Silent_Dreem@Yahoo.Com

What is file extension?

In Windows and some other operating systems, file extension is one or several letters at the end of a filename. Usually three or four letters. Filename extensions usually follow a period (dot) and indicate the type of information stored in the file. For example, in the filename program.exe, the extension is EXE, which indicates that the file is an executable program file.
(Depending on the operating system, the punctuation separating the extension from the rest of the file may or may not be considered part of the extension itself.)
File extensions are also used in Microsoft Windows to associate the right applications to open or edit these files. For example, when you double-click at file with extension .txt, Windows starts associated program Notepad (by default).
File associations are configurable. Users can change which software applications instaled at computer will open file format of any type.

Display file extensions at your Windows operating system

By default, Windows is configured to hide filename extensions, the (usually three-leter) portion of the filename following the period. Aside from creating a knowledge gap between experienced and inexperienced users, this "feature" also can make it difficult to differentiate files with the same filename prefix. Overall, hiding filename extensions makes Windows more difficult to use.

- Open My Computer, and select Folder Options from the Tools menu (or choose Options from the View menu in Windows 95).
- Click on the View tab, turn off Hide file extensions for known file types, and press OK.

Enable file extension viewing

The invisible extension - what you can't see, can hurt you. By default, Windows does not have file extension viewing enabled. This allows virus writers to distribute executable files disguised as something non-executable. For example, an .EXE file might appear to be an innocuous text file.

Enabling file extension viewing in Windows 95/98/NT

In Windows 95/98/NT, enable file extension viewing by opening Windows Explorer. Click View | Options | View and uncheck the box for "Hide file extensions for known file types". You can also do this by via Windows Explorer View | Options | File Types menu. Locate the desired file type(s) and check the "Always Show..." checkbox).

Enabling file extension viewing in Windows 2000 and XP

In Windows 2000 or XP, open Windows Explorer and choose Tools | Folder Options | View or Tools | Folder Options | File Types, locate the file type(s) desired and choose Advanced. Then check the box "Always Show Extension".

Enabling file extension viewing for .SHS files

The above instructions will display all file extensions except for .SHS files. To display .SHS file extensions, one additional step is required. After following the above instructions, users must then edit the Registry, HKEY_CLASSES_ROOT\Shell Scrap, deleting the value "NeverShowExt".

Executable file extensions

Following is a partial list of file types that should be considered suspicious when received in email and should not be opened unless you requested or expected the attachment:

ADE - Microsoft Access Project Extension
ADP - Microsoft Access Project
BAS - Visual Basic Class Module
BAT - Batch File
CHM - Compiled HTML Help File
CMD - Windows NT Command Script
COM - MS-DOS Application
CPL - Control Panel Extension
CRT - Security Certificate
DLL - Dynamic Link Library
DO* - Word Documents and Templates
EXE - Application
HLP - Windows Help File
HTA - HTML Applications
INF - Setup Information File
INS - Internet Communication Settings
ISP - Internet Communication Settings
JS - Script File
JSE - Script Encoded Script File
LNK - Shortcut
MDB - Microsoft Access Application
MDE - Microsoft Access MDE Database
MSC - Microsoft Common Console Document
MSI - Windows Installer Package
MSP - Windows Installer Patch
MST - Visual Test Source File
OCX - ActiveX Objects
PCD - Photo CD Image

PIF - Shortcut to MS-DOS Program
POT - PowerPoint Templates
PPT - PowerPoint Files
REG - Registration Entries
SCR - Screen Saver
SCT - Windows Script Component
SHB - Document Shortcut File
SHS - Shell Scrap Object
SYS - System Comfit/Driver
URL - Internet Shortcut (Uniform Resource Locator)
VB - VBScript File
VBE - VBScript Encoded Script File
VBS - VBScript Script File
WSC - Windows Script Component
WSF - Windows Script File
WSH - Windows Scripting Host Settings File
XL* - Excel Files and Templates

Computer File Extensions

Computer file extensions (or file types, formats, or suffixes as they are sometimes referred to) are those odd characters that follow the name of the file (e.g. myfile.***doc*** where doc is the extension). Most file extensions that the average person runs into are either 3 or 4 letters but there are file types that have fewer characters and also use numbers.

It is possible that when you look at a file, you may not see the extension, but rest assured that they are there anyway. If you can't see the extension, your computer is set to hide them. You can elect to see them but unless you have a reason to do so, you are potentially a little safer.

Extension Purposes

You probably know by now that you cannot open any file with any program that you desire. File extensions are used by your computer to identify how the file is to be used and what programs can be used to open them. For example, when your computer sees a .doc extension, it knows that it is a file that must be opened by Microsoft Word.

Other extensions such as .exe are what are referred to as an executable or program and there are instructions in the program that will tell your computer what to do.

Occasionally, you may see a file extension that your PC doesn't know. In that case, if you were to double click on that file, your PC will open up a dialog box and ask you to choose a program to open it.

Warning *- if you are presented with this option and you don't know what you are doing, it is better to hit cancel and leave it alone than to open it. You could do damage to your computer.*

If you do know what the extension is, our BIG LIST will help you by giving a brief explanation of the file format.

How to Open Files with Unknown File Extensions?

A **filename extension** is a suffix to the name of a computer file applied to indicate the encoding convention (file format) of its contents. File extensions can be considered a type of metadata that are commonly used to infer information about the way data might be stored in the file. While file extensions like .txt, .doc, .xls, .bmp, .jpg, .png etc. are quite common on windows, many may not be aware of files with extensions such as .pps, .gan, .abt, .mpp and many others.

A file that has no extension or that has an extension that is not listed in the Registry on your computer will need to have some program associated with its type before it can be opened or otherwise used. While a computers are configured to use Notepad for unknown file types but otherwise double-clicking on such a file will bring up the unknown file dialog box, where you can choose to pick a program from a list, by choosing the radio button “Select the program from a list” and clicking “OK”.When you choose to select a program, the “Open With” dialog box appears. Windows will list what it thinks are the best possibilities but it is often the case that none of them are appropriate program to open the file.This is where **OpenWith.org** is extremely useful.

OpenWith.org is a database of free programs to open many such unknown file extensions!!! OpenWith.org desktop Tool is a useful tool that lets you search for free software you can download, to open files of unknown file types.

- Free download **OpenWith.org** desktop tool from **here** and run (double click) it to install
- Once installed, if you right-click on a file you’ll notice a new line on the menu, “OpenWith.org – How do I Open this?” Click that and the application opens and searches for a suitable free program to open it. Though you need to be connected to the internet to use this tool, it is quite fast and often returns a range of results.
- If **OpenWith.org** knows about that file extension, it will list all compatible programs. If you already have one of the programs installed, it will say Installed. If not, it will ask you to Download.
    - Select the program you want to use. If you are unsure, you can double-click on each program and find more information about it.
- If the program you want to use isn’t already installed, click on the Download link. The program will be downloaded.

- Once the program is downloaded, a new folder will open with the installer. At this point, you need to run the installer to install the downloaded program. After you install the program, you will find Download changed to Installed.

Dr. Design - From File Extensions to Masked email

Another month, another waiting room full of patients for Dr. Design. As usual, he takes email address ails, multiple window woes, and the diagnosis of numerous file extensions in his stride...

File Extensions - Which is which?

Hey Doctor Design. There are so many different file extensions for HTML. .html, .htm, .xhtml, .shtml, etc... How do you know which one to use and for what? -- Tom

Tom, most of the extensions that are used for HTML are fairly simple to understand once someone has explained them to you. Let me run you through some of the basics, so you can sound as smart as I do at your next HTML party!

.htm: An HTML file that conforms to the 8/3 naming standard common in DOS. In plain English this is the "old" way of naming your files. 8/3 is where you get such amazing application names as winipcfg.exe, mywebpag.htm, etc. No reason to use this unless you like 3 character file extensions.

.html: An HTML file that has an .html extension. There isn't any difference between these files and the .htm files, besides the extra letter.

.xhtml: This extension is reserved for XML-compliant HTML, commonly referred to as, you guessed it, XHTML. It really stands for "extensible HTML". This extension is most common among Web developers who really want to stay with the times, as XHTML is really the future of HTML. XHTML files can equally be called .htm, .html, .xht and .xhtm. Because XHTML is really just properly formatted HTML, you can't tell the difference simply by looking at it.

.shtml: SHTML is simply HTML with some server-side directives thrown in for fun. The most common of these is SSI, which allows you to do things like put your header in one file, your menu in another file, and then dynamically include these into .shtml files on the fly. PHP, ASP, JSP etc. all allow you to do the same thing, however, they require you to actually use those languages. SHTML allows you to use the power of includes without learning one of those complex languages.

