dimensional barcode, which consists of a pattern of black and white (or coloured) dots or squares that encode the message. These must be read with a barcode reader that can read 2D barcodes. The barcode is square, rather than rectangular.



QR Code Example

Disabling BitLocker

Microsoft doesn't ask you if you want to encrypt all the data on your hard drive, it turns this feature on with every new installation.

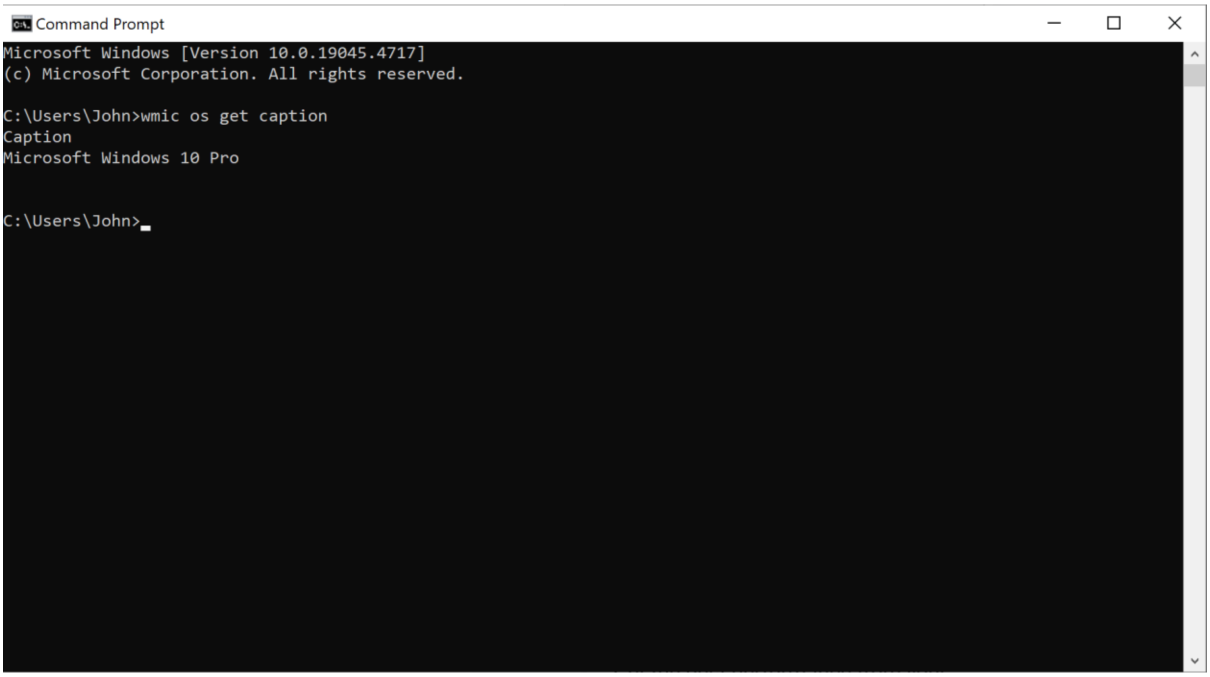
For Microsoft accounts, the key is stored in the Microsoft account, and the PIN is used to encrypt the BitLocker key into the motherboard's TPM (Trusted Platform Module), with both the password and key stored in the Microsoft account. If a Local account is used, the key is stored in plain text in the TPM.

Disable BitLocker prior to adding a computer to a company network that uses Microsoft Entra ID or Active Directory Domain Services so that when you enable BitLocker, the password and key will be subscribed into Entra ID or Active Directory Domain Services.

You can disable BitLocker fairly easily. However, the way to do this depends on the version of Windows you are running and whether you have Home or Pro installed.

