Active Content and Security

As far as I'm aware there is no method of surfing that is 100% secure. There is, however, a series of steps you can take to make your system safer, yet still enjoy the benefits of enhanced web pages.

Read through the whole of this document before making any changes.

1. Active Content

Web designers make use of three main types of extra code to make their sites more interesting. Collectively they are known as **Active Content,** and each is a potential source of infection, since these features can also be used by others to do things you would not want. Installing viruses or worms, harvesting personal details from Cookies, placing annoying pop-up ads and dropping Trojans that install Spyware are examples. Whatever technology is in use, there will always be malcontents or criminals that use it to cause distress or exploit it to their own ends.

Three types of Active Content are listed below. Changes to their status are made through **Internet Explorer / Tools / Internet Options / Security / Custom Level**

1. **Active X Controls**
2. **Scripting (including JavaScript)**
3. **Java Applets**

Disable by Default : Enable by Choice.

One way the Nimda Worm stung many people recently was through web sites, which had been hacked, and visitors had their **Active Content** entirely enabled. All they had to do was visit the site and the worm was downloaded on to their system, where it wreaked its particularly nasty havoc. This is why I suggest Disabling by Default and Enabling by Choice. Even then, one of your Trusted Sites could have been hacked.

Be careful when adding sites to your Trusted Zone

Note that **Disabling / Enabling** one type of Active Content does not affect the status of the others. You *could* disable all scripting by removing the **Windows Scripting Host** from your system, but this curtails all script, malicious or beneficent. This would not, however, affect Active X Controls.

Disabling ActiveX will prevent ActiveX controls and plugins from running, which include Shockwave Flash and Acrobat Reader (needed for *.pdf files). To see which Active X programs have been downloaded on to your system look in :

Internet Explorer / Tools / Internet Options/ General/Temporary Internet Files / Settings / View Objects

Disabling Scripting options will block many of those irritating pop-up' ads.

2. The Microsoft Java Virtual Machine (MS JVM)

To run some types of script (javascript) and Java applets – which are not closely related in spite of their similar names – requires you to have a Java Virtual Machine installed on your system. This is how to get the Microsoft version, not included by default in IE6.

Determining which JVM you have

To determine if you have it, and what version:

- Click the Start button
- Click Run
- Type WJVIEW.

The top line of the message box will give you the version of the MS JVM you have. It should be 5.00.3809. If it is a lower number than this, you have a version which is potentially insecure, and you should upgrade. If you have not got it at all, you will need to install the relevant Service Pack.

Upgrading the Java Virtual Machine : *visit* *http://java.sun.com/getjava/index.html*
(note : link not active in a *.pdf file)

You need to have **Active X, Scripting of Java Applets** and **Active Scripting** set to '**Enabled**' for this visit.

Enabling and Disabling Active Content

1. Go to **Internet Explorer / Tools / Internet Options/ Security**
2. Select **Internet Zone** and Custom Level
3. **Enable** :
   Download Signed Active X Controls,
   Run Active X Controls and Plug Ins,
   Script Active X Controls Marked as Safe.

4. Scroll down and set to **Enable** :
   Active Scripting
   Scripting of Java Applets

(Note : in doing this, you are in effect setting your Internet Zone to Trusted status. This will be changed later.)

---

3. Setting Zones

Using **Internet Explorer / Tools / Internet Options/ Security :**

1. Select **Internet Zone / Custom Level** again and set most things to **Disable,** except Java, which you can set to **High Safety.** This lets Java Applets run in a **Sandbox,** where unfriendly ones should not cause harm. You could also try the **Prompt** options, though I find that these become tedious after a while.

2. Select **Trusted Sites / Custom Level** and set everything to **Enable.** Java Applets can be set to **Low Safety.** In this Zone the 'Sites' button will be active. Click it and **uncheck** the 'Require Server Verification (https:)…' You will see a box into which addresses can be typed. This is how you add sites to the Trusted Zone if you have not got the IE toolbar buttons or Menu options.

3. Select **Restricted Sites / Custom Level** and set everything to **Disable.** Again you can add addresses manually to this zone using the typing box.

When surfing, if you come to a web site that gives an error message, or a blank page, yet you want to view its contents as the author intended, then you will need to add it to your **Trusted Sites**. You can do this automatically with the click of a Menu Option or Toolbar Button, if you follow the instructions in the document **IE Buttons Pack**, obtainable from Mercury Freeware (visit the Index Page and click IE Buttons Pack). If not you will need to do it manually as described above.

4. Privacy Settings

In Trusted Zones, Active Scripting will be enabled. There is a vulnerability through Cookies that can be blocked by disabling Active Scripting, or less intrusively through :

Internet Explorer / Tools / Internet Options / Privacy / Advanced :

If you click the 'Override Automatic Cookie Handling' the Options become active. Check **Accept** for 1st Party and **Block** for 3rd Party Cookies. This is necessary to prevent a possible harvesting of your details. Microsoft are about to supply a patch.

MerC
February 2003