While there are many others around, including, but not limited to: .php, .php3, .asp, .aspx, .xml, .cfm, .cfml, .jsp, .cgi, and .pl, this list should get you by for now. Besides, most of the extensions in the latter group are specific to a particular programming language (.asp for ASP files, .php for PHP files, etc).

Strip My Pages!

Doctor, I thought I had just read how to do this recently in one of your articles, but for the life of me I'm not able to find it! I assume that I could just put a link to another HTML page that displayed a stripped down version of that page in a table. By looking at the code from the "Print Article" versions of pages on SitePoint, it looks like a template is used with a table width of 468, although I am wondering if it is necessary to use the server side scripting language (php) to achieve this? -- Xanthé

While I could take half an hour to tell you how to go about this quickly and easily without using any server side code at all, I'll let an expert on the subject do it instead. Eric Meyer, a Standards Consultant at Netscape, recently wrote an article on this very subject for A List Apart. It covers everything you're looking for -- and more!

How do I mask an email Address?

Dr. Design: is there a way to mask the email address that appears in the 'to' field after clicking on the mailto link? For instance, instead of abc@xxx.com appearing, I want a name to appear thus: "ABC" -- Jamie

Hmm. Sneaky is we? Well Jamie, you'll be glad to know there is in fact a way of doing just such a thing! As I am sure you're aware, a normal mailto: link looks a lot like this:

```
<a her=mailto:me@me.com>mail me</a>
```

The following code will allow you to hide the email address and present a name instead:

```
<a her="mailto:Jeremy Wright<jwright@tacf.org>">Mail!</a>
```

Targeting the Main Window? Close the Popup

Hey Doc, is it possible to automatically close a pop-up window when the user clicks on a link that targets the main window? For example, I have a framed site. The main opens a pop-up window. The pop-up window has a link to a game that has to load in the main frame window. I got that part working, but the pop-up window remains on top. I know I could change the focus to the main window, but I'd like the pop-up window to automatically close itself if the user clicks on the game link. How's it done? - Anna

Anna, I assume your current link code looks something like this:

```
<a href="javascript: myFunc ;"> Go to the game! <a>
```

Simply change it to this, and you'll save your visitors valuable clicks before you know it!

```
<a href="javascript: myFunc; window.close () ;"> Go to the game! <a>
```

Dr. Design - From File Extensions to Masked email

Make my Button Create a Popup

Hi. When visitors subscribe to my mailing list, instead of the "Subscription Successful" window appearing, how can I get the submit button to create a small pop-up window that says "Subscription Successful"? Is this possible? Right now, my input code is:

```
<input type="submit" name="Submit" value="go">
```

-- Josh

Josh, this is a great question! By allowing your visitors to subscribe to your newsletter without ever leaving the page they're on, you enable them to continue browsing your site without the need to waste any clicks at all. Well done! While you might think you'll need some JavaScript on the Submit button of your form for this kind of thing, you'd probably be surprised to know that it has nothing to do with the button! All you need is some simple HTML!

I expect your current `<form>` code looks a lot like this:

```
<form method="POST" action="MyForm.asp">
```

Simply change it to look like this, and you're done!

```
<form method="POST" action="MyForm.asp" target="_blank">
```

One other thing you may want to do is allow your users to close that little window with the click of a button. Just in case you're unsure, here's the code:

```
<a href="javascript: window.close () ;"> close this window</a>
```

That's all for this month! To make your appointment for next time, email Dr. Design at drdesign@sitepoint.com today.

Spread the love!
Dr. Design

Web site review: Find those elusive file extensions with Whatis.com

Takeaway: Having trouble tracking down the meaning of a puzzling file extension? Check out Whatis.com and its list of over 4,000 file formats. Then, let us know what you think with Tec Republic's Rate this Site! Survey.

Have you ever had a client ask what file format is represented by an EPS extension? What about J62, EXE, JPG, LTM, or HDF? Sure, you're probably able to name several of these off the top of your head, and you can make an intelligent guess about some of the others. But some are less obvious, especially if they have more than one possible meaning. Now there's an online resource to solve this dilemma. Whatis.com comes to the rescue not only with an exhaustive list of file extensions, but also much more.

Tec Republic originally reviewed Whatis.com in May 1999 (click here to read that article), but many new features make this site worth a second look. Whatis.com serves primarily as an online IT information bank, focusing on the Internet and computers. Visitors can search the site either by keyword or scrolling through the exhaustive list of IT terms and acronyms.

Navigating the site
the home page is conveniently organized into three frames—a navigation bar, an alphabetic list, and a results window. The navigation bar on the left provides trouble-free movement throughout the site while also having a Quick Search feature. The alphabetical list displays all available entries beginning with a specific letter or number. Red-letter links located at the top of this frame are also provided for easier exploration. Once you locate the desired term or acronym and click on it, the results window springs to life with your requested information.

Finding those file extensions

While all this may seem great, you may be wondering, "What about the file extensions?" Here's how you find them. From the Whatis.com home page, click on the every file format in the world link. This will open an alphabetic listing of 4,431 file formats, last updated on 6/15/00 (according to Whatis.com). This list is divided into five main sections: A through E, F through J, K through O, P through T, and U through Z with Numbers. You can also utilize the red-letter links at the top of the page for faster navigation. Extensions are listed with a brief but detailed description. If an extension has more than one possible meaning, each is referenced separately.

Final thoughts

Whatis.com may not be the ultimate online encyclopedia, but it's a great reference tool. Whether you need the meaning of AGP or MCSE, or if you're looking for that unfamiliar file format, this Web site can help. The next time someone asks you what an HDF file is, you can respond, "It's a Help file (Help development kit), a hierarchical data file, or a National Center for Supercomputing Applications Geospatial Hierarchical Data format file." Just remember, this utility works only if your client hasn't renamed the file extension. If they've just decided to use their initials as the extension, all bets are off.

The Importance of File Extensions

Commentary by Thomas R. Pasawicz (aka DiamondBack)

August 16, 2001

Often in the writings on my website I comment that a virus can't be spread from "opening an e-mail." While technically this should be true, "innovations" in e-mail client software have blurred the distinction between what's an e-mail (a simple text file) and documents containing executable program code. The key to understanding the difference, and recognizing a potentially harmful file, is to be able to distinguish between "programs" and "data."

Programs are a list of instructions that direct a computer to perform specified tasks. Games, browsers, e-mail clients, etc. are all programs that allow you to perform useful tasks with your computer. Data is information that is used by programs, for example the words on this webpage are data, and the browser you are using to display them is a program. The information contained in a JPG photo file is data; the viewer you use to display the photo is a program. Generally speaking, data is harmless since it can't "do anything" by itself. In contrast, programs can be very harmful if they contain instructions that direct your computer to do something you normally wouldn't want it to do, such as delete all the files on your hard drive. Since sharing files is a common practice among Internet users, being able to tell the difference between a harmless data file and a potentially harmful program file is critical to maintaining the "health" of your computer and its operating system.

Since "Windows" is the most common operating system in use today, this article will use examples based on that system? While these examples are applicable to most operating systems (MacOS, Linux, etc.), the specifics are intended for Windows users.

Windows uses a "file extension" to determine what to do with a particular file type. Usually the file extension consists of two, three or four characters following a period. For example, in the file "mystory.txt", the "mystery" is the name of the file and the ".txt" is the file extension which tells Windows that the file (should) contains data in the form of ASCII text. The file type indicated by the extension can then be "associated" with a program that knows how to handle the data contained within it. In this case, a text file (.txt) may be associated with a text editing/display program such as NotePad, Write or MS Word. If "mystory.txt" is clicked on, the program associated with ".txt" files will be launched and the data in the file displayed. Another example might be "myphoto.jpg". In this case, ".jpg" is a common extension for a JPEG (Joint Photographers Expert Group) type file which contains data that represents a photograph or similar image. Clicking on "myphoto.jpg" should launch an associated program for viewing this type of data, on my system that would be CompuPic, on others it may be Internet Explorer or MS Paint. Any program capable of reading the data in a particular file may be associated with that file type via the file's extension.

