

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **Facilitators International LLP**

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.

PLANNED ATTACK ON OUR PRIVACY

With effect from March 2009, every UK Internet Service Provider (ISP) will be required to keep information on every email it handles on behalf of its subscribers, for a period of one year.

The new rules are the government's attempt to comply with a European Union directive, supposedly designed to assist in law enforcements' abilities to investigate serious crime.

The rules will force each ISP to retain the details of sender and receiver of every email originated in the UK (but not the content itself) for one year. It is estimated that a billion emails are generated each day in the UK, and the government will have to pay the ISPs to provide facilities for storing such a large amount of information.

Liberty, the civil rights organisation has protested at these plans and the extension of the idea, in which it is planned to create a central store of all this information on a government-controlled database.

Liberty's argument is based on many publicised cases recently where government departments have been less than professional in protecting private or sensitive information. It also argued that this is the proverbial sledge-hammer to crack a nut situation where billions of computerised records will be maintained at enormous cost, to catch a few individuals with criminal intent.

DESTROY YOUR OLD HARD DRIVE!

Have you recently discarded an old computer that has been collecting dust and which has now been replaced with a nice new gleaming state-of-the-art PC with all the latest add-on components? If you have, or plan to do so, have you considered what to do with the contents of the old system's hard disk drive?

A recent report indicates that most people, and that includes companies and even government departments, do not understand the implications of simply "migrating" information from the old system to the new one.

It is known that criminals often purchase second-hand PC systems from sources such as online auction sites like eBay or even retrieve PC equipment from rubbish tips. Why? Because the contents of hard disks can be easily retrieved by using any one of a number of now free software utilities.

These programs are specifically designed to recover "lost" files from computer hard disks after being accidentally deleted, or even following the formatting of a hard disk drive.

The criminals are able to use these same utilities to recover information from discarded drives that often contain personal or sensitive data, including bank account details, User IDs and passwords.

The report, by Which? Computing magazine, states that the organisation successfully retrieved 22,000 so-called "deleted" files from eight computers that were purchased on eBay.

It goes on to recommend that the only really sure way of ensuring that information contained on an old hard disk drive is irretrievable is to physically destroy the drive itself. Even formatting a hard disk drive, which used to be the recognized way of ensuring that disk drives were securely erased, is now no longer realistic. The technology required to retrieve information even from formatted drives is now readily available to anyone.

The hard disk from your old computer should therefore be removed from the system case – this is easily achieved by removing the cover, locating the drive and removing the retaining screws and connecting cables etc. It should then be completely destroyed using a hammer or some other implement. Only then should your old computer be discarded or even sold on an auction site (minus its hard drive!).

MILLIONS HIT BY NEW WINDOWS VIRUS

You might have read elsewhere in the press about a potentially virulent computer virus that was first discovered in October 2008.

We are adding our voice to the pleas of others to all users to make sure that their Windows operating systems and browsers are constantly updated with the latest patches to ensure that the hackers concerned in this incident do not gain access to and use your computer for their nefarious activities.

This particular virus, known under a number of names, including CONFIKER, DOWNADUP AND KIDO, is seen as particularly onerous since it easily infects PCs via the use of "thumb" or pen drives (USB connected storage devices) that are now very widely used to transfer information from PC to PC - which is of course the attraction for hackers.

It is estimated that many millions of PCs have already been infected quietly and are just waiting to be activated by the hackers to act as proxies in plundering other computers of sensitive and financially rewarding information.

Our plea is that everyone who reads this should review the configuration of their Windows operating system to ensure that it automatically downloads and installs the latest updates and software patches to avoid your computer(s) being hijacked in this way.

In order to check whether your system has been updated, simply go to Windows Update in CONTROL PANEL and view the history of the updates applied to your system. You should look for the security update for Windows with reference KB958644 which was made available within the last 7 days of October 2008.

You can also see the Microsoft Knowledge-base article (KB958644) here:

<http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03&displaylang=en>

DANGERS OF USING WI-FI NETWORKS

Once again, this is a warning about the potential threats arising from the use of Wi Fi networks. We have raised this as an issue in past editions, but it is worth repeating the facts, as they could affect your business or residential use of the Internet.

A US study recently concluded that only about 40% of Wi Fi routers are protected by the in-built encryption features, and have had the standard, default password changed. This means that a staggering 60% of routers are open to any hacker who is familiar with a particular brand of router.

These routers, or "access points" as they are often called, can be used to infect users with viruses, or obtain security information from those accessing the internet via the router.

If you are using a Wi Fi router, whether in the business or at home, then it is ESSENTIAL that you implement the built-in encryption AND change the default password used to configure and administer the router, usually via a web page contained within the router software.

The authors of the study suggested that the manufacturers of these devices should force new users to change the administration password when the device is initially configured, and also to automatically enable the encryption feature by default.

GOOGLE MAIL – OFFLINE ACCESS

The search engine giant Google has recently announced that it's facility to allow users to browse their mail while disconnected from the Internet is now available for beta trial.

The idea is that you will be able to read your mail and compose new mail items whilst offline, which Google has seen as a major problem for those using web-based email services, and inhibits companies in particular from using their service.

Google Labs (the research and development section of Google) has been working on the new feature for some time. If you are a Google Mail user, it might be worth trying the facility out to see if it meets your needs. The facility has to be enabled, and this can be done by logging on to your Google mail account, going to the SETTINGS link in the top right hand corner of the screen, then the LABS link at the top of the settings dialogue box.

When you save the settings and return to the Google mail main page, you will find an OFFLINE link has been added to the links at the top right hand corner of the screen. When you click this, Google will download the offline reader software and a copy of your mailbox to your local computer. **WARNING:** Do not do this if you are using a shared or public computer, as this will create a local copy of your mail. However, once done, you can then work with your mail as normal, without being connected to the Internet.

We think this is a useful facility, but the same functionality can be had by configuring your copy of Microsoft Outlook to access your Google Mail (and Yahoo Mail and Hotmail etc) services from within the inbox of Outlook. You can then read and reply to mail items on any of these services and send them next time you are connected.

RESPONDING TO THREATS

We are conscious that this month, some of the articles in *Understand IT* are all of a somewhat negative disposition. However, we make no apologies for this, as we feel that it is important to point out the realities of the current situation with regard to potential threats to your businesses. We feel that it is part of our function to help to raise the awareness of business managers of potential problems, hopefully before they affect their business.

If appropriate action is taken, then you can feel more confident that you are adequately protected from any external threats.

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly, PC Pro, BBC and other reputable sources..

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>