You can find out the version of Windows from a command prompt and run:

wmic os get caption



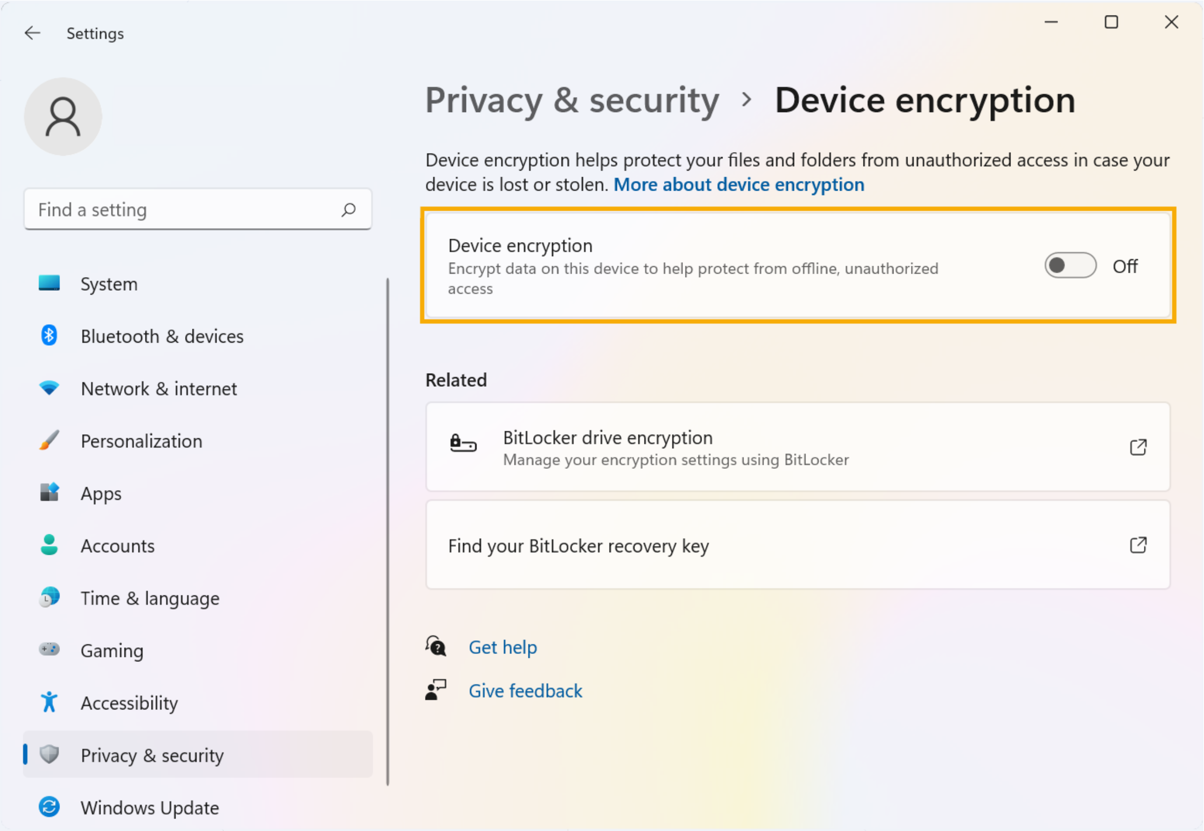
```
Microsoft Windows [Version 10.0.19045.4717]
(c) Microsoft Corporation. All rights reserved.

C:\Users\John>wmic os get caption
Caption
Microsoft Windows 10 Pro


C:\Users\John>
```

Windows 11 Home

Microsoft calls BitLocker for Windows 11 Home (BitLocker is not available for Windows 10 Home) Device encryption. Device encryption is found under Settings then Privacy & security then Device encryption. You can flip the toggle to the off position and then choose to turn off Device encryption.



