

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **FACILITATORS UK**

A publication designed to inform and enable businesses to understand the implications, costs and advantages of using Information and Communications Technology. Distributed through Chambers of Commerce.

MICROSOFT INTERNET EXPLORER MARKET SHARE DIPS

Recent industry estimates have indicated that the market share of Internet Explorer has reduced significantly in the past months. This is thought to result from users being tired of the endless stream of security patches issued by Microsoft to plug loopholes in the browser that could potentially allow unauthorised access and use of their computer.

This does not mean that Microsoft is suffering, since they still have 90+% of the market. It also does not mean that competitors are immune to security flaws either. Mozilla, one of Internet Explorers' rivals recently issued a software patch to cure a reported hole in its security. This only under-lines the fact that it is not necessarily the software that is at fault (although it maybe). It is just that having such a large slice of the market, it will automatically become the target of mischievous individuals who are looking for Internet users who just might have "left their door open" to an intruder by not ensuring their system security is adequate.

Have you reviewed the extensive facilities within Internet Explorer to ensure that your security is tight? If not, then see the following article for assistance.

INTERNET EXPLORER (IE) SECURITY

In case you have not yet looked into the features within Internet Explorer (the latest version is 6.0), then it is worthwhile looking at how you can ensure that your security is adequate. It should be "adequate" such that it allows you to do what you want on the Internet without it being too restrictive. The following notes may help to explain.

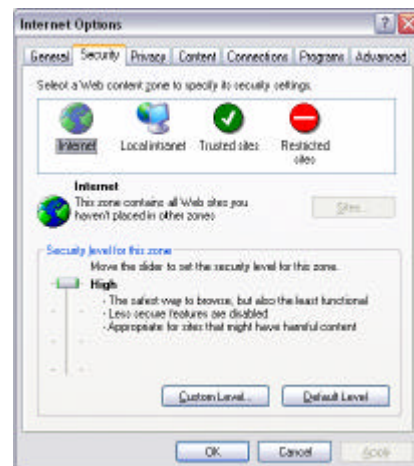
Most threats from using your browser on the Internet come from third parties by-passing your security in some way. They can then run a small program on your computer (a script) without your knowledge. This may allow them to use your computer to carry out illegal or malicious activities, or to steal or damage information on your computer.

Some unscrupulous web-sites can also place information on your computer and run scripts that can potentially damage or otherwise harm your computer.

IE provides some extensive facilities for controlling which sites you can visit and which you cannot, and those that you do, it can restrict how that site interacts with your computer. The problem is one of degree.

It is wise to be cautious and make security as tight as possible. However, it should not be so tight (unless you deem it necessary) so as to limit or in some way restrict what you need to do when browsing the Internet. As with many things, it is a question of judgement of your situation, vulnerability and what you want to do when browsing the Internet.

In order to view and make changes to the security configuration of your copy of IE, you need to go to **TOOLS** and **INTERNET OPTIONS**. Here you will see a multi-tabbed dialogue box. Select the **SECURITY** tab. On the security tab (see below) you will find that the security settings are configured into four categories: Internet, Local intranet, Trusted sites and Restricted sites.



Each of these zones can be configured independently as follows:

Internet Zone

The settings in this zone will cover all web sites that you visit that are NOT specifically listed in any of the other three zones. You cannot put a web site address in more than one zone. There are four levels of security that can be automatically applied in this zone – High (the safest), Medium (this is the default and recommended setting), Medium-Low and Low. As you move the slider control to each setting, a description of what is allowed and what is not appears to the right of the slider bar.

Local Intranet

This zone automatically includes your local computer drives and any network drives that you have mapped or local web sites that exist on this computer or on your local area network (LAN).

Trusted sites Zone

This zone is provided so that you can specifically list web sites that you implicitly trust. They could include your bank web sites for example, most of whom have impeccable security and would not compromise your system in any way. By clicking on the SITES button in this zone, a dialogue box appears where you can enter the web addresses (URLs) of any site that you trust completely.

