How To...

Maximise your browser security

Wayne Williams shows you how to customise your browser's settings to make it more secure

Part 1 | Internet Explorer 8

Part One

Internet Explorer used to be considered something of a leaky boat when it came to security. By making it an integral part of Windows, Microsoft inadvertently gave virus writers, hackers and spyware developers a direct route into the heart of the operating system. IE7 went some way towards overcoming this problem by beefing up the default security settings and introducing new features like Protected Mode and a phishing filter. The follow-up, IE8, builds on these features, and with a few simple tweaks can be made even more secure. If you haven't already upgraded and want the latest security features, you should upgrade to IE8 immediately from http://microsoft.com/uk/ie8.

Changing zones

Internet Explorer uses security zones to determine how it should treat each website it opens. To access the zone settings, go to Tools, Internet Options and click the Security tab. IE offers five actual zones – Local machine (which you can't see or configure here), Internet, Local intranet, Trusted sites and Restricted sites. Internet has three security levels, starting at Medium. The default setting is Medium-high, which automatically blocks unsigned ActiveX controls and asks you before downloading any potentially unsafe content. In theory, you can make the browser more secure simply by selecting the High setting. This disables less secure features and offers the maximum safeguards, but can actually interfere with your browsing and stop some sites from displaying properly. If that happens you can always add them to the Trusted zone, but only if you're absolutely certain they are 100 per cent safe.

You can configure four security zones within Internet Explorer 8

Clicking 'Custom level' gives you greater control over which features are allowed, but unless you know what you're doing this can also cause problems. We recommend changing the following:

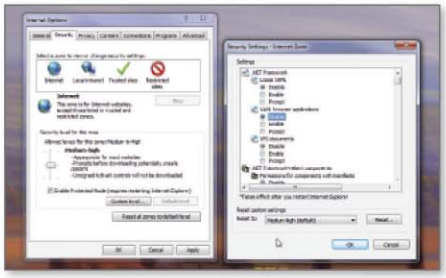
.NET FRAMEWORK

- Disable Loose XAML, 'XAML browser applications' and 'XPS documents'.

.NET FRAMEWORK-RELIANT COMPONENTS

- Disable 'Permissions for components with manifests', 'Run components not signed with Authenticode' and 'Run components signed with Authenticode'.

Missed Part 3 of our synchronisation How To? Download it at www.webuser.co.uk/243



If you opt to customise the security levels, ensure you select the correct options

ACTIVEX CONTROLS AND PLUG-INS

■ Disable 'Download signed ActiveX controls' and 'Script ActiveX controls marked safe for scripting', and change 'Run ActiveX controls and plug-ins' to 'Administrator approved'.

ENABLE .NET FRAMEWORK SETUP

■ Disable 'Enable .NET Framework setup'.

MISCELLANEOUS

■ Disable 'Allow web pages to use restricted protocols for active content', 'Installation of desktop items', 'Launching applications and unsafe files', and 'Launching programs and files in an IFRAME'.

SCRIPTING

■ Disable 'Allow Programmatic clipboard access'.

USER AUTHENTICATION

■ Change Logon to 'Anonymous logon'.

If you accidentally make a change that IE considers unsafe, it will warn you and offer to change it back. If you find this custom set-up causes you problems, you can always reset the zone back to the Medium-high default.

If you use Windows 7 or Vista, make sure the Enable Protected Mode check box is always ticked as this will make it harder for malicious software to install itself on your computer. If you disable Windows 7/Vista's UAC feature, Protected Mode will also be turned off.

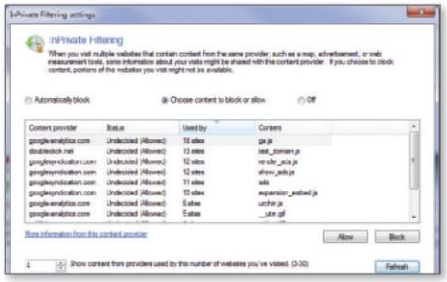
Privacy

Click the Privacy tab under Internet Options to change how IE handles cookies. There are six settings available. Move the slider to the top and the browser will block all cookies. Move it to the bottom and it will accept them all instead. The default Medium setting is probably fine, but nudging it up to Medium-high will give you a little additional protection.

A setting of Medium is probably adequate for cookie handling

Use InPrivate Filtering

InPrivate Filtering is a useful feature that prevents your browser from supplying information about you to websites or third-parties such as advertisers. Turn it on by going to Safety, InPrivate Filtering.



Surf the web incognito by turning on the InPrivate Filtering function

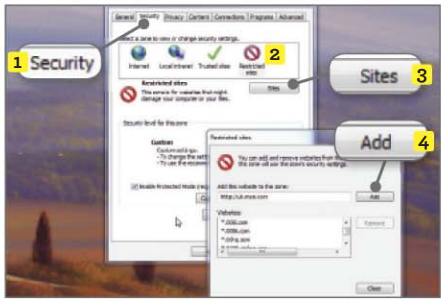
You can set it to automatically block your data globally (which could cause problems with some sites), or specify the content you want to either block or allow.

SmartScreen Filter

IE8's SmartScreen Filter replaces IE7's phishing filter and warns you if you attempt to visit any sites it considers unsafe. Activate the feature by going to Safety, SmartScreen Filter, Turn On SmartScreen Filter. If you suspect a site might be dodgy, you can check it by going to Safety, SmartScreen Filter and selecting Check This Website.

Receive warnings about unsafe websites by activating the SmartScreen Filter

MINI WORKSHOP | Protect IE using SpywareBlaster



1 SpywareBlaster (www.javacoolsoftware.com) secures your browser against unwanted software and sites. Run it and click the option to enable protection in IE. On the next screen, tick ActiveX Protection 1 and Cookie Protection. 2 Remove individual items from the block list if required, 3 then click Protect Against Checked Items. 4

2 Click the Restricted Sites link on the left 1 and then tick the Restricted Sites Protection box. 2 Again, you can customise the block list. 3 It's definitely worth having a quick look through it if nothing else, just to see what's included. Click Protect Against Checked Items 4 to add them to IE's Restricted Sites zone.

3 To make sure all the sites have been properly added, open Internet Explorer and go to Tools, Internet Options. Click the Security Tab 1 and then click the 'Restricted sites' zone. 2 Click the Sites button 3 to see all the dodgy locations listed. You can add further sites yourself should you need to. 4

NEXT ISSUE **How To...** Make Mozilla Firefox even more secure

On sale 29 July