

Doctors Orders

Welcome

Welcome to the latest edition of the Computer Doctors Newsletter. We have finally completed the waiting area in our "Doctors Surgery". Which means that customers wishing to wait while we fix their PC's will have somewhere to sit and have a coffee.

We also have some PC accessories on display and to launch the "Surgery" we have slashed the prices on many items, just in time for Christmas. (More inside).

Who would have thought that boring old VAT would be the popular subject it is at the moment. Whilst most members of the public are positive that retailers in general, will not pass on the savings to their customers, we would like to reassure all our customers that our accounts department has been beavering away all week changing prices so that all our customers get the benefit of the reduction.

As this is the last newsletter before Christmas we would all like to take this opportunity to say Merry Christmas to all our customers who have used our service over the last 12 months. We know that when times are hard, as they are at the moment, sometimes good service is something that gets left by the wayside as people search for the cheapest prices. We would like to thank all our regular customers for sticking with us through this tough period and we promise in return to give you the best possible service and value for money that we can muster.

A very merry Christmas and a prosperous new year.

From the Computer Doctors.



Inside this issue

- [Doctors Surgery open for business](#)
- [Acronis True Image Home 2009](#)
- [Sinowal, the super-Trojan](#)
- [If "The Matrix" ran on Windows Vista](#)
- [The basics - Connecting your PC](#)
- [The first backup is always the hardest](#)
- [Passwords, who needs 'em.](#)

Doctors Surgery open for business.

We're definitely please to announce that our surgery is finally open. This will allow customers who have a problem with their PC to pop in and have it diagnosed, and



possibly fixed, while they wait.

There will still be instances where a hardware test will need to be carried out to diagnose a

fault accurately and we do not want to reduce our normally high level of accurate fault diagnosing because of a while-you-wait fix. This would benefit neither us nor the customer. But there are a lot of instances where a repair or upgrade can be carried out while the customer waits.

We shall also be keeping a larger stock of the popular upgrade items such as RAM memory, which is our most popular upgrade on laptops and desktops at the moment. If you need a RAM upgrade and lets face it, with the increased demands of XP service pack 3 and Vista

service pack 1, you can't have too much RAM and its never been a better price. A 512Mb stick of DDR-2 RAM (the latest type) is just £12.05 and we'll fit it for free while you wait if you wish.



Also, just to get the ball rolling and because its 3 weeks to Christmas, we have a host of special introductory offers

that are too good to miss. For example we have manufacturer refurbished IBM laptops at £199.00, brand new Toshiba laptops from £375.00, Sony multi standard DVD writers with black or silver fronts for just £25.96 including free fitting, while you wait. Dual core Viper PC towers complete with various XP and Vista options, from £293.00. For full Viper specification see our website.

<http://www.computerdoctors.uk.net/shop/vcs.htm>

(All prices include vat at 15%)

manufacturer refurbished IBM laptops at £199.00

Spyware Doctor

Spyware Doctor is a paid for product and is widely acknowledged as the best anti-spyware program at this moment in time.

It is quite demanding and requires a reasonably quick PC with plenty of RAM so if your PC is entry level and over 3 years old, you'd be better of with Spybot Search and destroy.

If you want to try Spyware Doctor a free trial scan is available from our free download page. If you like it, it costs £29.95 and can be installed on 3 PC's.

<http://www.computerdoctors.uk.net/pages/links.htm>

As part of the refurbishment we have treated ourselves to a new reception area where customers can deliver their PC's for repair, collect repaired PC's and collect items purchased on our website that are marked for "reserve and collect at shop".



Our new facilities will ensure that we can continue to give our customers the best possible service we can and create a pleasant atmosphere where people can pop in for some sound advice,

arrange a bit of TLC for their PC or just indulge in a little retail therapy.

For those customers that have never been to our Northampton workshop we have a map on our website with a link to Google maps where you can enter your postcode and it will work our a route for you.

