

Session 2 – Safe and Secure

1 INTRODUCTION TO THE SESSION

This is the second of 6 sessions in which you will be shown the basics of using a Windows computer.

You will want to know that anything you do with your computer is safe and secure, and that if you do make a big mistake, or if you are a victim of hacking, you can recover from it. There are some simple rules and procedures that you can adopt to keep you, your system and your data safe.

1.1 Internet Resources

One of the aims of this course is to make you feel comfortable to use the internet to find information, solve problems, and follow instructions, so we will be using the internet to help with some of the topics.

2 REVISION

Before beginning the topics for this session we will quickly review session 1 and see if you have made any changes to the way you use your computer, or have any follow-up questions.

3 SECURITY AND INTEGRITY

The terms 'security' and 'integrity' are often misused to mean the same thing. In fact, they have technical definitions:

In your internet browser type:

what is the difference between security and integrity?

4 TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) improves security by using two separate ways to verify your identity.

- Intellectual knowledge: Password, PIN, security question.
- A physical or virtual object: Smartphone, text message code, authenticator app, USB security dongle.
- Personal characteristics: fingerprint, facial recognition, voice print.

Combining two of these together makes it very much harder for criminals to access your accounts and data.

5 PASSCODES, PASSWORDS AND PASSKEYS

Passcodes, passwords and passkeys offer three levels of security:

	Typical format	Typical use	Security strength
Passcode	4 to 6 digits	Unlocking a phone	Poor
Password	Characters, digits or symbols	Accessing an on-line shop	Good
Passkey	Passcode or biometrics	Accessing internet banking	Excellent

The National Cyber Security Centre recommends using passkeys over passwords wherever available.

Have a look at:

<https://www.ncsc.gov.uk/passkeys>

6 STRONG PASSWORDS

Research shows that the primary feature of good passwords is simply their length; the more characters the better; 12 is recommended for optimal protection. Including numbers or special characters actually makes little difference. A simple way to create, and remember, long passwords is to assemble 3 or more random words. If the system requires you to use numbers or special characters you can sprinkle them between the words, for example:

Many\$Apply9Effect

Just flick through the dictionary, or any random book, and pick random words.

7 PASSWORD MANAGERS

A password manager is a secure tool that stores your login details in an encrypted vault protected by a single master password or passcode. It can also generate strong passwords and auto-fill details on log-in screens. It uses powerful encryption so your data remain safe from hackers. Popular options include independent services like Bitwarden or 1Password, as well as built-in tools like Google Password Manager.

There are two ways to use a Password Manager:

- Use it to store passwords that you have created yourself. This is useful for storing the credentials of existing accounts.
- Use it to generate long, random, unique passwords for each account. This is useful for new accounts or where security is paramount.

Signing in to websites and apps is much quicker because the Password Manager will Auto-Fill your username and password when the sign-in screen pops up.

8 BACKUP

Most people know that they should keep back-up copies of their data, but few do!

The important considerations when backing-up your files are:

- When: How often the files are copied, e.g. daily, weekly, monthly, ad-hoc. Decide how many day's work you are prepared to re-do if an important file is lost.
- How:
 - Full: Everything is copied (even if not changed). Convenient to know that all your files are on the last backup, but uses much more space.
 - Incremental: Only files that have changed since last backup are copied. Much less space used, but you have to search back through backups to find the last time a file was copied.
- Where:
 - On same hard drive as originals. Not really a backup!
 - On separate hard drive in same machine. If machine is stolen you've lost everything.
 - On external media (hard drive, USB stick). Hide the drive somewhere when not in use to protect against thieves. Use a fireproof safe or keep it in a different building to protect against fire.
 - To 'The Cloud'. Very convenient (if you trust the cloud service provider). By setting up an automatic backup schedule you can just leave your system to get on with it.

