07 Virus and Malware protection

'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software. **It is right to be concerned about infections but with the appropriate precautions it should not stop you from enjoying life with a computer.**

Malware includes the following

- **Adware** : least dangerous but displays adverts on your computer from which the originators derive payment.
- **Backdoors** : Backdoors are much the same as Trojans or Worms, except that they open a “backdoor” onto a computer, providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.
- **Browser Hijacker:** I*f your homepage changes you may have been infected with one form or another of a Browser Hijacker.*
  - If on Firefox go to Options on the Tools menu. Check whether the Home Page on the General Options has changed. Then check the Search options and see if it contains a search engine you do not recognise. One such hijacker is AVG.nation so be vigilant about the abuse of known names. Use Google if necessary to search for details about the unknown search engine.
  - This dangerous Malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not removing the Malware lets the source developers capture your surfing interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in every case they allow other more infectious malware.
  - ***You will almost certainly need expert help to remove a hijacker as it can involve multiple steps including editing the system registry.***
- **Computer viruses** : A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run.
  - Often this is spread by sharing software or files between computers. Ensure you force a virus scan on any device you are attaching from an outside source. You can usually do this by right clicking on the device entry in File Explorer.
  - In attachments with email. A plain text email cannot spread a virus but it is technically possible but unlikely for a rich text email to contain a virus. NEVER EVER open an attachment from someone you do not know or were not expecting. **A good technique is to drag an attachment to your desktop and right click on it to force an anti-virus scan.**
  - From websites, particularly when downloading software. Apply the same rule of forcing a scan before executing the new software.
  - Other methods viruses replicate includes via a network.
  - Due to its means of replication it can spread very quickly
- **Keyloggers:** Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program
- **Ransomware:** see more details below.
- **Rogue security software:** This one deceives or misleads users. It pretends to be a good program to remove Malware infections, but all the while it **is** the Malware. So if you are infected be extra careful in using free or even one time purchase software off the web to

resolve your problem.

- **Rootkit** : It is the hardest of all Malware to detect and therefore to remove. It is designed to permit the other information gathering Malware to get the identity information from your computer without you realizing anything is going on.
- **Spyware** : software that spies on you, tracking your internet activities in order to send advertising (adware) back to your system.
- **Trojans or Trojan Horses**: The most dangerous Malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources. They are also used to create a "denial-of-service attack " which is an attempt to make a machine or network resource unavailable to those attempting to reach it.
- **Scareware :** malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection.
- **Worms :** A program that replicates itself and destroys data and files on the computer. Worms work to "eat" the system operating files and data files until the drive is empty.
- and other malicious programs.

Summary:
It can take the form of executable code, scripts, active content, and other software. The main sources are

- email attachments
- web browsing
- from external devices, e.g usb flash drives
- in a company through the in-house network

What you need to do

- Don't open attachments from unknown sources. Scan the attachments from those you do know before opening. Just to scare you, even PDFs can contain viruses but this is currently very rare
- Be vigilant with connecting foreign devices
- Be vigilant in any downloading of software from the web
- Ensure you have anti-virus and malware protection software
- Periodically run scans from the above even if it has real time protection.
- Ensure Windows firewall is ON
- Don't Panic. If you are sensible the chance of a serious infection is low. Having used the web since its inception in the 90's and only ever using free software for my personal computers I have yet to suffer damage from malware.

Ransomware

This is a relatively new type of malware and the fastest growing.

1. Your computer gets infected. The most common method is as an attachment to an email either as a zip or a "docm"
2. It activates a program which encryptes your files. It uses an advanced encryption method that cannot be reversed without having the decryption key.
3. The names of the files are altered and a document is inserted in to each folder where files have been encrypted.
4. If you open the document it instructs you to register for the "tor" network (the dark web), to purchase bit coins of a specified amount, and to transfer these. The tor network prevents the

other party from being detected by routing the messages through multiple anonymous servers.

5. Of course there is no guarantee that after payment they will send you the means of decrypting the files.
6. It is hoped that you have a recent backup as there is little else you can do to recover your files.

Software to help

It is important that you have the following running and regularly updated software.