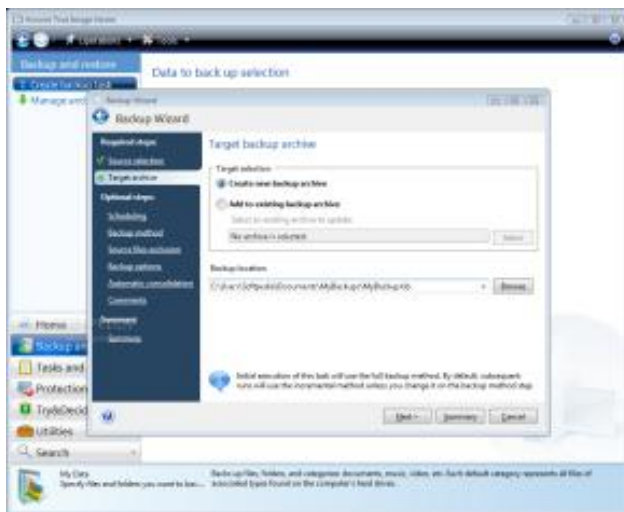
<http://www.computerdoctors.uk.net/pages/map.htm>

Acronis True Image Home 2009

Never heard of Acronis? You don't know what your missing. It's simply the best backup image software available.

We've been using True Image since version 6 and have tracked the program through to version 11. With each release, the product has improved, though at the same time it's grown larger. Thankfully, the just-released 2009 version (V12) has reversed this size-bloat trend; at 88.7MB, the new model is considerably slimmer than version 11's hefty 139.9MB.

True Image Home 2009 features a new interface and numerous enhancements that further improve the utility's drive-imaging performance. More importantly, True Image's data-backup features are improved significantly in the most recent release.



The program's new Vista-style interface will initially disorient regular True Image users who, like me, have become accustomed to the traditional Acronis way of doing things. However, after the initial shock, True Image veterans will realize that the program's new interface is a big step up from the old one.

It's now easier for beginners to use the program, which is organized more logically in addition to being more pleasing to the eye. However, like the ribbon interface introduced with Microsoft Office 2007, some users won't care for the app's new look simply because it's different.

Major new features in the 2009 version of the program include the following:

- Full-text searches of images using either Windows Desktop Search or Google Desktop Search
- A one-click option for predefined backups
- Automatic resumption of backups for drives that were unavailable during the initial backup
- Automatic shutdown after backup or restoration
- The ability to store images in standard .zip format rather

than having to use Acronis' proprietary .tib format

- The ability to select the number of backups to retain

All these features are useful improvements, but the last two really open up the potential of the product for data-file backups rather than simply disk imaging alone.

In particular, the ability to store your disk images in the .zip format is most welcome. You can now read your backup files on systems that don't have True Image installed.

I wish the program would let you store your file backups in the file's native format. For example, I'd like to store backups of .doc files as .doc files. Hopefully, this is a feature that will be added to a future version of the program.

The other valuable addition to True Image Home 2009 is the ability to maintain several unique copies of your full data backups. Rather than always overwriting the last backup, True Image can now rename and save previous copies, up to any number you prescribe.

The program's backup-renaming scheme is quite simple: if your initial backup file was called mydata.tib, then subsequent backups are renamed mydata1.tib, mydata2.tib, etc. This is not quite so elegant as date-stamping the backups but is sufficient for most purposes.

The "Automatic consolidation" dialog in the program's backup wizard lets you set the maximum number of backups to be kept, the maximum size of your backup archives, and the maximum length of time your archives are to be retained.

True Image Home 2009 offers a comprehensive solution that meets all your backup needs. The program allows you to back up both your Windows system and your key data files with a high degree of reliability and with minimum effort.

Along with the program, Acronis have changed the way that they market the product. Previous versions were sold in CD form to a wholesaler, who sold to a retailer, like us and we sold to our customers. Obviously, this conventional method of selling is changing as manufacturers of software realise that each time the product changes hands they lose a bit more profit.

Now they sell direct from their website as either a download or a CD in the post.

The price, has actually increased from what we used to sell it at, but that's just sour grapes on our part. This is such a brilliant piece of software we recommend it even though we can no longer sell it.

<http://www.acronis.co.uk/homecomputing/products/trueimage/>



Sinowal, the super-Trojan

This is not the story of a brave citizen of Troy, but a clever piece of malware that has been evading its enemies for years!

The sneaky "drive-by download" known as Sinowal has been, credited with stealing more than 500,000 bank-account passwords, credit-card numbers, and other sensitive financial information.

This exploit has foiled antivirus software manufacturers time and again over the years, and it provides us in real time a look at the future of Windows infections.