Privacy & security > Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen. More about device encryption

Device encryption
Encrypt data on this device to help protect from offline, unauthorized access — Off

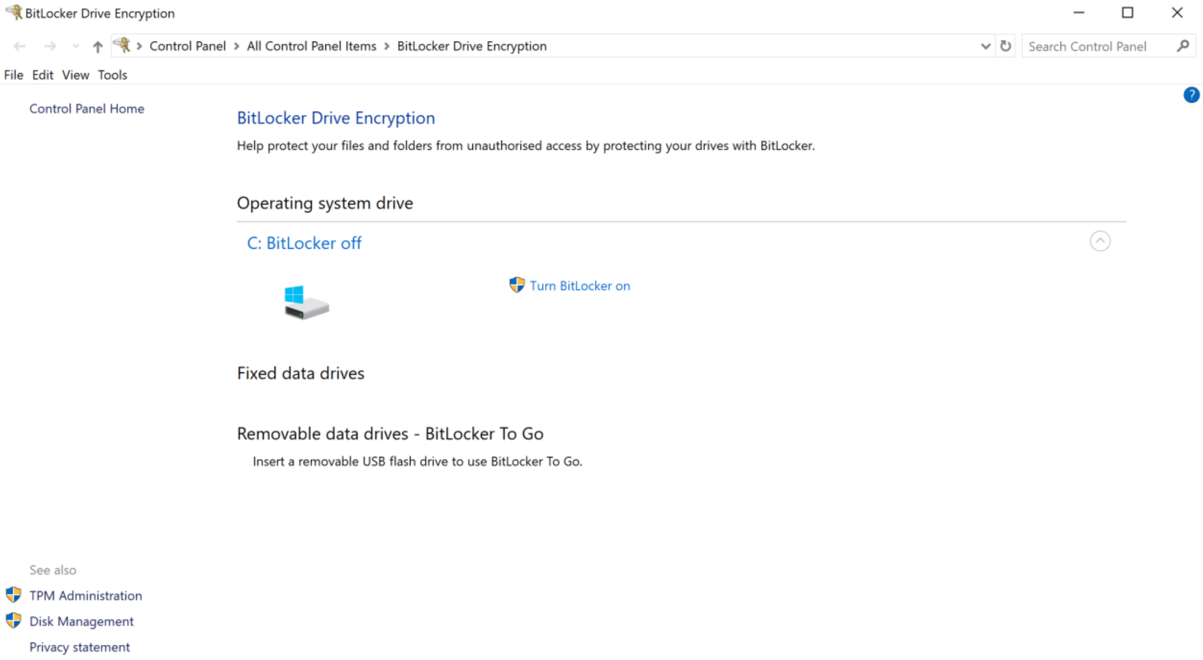
Related

BitLocker drive encryption
Manage your encryption settings using BitLocker

Find your BitLocker recovery key

Windows 10 and Windows 11 Pro

In Windows 10 Pro and Windows 11 Pro, Device encryption is called BitLocker Drive Encryption (also called Standard BitLocker encryption) but to disable this, you need to search for Manage BitLocker.



BitLocker Drive Encryption
Control Panel > All Control Panel Items > BitLocker Drive Encryption
Search Control Panel
File Edit View Tools
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Backup your Web Browser

We use web browsers on an almost daily basis, and it is worth remembering to keep a backup of the following to a file that you include in your backup methodology:

Backup Web Passwords

Export passwords from Chrome:

1. Open Chrome and click on Settings (three vertical dots)
2. Open Autofill and passwords tab and select Google Password Manager
3. Click on Settings then click on Download File under Export
4. You may need to enter your password or PIN to export your passwords.
5. Your passwords will be saved in a .csv format

Export passwords from Microsoft Edge:

1. From the Edge menu in the toolbar, choose Settings then Passwords
2. Click at the top right of the list of saved passwords and select Export Passwords
3. Click Export Passwords and you may need to enter the password or PIN to export your passwords.
4. Your passwords will be saved in Microsoft Edge Passwords.csv

Export passwords from Mozilla Firefox:

1. From the Tools menu, choose Settings
2. Click on Privacy & Security and scroll to Passwords and click Saved Passwords
3. Click the three dots and choose Export passwords
4. Click Continue to Export
5. You may need to enter your password or PIN to export your passwords
6. You will see a save box to save your passwords as csv

Export passwords from Safari on Mac:

1. Open Safari and from the Safari menu, choose either Preferences or Settings
2. Select the Passwords icon and enter your device’s password
3. Click the three dots icon and choose to export all passwords
4. Confirm you wish to export your passwords

Backup Bookmarks/Favourites

Export bookmarks from Chrome:

1. Open Chrome and click Settings
2. Open Bookmarks & lists
3. Choose Bookmark manager
4. From the three dots choose Export Bookmarks

Export bookmarks from Mozilla Firefox:

1. Open Mozilla Firefox
2. From the Bookmarks menu, choose Bookmarks manager
3. You can choose to Backup as JSON or export as HTML from import and backup icon
4. Save the file on your computer.

