



Doctors Orders

Hello welcome to February. January saw many direct malware attacks on Avast antivirus, a program that many of our customers use. The malware manages to disable Avast and provides a "Fix It" button which surreptitiously, downloads more malware. Some of the versions even then charge you for the privilege!

To complicate matters, Avast have redesigned the program slightly and become more aggressive in nagging you into buying one of their two paid-for versions.

Whilst Avast is technically very able, its nagging does put some people off. So for those people we recommend Microsoft Security Essentials (on our free download page under "Anti-Spyware Software"). It is an antivirus and antispyware all in one and being a Microsoft product gets its security updates with the normal windows updates. So don't ignore these when offered. Also, don't forget to remove Avast before installing Security Essentials, otherwise they will fight for the same space and slow your PC to a crawl. If you need us to do this for you, just give us a call.

No doubt Avast will quickly bring out an update to ward of this latest threat, so if you want to stay with Avast its still the best free antivirus there is.

The best overall, in our opinion, is Kaspersky Internet Security and costs £25 from us installed, or £40 installed for the 3 user version.

I hope you enjoy the info, tips and tricks this month and don't forget, we are always happy to receive your comments at:

sales@computerdoctors.co.uk



Craig

<http://twitter.com/CraigtheTrainee>

Inside this issue

- Private browsing - An extra level of security Online
- Say goodbye to BIOS — and hello to UEFI!
- Viper lowers PC prices as Hard Drive prices stabilise
- Welcome to the 64-bit era of Windows
- Using Windows "Safe Boot" To Diagnose and Repair Problems
- How To control Non-Active Windows With The Mouse
- What is the Difference Between Malware, Virus, Root-kits, Spyware, Worm and Trojans
- Our price List
- View from the backside

Private browsing - An extra level of security Online

Private browsing is built into all the latest browsers and can be configured with just a few clicks. Lets face it, on the Internet you can do with all the help you can get these days.

In Internet Explorer 9, click the Settings gearwheel icon, and select **InPrivate Browsing** from the Safety menu (see Figure 1); or select it by pressing Ctrl+Shift+P; or choose it from the New Tab page. Microsoft offers complete instructions on a Help & How-to page: <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private> IE also offers separate, always-on Tracking Protection, if you wish it, as described here: <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/tracking-protection>

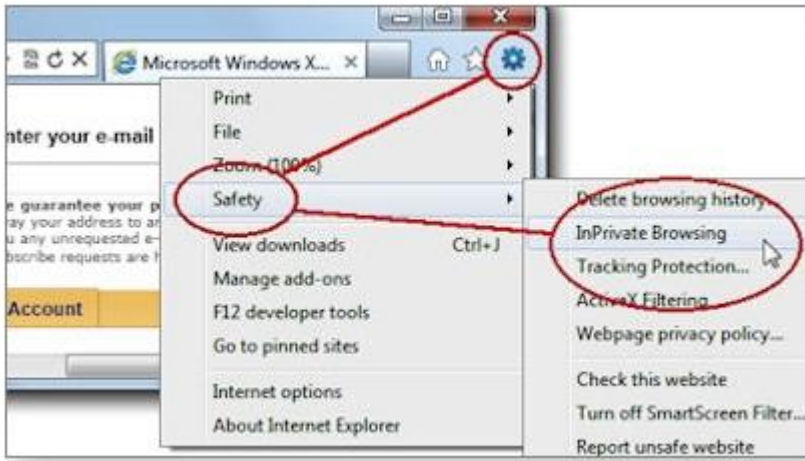


Figure 1. Internet Explorer 9's InPrivate Browsing is always just a few clicks away, via the Safety menu.

In Firefox, the same type of privacy-protecting function is called Private Browsing. (See Figure 2.) To use it, click the Firefox menu and select Start Private Browsing. Mozilla's full explanation is on a Firefox help page: <http://support.mozilla.org/en-US/kb/Private%20Browsing>



Figure 2. Two clicks are all it takes to access Firefox's Private Browsing.

Chrome calls its version of this feature incognito mode. (See Figure 3.) Click Settings (the wrench icon), then New incognito window. Google's explanation is on a "How to use Chrome" page: <http://support.google.com/chrome/bin/answer.py?hl=en&answer=95464>



Figure 3. Chrome's Incognito is readily available and requires no additional software.

Say goodbye to BIOS — and hello to UEFI!