8.1 Local Backup

For a local backup, e.g. to a hard-drive, either internal or external, use 'File History'

NOTE: Do not get confused with the Backup and Restore (Windows 7) as this is now out-of-date.

-  (Start) > Windows System > Control Panel > System and Security > File History

Or

-  (God Mode) > File History > Save backup copies...

You can specify:

- Which drive you want to write the backup to, including networked storage.
- If there are any folders you don't want to backup.
- How often to save copies.
- How long to keep the backups.

8.2 Cloud Backup

There are several Cloud Storage options that can be used for backup. They all work in much the same way. A folder is created on your machine that is automatically synchronised with a file server that is accessed via the internet. When you put a file into the folder it is automatically and immediately copied to the server. Similarly, if you delete a file from the folder it is automatically deleted from the server.

Since the server is accessible via the internet, you can access your cloud storage from any device, so you can, for example, use it to transfer files between a laptop and tablet.

All cloud storage systems require creation of an account and installation of an app on your computer to do the synchronising. Then, to use them for automatic backup, you need to do further set-up, usually using another app, to manage the automatic regular backup of your other folders.

Typical example are:

- OneDrive: Use Windows Backup to manage your backups:
- Google Drive: Use Drive For Desktop to manage your backups.

There are many websites that describe the pros and cons of the various cloud storage providers. When you have decided which one suits your needs best, you will be able to find YouTube videos that take you through the set-up process step-by-step, which, although it may be a bit tricky, you only have to do once.

9 RESTORE

It is not sufficient to set up a backup process and assume it is working. You have to do regular test of the restore process to:

- Check that your files are actually been backed up properly.
- Practice restoring, so you can do it confidently if you ever need to do it for real.

You can practice by restoring a non-critical file, such as a shopping list.

To restore from File History, use:

-  (Start) > Windows System > Control Panel > System and Security > File History > Restore personal files

Or

-  (God Mode) > File History > Restore your files...

10 SYSTEM RECOVERY AND RESTORE

In addition to your data files, there are many other files to do with the operating system and your apps. There are some things you can do to enable you to recover those if they are lost or corrupted.

- Create a **System Recovery image**.
- Create a **Restore point**.
- Keep downloaded installation files.

10.1 System Recovery

System Image Recovery in Windows 10 is a built-in feature that lets you restore your entire computer, including the operating system, settings, apps, and personal files, from a previously saved backup copy called a 'system image'.

A system image is a snapshot of an entire hard drive¹. On most computers the Operating system and associated files are on the 'C:' drive and user data is on the 'D:' drive. So the System Image is a copy of the 'C:' drive. You need a sufficiently large external hard drive, USB memory stick, writeable optical media (blue-ray), or a network location to store the image file.

To create a system image, connect your external storage device, then:

- Type **Recover** in the search bar > **Create a recovery drive**.

Or

-  (God Mode) > System > Create recovery drive.

Always select the **Backup System Files** option.

Note: It can take a long time (hours) to write all the data to a USB stick.

Restoring an image replaces everything on the drive, erasing anything saved on the drive after the system image was created. Your PC returns to the exact working condition it was in when you made that specific image.

You can restore the system image:

- If you have a major system failure. For instance, if your computer won't boot up. In these circumstances you can usually access it via the Windows Recovery Environment (WinRE).
- To recover from a virus or bad update.
- After you install a new physical hard drive and need to put your old environment back onto it.

How you restore an image depends on whether your computer is able to boot up or not. Find the instructions on the internet (using another computer of course!)

¹ A physical hard drive can be divided into 'partitions', each partition behaves as a separate drive. So your 'C:' and 'D:' drives may actually be partitions on the same physical drive, but they work as two separate hard drives.

10.2 Restore Points

A restore point in Windows 10 is a saved snapshot of certain key system files. It is not as comprehensive as a recovery image, but is much quicker, smaller and is stored on your internal hard drive. Restore points are intended to recover from bad updates. They do not remove viruses and can't be used to start a system that won't boot up.