Export Favourites from Microsoft Edge:

1. Open Microsoft Edge, click on the Favourites icon
2. Click on the three dots and choose Export Favorites.
3. Save the file on your computer.

Export Bookmarks from Safari:

1. Open Safari, and choose from the File menu, Export, Bookmarks
2. This will export the bookmarks as “Safari Bookmarks.html”

Backing up social media

This is a difficult topic because there are so many different platforms out there. You can export your data from the different platforms, but that data won't be in a form you can easily import if you lose your account to a hacker.

Export your Instagram account

1. Go to accountscenter.facebook.com.
2. Click **Your information and permissions**.
3. From the Your information and permissions page, click **Download your information**.
4. In the popup that appears, click **Download of transfer information**.
5. Click the Instagram account you want to download your data from.
6. Click **Next**.
7. Choose **all available information**.
8. Choose **download it to your device**.
9. Click **Next**.
10. Click **Create files.**

It can take up to two weeks to get all your Instagram data. Once it's ready, it'll be sent to the email address you entered, and you'll have four days to download your files.

Export your Facebook account

1. Go to accountscenter.facebook.com.
2. Click **Your information and permissions**.
3. From the Your information and permissions page, click **Download your information**.
4. In the popup that appears, click Download of transfer information.
5. Click the Facebook account you want to download your data from.
6. Click **Next**.
7. Choose **all available information**.
8. Choose **download it to your device**.
9. Click **Next**.
10. Click **Create files.**

Export your LinkedIn account

1. Click your profile picture in the upper-right corner of your screen and select **Settings & Privacy**.
2. In the left panel, select **Data privacy** and then **Get a copy of your data**.
3. Choose to download **larger data archive**.
4. Click **Request archive**.

You'll receive an email with a link to download a .zip file containing your archive files from LinkedIn's website after about 24 hours.

Export your TikTok account

You will need to use a mobile app to export your account data from TikTok.

1. Tap **Profile** at the bottom of the screen.
2. Tap the **Menu**, and then **Settings and privacy**.
3. Tap **Account**.
4. Select **Download your data**.
5. Select the file format you want (**TXT** or **JSON**), then click **Request data**.

Note that it takes a few days for the data to be ready for download and is only available for 4 days.

Export your Twitter (X) account

1. Click **More** in the lower-left corner. (On mobile, you'll click on your **profile picture** to see the menu.)
2. Click **Settings and Support**, then select **Settings and privacy**.
3. Click **Your account**.
4. Select **Download an archive of your data**. You'll need to verify your password and enter a verification code.
5. Click **Request archive**.

Export your YouTube account

1. Click your **profile photo in the upper-right corner** and select **Your data in YouTube**.
2. Click **Download YouTube data**.
3. If you have multiple YouTube products, you can select which products to include.
4. YouTube has the option to specify how you'll receive the file, how frequently you want the export to occur, and the maximum file size.
5. And within the **transfer options**, you can have YouTube automatically save your export to a destination like **Drive** or **Dropbox**.
6. When you're ready, click **Create export**. Your content will end up wherever you sent it.

Using a downloader

There is a different approach if you only want your photos and videos and that is using a downloader like the 4K Video Downloader suite:

1. 4K Video Downloader for your YouTube videos, you can use this tool to download videos and shorts to your computer, you can also use the tool to download subscriptions and playlists. This is not limited to your videos.
2. 4K Stogram for your Instagram photos and videos, you can download reels as well. It enables you to see others content by date rather than by the algorithm.
3. 4K Tokkit for your Tiktok video content.

