

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.

SAVING USER IDs AND PASSWORDS ON YOUR COMPUTER

If you have ever visited a web site that requires that you register with it before you can access any of its information, then you will have been asked to provide a User ID and password.

When logging into the site on subsequent visits you may have noticed that many sites have a small check box, usually marked "Save Password". Often this box is checked by default. The effect of saving your User ID and password locally on your computer is that next time you log into that site, Internet Explorer will automatically log you on. The downside to this is that anyone using your computer can also visit that site and it will log on and provide access to what could be, confidential or sensitive information.

You can of course opt not to save the User ID and password, in which case you need to enter it every time you access that site. If you visit many such sites, then it can be difficult to remember different IDs and passwords, unless you use the same ID and password for each one.

You need not normally worry about major bank sites, since under no circumstances would they provide you with an option to save your password, or any other sensitive information locally on your computer.

In some cases, the "Save password" box is checked by default, and it is easy to hit the logon button and not notice that it is checked. This will save your ID and password when perhaps you would rather not have.

The ID and password information is saved in a number of different places, depending on what version of operating system you are using:

Older versions – Windows '95, '98 and ME all keep them in a password list file in the Windows folder. It has a PWL file extension name i.e. user.pwl, which is unencrypted and therefore accessed easily – not very secure!

Later versions of Windows – 2000 and XP use sophisticated encryption to store the information and it can only be accessed once the user has logged on and uses advanced tools to access the file.

Finally, many web sites use "cookies" to save ID and password information on your computer. Whilst it is possible to view the list of cookies on your computer, locating the correct one is not straight-forward.

Should you wish to delete or edit the ID and password information saved on your computer, the following are the steps you should take, depending on which operating system you are using:

Windows '95, '98 and ME

To remove any saved IDs and passwords from your computer, you can simply just delete the user.pwl file. However, you will then delete ALL saved information – you may not want this. Instead, there is a utility (pwedit.exe) that you will either have on the original Windows CD, or can be downloaded from the Microsoft web site (see <http://support.microsoft.com/default.aspx?scid=kb;EN-US;135315>). This will allow you to edit the password file list and remove any that you no longer want.

Windows XP

With the later versions of Windows, the ID and password information is kept in a much more secure encrypted form, and is not so easily accessible. You can access it by taking the following steps:

1. Go to CONTROL PANEL
2. Select USER ACCOUNTS (this assumes that you have administrative rights to do this....)
3. Select the account that you wish to modify
4. Select MANAGE MY NETWORK PASSWORDS

This will bring up a list of any User IDs and passwords that you have saved. You can then delete any that you do not wish to retain. NB: If any that you know have been saved, do not appear in this list, then follow the process described below.

Cookies

If you have tried either of the above, and you are still being logged on to specific web sites, then it is probable that the developers of the site(s) in question have used "cookies" to store your User information. You can sift through the cookies on your computer and try to delete the correct one, but this can be difficult as you might have hundreds of cookies on your system. The easiest way is to delete all cookies, but again, this will result in the loss of all your saved IDs and passwords. However, if you know them all, it should not be a problem to re-enter them on each web site that you visit. To delete ALL cookies, go to CONTROL PANEL, select INTERNET OPTIONS and hit the DELETE COOKIES button in the centre panel of the dialogue box. You should no longer be automatically logged on to any of your registered web sites.

WINDOWS XP – SERVICE PACK 2

Microsoft have been severely criticised over the past 2 years (if not longer...) for the number of security flaws found in its Windows operating system.

Most of the recent viruses have been designed to exploit some of the known flaws in Windows. In response, Microsoft then issues software “patches” or fixes to close individual “vulnerabilities”. Microsoft has now announced that is preparing to issue Service Pack 2 for Windows XP soon and it will contain significant enhancements that it hopes will tackle the types of flaws that have made the operating system so vulnerable in the past.

Some of the 'new' features it will contain are simply switching on existing facilities which had been left switched off by default. The enhancements will include:

- The turning on of the Internet Connection Firewall (ICF) by default (it is currently de-activated when XP is installed). This is a software facility for stopping unauthorized access to your computer – often a serious problem, particularly when using broadband to connect to the Internet, being permanently connected.
- It will automatically close any TCP/IP ports not in use. These are the communication channels that allow you to have multiple Internet facilities running at the same time (browsing multiple web sites, chatting using MSN Messenger or Yahoo Messenger etc etc.)
- There will be a new “tool” in the Service Pack which will detect third party firewall and antivirus products on the computer and notify the users whether or not they are enabled.
- Major fixes to some of the more complex technical problems that have left users of Windows vulnerable to remote “hacking” of their computers will also be included.

Microsoft has been criticised most vociferously recently because of the ease with which viruses such as SoBig.F spread through Microsoft email systems. It admits that encouraging users not to open attachments from sources that are not familiar is only a partial solution. It therefore plans to implement more secure default settings and better attachment control for both Outlook and MSN Messenger Microsoft’s live “chat” program).

Finally there will be improvements to Internet Explorer to guard against malicious programs being run and spyware being placed onto user's computers.

Microsoft hopes that these improvements will help to reduce the number of attacks on its products and recover its reputation for security. They have confirmed that they will still issue security bulletins and patches for any future flaws that are discovered.

COMPUTER FIREWALLS

A personal firewall is a software application used to protect a single Internet-connected computer from intruders. Personal firewall protection is especially useful for users with "always-on" connections such as DSL or cable modem. Such connections use a fixed IP address that makes them especially vulnerable to potential hackers. Often compared to anti-virus applications, personal firewalls work in the background at the hardware level. Here they protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.

Network or Server Firewalls carry out a similar function, but are designed to protect an entire network, and are therefore more complex, offering a wider range of facilities and are more expensive.

If you have broadband-type Internet access, you should seriously consider installing a firewall to protect your computer or Network.

PC Pro, the respected UK computer magazine, recently published a review of a number of software firewall products, which included the following:

[Zone Labs ZoneAlarm Pro 4.5 with Web Filtering](#)

[Agnitum Outpost Personal Firewall Pro 2](#)

[Kaspersky Anti-Hacker 1.5](#)

[Kerio Personal Firewall 4](#)

[Norton Personal Firewall 2004](#)

[Intego NetBarrier 2003](#)

[ISS BlackICE PC Protection 3.6](#)

[McAfee Personal Firewall Plus 2004 5](#)

[Sygate Personal Firewall Pro 5.5](#)

[Tiny Personal Firewall 5](#)

Go to: http://www.pcpro.co.uk/?news/news_index.php and follow the “Internet and Telecoms” Channel link on the home page, then the “LABS – Personal Firewalls” article to read the reviews of each product.

If you have any queries or support needs, then email Alan Finch at alan.finch@maydayconsulting.co.uk.

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.

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>