As previously mentioned, some files are not strictly data but contain instructions which the computer is expected to execute. In the above example, if "mystory.txt" is associated with Notepad, then the file "notepad.exe" will be launched to display the contents of "mystory.txt". Windows knows that ".exe" denotes an executable program file and will follow the instructions contained in such files. While ".exe" is the most common executable file extension, it is far from the only one. Some of the most common executable file types are:

.exe - Executable files, typically an application program.
.com - MS-DOS "command" file
.bat - Batch file
.js - Javascript file
.vb or **.vbs** - Visual BASIC file
.scr - Screen Saver

Some files don't directly execute, but can make changes to your system registry which controls how your computer behaves. Two common ones are:

.inf - Setup Information
.reg - Registration entires

You should also watch out for files that may link (aka "shortcut") to an executable file, such as **.lnk** or **.pif**. While the shortcut/link isn't executable, it may point to a file which is.

Extension	Type of File
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript file
.jse	Jscript Encoded Script file
.lnk	Shortcut
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD image, MS Visual compiled script

.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript Encoded script file
.vbs	VBScript file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

I want to make clear that these are only the most common executables, there are many other file types which could trigger a dangerous series of events. Microsoft lists the file types in the table on the right as "Level 1" (i.e. "unsafe").

Woah! Who can remember all those? (Not me, that's for sure.) And even this isn't a complete list (by far), new file types can be introduced with each new program you install on your system. A better approach to take regarding file extensions is *if you don't recognize what kind of file it is, then don't mess around with it.* If instead you decide "let's just click on it and see what happens" you are asking for trouble... big trouble!

Likewise, it would be nearly impossible to list all the "safe" file types, though under normal circumstances the following very common file types are of the "data" variety and shouldn't pose a threat:

.txt - ASCII text file
.jpg or **.jpeg** - photo format
.gif or **.png** or **.bmp** - image formats
.mpg or **.avi** or **.qt** - movie formats
.wav or **.mp3** - sound formats

Another common format used for exchanging text documents is ".doc", usually associated with MS Word. A document should be just that, a file containing information, i.e. data. But Microsoft decided that it would be a great idea if documents could also contain small program scripts called "macros." This was done to make the documents more "powerful" and they succeeded... powerful "macro viruses" may be embedded in MS Word documents which can infect other MS Word documents and destroy the (often important) data contained in them. And since these "macro viruses" can automatically attach themselves to other MS Word docs, they can easily be spread to other MS Word users when exchanging .doc files. Thank you, Microsoft, for taking a harmless formatted text document and giving it the ability to wipeout entire directories of important MS Word files while spreading to other systems... the malicious programmers who create these "macro viruses" couldn't have done it without you. My advice is don't use MS Word... you can still view .doc files using MS Write or using the MS Word Viewer, neither of which will execute any macros (AFAIK). Or you could disable the macro function in MS Word (and Excel while you're at it). Personally, I don't see any legitimate use for them 99.9% of the time anyway.

One of the most infamous macro viruses was W97.Melissa.A... better known simply as the Melissa Virus. This nasty little bugger would hide in MS Word docs and upon the document's opening would mail up to 50 copies of itself using Microsoft Outlook. The subject of the e-mail would be "Important Message From USERNAME", where USERNAME is taken from the MS Word setting. This clever little script even kept track of who it had e-mailed itself to from each infected system, so as not to send multiple e-mails to the same people and arouse suspicion. It would also infect other MS Word docs using the "normal" method of infection, so it could be spread even if Outlook couldn't be found. Its "payload"... i.e. the code meant to "detonate" (execute) after it had time to spread, would append the following text to infected Word docs: *"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Games over. I'm outta here."* Fairly harmless compared to what it *could have* done.

MS Word docs aren't the only "formatted text" files you need to be concerned about... even good old HTML (Hyper Text Markup Language), the language intended for displaying webpages, has been given "new powers" that allow VBS (Visual Basic Scripts) to be embedded into the HTML and immediately run when a webpage is loaded. As a website developer I'm not opposed to using scripts in HTML documents, I use JavaScript all the time. But in Microsoft's haste to offer an "alternative" to Java (meaning: kill it), they were sloppy with its implementation. "Malicious" JavaScript’s do exist, but they are relatively rare... that is, rare compared to malicious VBScripts (IMHO). I believe part of the reason for this stems from Microsoft's attempt to integrate their Web Browser into the Windows operating system. For example, MS Outlook (the e-mail client that ships with Windows) uses much of the same code developed for their Web Browser, allowing e-mails to be viewed as HTML pages... including any embedded VBScripts. Prior to this, e-mail was a text only format (and perfectly harmless, I might add). Then some formatting was added... bold text, colors, background images and links for example. Still harmless, though unnecessary for most e-mail messages. The worst that could happen from "opening an e-mail" would be a screen full of gaudy formatted text, but at least it couldn't hurt anything beyond your eyesight. With the introduction of HTML and VBScripts, the equation changed. Now opening an e-mail could trigger a program, and such programs could exploit flaws in the VBS parser (i.e. the program that interprets the script commands, allowing a malicious script to do things beyond what was intended for such scripts to do... and that is not good).

One example of a VBS e-mail virus (technically a "worm") is the VBS.KAKWORM. Kakworm exploited some vulnerabilities in MS Internet Explorer and MS Outlook Express (where have I heard that before?). Kakworm hid its VBScript in the e-mail message's HTML signature and dropped KAK.HTA file into the Windows start-up folder. After that, each time an MS Outlook user sent an e-mail, Kakworm would attach itself to the HTML signature, quickly spreading among the "Typhoid Marys" of the Internet... MS Outlook users. I received it a number of times, fortunately I use Eudora, which merely displayed the VBS code rather than executing it (I don't want my e-mail client executing ANYTHING without my express permission).

Another infamous example is the "Love Letter Worm"... a VBScript that could spread itself not only though e-mail (or more accurately, through MS Outlook), but also Internet Relay Chat (using mIRC), USENET News or shared files. Being so versitile, this worm spread far and wide, shutting down e-mail servers and clogging corporate networks. When spread via e-mail, it would send copies of itself through Outlook with the subject "ILOVEYOU" and the body message "kindly check the attached LOVELETTER coming from me." The "loveletter" was a VBScript by the name of "LOVE-LETTER-FOR-YOU.TXT.VBS"... anyone careless enough to open the attached love letter would run the script, infecting their computer and possibly helping it spread. It would seek out and replace exiting vbs and vbe files with a copy of itself. Files with js, jse, css, wsh, sct, or hta extensions would have their code replaced and the extension changed to .vbs (eg. "website.css" would be replaced with a copy of the worm code in a file called "website.vbs"). Any jpg, jpeg, mp2 or mp3 files would be replaced by the worm and have ".vbs" appended to their file name. If nothing else, many important existing files could be trashed... replaced by this missile of love.

It's impossible to determine how much damage (not to mention embarrassment) Melissa, Kakworm and Love Letter have caused. They have probably inflected thousands, if not millions, of computers and may return again in various forms as new flaws in MS products are uncovered. In fairness, I can't place all the blame on Microsoft, other products such as Netscape and Eudora are starting to follow in Microsoft's footsteps, making increased use of scripting and other "enhancements" to attract users accustomed to Microsoft's bloat ware. I strongly suggest that you turn off or disable these "features" whenever you can, they just aren't worth the risks they carry. E-mail and Newsgroups are wonderful tools for exchanging information... simple text and maybe an occasional graphic, but there is no need to expose your computer, network or the entire Internet to executable code that can wreak havoc.

Getting back to file extensions, it doesn't do you any good to know what to look for if you can't see it. In arguably one of Microsoft's most boneheaded decisions, they ship Windows configured to "hide" certain files and "known" file extensions. The idea was to make viewing file directories less cluttered and confusing... it was stupid idea. A "known" file is any file that has been associated with an application, which would be most of the common files on your system such as .txt or .jpg. It also hides .exe and .com extensions, making a .txt file indistinguishable from an executable file, aside from the icon displayed (these can be faked). It can also be very misleading, a file with the name "myphoto.jpg.exe" (an executable program) would appear as "myphoto.jpg" with the real extension (.exe) hidden. What in the world were they thinking when they gave the approval for this "feature?" Aside from not showing much respect for their user's intelligence (and desire to be able to see what kind of files they have on their system), they gave malicious program writers a huge edge when trying to sneak their evil wares onto an unsuspecting user's computer.

But enough Microsoft bashing (for now), here's how to disable the file and extension hiding: Run MS Desktop Explorer or the Control Panel from the Start/Settings button. Click on the "View" dropdown menu and select "Folder Options...". In the window that opens, click on the "View" tab and you should see a box with a "tree view" of options that can be checked or unchecked. Both of the settings you want are in the "Files and Folders" branch. Under "Hidden files" click on "Show all files" then make sure to **uncheck** the box next to "Hide file extensions for known file types". To complete the process, click the Apply button. There, you just improved the security of your system by about 150%, provided you familiarize yourself with the file extensions we've been taking about (now that you can actually see them).