Imagine a very clever keylogger sitting on your system, watching unobtrusively as you type, kicking in and recording your keystrokes only when you visit one of 2,700 sensitive sites. The list is controlled by the malware's creators and includes many of the world's most popular banking and investment services.

That's Sinowal, a super-Trojan that uses a technique called HTML injection to put substitute information on your browser's screen. The bad info prompts you to type an account number and/or a password. Of course, Sinowal gathers all the information and sends it back home — over a fancy, secure, encrypted connection, no less.

Sinowal has been around for many years. (Most virus researchers nowadays refer to Sinowal as "Mebroot," but Sinowal is the name you'll see most often in the press. Parts of the old Sinowal went into making Mebroot. It isn't clear whether the same programmers who originally came up with Sinowal are also now working on Mebroot. Mebroot's the current villain.)

That's a long, long lifespan for a Trojan. It's important for you to know how to protect yourself.

A serious infection most antivirus apps miss

I haven't even told you the scariest part yet.

Sinowal/Mebroot works by infecting Windows XP's Master Boot Record (MBR) — it takes over the tiny program that's used to boot Windows. MBR infections have existed since the dawn of DOS. (You'd think that Microsoft would've figured out a way to protect the MBR by now — but you'd be wrong.)

Vista SP1 blocks the simplest MBR access, but the initial sectors are still programmatically accessible, according to a highly technical post by GMER, the antirootkit software manufacturer.

The key to Sinowal/Mebroot's "success" is that it's so sneaky and is able to accomplish its dirty work in many different ways. How sneaky? Consider this: Sinowal/Mebroot doesn't run straight out to your MBR and over-

write it. Instead, the Trojan waits for 8 minutes before it even begins to analyze your computer and change the Registry. Digging into the MBR doesn't start until 10 minutes after that

Sinowal/Mebroot erases all of its tracks and then reboots the PC using the adulterated MBR and new Registry settings 42 minutes into the process.

Once Sinowal/Mebroot is in your system, the Trojan runs stealthily, loading itself in true rootkit fashion before Windows starts. The worm flies under the radar by running inside the kernel, the lowest level of Windows, where it sets up its own network communication system, whose external data transmissions use 128-bit encryption. The people who run Sinowal/Mebroot have registered thousands of .com, .net, and .biz domains for use in the scheme, to store their ill gotten gains.

Wait, there's more: Sinowal/Mebroot cloaks itself entirely and uses no executable files that you can see. The changes it makes to the Registry are very hard to find. Also, there's no driver module in the module list, and no Sinowal/Mebroot-related svchost.exe or rundll32.exe processes appear in the Task Manager's Processes list.

Once Sinowal/Mebroot has established its own internal communication software, the Trojan can download and run software fed to it by its creators. Likewise, the downloaded programs can run undetected at the kernel level.

Sinowal/Mebroot isn't so much a Trojan as a parasitic operating system that runs inside Windows.

Windows XP users are particularly vulnerable

So, what can you do to thwart this menace? Your firewall won't help: Sinowal/Mebroot bypasses Windows' normal communication routines, so it works outside your computer's firewall.

Your antivirus program may help, for a while. Time and time again, however, Sinowal/Mebroot's creators have modified the program well enough to escape detection. AV vendors scramble to catch the latest versions, but with one or two new Sinowal/Mebroot iterations being released every month, the vendors are trying to hit a very fleet — and intelligent — target.

Similarly, you can't rely on rootkit scanners for protection. Even the best rootkit scanners miss some versions of Sinowal/Mebroot.

Truth be told, there is no single way to reliably protect yourself from Sinowal/Mebroot, short of disconnecting your computer from the Internet and not opening any files. But there are some historical patterns to the exploit that we can learn from.

First of all, most of the Sinowal/Mebrook infections I've heard about got into the afflicted PCs via well-known and already-patched security holes in Adobe Reader, Flash Player, or Apple QuickTime. These are not the only Sinowal/Mebrook infection vectors by a long shot, but they seem to be preferred by the Trojan's creators. You can minimize your risk of infection by keeping all of your third-party programs updated to the latest versions.

In addition, Sinowal/Mebrook — at least in its current incarnation — doesn't infect Vista systems. Windows XP remains its primary target, because Vista's boot method is different and its User Account Control regime gets in the worm's way.