After rolling back to a Restore Point, any drivers, updates, or apps installed after that specific restore point was created are lost, but your personal files remain untouched.

They are created:

- Automatically before installing new updates, drivers, or software.
- Automatically once a day if this feature is turned on.
- Manually, before making big changes to your PC, using:



(God Mode) > System > Create restore point.

Creating a Restore point only takes a few seconds.

10.3 Installation File Archive

When you download a new app, or an updated version of an app, it is worth keeping the downloaded file. This enables you to re-install exactly the same version of the app if you ever need to, without downloading it again. It also allows you to re-install an app if the version you want to use is no longer available to download.

Just create a folder on your 'C:' drive and put each app in a suitably named sub-folder.

11 Password Protecting Files.

There is no simple built-in method for password protecting files in Windows. Some application programs have password protection, for example, the LibreOffice apps all have a password protection facility, using:

File > Properties > Security > Protect

In MS Word, you can use:

File > Info > Protect Document > Encrypt with Password

Any file can be protected by using 7-Zip (or similar compression app).

Select the files or folders you want to protect and right-click your selection:

7-Zip > Add to archive > Enter password (twice) > OK

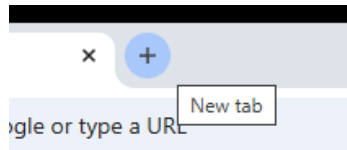
Note that this created a protected copy of the files; the originals are still unprotected, so you may want to delete them.

WARNING: If you forget your password you will never be able to recover the document (except from a backup taken before it was protected).

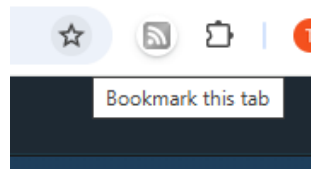
12 INTERNET BROWSING

We have already explored some useful features of internet browsers, including:

- Tabs: You can open several web pages in different tabs at the same time.

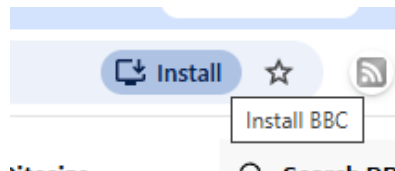


- **Bookmarks:** You can save the URL of favourite sites or pages for quick access.



Two features that we haven't yet seen are:

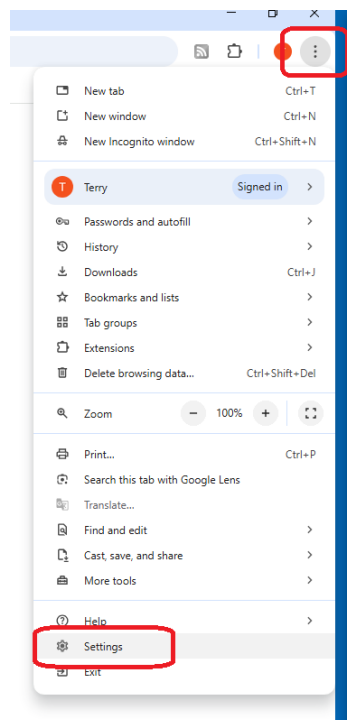
- **Extensions:** You can install extra features to the browser. These are provided by the website you visit and are usually offered as optional installs, though some may be installed automatically.



- In Windows, you can open multiple copies of most apps from the task bar using [SHIFT]+click. This is very useful for opening more than one separate copy of your Browser so that you can view two web pages at the same time.