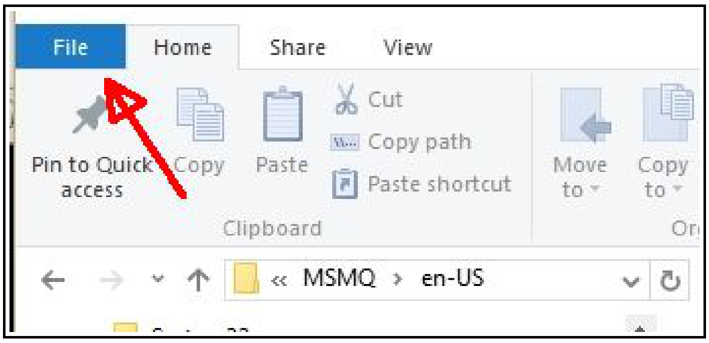
1. **A recognised Anti-virus program.** Generally the free products are adequate. The argument being that if they are below par for the free version they will not be able to sell the purchased product. They only need to convince a small fraction of those using the free product to upgrade to the chargeable one to be profitable.
   1. Avira
   2. BitDefender
   3. AVG
   4. Avast
   5. There are others but the above are the top rated.
2. A general malware program. **Malwarebytes** is strongly recommended. It will identify and remove PUPs (Potentially Unwanted Programs) which ,while not in themselves always dangerous, can have severe performance implications. One person I helped had 2214 (yes 2214) PUPs that had to be removed.
3. Ensure that Windows firewall is operational. In Control Panel select "Security and Maintenance". Click on Security to see the settings and the state of your security software.
4. Banking software as recommended by your bank.

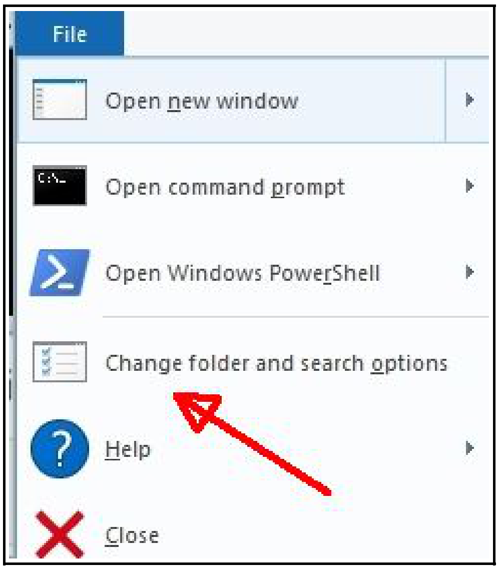
Backups

It is essential that you do regular backups.

- Ideally you should use different devices in case one gets infected.
- A good approach is to
  - use either a large capacity usb flash drive or external disk for full backups. However, if you already have a virus on your system this will probably be replicated on to the device.
  - and then write DVDs to periodically backup your most important files. These are cheap and you easily store a lot of old backups.
  - Photos often take the largest space. Backup up your old ones and keep that clearly marked. Then you only need backup up the new folders.

A more detailed guide to backing up is being compiled.

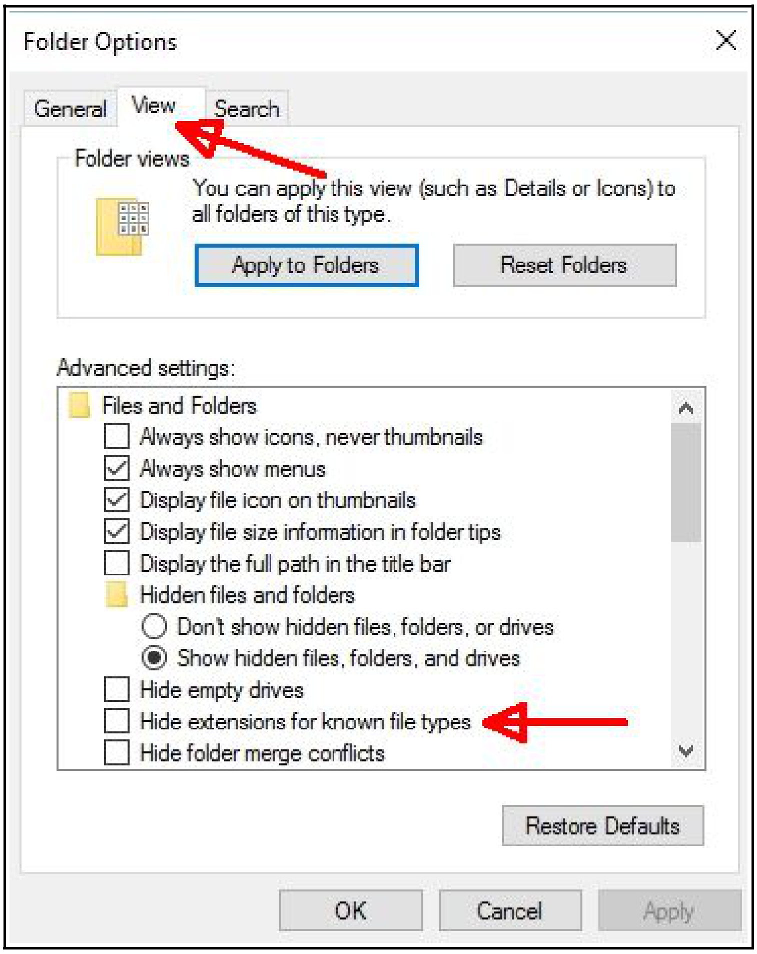




Changing Windows settings

File associations :Windows uses the last word (after the rightmost full stop) to identify the type of file and what action it must perform. For example, if it encounters a ".doc" file it will open the word processor, a ".jpg" file it will open the image viewer.