Don't look to your bank for Sinowal safeguards

So, you'd think the banks and financial institutions being targeted by Sinowal/Mebrook would be up in arms. Half a million compromised accounts for sale, on the Internet, by an unknown, sophisticated, and capable team that's still harvesting accounts should send a shiver up any banker's spine.

From a banking perspective, frauds like this have never qualified as a major threat. A banker looks at his profit & loss sheets and writes off this kind of fraud as simply a cost of doing business. Such fraud may amount to billions of pounds each year, but the cost is spread across all sectors of the banking industry all over the world.

If the bankers aren't going to take up the fight against Sinowal/Mebrook, who will? The antivirus software companies have a long tradition of crying wolf, and their credibility has suffered as a result.

In this particular case, the major AV packages have failed to detect Sinowal/Mebrook over and over again. It's hard to imagine one of the AV companies drumming up enough user interest — or enough business — to fund a fight against the threat. Besides, the AV companies are chasing the horse after the stable door has been bolted.

The folks who produce malware these days constantly tweak their products, often using "VirusTotal" or a proprietary set of scanners to make sure their programs pass muster. Shortly after — before the AV companies can update their signatures — the bad guys unleash a new version. AV companies know that and are moving to behavioural monitoring and other techniques to try to catch malware before it can do any harm.

The only company that seems to be in a position to fix the Master Boot Record problem is Microsoft. But it's hard to imagine MS management devoting the time and resources necessary to fix major security holes in a seven-year-old product, particularly when Vista doesn't appear to have the same flaw.

This is short-sighted, however. It's only a matter of time

before Sinowal/Mebrook — or an even-more-dangerous offshoot — finds a way to do its damage on Vista systems as well.

If Microsoft decides to take on Sinowal/Mebrook, the company is up against a formidable opponent that draws on many talented programmers. I recently heard someone estimate that a team of 10 top programmers would need four full months of work to put together the basic setup.

So what's the punch line I hear you ask. Isn't this the usually the part where the Computer Doctor tells us how to fix it?

Well, not this time. All we can do is run our antivirus and anti-spyware programs on a regular basis and hope that this one passes us by! Although, one possibility is to enable the "Tea Timer" option in "Spybot Search and Destroy" (the option that nearly everybody disables, because it keeps popping up every time a change is made to the registry). This should monitor registry changes and may warn you if Sinowal/Mebrook starts to install.

As always, for Spybot and all other free software, visit our free download page.

<http://www.computerdoctors.uk.net/pages/links.htm>

If The Matrix ran on Windows Vista!

If you're a fan of The Matrix trilogy, ever wondered how it would run under Windows?

Science fiction has long been popular with computer geeks: (like us) sci-fi films such as Blade Runner and The Matrix glorify the techie life. Supercomputer fantasies are all well and good, but come on! How do the movie industry get their films so flawless. By throwing big bucks at it, that's how!

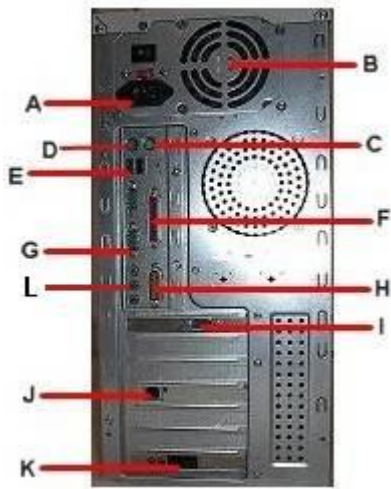
What if characters Neo and Morpheus had to deal with the same technological frustrations that plague the rest of us? Take a look at a hilarious spoof exploring this very possibility. It's all the fun of The Matrix minus Keanu Reeves! What could be better?

<http://uk.youtube.com/watch?v=yX8yrOAjFKM>



The Basics - Connecting your PC

When a customer wants to drop their PC into our workshop, we casually say "Just unplug the tower and drop it in, we don't need any cables, just the tower". Often comes back the reply, "That's easy for you to say". Many people are worried that if they disconnect their PC they will never be able to get the myriad of cables back in the right place.



Its not as complicated as it looks, as nearly all the plugs are different and those that are not are usually colour coded.

