

**CAUTION: Some files can automatically infect your system with a virus or damage your data.**

The filename extension is used by Windows to determine an appropriate program to use when opening the file. Example: MYRESUME.DOC has a filename extension of .DOC. That tells windows to use Word to open the file.

Part of the WINDOWS setup, is to specify possible filename extensions and designate what action or program will be associated with the file and used to run the file. Thus on our company systems we have specified for Windows that WORD should be used to open filename extensions .DOC. A company using WordPerfect would set up the Windows system so that it used WordpPerfect to open filename extensions .DOC

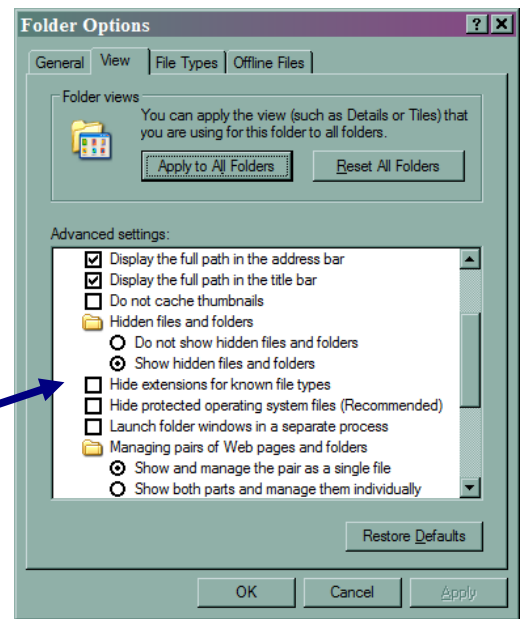
Windows can also run some filename extensions automatically without an associated program. That is the file can “execute” and run itself. Example: NOTEPAD.EXE is an executable file, that will run by itself inside of WINDOWS. They call these ‘executable’ file types.

When you double click or run a file, windows opens the associated application to open the file. If the file is a Windows executable file, it will start running and do whatever it was designed to do. Example: DELETEALLFILES.EXE will start deleting all files.

It is important that you NEVER click to run a file unless you are sure it is not infected or a malicious. It is important that you NEVER NEVER run an executable file unless you are sure what it is for, who sent it to you and that it is safe to do so.

Very the source and purpose of any file before opening it and at the very least, use your virus scanning software to check the file. Right Click on the file in MYCOMPUTER [without opening it] and select SCAN for viruses on the menu.

Turn on the functionality in Windows that show the full filename – including the filename extensions. MY COMPUTER > TOOLS > FOLDER OPTIONS > VIEW uncheck “HIDE Extensions”



There are many types of files which are ‘executable’ in Windows, all of which could be used to infect your system or cause damage. Such as: myfile.BAT, myfile.COM, myfile.EXE, myfile.REG, etc. Extreme caution should be exercised when you see these file extensions.

Here is a link to a longer list of executable file types [http://antiques-internet.com/exe\\_types.htm](http://antiques-internet.com/exe_types.htm)

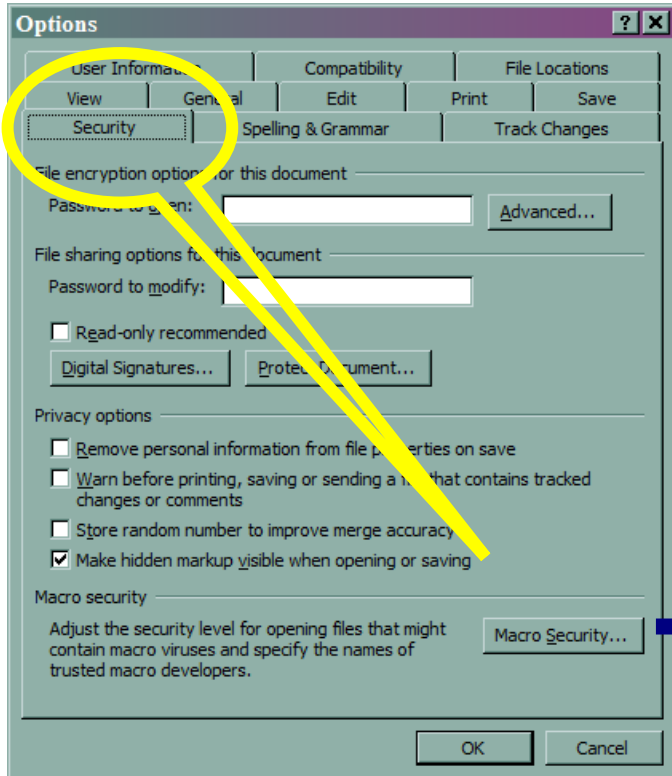
Bonus Tip: Some devious people will try to fool you by giving a file the appearance of having an innocuous filename extension or by using two or three extensions. It’s the last extension after the last period that counts.

Example: mysweetkitty%20.prettyflowers.pic.txt%20.exe This is an EXE executable file and since someone went to a lot of trouble to try and confuse you - probably does not contain cute pictures of kittens.

More resources discussing file types:

<http://antivirus.about.com/od/windowsbasics/l/blfileassoc.htm>

Notice that the list of files which people should be careful of are Word, Excel and PowerPoint files. That is because those programs can automatically run a malicious macro when the document first opens. To protect yourself, change the Security option in Word, Excel and PowerPoint to prevent Macros from running automatically.



Set the MACRO security level in WORD, EXCEL and POWERPOINT to prevent malicious MACROS from automatically running when you first open a document. A minimum should be MEDIUM.

TOOLS menu > OPTIONS