Storing passwords as barcodes

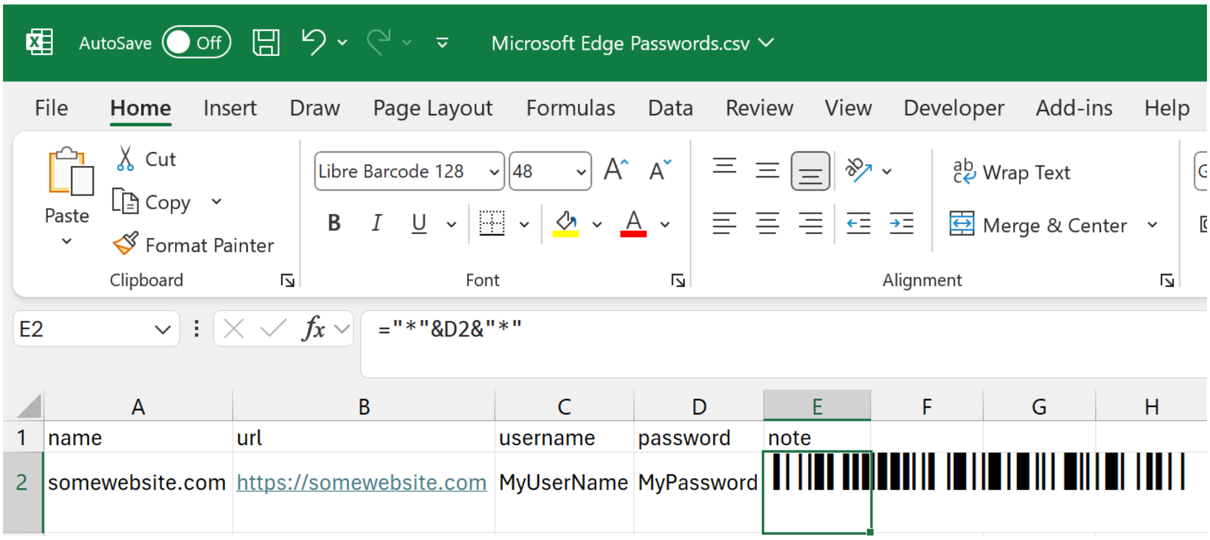
Since your passwords are exported from your web browser in CSV (Comma Separated Values) they can be read into a Spreadsheet program. You will need a font known as Libre Barcode 128 or Code-128

Download the font and open it, then click Install.

Open the exported CSV file with your passwords in your Spreadsheet program. Below is an example of this. In the example, I'm using Excel.

1. In the note column, I have added this formula: ="*"&D2&"*"
2. Set this cell font to Libre Barcode 128.
3. This cell now contains a Code 128 barcode that changes when the password field is updated.
4. Copy this formula down each row of your password backup.
5. Save this file as a .xlsx so that it preserves the formatting we have applied.

What this formula does is add the barcode start symbol * at the beginning of the cell E2, then include the contents of the cell D2 then adds the barcode stop symbol * at the end. The text in E2 reads *MyPassword*. By changing this into the barcode font, the barcode is displayed instead.



E2 ="*"&D2&"*"

	A	B	C	D	E
1	name	url	username	password	note
2	somewebsite.com	https://somewebsite.com	MyUserName	MyPassword	

Remember to backup your barcode font so you can change your spreadsheet passwords when they change, and the barcode will automatically update. You can then print out the spreadsheet to have a hard copy to place in a secure location where you keep your passwords.

Two Factor Authentication

Two Factor Authentication is a new way to help prevent hackers from getting into your account. The principle is that it is something you own and something you know. It is an addition to your password.

The site creates a key in the form of a QR code or a series of characters. This is used to generate (usually) 6-digit numbers that change every 30 seconds (called OTP or One Time Passcode)

The site will then provide you with an extra box to enter this 6-digit number occasionally, usually when you need to log in from a new device.

