

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.

STOPBADWARE ORGANISATION AND WEB SITE

Many companies and private individuals have had the integrity of their systems threatened by the unauthorised installation of small malicious programs on their computers by web sites that they have visited.

In the past, much of this “trojan” software has been delivered and installed on unsuspecting users, attached to emails that entice the receiver to open them, which then automatically installs the software. With anti-virus software now more intelligent and successful at spotting malicious software delivered in emails, perpetrators have now moved on to disseminating their malicious software via web sites.

Unfortunately, many of these threats can come from respected, ostensibly reliable web sites. However, when they have been infiltrated by third parties who have installed small, almost invisible pieces of malicious software, they can then, theoretically compromise the PC of anyone visiting that site.

Once an individual’s computer system has been compromised, it can then act as a remotely controlled “robot” to glean information from others, or the parasitic software will sit silently and monitor what the user is doing and harvest information like the user’s various User ID’s, passwords and other potentially valuable information, and relay that to the originator of the software.

An organisation has been established to act as a central “clearing house” for information regarding the identification of malicious software, and the web sites that are propagating it. The site also tries to identify the perpetrators behind these threats to the integrity of the Internet and instigate action to close down their operations.

The organisation’s web site provides both a source for circulating information regarding these threats and a centre for reporting incidents and information about new threats. There is a searchable, online database of offending web sites that details what threats each site presents. The site can be found at <http://www.stopbadware.org>.

The organisation is backed by Google, Lenovo and others, and leading experts in technology are on the executive committee.

If you encounter a suspicious web site or piece of malicious software (“malware” or “badware”), then it is worth visiting the above site and checking it out.

RECOVERING “LOST” FILES

We constantly hear stories from clients and others about the damage to their businesses from the inadvertent loss of information from their PC systems.

Such losses can be due to carelessness, although deleted files would normally be placed in the Recycle Bin first, from where they can be restored easily if they have been deleted by mistake. However, information loss can result for any one of a number of reasons as the results from a survey recently highlighted:

- Hardware Malfunction – 44% of all Data Loss
- User Error – 32% of all Data Loss
- Software Corruption – 14% of all Data Loss
- Computer Viruses – 7% of all Data Loss
- Natural Disasters – 3% of all Data Loss

Source: Nucleus Data Recovery, New Delhi, India

With hard disk capacities climbing dramatically (a one terabyte (one thousand gigabytes) disk will soon become quite common), then the amount of information that can potentially be lost in a single incident is significant and can have serious consequences for a business.

Despite pleas to businesses to ensure that their critical data is backed up in an appropriate way, there are still disasters occurring quite frequently.

Such major incidents can be very disruptive, and often presents a major problem for recovery of the lost information. A few years ago, there were a small number of organisations around that could, for example, take your system hard disk away and retrieve information from it even after an accidental re-formatting of the disk, or failure of the disk hardware.

Successful retrieval in these situations did (and still does) depend on there being no serious physical damage to the surfaces of the disk itself. Even when a disk is formatted using the operating system tools, it does not necessarily result in the complete and irretrievable deletion of the disk content, although this does depend on the type of formatting operation carried out.

Today, there are many more options available to recover “lost” files from a disk, and they can be done by yourself, or your IT support technician on-site.

Using any one of a number of inexpensive or even free programs, then files can be retrieved and restored in any of the above scenarios.

Here is just some of the software that we have encountered recently that can be used to recover files:

Recover My Files

PC Inspector - File Recovery 4

SoftPerfect File Recovery

iUndelete

VirtualLab Data Recovery.

Most of this software can be downloaded from the Internet (try www.download.com) and tested before you buy. However, beware - you can usually try the software to determine what files can be recovered, but most of these programs will not allow you to actually retrieve those files until the software is purchased.

This ability to recover deleted files, even from a formatted hard disk, is of course a double-edged sword. If you can retrieve deleted information, then it means that your critical or sensitive information can never be quite secure, even when deleted. To be absolutely sure that your deleted information is gone for ever, you should carry out a very low-level type of format of your hard disks. To do this, we recommend enlisting the help of your IT organisation.

Call Alan Finch on 01224 697457 for assistance if you are concerned about lost files or need to be sure your deleted sensitive information is not still lurking around on your computer system!

RECOVERING "LOST" DEVICES

In the last article, we discussed how it is possible to recover deleted files. In this article, we cover a related topic of "lost" storage devices.

We are now all using different types of storage media on our computer systems – much of which can be connected to your computer and removed easily using USB or "Firewire" connecting cables. These devices can include:

- Hard disks – external, stand-alone storage
- "Thumb" or "Pen" drives – removable storage - these can now come in sizes up to 8 or even 16Gb capacity.
- Card readers – these are typically devices that are used to read (and write) information from and to the myriad of different format memory cards that are used in mobile phones, cameras, media players etc. Many of these card readers have multiple slots, and when plugged into your computer each slot acts like an individual hard disk.

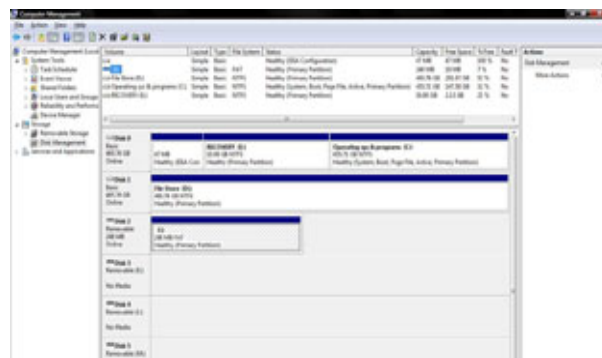
In addition to these devices, that can be connected to and removed from your computer system at any time, you might be connected to an internal network, with network drives "mapped" to your computer. This means that a folder, collections of folders or even a complete hard disk or CD drive on another computer on your network can be configured to appear as a local hard disk drive to your own computer. So that you can use these devices, network drives etc., Windows allocates each device, whether real or virtual a drive letter. With so many possibilities, it is not difficult to imagine that Windows can often become confused, with some devices only being connected periodically when needed.

Windows will normally remember which drive letters it has used for which device, if it is plugged into the same USB port for example. However, if you have many USB ports available, you may use a different port each time.

We have had many calls from clients who claim that their computer does not "see" or display a thumb drive, card reader drive or external removable hard disk when it is connected. The reason is almost always that the drive letter that Windows has allocated to the drive, conflicts with an existing drive that is also now connected.

This conflict can be resolved quite easily by using the DISK MANAGEMENT feature within Windows Control panel. It involves re-allocating drive letters, and would suggest delegating this task to your IT Support professional, as there can often be unexpected problems when changing the letter by which a drive is referenced.

The feature presents a dialogue box like that shown below:



From this panel, you can see all the physical drives connected to your system (it will not show networked drives). Your IT technician can then identify which drives are in conflict and change the drive letter to avoid that conflict. The "lost" drive will then re-appear in My Computer or Windows Explorer.

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>