Restricted sites Zone

This zone already contains a list of web sites that are deemed to be a danger by default, and it will deny all access to these sites. You can add any sites that you specifically want to deny access to for you or any other users of your computer.

The most obvious way of configuring your copy of IE would be to set the Internet Zone to Medium (recommended) or even High (if you are particularly concerned about security), and then enter the web site addresses of your most trusted sites into the Trusted Sites zone. In this way, you are fully protected from interference from all web sites, since only your trusted sites will be able to run scripts and place information on your computer.

Some words of caution

If you follow the above route, you must be sure to enter the correct web addresses of your trusted sites into the trusted zone listing. It must also include any variations in web addresses – for example, when accessing many sites, bank sites for instance, they will often re-direct you to other internal bank sites for specific functions. The web addresses of these redirections must also be included in the list, or else they will be unavailable to you. Similarly, if any scripts are run by these re-directed sites, then you will not be able to access the sites' facilities. You may therefore find that sites that you do want to visit will not function correctly.

From experience, the process of populating your list of trusted sites can be tricky and a little laborious at first. It can also be a little frustrating at first, until you manage to get the correct balance between satisfying the need for tight security and operational expedience. The judgement is yours.

For further assistance in configuring the security in IE, visit the following web site, or call Alan Finch on (01224) 697457 who will be glad to provide advice and guidance.

<http://www.microsoft.com/security/incident/settings.msp>

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly.

May Day Consulting Limited and your Chamber of Commerce have endeavoured to ensure the accuracy of the information contained in this publication, but do not accept liability for any inaccuracy or omission contained within it.

Information on other Business and IT services can be found on our web site at: <http://www.maydayconsulting.co.uk> or by calling Alan Finch on 07968 262079.

MICROSOFT ENDS SECURITY SUPPORT FOR WINDOWS NT WORKSTATION 4

For those businesses, or even home users, who maybe still running Microsoft Windows NT Workstation version 4, then it is important that you understand the importance of Microsoft's withdrawal of support for critical fixes or "patches" to this version of the Windows operating system family.

Microsoft did announce in 2003 that it would discontinue issuing of security fixes for NT4 workstation on June 30, 2004. They will now only issue fixes that appear to specifically target this version of Windows, and only if it becomes a high-profile and widespread issue.

Gartner, a leading IT industry consultancy, has stated that "...Microsoft risks a public relations nightmare, should an exploit circulate for NTW4 and require the company to make a fix available. If the media reports that a worm has shut down a major corporation or government agency, Microsoft likely will be forced to rethink its policy."

If you are still using the Windows NT Workstation 4 operating system, then it would be wise to seek advice on what action to take. Call Alan Finch on (01224) 697457 for professional advice and assistance.

Web Accessibility and UK Law

There is widespread speculation about new legislation being introduced in the UK to ensure that websites are accessible to disabled users. Although widely thought that the new laws, to be implemented in October of this year, apply to web sites, this final part of the Act actually refers to service providers having to consider making permanent physical adjustments to their premises and is not related to the Internet in any way. However the RNIB have a [web accessibility resources area](http://www.rnib.org.uk/xpedito/groups/public/document/s/PublicWebsite/public_webaccesscentre.hcsp) on their website, offering advice and tips. Go to: http://www.rnib.org.uk/xpedito/groups/public/document/s/PublicWebsite/public_webaccesscentre.hcsp

..... AND FINALLY.....

It is some time since we included some humour in *Understand IT*, and this might appeal to those of you who may have been recipients of or been angered by the receipt of one of the many e-mail scams that seem to emanate mostly from Nigeria. Read this to see how some enterprising individuals have got their own back! The article is too long to reproduce here, so we provide the web link so that you can read it online:

<http://news.bbc.co.uk/1/hi/world/africa/3887493.stm>

May Day Consulting Ltd

.....stress free IT

9 Benbecula Road
ABERDEEN AB16 1FT
Tel: (01224) 697457

E-mail: info@maydayconsulting.co.uk
Internet: <http://www.maydayconsulting.co.uk>