Which brings us to W32.Sircam.Worm@mm... or Sir Cam for short. In the past few weeks I've received 202 e-mails sent from Sir Cam infected computers, more than any other virus/worm/trojan to date. Sir Cam is very clever and rather means, a combination that is going to hurt a lot of people. Sir Cam arrives as a very personally looking e-mail with a file attachment. There are several different body messages and it is even bilingual... either English or Spanish depending on the language it detects on the host system. In English, the message will begin with "Hi! How are you?" followed by one of the following:

I send you this file in order to have your advice
I hope you can help me with this file that I send
I hope you like the file that I send you
This is the file with the information that you ask for

The last line is "See you later. Thanks". Without further thought, many people then open the attached file, and Sir Cam goes to work on their system. First it creates copies of itself in two locations, then it makes a copy of the file it was masquerading as to be opened normally. IOWs, if Sir Cam arrived as a MS Word file, then MS Word would open a display a file. Sir Cam can also pretend to be an Excel (.xls) or Zip file... either of which will appear to open normally. At this point the victim might wonder why this file was sent to them, perhaps replying with the requested "advice" or just closing and ignoring it. Sir Cam however is now getting the victim's name and e-mail address from the system registry, and making a list of the files in the "My Documents" directory. One of these files will be selected and Sir Cam will attach itself to a copy of the file. Next Sir Cam searches for any .web (Windows Address Book) files, such as those used by Outlook to store e-mail addresses (it will also check a few other locations likely to have e-mail addresses, it's a very hardworking worm). Armed with all the e-mail addresses it could find and a newly infected file to send, Sir Cam uses its own SMTP engine (i.e. built-in e-mail sending program) to send out messages with attachments to a new group of potential victims, with the subject of the message being the name of the file it found.

What makes Sir Cam clever is the way it searches the My Documents directory for a file to infect and send. Since most Microsoft programs use this as the default directory to save user created files, the odds are very good it will find a file (Word doc, Excel spreadsheet or Zipped file) created by the user of the system. Where other e-mail worms have used the same subject title, Sir Cam uses the name of the file it found, hence warnings not to "open an e-mail called..." are useless. Same for warnings not to open an attachment with a certain name, Sir Cam could pick any file name it finds on the host system. The only change it makes (other than attaching itself) to the file being sent is to the extension... it will append it with one of the following: .bat, .com, .lnk or .pif. Since by default Windows "hides" these "known" file extensions, the file name displayed look may look like a .doc, .xls or .zip. So between the innocent looking extension and the "personal" name of the file, it may really look like a file someone sent for an opinion... and since it displays normally the victim might not have any reason to suspect it wasn't intentionally sent.

Of course the "sender" may never have wanted (or expected) the file to be sent to everyone in their address book, and it could be very embarrassing if the file contained "private" information (look in your "My Documents" directory and see if there is anything in there you wouldn't want to have shared with everyone in your address book *smile*). If that was all Sir Cam did then I'd say it was a very clever and potentially embarrassing little fellow, but Sir Cam isn't finished trying to ruin your day. It is "network aware," meaning if you are connected to a LAN (local area network, common in may workplaces) it will begin to spread itself to every other computer on the local net. If that happens on an office network, it's quite likely your employer will frown on this, but you may find other folks in the unemployment line to commiserate with.

Sir Cam packs a nasty payload which may be detonated in a number of ways. It has a 1 in 20 chance of deleting all files and directories on the C drive. This only occurs on systems where the date is October 16 and which are using D/M/Y as the date format. It always occurs if the attached file contains "FS2" not followed by "sc" (don't ask me why, it just does). There is a 1 in 50 chance it will fill all remaining space on the C drive by adding text to the file c:\recycled\sircam.sys. Sir Cam also changes settings in the Windows Registry file so it will be executed every time any exe file is run... its payload will detonate after 8,000 executions. Regardless of what triggers the payload, there is a very good chance that Sir Cam will have had plenty of time to spread before doing anything that may tip-off a victim. Sir Cam is yet another example of why you want to be able to see (and pay attention to) file extensions... seeing a file attachment called "my_favorite_jokes.doc.*com*" may just tip you off that something isn't quite right ("Why is my friend sending a Word file with a .com extension? Maybe I'd better ask before I run it.").

Sometimes having the file extensions unhidden isn't enough... Windows 9x and up allows for "long file names"... sometimes so long that the entire file name can't be displayed in Explorer or other application programs. For example, here's a screen capture of a file being received through the popular ICQ program:

The Importance of File Extensions

Commentary by Thomas R. Pasawicz (aka DiamondBack)

August 16, 2001

Often in the writings on my website I comment that a virus can't be spread from "opening an e-mail." While technically this should be true, "innovations" in e-mail client software have blurred the distinction between what's an e-mail (a simple text file) and documents containing executable program code. The key to understanding the difference, and recognizing a potentially harmful file, is to be able to distinguish between "programs" and "data."

Programs are a list of instructions that direct a computer to perform specified tasks. Games, browsers, e-mail clients, etc. are all programs that allow you to perform useful tasks with your computer. Data is information that is used by programs, for example the words on this webpage is data, the browser you are using to display them is a program. The information contained in a JPG photo file is data, the viewer you use to display the photo is a program. Generally speaking, data is harmless since it can't "do anything" by itself. In contrast, programs can be very harmful if they contain instructions that direct your computer to do something you normally wouldn't want it to do, such as delete all the files on your hard drive. Since sharing files is a common practice among Internet users, being able to tell the difference between a harmless data file and a potentially harmful program file is critical to maintaining the "health" of your computer and its operating system.

Since "Windows" is the most common operating system in use today, this article will use examples based on that system. While these examples are applicable to most operating systems (MacOS, Linux, etc.), the specifics are intended for Windows users.

Windows uses a "file extension" to determine what to do with a particular file type. Usually the file extension consists of two, three or four characters following a period. For example, in the file "mystory.txt", the "mystery" is the name of the file and the ".txt" is the file extension which tells Windows that the file (should) contains data in the form of ASCII text. The file type indicated by the extension can then be "associated" with a program that knows how to handle the data contained within it. In this case, a text file (.txt) may be associated with a text editing/display program such as Notepad, Write or

MS Word. If "mystory.txt" is clicked on, the program associated with ".txt" files will be launched and the data in the file displayed. Another example might be "myphoto.jpg". In this case, ".jpg" is a common extension for a JPEG (Joint Photographers Expert Group) type file which contains data that represents a photograph or similar image. Clicking on "myphoto.jpg" should launch an associated program for viewing this type of data, on my system that would be CompuPic, on others it may be Internet Explorer or MS Paint. Any program capable of reading the data in a particular file may be associated with that file type via the file's extension.

As previously mentioned, some files are not strictly data but contain instructions which the computer is expected to execute. In the above example, if "mystory.txt" is associated with Notepad, then the file "notepad.exe" will be launched to display the contents of "mystory.txt". Windows knows that ".exe" denotes an executable program file and will follow the instructions contained in such files. While ".exe" is the most common executable file extension, it is far from the only one. Some of the most common executable file types are:

.exe - Executable files, typically an application program.
.com - MS-DOS "command" file
.bat - Batch file
.js - Javascript file
.vb or **.vbs** - Visual BASIC file
.scr - Screen Saver

Some files don't directly execute, but can make changes to your system registry which controls how your computer behaves. Two common ones are:

.inf - Setup Information
.reg - Registration entires

You should also watch out for files that may link (aka "shortcut") to an executable file, such as **.lnk** or **.pif**. While the shortcut/link isn't executable, it may point to a file which is.

Extension	Type of File
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program

.cpl	Control Panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript file
.jse	Jscript Encoded Script file
.lnk	Shortcut
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD image, MS Visual compiled script
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript Encoded script file
.vbs	VBScript file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

I want to make clear that these are only the most common executables, there are many other file types which could trigger a dangerous series of events. Microsoft lists the file types in the table on the right as "Level 1" (ie. "unsafe").

Woah! Who can remember all those? (Not me, that's for sure.) And even this isn't a complete list (by far), new file types can be introduced with each new program you install on your system. A better approach to take regarding file extensions is *if you don't recognize what kind of file it is, then don't mess around with it.* If instead you decide "let's just click on it and see what happens" you are asking for trouble... big trouble!