Java script is a programming language and files with the ".js" extension will be found with emails and internet browsers.


Folder Options

General | View | Search

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Apply to Folders | Reset Folders

Advanced settings:

- Files and Folders
  - □ Always show icons, never thumbnails
  - ☑ Always show menus
  - ☑ Display file icon on thumbnails
  - ☑ Display file size information in folder tips
  - □ Display the full path in the title bar
  - Hidden files and folders
    - ○ Don't show hidden files, folders, or drives
    - ● Show hidden files, folders, and drives
  - □ Hide empty drives
  - □ Hide extensions for known file types
  - □ Hide folder merge conflicts

Restore Defaults

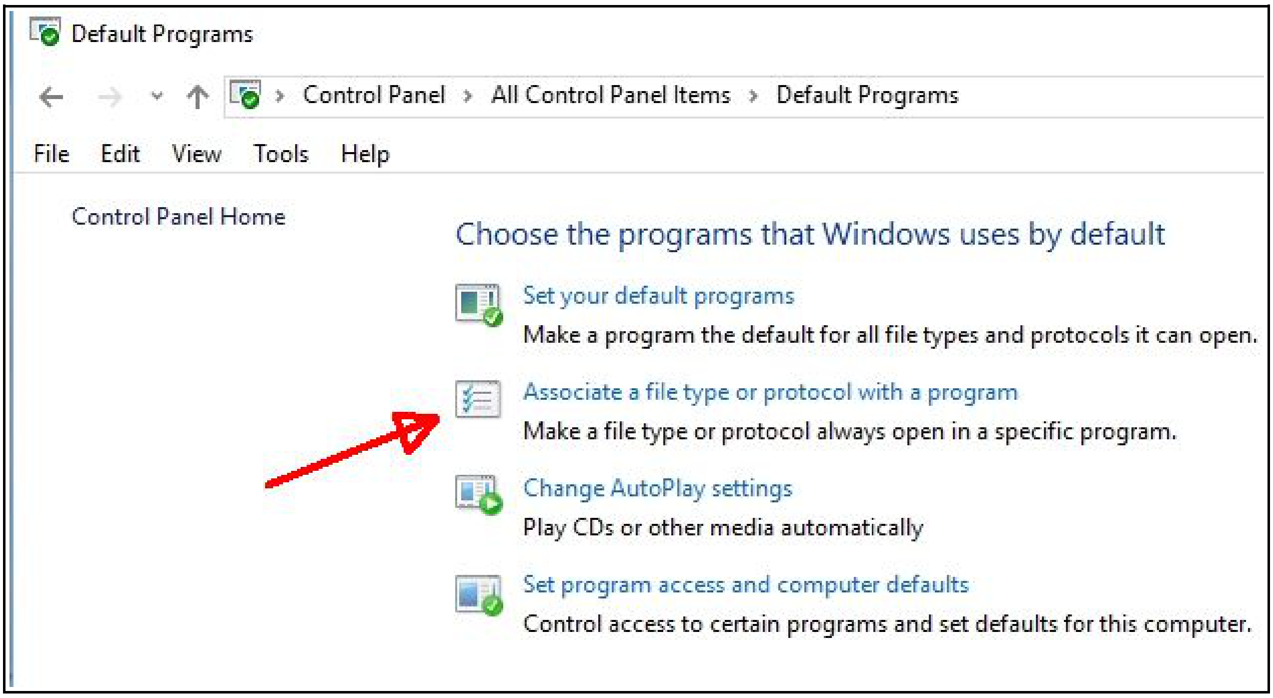
OK | Cancel | Apply

By default Windows does not display the extension of files. Thus a javascript attachment could appear as "innocent.txt" when its full name is "innocent.txt.js". Hence, even someone attempting to be vigilant about ".js" files would be mislead.