Two Factor Authentication works well, but it does have disadvantages, and the biggest disadvantage is the fact that it has no site-specific information in it. A hacker can create a website that looks official, you enter your account details, and it reads the 6 digits you enter, then replays them on the official site within that 30-second window and then can gain access to your account, change your password and lock you out.

Using Two Factor Authentication

If you are using a laptop or desktop, look at **authenticator.cc** which provides a browser extension for Firefox, Microsoft Edge or Google Chrome.

1. Once you have installed the extension, you will see a symbol to open the box to list all your authentication codes. As this is your first time, you won't see any.
2. Click on the **Scan QR Code** button. Now you can capture the QR code using the mouse to draw a box around the code on the website you are adding.
3. You will see a 6 or 8-digit code appear on the screen which refreshes every 30 seconds.

If you don't have a QR Code to scan, you can enter the details manually:

1. Click on the Pencil to edit your list of authentication codes and press the **+** button.
2. Click on Manual entry.
3. Enter the issuer, if the code is for Facebook, then enter the word Facebook. Its descriptive but you can call this whatever you wish.
4. Enter the secret the site shares with you.
5. If the site uses a different refresh period, you can set this in the Advanced section between 15 and 45 seconds.

You can also backup your list of authentication codes to your computer or to Google Drive, Microsoft OneDrive or Dropbox.

If you are on a mobile device, look at **2FAS**.

Apple version:

1. Click on the + symbol and scan the QR code with your device’s camera.
2. Your 6 or 8-digit code will be displayed.

Android version:

1. Click the ⁝ symbol and scan the QR Code with your device’s camera.
2. Your 6 or 8-digit code will be displayed.

If you don’t have a QR Code, you can manually add the service name and secret key.

2FAS also has a browser extension, and you can easily import and export your list of authentication codes between the browser extension, Apple and Android versions.

Passkeys

Passkeys is the replacement for passwords and two factor authentication by fixing both problems at the same time. Passwords can be guessed, and two factor authentication can be replayed. Passkeys have been developed to replace passwords by using something you have in a different way.

You register biometric information into your device, and it creates a unique device key from that information. You visit a website you have a login for and proceed to login as normal with your email address and password, then the website gives your device a unique website key. Your device and website create a lock that only the device key and website keys will fit.

If you visited a copy of the website, the website key wouldn’t match the lock and prevent you from logging in, so your account cannot be compromised.

Gradually, more and more providers are switching to passkeys.

If your device lacks biometric capabilities, you can add them with a USB fingerprint reader. Note that the cheaper ones are hit and miss to get to work. Fingerprint readers also rely on the oils in your skin, so overly dry or wet fingers will hamper operation.

Cloud Storage

Cloud storage is the ability to store your data on a computer on the Internet somewhere. This is not a true backup, especially when Microsoft calls part of their OneDrive storage "Windows Backup" as it is more a synchronisation or a mirror of what you have on your computer. If the files on your computer get corrupted, or encrypted by a malware infection, then so does your cloud storage.

Cloud storage has its uses however, if you have more than one device, the files can be accessed across those devices easily, as each file and folder is synchronized.

Apple's cloud storage is called iCloud, and newer Macs will automatically sync files to the iCloud. You get 5GB for free, but you can pay for iCloud+ which gives you 50GB, 200GB, 2TB (2000GB), 6TB and 12TB.

Microsoft's cloud storage is called OneDrive, and you also get 5GB for free[3]. If you sign up for Microsoft 365 Personal, you get 1TB of cloud storage along with the office package for 5 devices. If you sign up for Microsoft 365 Family, each family member gets 1TB of cloud storage.

For businesses, OneDrive is designed for personal cloud storage within a business and SharePoint is designed for sharing data between teams and departments.

There are other cloud storage provides that offer synchronisation between devices and their cloud offerings, such as Box; DropBox; Google Drive[4]; Zoho Workdrive; etc.

[3] The 5GB is part of the 15GB allocated to email, so if you fill up your 5GB you may have trouble sending and receiving email.

[4] Google Drive limit also affects Google Mail.