Likewise, it would be nearly impossible to list all the "safe" file types, though under normal circumstances the following very common file types are of the "data" variety and shouldn't pose a threat:

.txt - ASCII text file
.jpg or **.jpeg** - photo format
.gif or **.png** or **.bmp** - image formats
.mpg or **.avi** or **.qt** - movie formats
.wav or **.mp3** - sound formats

Another common format used for exchanging text documents is ".doc", usually associated with MS Word. A document should be just that, a file containing information, ie. data. But Microsoft decided that it would be a great idea if documents could also contain small program scripts called "macros." This was done to make the documents more "powerful" and they succeeded... powerful "macro viruses" may be embedded in MS Word documents which can infect other MS Word documents and destroy the (often important) data contained in them. And since these "macro viruses" can automatically attach themselves to other MS Word docs, they can easily be spread to other MS Word users when exchanging .doc files. Thank you, Microsoft, for taking a harmless formatted text document and giving it the ability to wipeout entire directories of important MS Word files while spreading to other systems... the malicious programmers who create these "macro viruses" couldn't have done it without you. My advice is don't use MS Word... you can still view .doc files using MS Write or using the MS Word Viewer, neither of which will execute any macros (AFAIK). Or you could disable the macro function in MS Word (and Excel while you're at it). Personally, I don't see any legitimate use for them 99.9% of the time anyway.

One of the most infamous macro viruses was W97.Melissa.A... better known simply as the Melissa Virus. This nasty little bugger would hide in MS Word docs and upon the document's opening would mail up to 50 copies of itself using Microsoft Outlook. The subject of the e-mail would be "Important Message From USERNAME", where USERNAME is taken from the MS Word setting. This clever little script even kept track of who it had e-mailed itself to from each infected system, so as not to send multiple e-mails to the same people and arouse suspicion. It would also infect other MS Word docs using the "normal" method of infection, so it could be spread even if Outlook couldn't be found. Its "payload"... ie. the code meant to "detonate" (execute) after it had time to spread, would append the following text to infected Word docs: *"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."* Fairly harmless compared to what it *could have* done.

MS Word docs aren't the only "formatted text" files you need to be concerned about... even good old HTML (Hyper Text Markup Language), the language intended for displaying WebPages, has been given "new powers" that allow VBS (Visual Basic Scripts) to be embedded into the HTML and immediately run when a webpage is loaded. As a website developer I'm not opposed to using scripts in HTML documents, I use JavaScript all the time. But in Microsoft's haste to offer an "alternative" to Java (meaning: kill it), they were sloppy with its implementation. "Malicious" JavaScript's do exist, but they are relatively rare... that is, rare compared to malicious VBScripts (IMHO). I believe part of the reason for this stems from Microsoft's attempt to integrate their Web Browser into the Windows operating system. For example, MS Outlook (the e-mail client that ships with Windows) uses much of the same code developed for their Web Browser, allowing e-mails to be viewed as HTML pages... including any embedded VBScripts. Prior to this, e-mail was a text only format (and perfectly harmless, I might add). Then some formatting was added... bold text, colors, background images and links for example. Still harmless, though unnecessary for most e-mail messages. The worst that could happen from "opening an e-mail" would be a screen full of gaudy formatted text, but at least it couldn't hurt anything beyond your eyesight. With the introduction of HTML and VBScripts, the equation changed. Now opening an e-mail could trigger a program, and such programs could exploit flaws in the VBS parser (ie. the program that interprets the script commands, allowing a malicious script to do things beyond what was intended for such scripts to do... and that is not good).

One example of a VBS e-mail virus (technically a "worm") is the VBS.KAKWORM. Kakworm exploited some vulnerabilities in MS Internet Explorer and MS Outlook Express (where have I heard that before?). Kakworm hid its VBScript in the e-mail message's HTML signature and dropped KAK.HTA file into the Windows start-up folder. After that, each time an MS Outlook user sent an e-mail, Kakworm would attach itself to the HTML signature, quickly spreading among the "Typhoid Marys" of the Internet... MS Outlook users. I received it a number of times, fortunately I use Eudora, which merely displayed the VBS code rather than executing it (I don't want my e-mail client executing ANYTHING without my express permission).

Another infamous example is the "Love Letter Worm"... a VBScript that could spread itself not only though e-mail (or more accurately, through MS Outlook), but also Internet Relay Chat (using mIRC), USENET News or shared files. Being so versitile, this worm spread far and wide, shutting down e-mail servers and clogging corporate networks. When spread via e-mail, it would send copies of itself through Outlook with the subject "ILOVEYOU" and the body message "kindly check the attached LOVELETTER coming from me." The "loveletter" was a VBScript by the name of "LOVE-LETTER-FOR-YOU.TXT.VBS"... anyone careless enough to open the attached love letter would run the script, infecting their computer and possibly helping it spread. It would seek out and replace exiting vbs and vbe files with a copy of itself. Files with js, jse, css, wsh, sct, or hta extensions would have their code replaced and the extension changed to .vbs (eg. "website.css" would be replaced with a copy of the worm code in a file called "website.vbs"). Any jpg, jpeg, mp2 or mp3 files would be replaced by the worm and have ".vbs" appended to their file name. If nothing else, many important existing files could be trashed... replaced by this missile of love.

It's impossible to determine how much damage (not to mention embarrassment) Melissa, Kakworm and Love Letter have caused. They have probably inflected thousands, if not millions, of computers and may return again in various forms as new flaws in MS products are uncovered. In fairness, I can't place all the blame on Microsoft, other products such as Netscape and Eudora are starting to follow in Microsoft's footsteps, making increased use of scripting and other "enhancements" to attract users accustomed to Microsoft's bloat ware. I strongly suggest that you turn off or disable these "features" whenever you can, they just aren't worth the risks they carry. E-mail and Newsgroups are wonderful tools for exchanging information... simple text and maybe an occasional graphic, but there is no need to expose your computer, network or the entire Internet to executable code that can wreak havoc.

Getting back to file extensions, it doesn't do you any good to know what to look for if you can't see it. In arguably one of Microsoft's most boneheaded decisions, they ship Windows configured to "hide" certain files and "known" file extensions. The idea was to make viewing file directories less cluttered and confusing... it was stupid idea. A "known" file is any file that has been associated with an application, which would be most of the common files on your system such as .txt or .jpg. It also hides .exe and .com extensions, making a .txt file indistinguishable from an executable file, aside from the icon displayed (these can be faked). It can also be very misleading, a file with the name "myphoto.jpg.exe" (an executable program) would appear as "myphoto.jpg" with the real extension (.exe) hidden. What in the world were they thinking when they gave the approval for this "feature?" Aside from not showing much respect for their user's intelligence (and desire to be able to see what kind of files they have on their system), they gave malicious program writers a huge edge when trying to sneak their evil wares onto an unsuspecting user's computer.

But enough Microsoft bashing (for now), here's how to disable the file and extension hiding: Run MS Desktop Explorer or the Control Panel from the Start/Settings button. Click on the "View" dropdown menu and select "Folder Options...". In the window that opens, click on the "View" tab and you should see a box with a "tree view" of options that can be checked or unchecked. Both of the settings you want are in the "Files and Folders" branch. Under "Hidden files" click on "Show all files" then make sure to **uncheck** the box next to "Hide file extensions for known file types". To complete the process, click the Apply button. There, you just improved the security of your system by about 150%, provided you familiarize yourself with the file extensions we've been taking about (now that you can actually see them).