Ideally, if you can get to the rear of your PC with all the cables connected, just take the time to have a look at it. PC's do vary slightly

but you will find something similar to the above. You can follow the cables to the peripherals that you have plugged in and see where they go. Some people even tie tags around the cables with the name of the peripheral e.g. "Printer" or "Monitor".

A: Power Connector - sometimes an on/off (I/O) switch is provided. Also some power supplies have a small, usually red, slider switch to change the input voltage between 120v and 240v. This switch must never be moved to 120v whilst in the UK.

B: Power Supply Fan - The power supply fan blows hot air out of the PC and provides ventilation for the power supply and other PC internals.

C: Mouse Port coloured green.

D: Keyboard Port coloured purple
These ports are also known as the mini-DIN or PS/2 connectors. The older computers came with a larger port known as a DIN connector.

E: USB Port - (Universal Serial Bus).
This port (in theory) can connect up to 127 peripherals (such as mice, modems, keyboards, etc.) all at once. It also enables hot-swapping which is being able to connect and disconnect peripherals without powering down the PC. Efforts are being made by some PC manufacturers to replace all ports with USB.

F: Parallel Port (Printer Port) - Most modern printers use a USB connection.

G: Serial Port (COM Port) - This port can be used to connect a computer peripheral such as a modem, although most now use USB.

H: Game Port - The game port is a 15-pin female analogue port used to connect game controllers such as joysticks although most now use USB.
It can also be used as a Musical Instrument Digital Interface (MIDI) Port for connecting a computer peripheral such as a synthesizer and is located on the sound card.

I: Monitor Port - This can be a VGA port, coloured blue or a digital (DVI) port coloured white. Adapters are available from either port to match the monitor plug.

J: Ethernet Port (RJ-45) - Connects to a network hub or a broadband modem/router.

K: Modem - This is a dial-up modem port, not used so much since broadband, but found on many older PC's. This socket is very similar to an Ethernet port but slightly smaller all round. A modem plug will plug into an Ethernet port by mistake, but an Ethernet plug will not fit into a modem socket. Both plugs have a small plastic clip on the side so can easily be mistaken for the other.

L: Three or more ports coloured green (line out, most often used for speakers), pink (microphone), blue (line in. A connection from an external sound source).
Sometimes extra coloured ports are provided to enable surround sound speakers to be used.

Just to add to the confusion some dial-up modems have a green and a pink sound socket on the same plate. These will accept the plugs from your speakers but will give no sound.

So there we have it. As with all computer equipment, changes are being made as we speak and extra ports can be found on some PC's for specific purposes. A Firewire port, similar to a USB port, but not interchangeable, is used to connect some camcorders.

Also with the advent of high definition TV some PC's have HDMI and RCA ports and even SCART sockets to connect to your television. None of these are interchangeable so should not present any problems when reconnecting your PC.

When you get your PC back, if you haven't marked the leads, look at each lead in turn and find the corresponding socket on the PC. Then turn on the PC as normal. Good luck.

The first backup's always the hardest

A customer emailed "Ask The Doctor"

<http://www.computerdoctors.uk.net/pages/askthedoc.htm>

saying that lots of programs suggest backing up your system before installing, including the service pack 3 upgrade from Microsoft. But nobody tells you how to go about this

He went on to say, "I haven't yet installed XP SP3 and would like to follow this advice. But I need instructions on just what to do and what should be copied to DVD."

If you're not currently using any backup software, I suggest you try Windows' built-in backup tools first. (After all, you've already paid for them.) Windows' backup feature is basic but gets the job done. The utility also gives you a point of comparison if you decide to try third-party backup tools later on. Its not always installed on every version of Windows, so if yours is not, here's how to install it.

Go to **Start > All Programs > Accessories > System Tools**. If **Backup** isn't listed, insert the Windows CD that came with your PC. If a welcome screen appears, ignore this. Open **My Computer**, right click on the CD drive icon and select **Explore** from the menu that appears. Now open the folders **Valueadd > MSFT > ntbackup** and double click on **ntbackup.msi**. This will install backup to your PC.

To learn about the version of backup in your copy of Windows, click Start, Help and Support. Type the word backup into the search box at the top of the window and press Enter. The Help system will deliver comprehensive information on using the specific version of backup available to you.