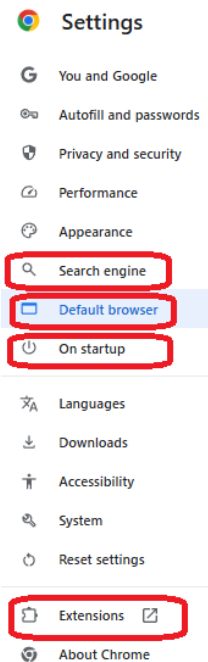
13 BROWSER SETTINGS AND PROBLEMS

If you find that your browser or search engine has taken on 'a mind of its own' it is probably because some site you have visited has altered one or more of your settings. Open your browser menu and click on 'Settings'



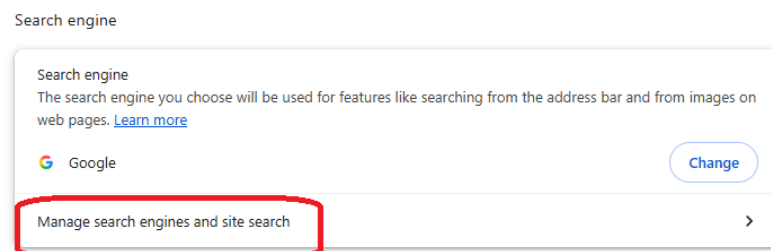
There are 4 settings to look at:

- Search Engine
- Default Browser
- Extensions
- On Startup

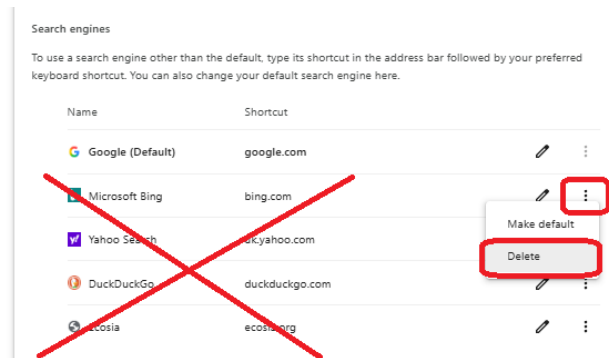


13.1 Search Engine Settings

Click on 'Manage search engines and site search'



Delete all but the one you want to use.

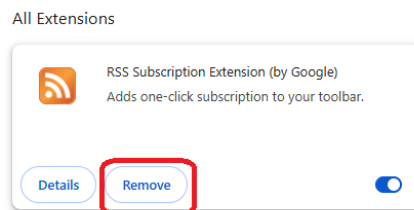


13.2 Default Browser Settings

On the Default Browser setting, ensure Google Chrome (or whatever you want to use) is set to your default browser.

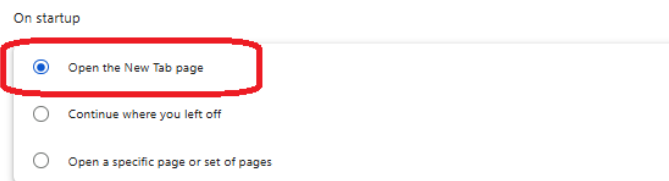
13.3 Extensions settings

Remove all extensions, except ones you know are OK, even the ones that look OK, because they might be infected with malware.



13.4 On Startup Settings

Make sure you start on a blank page. i.e. URL bar is empty when you open the browser.



13.5 Safe Browsing

Knowing which websites to trust, and which to avoid, can be difficult, and there are no absolute rules, but there are some good guidelines:

In your web-browser, search for

how to recognise reputable websites

13.6 Click-bait

Click-bait is a 'teaser' that encourage you to click on a link – to who knows where?!

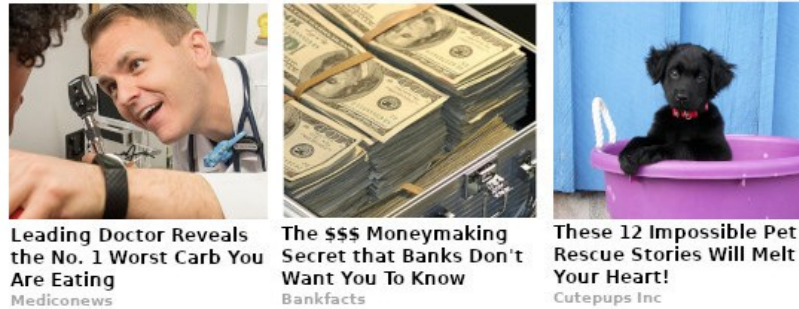


Image: wikimedia.org

Why do they exist:

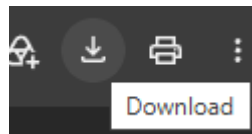
- To collect your personal information, for example, if they offer to tell your horoscope, it's because they want to get your date of birth.
- Install malicious software on your computer.
- To earn advertising revenue.

Just avoid them, and never click on something that just pops up without you asking for it.

13.7 Downloading

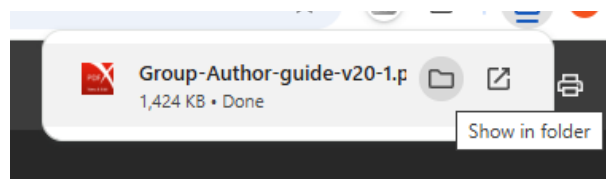
For an example of downloading, we will use the ssu3a website:

*Go to the **Documents** page, click on a document, Click on Download*



The system may prompt you for a location, or it may go straight into one of your default Download folders. After the document is downloaded you can open the folder it has gone into:

Clicking the Downloads icon



Then click on Show in Folder

Be vigilant when downloading from the internet, as adverts are often inserted into pages and are designed to mislead you into clicking the wrong button.

13.8 Download Folders

If a file is downloaded automatically (without asking where to put it) it will typically go into one of two default folders for downloads:

- A Download folder on your C: drive, mostly used for apps and files accessible only by one user.

C:\Users\<username>\Downloads

In File Manager this is listed under This PC

- A Download folder on your data drive (D:), mostly used for apps and files that anyone can access.

D:\Downloads

14 SEARCH STRATEGIES

You can control search results by using specific keywords, advanced search operators, and alternative tools.

14.1 Use Search Operators

You can force a search engine to interpret what you type in specific ways:

- To find exact matches, put quotation marks around words, e.g., "Solihull city council".
- To do a search within a specific website, type `site:` before a web address, e.g., `site:bbc.co.uk news`.
- To remove unrelated results, you can exclude words by putting a minus sign before the word, e.g., `-apple`.
- If you don't know, or don't care about some of the words in your search, you can use an asterisk (*) as a placeholder, e.g. searching for "I love * so much" matches phrases like "I love this game so much" or "I love my dog so much".

14.2 Use The Right Search Engine

The results returned from a search very much depend on the search engine you are using, for:

- For a broad range of results, use a general engine such as Google or Bing.
- For searching without personalisation, use DuckDuckGo.
- For academic sources use Google Scholar.

15 Artificial Intelligence

As we have seen, when you do a Google search, the first result shown is the Google AI Overview. Some of the text in this document has been based on Google AI results, as it is a quick way to assemble facts and be more productive. However, it is always wise to check against other trusted sources; Wikipedia, for example, has been used to check some of the material in this document.

AI is most powerful when it is used in conjunction with other tools and apps. In the following sessions of this course we will see AI used to help with word processing, spreadsheets, graphics etc.

16 SUMMARY OF THE SESSION

In this session you have...

- Reviewed what we did in session 1.
- Used the internet to find information.
- Defined 'security' and 'integrity'
- Learned about 2FA
- Learned about passcodes, passwords and passkeys
- Discussed strong passwords and password managers and password protecting files.
- Looked at options for backing up files.
- Learned about system recovery and system restore points

- Had some tips about internet browsing, browser settings and solving browser problems.
- Started to look at AI.

17 CLOSE

Finally, here is some homework for you:

If you have not done so recently:

Make a System Restore Point

Make a Recovery Image on a USB stick.

Make a backup of your Documents folder.