Which brings us to W32.Sircam.Worm@mm... or Sir Cam for short. In the past few weeks I've received 202 e-mails sent from Sir Cam infected computers, more than any other virus/worm/trojan to date. Sir Cam is very clever and rather means, a combination that is going to hurt a lot of people. Sir Cam arrives as a very personally looking e-mail with a file attachment. There are several different body messages and it is even bilingual... either English or Spanish depending on the language it detects on the host system. In English, the message will begin with "Hi! How are you?" followed by one of the following:

I send you this file in order to have your advice
I hope you can help me with this file that I send
I hope you like the file that I send you
This is the file with the information that you ask for

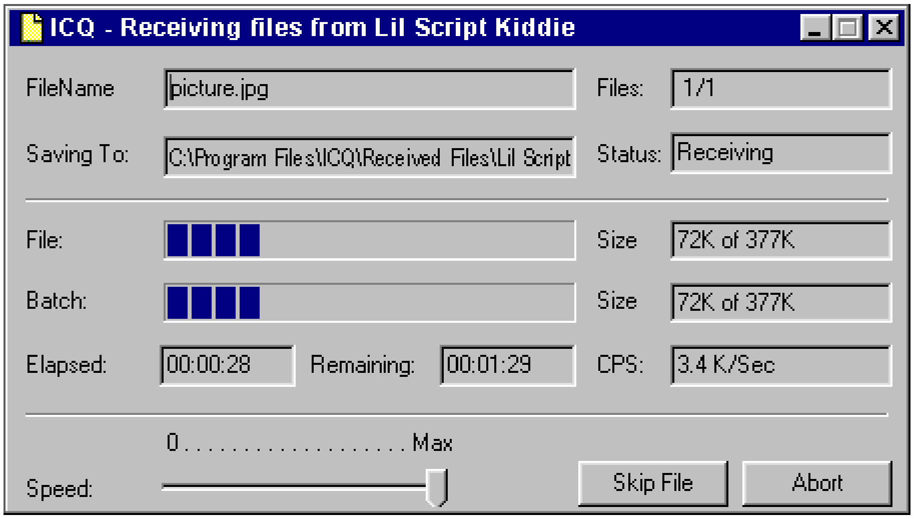
The last line is "See you later. Thanks". Without further thought, many people then open the attached file, and Sir Cam goes to work on their system. First it creates copies of itself in two locations, then it makes a copy of the file it was masquerading as to be opened normally. IOWs, if Sir Cam arrived as a MS Word file, then MS Word would open an display a file. Sir Cam can also pretend to be an Excel (.xls) or Zip file... either of which will appear to open normally. At this point the victim might wonder why this file was sent to them, perhaps replying with the requested "advice" or just closing and ignoring it. Sir Cam however is now getting the victim's name and e-mail address from the system registry, and making a list of the files in the "My Documents" directory. One of these files will be selected and Sir Cam will attach itself to a copy of the file. Next Sir Cam searches for any .web (Windows Address Book) files, such as those used by Outlook to store e-mail addresses (it will also check a few other locations likely to have e-mail addresses, it's a very hardworking worm). Armed with all the e-mail addresses it could find and a newly infected file to send, Sir Cam uses its own SMTP engine (ie. built-in e-mail sending program) to send out messages with attachments to a new group of potential victims, with the subject of the message being the name of the file it found.

What makes Sir Cam clever is the way it searches the My Documents directory for a file to infect and send. Since most Microsoft programs use this as the default directory to save user created files, the odds are very good it will find a file (Word doc, Excel spreadsheet or Zipped file) created by the user of the system. Where other e-mail worms have used the same subject title, Sir Cam uses the name of the file it found, hence warnings not to "open an e-mail called..." are useless. Same for warnings not to open an attachment with a certain name, Sir Cam could pick any file name it finds on the host system. The only change it makes (other than attaching itself) to the file being sent is to the extension... it will append it with one of the following: .bat, .com, .lnk or .pif. Since by default Windows "hides" these "known" file extensions, the file name displayed look may look like a .doc, .xls or .zip. So between the innocent looking extension and the "personal" name of the file, it may really look like a file someone sent for an opinion... and since it displays normally the victim might not have any reason to suspect it wasn't intentionally sent.

Of course the "sender" may never have wanted (or expected) the file to be sent to everyone in their address book, and it could be very embarrassing if the file contained "private" information (look in your "My Documents" directory and see if there is anything in there you wouldn't want to have shared with everyone in your address book *smile*). If that was all Sir Cam did then I'd say it was a very clever and potentially embarrassing little fellow, but Sir Cam isn't finished trying to ruin your day. It is "network aware," meaning if you are connected to a LAN (local area network, common in may workplaces) it will begin to spread itself to every other computer on the local net. If that happens on an office network, it's quite likely your employer will frown on this, but you may find other folks in the unemployment line to commiserate with.

Sir Cam packs a nasty payload which may be detonated in a number of ways. It has a 1 in 20 chance of deleting all files and directories on the C drive. This only occurs on systems where the date is October 16 and which are using D/M/Y as the date format. It always occurs if the attached file contains "FS2" not followed by "sc" (don't ask me why, it just does). There is a 1 in 50 chance it will fill all remaining space on the C drive by adding text to the file c:\recycled\sircam.sys. Sir Cam also changes settings in the Windows Registry file so it will be executed every time any exe file is run... its payload will detonate after 8,000 executions. Regardless of what triggers the payload, there is a very good chance that Sir Cam will have had plenty of time to spread before doing anything that may tip-off a victim. Sir Cam is yet another example of why you want to be able to see (and pay attention to) file extensions... seeing a file attachment called "my_favorite_jokes.doc*.com*" may just tip you off that something isn't quite right ("Why is my friend sending a Word file with a .com extension? Maybe I'd better ask before I run it.").

Sometimes having the file extensions unhidden isn't enough... Windows 9x and up allows for "long file names"... sometimes so long that the entire file name can't be displayed in Explorer or other application programs. For example, here's a screen capture of a file being received through the popular ICQ program:



ICQ - Receiving files from Lil Script Kiddie

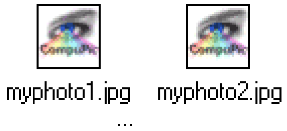
FileName: picture.jpg
Files: 1/1
Saving To: C:\Program Files\ICQ\Received Files\Lil Script
Status: Receiving
File:
Size: 72K of 377K
Batch:
Size: 72K of 377K
Elapsed: 00:00:28
Remaining: 00:01:29
CPS: 3.4 K/Sec
Speed: 0 . . . . Max

Looks like a normal file called "picture. jpg"... doesn't it? But the real name of the file was:

picture. jpg   .exe

All the spaces after the ".jpg" pushed the real extension, ".exe", so far to the right that it wasn't displayed in the file name box, and there was no indication that the file name extended beyond the limited space provided. This trick has been used many times to slip an executable file into an unsuspecting ICQ user's computer and get them to run it (after the transfer, ICQ gives the option to immediately launch the received file). More often than not, the exe is a "backdoor" program which gives the sender the ability to control the victim's computer... stealing or altering files at will. This has also been the source of widespread speculation that a "jpg" file can contain an executable program... *it can't,* but an exe can easily be mistaken for a jpg using a method like this. Note that if an exe file has its extension changed to jpg, Windows will usually attempt to display the file in the associated file viewer which will either crash, display a garbled graphic or binary code... but it will not attempt to execute the program code because it is treating it as a jpg, not an executable. Try it yourself... makes a copy of a (harmless) exe file, rename it as a jpg and then attempt to view it. If for some reason the renamed exe is actually executed, you need to find a new picture viewer, because the one you have is severely flawed.

It's not just programs like ICQ, Windows can also make it difficult to detect a long file name hiding an extension. Take a look at this screen capture from MS Desktop Explorer:



Notice anything different about myphoto1 and myphoto2? One is a photo of my smiling face, the other is an exe file which upon running will immediately reformat the hard drive (please, no comments on which is the worst fate *g*). The only clue Explorer gives is the "..." under "myphoto1.jpg" which indicates that the file name continues. In this case, if you looked at the entire file name it would reveal the ".exe" at the end of the name. It's easy to miss those eclipses if you're not paying attention, and the price of clicking on that first file is high.

I Don't Know And I Don't Care

There are two "excuses" I often hear from people who have allowed their computers to spread a worm or virus. The first is that they are "new to computers" and didn't know better, the other is that there is "nothing important" on their computer so they aren't concerned about malicious programs. Let's take these one at a time.

Being "new to computers" (or "the Net") is the reason why you should take some time to educate yourself about the risks associated with being connected to a worldwide network. Imaging you were driving down the road and someone came along and slammed into you, destroying your vehicle and possibly injuring you and your passengers. When they are questioned about what happened, they innocently reply that they are "new to driving" and didn't know how to use the brakes. Might you think that they should have damn well learned how to apply the brakes before heading out on the highway where they could pose a threat to other drivers? The point is if you are going to be connected to the "Information Superhighway" (ie. the Internet), then you have a responsibility to learn how to remain in control of your hardware and software. I can understand that when you first get connected there is a whole new, and often strange, world for you to explore... full of confusing acronyms and seemingly incomprehensible terminology. Of course you can't learn it all in one night, and "accidents" will happen. But you can't claim the "newbie defense" forever, so please make a point of learning as much as you can and keeping your system secure. There are many, many websites devoted to security, tailored to all levels of experience and understanding. If one is too complicated for you, move on to the next. And ask questions, everyone you meet on the net was once a newbie... some have learned valuable lessons that they will gladly pass along to you... if you'll take the time to listen.