Two steps are necessary to resolve this issue

1. Change the windows setting which controls whether file extensions should be displayed.
   1. Open File Explorer, the program you use to view your folders and files. You can check in, say, your Pictures folders and see if the items show the extensions such as "sunset.jpg". If not then proceed as below.
   2. Windows 10 : Click the File option and from the menu select "Change folder and search options. It may also appear simply as "Options".
   3. Earlier versions of Windows : Select a similar option from the Tools menu
   4. You should now have a new window headed "Folder Options"
   5. Look for the option "Hide Extensions for known file types"
   6. If the box is ticked click the box so that it is empty.
   7. Press OK to save the settings and exit.
2. The second step is to suppress the running of "js" javascript files. In doing this you may

prevent some genuine email attachments from running but this is better than the risks of allowing malware to execute.


Default Programs
Control Panel › All Control Panel Items › Default Programs
File Edit View Tools Help
Control Panel Home

Choose the programs that Windows uses by default

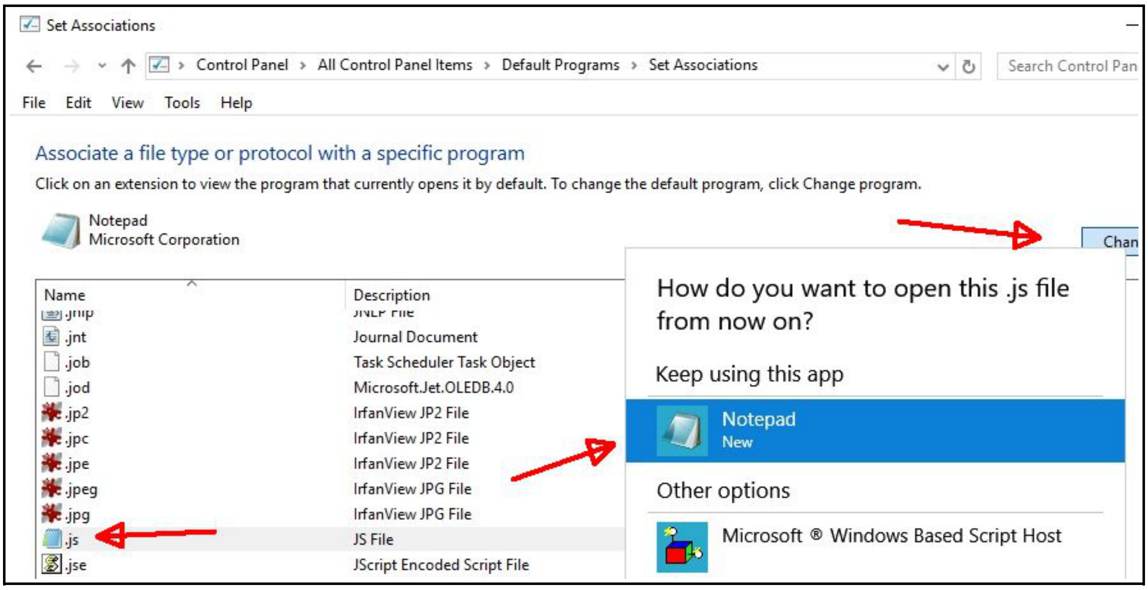
Set your default programs
Make a program the default for all file types and protocols it can open.

Associate a file type or protocol with a program
Make a file type or protocol always open in a specific program.

Change AutoPlay settings
Play CDs or other media automatically

Set program access and computer defaults
Control access to certain programs and set defaults for this computer.

1. From the Control Panel select Default Programs.
2. Select Associate a file type or protocol with a program
3. The display will take a few seconds while Windows sorts its table of associated file extensions. In the left column you will see the list of extensions probably starting with .001
4. Use the scroll box on the left until you find ".js" and click anywhere on the line to select.


Set Associations
Control Panel › All Control Panel Items › Default Programs › Set Associations
Search Control Pan
File Edit View Tools Help
Chan

Associate a file type or protocol with a specific program

Click on an extension to view the program that currently opens it by default. To change the default program, click Change program.

Notepad
Microsoft Corporation

Name	Description
.jnlp	JNLP File
.jnt	Journal Document
.job	Task Scheduler Task Object
.jod	Microsoft.Jet.OLEDB.4.0
.jp2	IrfanView JP2 File
.jpc	IrfanView JP2 File
.jpe	IrfanView JP2 File
.jpeg	IrfanView JPG File
.jpg	IrfanView JPG File
.js	JS File
.jse	JScript Encoded Script File

How do you want to open this .js file from now on?

Keep using this app

Notepad
New

Other options

Microsoft ® Windows Based Script Host

5. Make a note of the setting in the Current Default column. If you ever need to reverse this option you will need to set it back to this setting.
6. Click on the "Change Program" box on the right side of the display.
7. This should show a list of options. If necessary click on the "more apps" and select "Notepad".

8. The Current Default column should now show "Notepad". Click OK and close the window
9. The effect of this is that js javascript attachments will no longer run but Notepad will open showing you the text of the javascript.