Ideally, your first backup should include every file stored in the partition where Windows resides. If that's too much data for your backup medium to handle, make copies of your own files and programs, concentrating on those that you couldn't easily recover, reinstall, or recreate from other sources.

After using Windows' backup tool for a while, you may find that the program is not suited to your backup needs or preferences. You can then try any of the myriad third-party backup tools out there. (We had a look at backup options — including free backup software and services — on page 4 of the October newsletter).

<http://www.computerdoctors.uk.net/newsletter/NL0810.pdf>

All backup software compresses the files to be backed up into one large compressed file to enable you to store it on a CD or DVD disk. Which means if your PC dies you will need to reinstall Windows and the backup software before you can restore your saved files. This is why drive image software like Acronis has become so popular, you can restore your whole system including Windows, drivers, applications and data in around 20 minutes.

(See article on page 3 of this newsletter for taking an entire image of your system to use as a backup).

Alternatively, if you just want to save your documents and pictures, a lot of people find it easier to just copy their files onto an external USB hard drive so that if their PC dies, they can just plug the USB drive into another PC to see their saved files.

Almost any backup is better than no backup, so the exact way you back up your files is less important than simply doing it. Find a backup tool you're comfortable with, and then use it!

We urge all our customers to make backups and it needn't be costly or time consuming. So if you have documents or photos that you wouldn't want to lose. Give our sales a call to discuss the options. Even if you choose a free option, we are just happy that you are doing it.



Tip

If you take the time to organise your documents, photos and music, it helps enormously when making a backup. So make sure that all your personal files are stored together.

The "My Documents" folder is an ideal place to do this and each user on the PC can have a separate "My Documents" folder if they wish. It has separate folders for "My Photos", "My Music" and so on, in which to place your different file types.

If you have a collection of pictures showing pre-war bus tickets, you can easily create a new folder inside the "My Documents" folder, called "My Bus Tickets".

Tip

These days everybody carries around a host of passwords in their head. In fact so many that we often use the same one over and over again just so that we don't get too many. Banks often suggest using intermingled letters and numbers plus upper and lower case letters. I would defy anyone to remember a password such as this, unless you have a brain like Einstein.

A good way of creating a reasonably secure password is to take a line from a song and use the first letter of each word to create a password. For example "Oh for the wing of a dove" becomes OFTWOAD which would make a good password for a 4x4 enthusiast with a speech impediment.

This could become a new game for the children on those long car journeys. Just think, visiting the in-laws this Christmas could furnish you with a completely new set of ultra secure passwords!

Passwords, who needs 'em

Passwords can be tricky things. You want to make them complicated enough so that no one can guess them, but simple enough so that you can remember them. Its not a good idea to use the same password for all, as some places that you'd use it are very insecure. It's a good idea to have three main passwords for each level of security.

Low security would be to log onto a website that has none of your personal information, say to get a free sample or guide. The name of your pet or mothers maiden name is fine for this.

Medium security might be for login onto online services that have your personal information but no financial details such as bank account numbers or credit card details. Avoid using your username, date of birth, street name in fact avoid real words altogether as well as passwords consisting of just numbers. Spy software can run through millions of possible numeric passwords in seconds.

High security can be used for financial services or anywhere that's important to you. Generally use over 7 characters and make that a mixture of letters and numbers.

A complete no-no with all passwords, is to write them down. The possibility that someone may find it reduces the security by 99%. If you can't remember it, change it to one that you can.

Computer Doctors Ltd
Unit 12 Blackthorn Ind.
Est.
Blackthorn Road
Northampton
NN3 8PT

If this has been passed to you from a friend and you would like your own regular copy, just go to:

www.computerdoctors.uk.net/pages/newsletter.htm

Contact us

General information & to book a call out

Tel: 01604 411 444 (9-6 Mon-Fri, 9-1 sat)

Sales & On-Line Purchases

Tel: 01604 415 984 (9-6 Mon-Fri, 9-1 sat)

Fax: 0871 251 9099

Email: sales@computerdoctors.uk.net

Shop: www.computerdoctors.uk.net/shop

Technical Support

Free: tech@computerdoctors.uk.net

Tel: 0905 121 1097 (9.30-4.30 Mon-Fri)

(Calls cost £1.00 per minute)

Web: www.computerdoctors.uk.net