The other excuse, that there is nothing "important" on someone's computer is pretty lame when you consider how many malicious program use one compromised computer to spread it to others. Maybe you don't care about the files on your computer, but I certainly care about the files on mine and won't be very sympathetic if both our hard drives get trashed. Another way to look at it, maybe you don't care if you burn down your own house, but if the whole block catches on fire your neighbors are going to come looking for you. If you really don't care about the files on your computer, fine... just pull the plug on your Internet connection so you don't affect anyone else. Otherwise, what you do (or allow to happen) to your computer can affect everyone else, starting with your friends and contacts.

Here's another thought to toss out for consideration. We've all seen those sleazy lawyers who are always looking for a reason to sue someone for negligence... you know, the ones on the late night commercials that ask "Have you or someone you know been injured in a slip and fall accident?" They are correct when they say "negligence is no excuse, you may be entitled to cash damage awards." Just because someone forgot to put out the "Caution slippery when wet" sign and someone else fell down, the "defendant" is often going to pay dearly for their carelessness. Now eventually one of these sleazy lawyers is going to realize that there is a gold mine to be found on the Internet... not from porn sites and mass merchandising, but from suing people and companies who were careless with their computers and caused damage to someone else. I can hear it now... "have you or someone you know lost important data due to a virus sent from someone else's computer? If so, contact the law offices of..." Really, it could happen, and the settlements could be huge if the virus/worm was traced back to a large company with deep pockets... or even to YOU. All the lawyer has to prove was that the "accident" was preventable (they usually are) and that the reason the plaintiff ran the attached file was because they trusted the sender. Never mind that both parties were guilty of the same thing, that's not relevant (maybe the defendant can try to sue the person/company that sent the virus to them). And if I know lawyers, they'll probably try to trace the path the virus/worm took and sue everyone who passed it along. The bottom line is, someone, somewhere, is going to be dragged into court over negligent operation of a computer that resulted in damage to other systems... I'm surprised it hasn't happened already.

*** Blank space left for update with story of sleazy sue-happy cyberlawyer(s). ***

I hope this article has been helpful and given you a better appreciation for the importance of recognizing file extensions. I know it's not a very exciting subject, but neither is reformatting you hard drive and reinstalling all your software. Good luck... and be sure to practice *safe hex*.

One of Microsoft's attempts at "user friendliness" is that recent versions of Windows are set to *hide file extensions*. What's a file extension? As an example, it is the ".exe" that is at the end of a program's name.

Unfortunately, Microsoft decided that we don't really need to know what file extensions are. Even worse, they decided that Microsoft programs including Windows might not always consider the file extension, when deciding which program to use with a file.

Huh? That was a lot of words. Let's take it in shorter sentences.

A file extension is the ending of a file name. For example, Microsoft Word's file name is WINWORD.EXE. Word, by default, declares to Windows that it owns files with the extension ".doc". So, if you double-click on a file ending with .doc, Word will try to open it. Similarly, the Notepad program "notepad.exe" declares ownership of the .txt file extension. [By the way, Windows is not case sensitive, so it views Notepad.exe and notepad.EXE and NoTePaD.EXe as the same thing.]

Finally, by default, you do not see file extensions -- Windows hides them.

OK, so what's the problem?

The problem is that, in older versions of Windows, the period (".") was not a valid character for a file name -- it was only valid as a separator between the first part of a filename and the file's extension.

Windows XP, and I think Win2000, changed that. They joined the Linux/Unix naming conventions to an extent with that change. Now, a period is valid within the file name, or even multiple periods, in addition to the one separating the filename from the file extension.

So, you could rename WINWORD.EXE to Win.Word.2000.exe, if you wanted. It would still execute the same program. (Of course, if you did, you would have to change any Word shortcut, too, so that the shortcut still worked.)

Now, let's look at another case. Say you get an email with an attachment labelled my-neat-pictures-from-the-beach.jpg . We all know .jpg files are image files -- picture files -- so, it's safe, right?

Wrong! With the Windows defaults, which hide the file extension, the file might really be my-neat-pictures-from-the-beach.jpg.exe -- see the problem? It might really be a program.

The fix is to turn off the Windows setting "hide file extensions."

Turning Off the "Hide File Extensions" Setting

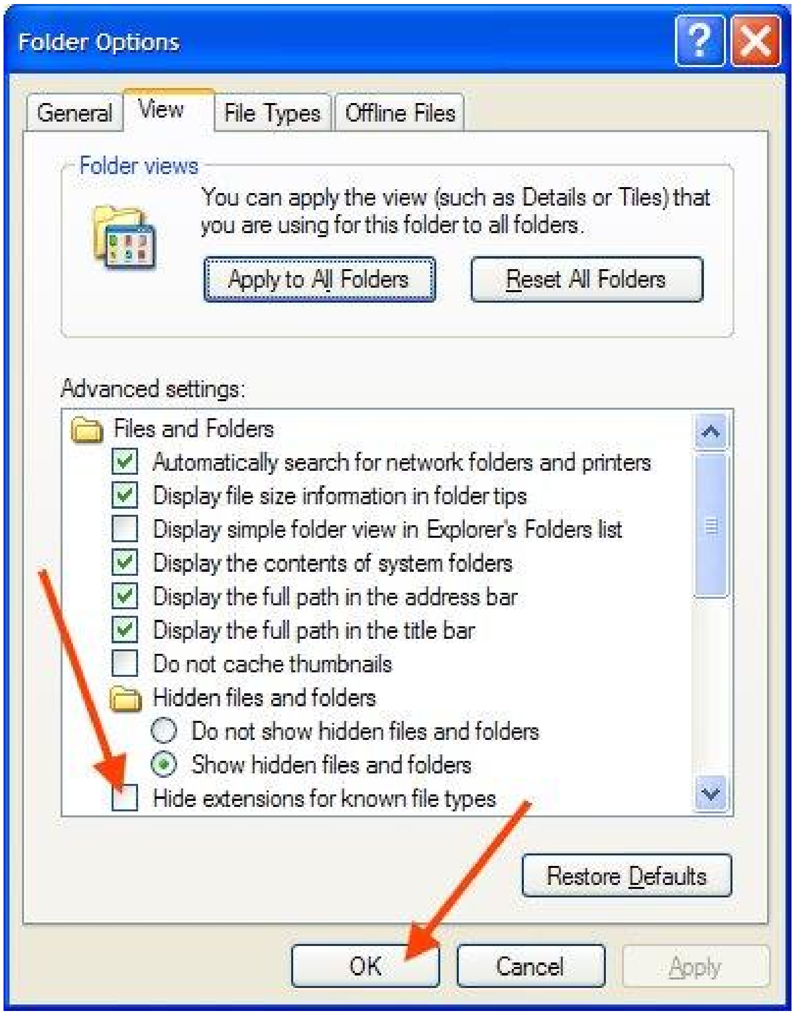
One of the first things I do on my computers is to turn off the Hide File Extensions setting. I also do this on almost every PC on which I work.

Whether you are using Windows 95, 98, Me, 2000 or XP, the technique is similar.

In Windows XP, open up Windows Explorer. Right-click on the Start button. Then, left-click on Explore.

Click on Tools, Folder Options, View.

Then, uncheck "Hide extensions for known file types."



Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

Files and Folders

- ☑ Automatically search for network folders and printers
- ☑ Display file size information in folder tips
- □ Display simple folder view in Explorer's Folders list
- ☑ Display the contents of system folders
- ☑ Display the full path in the address bar
- ☑ Display the full path in the title bar
- □ Do not cache thumbnails

Hidden files and folders

- ○ Do not show hidden files and folders
- ● Show hidden files and folders

- □ Hide extensions for known file types

Link to this page — just add this code to your web page!

```
<a
href="http://www.terryscomputertips.com/computers/hidden-file-extensions
.php">Hidden File Extensions in Windows</a>
```