Cloning

Cloning is a process that copies the entire contents of a drive onto another drive. All the data on one drive will appear on the other drive. It’s often used if you are replacing a drive in a computer with a newer one, since it preserves the operating system, all the installed programs, settings, and all your data.

The process of cloning a drive can take a long time but the result is that you get exactly the same machine without having to start afresh with a clean installation, reinstall all your programs and customise all the settings to how you prefer Windows to look.

Disk Image

A disk image (often called a virtual drive) is basically a whole drive that is stored in a single file on the computer.

Apple software used to be supplied on floppy disks, but it was found that these could be delivered as a disk image instead, which turned out to be the most efficient way to install software on a Mac. The user would download the disk image and then open it as if it were a floppy disk, run the installer and then drag the floppy disk to the trash can to eject it.

You can create blank disk images or create one from a drive using Disk Utility (located in Utilities folder inside Applications in Finder)

On Windows, virtual hard drives (VHD and VHDX) can be created from physical drives and can be connected as if they are physical drives. Virtual drives also have their place in something called a **Virtual Machine**.

A **Virtual Machine** allows you to run an operating system in a secure isolated environment on your computer, for instance you can run an older copy of Windows or run Windows on a Mac. The Virtual Machine can be given access to devices like printers and to the host computer, so files can be made accessible between the computers.

Often you may have a program that only runs on an older version of Windows, like XP or Windows 7 and you don’t want to expose a computer to the Internet where it could get hacked or virus ridden, then running it in a Virtual Machine is the way to do that.

Introduction to PARA Method

PARA is a method of organizing your data into an easier structure so you can find everything quicker, in addition to categorising your data by how much you use it. You basically create 4 folders in your documents area:

1. Project – This contains files and folders of everything that is based on scheduled deadline that is in the future. These will be the most accessed files.
2. Area – This contains files and folder you are currently working on that are not based on a scheduled deadline; however, these files are actively used.
3. Resource – This contains your files and folders you refer to but are not being worked on. You are making these resources available to you.
4. Archive – Everything that has a completed deadline or is no longer used. These are your least accessed files.

You start by creating an archives folder with a folder inside that has the current date and put everything inside that folder. You can then take out the relative files and folders that will serve as projects, areas and resources. As you complete a “project” or “area”, you create a new folder in the Archives folder and move those files and folders into that new folder.

Effectively, you are decluttering and organising your files by storing them in named folders and categories where you will find them quickly when you come back to them later.

Since you categorise your data into most important and most accessed files, you will want to back those files up more often than you would the Archive files. This makes your backup process faster and more fun.

Conclusion and Links

Now you know how to backup data, you can apply the 3-2-1 rule to your data:

- Have **3** copies of your data, one in a backup and two others as copies.
- Use **2** different types of media for storage.
- Make sure **1** copy is off-site in case of disaster.

Useful links:

- Treesize Free: https://www.jam-software.com/treesize_free
- OmniDiskSweeper: https://www.omnigroup.com/more
- Apple iCloud plans and pricing: https://support.apple.com/en-gb/108047
- Microsoft OneDrive plans and pricing: www.microsoft.com/en-gb/microsoft-365/onedrive/compare-onedrive-plans
- Dropbox: www.dropbox.com
- Box: www.box.com
- Google Drive: www.google.co.uk/intl/en-GB/drive/
- Zoho Workdrive: www.zoho.com/workdrive/
- Tiago Forte’s PARA Method: https://fortelabs.com/blog/para/
- 4K Video Downloader: https://www.4kdownload.com/
- 2FAS Authentication: https://2fas.com
- Authenticator.cc: https://authenticator.cc/

Online Barcode Generators:

- Barcode Factory: https://www.barcodefactory.com/free-barcode-generator
- Terry Burton has categorized barcodes: https://www.terryburton.co.uk/barcodewriter/generator/

Barcode Fonts:

- Libre Barcode 128: https://fonts.google.com/specimen/Libre+Barcode+128
- Code-128: https://www.dafont.com/font-comment.php?file=code_128