What is a File Extension?

A file extension is a three or four-letter code that appears at the end of a filename and indicates the type of file it is. For example, .txt stands for text files, .jpg stands for image files and .docx stands for Microsoft Word documents. By knowing what kind of file, it is, your computer will be able to correctly open the file using the correct program.

Why are there different types of File Extensions?

Different file extensions have been designed by software makers to help computers identify which program should be used to open them. This is because certain programs only work with specific file formats, so knowing the filename's extension can help you quickly figure out if you need to install another program in order to open the file.

What happens when I try to open a file without an extension?

When a file does not have an extension, your computer will not know which application should be used to open it. In this case, you may get an error message such as “Windows cannot open this type of file” when you try to double-click on it. You can usually fix this problem by figuring out the correct extension for the file in question and then adding it manually.

Can I change the File Extension?

In most cases NO - changing the name of your files does not necessarily mean their extensions will also change too. For example, renaming a JPEG image (which has a .jpg extension) will not change its format from JPEG into something else just because you changed its name. But if you simply want to make sure that your files are all named in one specific way with no extra characters or symbols. Renaming them can still be useful in some cases. Just don't try to change the file extension.

Are there any dangers involved when changing File Extensions?

YES - Most files are safe if you change their names but changing the extensions can cause problems. Like executable (.exe) and batch (.bat) files which can cause damage if they are altered in any way. It is best not to take any chances, especially if you do not know exactly what kind of information these types of files contain or how they could affect your system if opened incorrectly.

What do I do if I download a file with an unrecognized extension?

If you ever come across a strange looking filename ending with some letters or numbers that do not familiarize you first use Google to find out more about them before attempting to open or run them on your computer (the same goes for ones that look like actual words but do not

match up with known extensions). If after doing some research things still do not look clear. Just delete it immediately and never attempt to run it on your system.

What is the difference between a file name and File Extension?

The main difference between a file name and its extension is that while the filename identifies what type of file it is, the file extension provides more information such as which program should be used to open it. For example - a .docx file typically represents a Microsoft Word document, but without knowing the extension your computer will not know what program should be used to open it.

How do I change my File Extensions in Windows?

It is not recommend to manually change File Extensions. They are set for a rason. Changing the File Extension will cause that file not to open.

Are there any benefits to having different kinds of File Extensions?

Yes - by having different types of files with unique extensions, your computer will have an easier time finding which program needs to be used in order to open them correctly. This is especially useful for people who use lots of different applications or work with lots of media files since different programs can handle these differently. It also makes it easier for programs like Microsoft Office or Adobe Photoshop to recognize specific formats when editing or creating documents.

Should I be worried about malicious File Extensions?

Yes - some file extensions are associated with malicious programs and can-do severe damage to your computer if they are opened. To stay safe, it is best to only open files whose filename and/or extension you recognize and that come from reliable sources. To further reduce the risks of getting infected, always keep your antivirus up to date as well.

What is a common example of a malicious File Extension?

The most common type of malicious file extension is .exe. This usually indicates an executable program which could contain a virus or other form of malware. Other malicious file extensions include .bat (batch files), .cmd (command files) and .vbs (Visual Basic script files). It is best not to open any of these types of files unless you know exactly what they are and where they came from.

Is there any way to see what program will open a file by its name or extension?

Yes - if you are trying to figure out what kind of application is associated with a specific file type, one option is to search for its filename or extension on Google. For example - searching for "XLSX" should provide plenty of results that explain what kind of file it is, and which program

should be used to open it. Another option is looking at the properties window for the file in question (right-click on the filename then select Properties). Here you should be able to find basic information such as size, date modified, version and type along with the default or preferred programs used for opening it.

What are some of the risks associated with sharing files over the Internet?

Sharing files over the internet can be risky for both you and the person receiving them. For you, this means potentially exposing yourself to viruses, malware, or ransomware if the file you are sharing is from a malicious or untrustworthy source. Additionally, when sending sensitive information online there is always a risk that your data could be intercepted by hackers or accessed by other unauthorized parties.

What precautions can I take to protect myself when downloading files?

When downloading files, it is important to be mindful of where they are coming from and what kind of files they are. Be sure that the website or source you are downloading from is trustworthy and not known for spreading malicious software. Additionally, scanning all downloaded files with an up-to-date antivirus program is necessary. This will ensure any threats are detected before they can do any damage. Finally, avoid opening any file types from unknown senders or sources as these could potentially contain malicious content.