Show File Extention

Show File Extensions in Windows XP

Follow these steps to show file extensions in Windows XP

1. Go to My Computer and choose Tools | Folder Options, as shown in **Figure 1**.

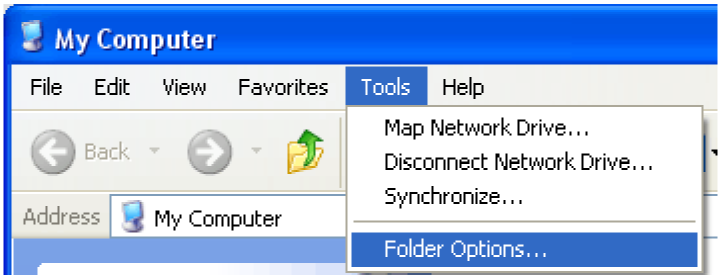
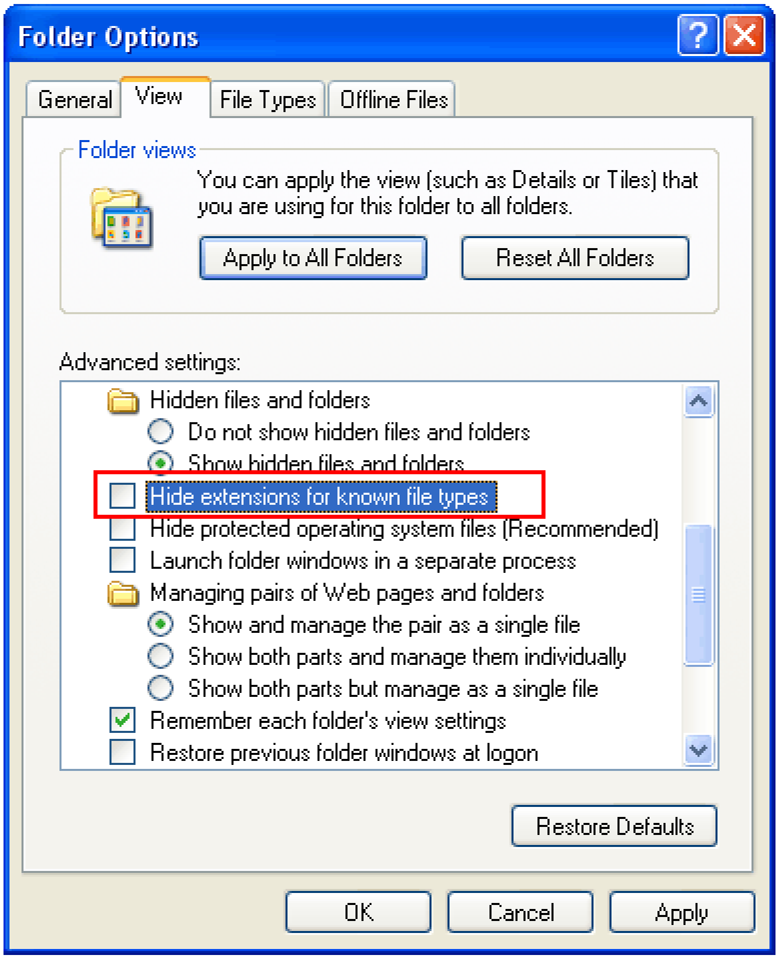


Figure 1: Folder Options

2. This opens the Folder Options dialog box that you can see in **Figure 2 --** in this multi-tabbled dialog box, select the View tab (again, refer to **Figure 2**). Scroll down the list of Advanced Settings, and deselect the **Hide extensions for known file types** option. Click OK.



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

Hidden files and folders
- ○ Do not show hidden files and folders
- ● Show hidden files and folders

□ Hide extensions for known file types

□ Hide protected operating system files (Recommended)

□ Launch folder windows in a separate process

Managing pairs of Web pages and folders
- ● Show and manage the pair as a single file
- ○ Show both parts and manage them individually
- ○ Show both parts but manage as a single file

☑ Remember each folder's view settings

□ Restore previous folder windows at logon

Figure 2: Hide extensions for known file types

Back

Show File Extensions in Windows Vista

Follow these steps to show file extensions in Windows Vista:

1. Go to My Computer and choose Organize | Folder and Search Options, as shown in **Figure 3**.

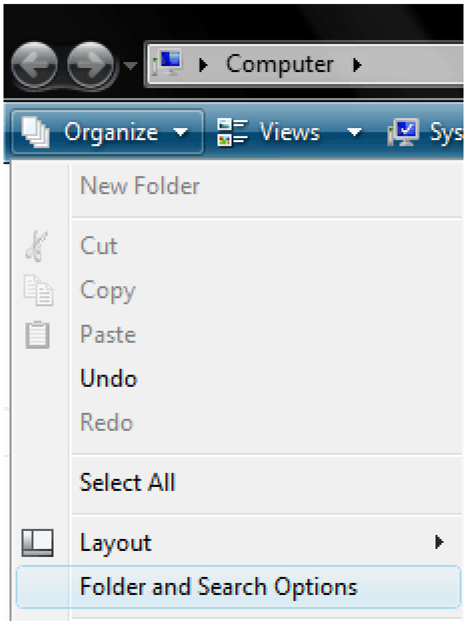
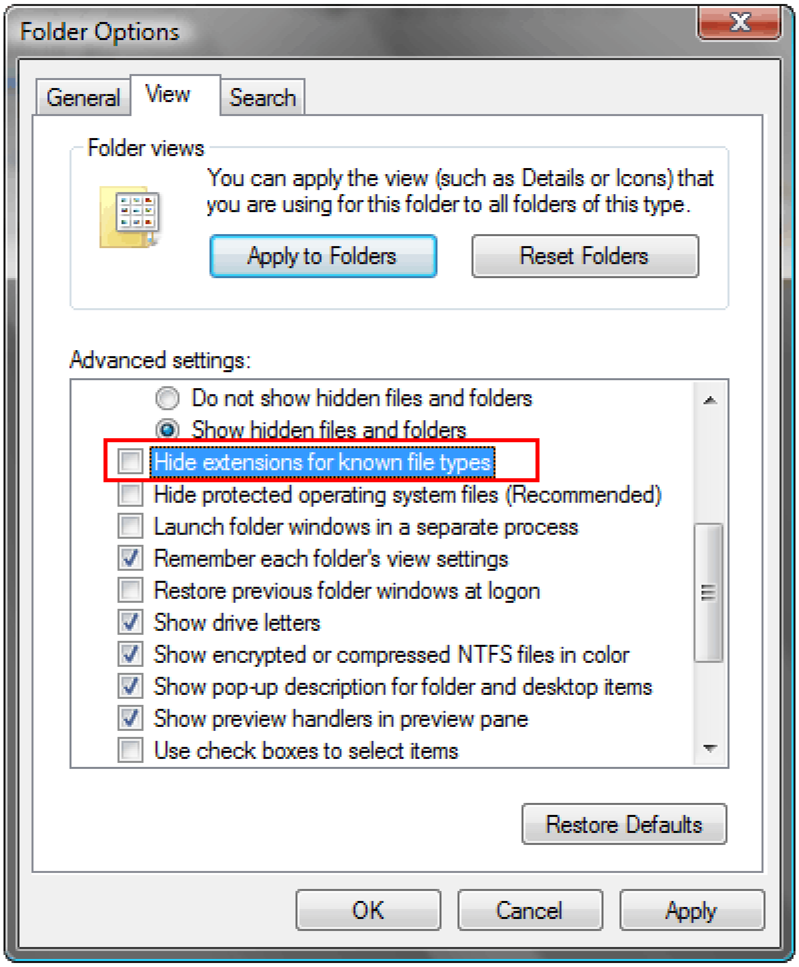


Figure 3: Folder and Search Options

2. This opens the Folder Options dialog box (see **Figure 4**). Select the View tab -- scroll down under Advanced Settings -- and deselect the **Hide extensions for known file types** option. Click OK.



Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

○ Do not show hidden files and folders
● Show hidden files and folders
□ Hide extensions for known file types
□ Hide protected operating system files (Recommended)
□ Launch folder windows in a separate process
☑ Remember each folder's view settings
□ Restore previous folder windows at logon
☑ Show drive letters
☑ Show encrypted or compressed NTFS files in color
☑ Show pop-up description for folder and desktop items
☑ Show preview handlers in preview pane
□ Use check boxes to select items

Figure 4: Hide extensions for known file types

File Extension Database

Computer system files can be divided into two main groups which both of them are very important and perform a crucial role in your machine's stability and performance. The first group of files is system files, which ensures your system's stability. The second group of files is application files that are used in order to load various programs smoothly. The third group of files is considered undesirable and malicious files.

Malicious files are designed to infect your machine and perform spy ware tasks such as collect personal information about you, cause your computer to run slowly, and change the settings on your computer. In many cases, spy ware needs to use a legitimate program or file in order to run so it is important to differentiate between a valid file and one associated with a spy ware.

Our file extension database lists spy ware files according to their file name, helps you identify the spy ware program associated with it, and you can remove it manually or automatically from your PC

Email Me:
Silent_Dreem@Yahoo.Com
Mobile No:0301-3822316