If you've ever struggled with your PC's BIOS — or been knee-capped by a rootkit that assailed the BIOS — you undoubtedly wondered why this archaic part of every PC wasn't scrapped long ago.

Well, be of good cheer: Windows 8 will finally pull the PC industry out of the BIOS generation and into a far more capable — and controversial — alternative, the Unified Extensible Firmware Interface.

To best understand where we're headed, it's helpful to look at where we've been. An integral part of every PC, the Basic Input/Output System spans the entire history of the personal computer — more than 30 years. The very first IBM PC had a BIOS. And despite extraordinary advances in hardware and software, the BIOS we still puzzle over today is not much different from the one in that original PC.

Essentially a miniature OS, the BIOS has a simple but critical function — when a PC powers up, the BIOS checks that all hardware is in order (the POST or "power-on self-test" sequence); fires up the full operating system on the machine, such as Windows (using OS loader code); and then hands all control of the computer over to the OS.

Although older operating systems (such as DOS) relied on the BIOS to perform input and output functions, modern OSes (including Windows) have their own device drivers and completely bypass the BIOS after they're up and running.

These days, it's rare that a PC user is forced to invoke the BIOS's cryptic and somewhat enigmatic user interface. Usually, it's in response to some near-catastrophic system failure.

The Unified Extensible Firmware Interface (UEFI) is essentially the next generation of BIOS. It's a system that potentially offers new and more advanced control of the boot-up process. If your PC is less than two or three years old, chances are good that it already has UEFI (<http://www.uefi.org/home/>) capabilities. Chances are very good that you didn't know that, because the hardware manufacturers have been carefully keeping the old BIOS interface as your default boot system. But that will change with Windows 8.

How UEFI is different from/better than BIOS

The standard BIOS has all sorts of problems, not least of which is its susceptibility to malware. For example, there are rootkits that hook themselves into the BIOS OS-loader code, permitting them to run underneath Windows. They're difficult to remove and will re-infect Windows over and over.

And because the BIOS sits on a chip on the motherboard, it's more difficult to update than an operating system or an application. So most PC users never update their BIOS, leaving the PC possibly incompatible with newer operating systems. (The early PC BIOS was hard-coded on a chip, so upgrading required replacing the entire chip or PROM.)

The UEFI is a more sophisticated system that runs before your primary OS kicks in. Unlike the BIOS, UEFI can access all PC hardware, including the mouse and network connections. It can take advantage of modern video cards and monitors. It can even access the Internet.

And as you can see in Figure 1, UEFI offers a modern, easy-to-decipher user interface. It could make dual-booting simpler, more visual, and controllable by mouse or touch. If you've ever played with your BIOS, you discover that UEFI is in a whole new dimension.



Figure 1. The Asus.com website offers this view of a UEFI-interface screen — clearly, an improvement over the typical BIOS UI we're faced with today.

Unlike the BIOS, the UEFI can exist on a disk, just like any other program — or in non-volatile memory on the motherboard or even on a network share.

At this point, it's important to note that systems can run either the BIOS or the UEFI — or both. When they're both used, the BIOS goes first to run POST, then the UEFI takes over and hooks into any calls that may be made to the BIOS. (Windows typically doesn't make calls directly to the BIOS, but other operating systems might — and the UEFI will handle them, not the BIOS.)

The UEFI can also run without the BIOS — it can take care of all OS loading/interface functions previously handled by the BIOS. The only thing the UEFI can't do is perform the POST or run the initial setup (configuring the CPU, memory, and other hardware). PCs that have the UEFI but no BIOS have separate programs for POST and setup that run automatically when the PC is powered on.

As we all know, the BIOS initialization process — including POST — seems to take a long time. The UEFI, on the other hand, can run quickly.

Moreover, a BIOS is easily reverse-engineered and typically has no internal security protection, making it a sitting duck for malware. A UEFI can run malware-dodging techniques such as policing operating systems prior to loading them — which might make rootkit writers' lives considerably more difficult. For example, the UEFI could refuse to run operating systems that lack proper digital security signatures.

And that's where the UEFI controversy begins.

Windows 8 will implement UEFI in new ways

Back in September, Microsoft wrote voluminously about the UEFI in Windows 8. The first post, (<http://blogs.msdn.com/b/b8/archive/2011/09/20/reengineering-the-windows-boot-experience.aspx>)

"Reengineering the Windows boot experience," talks about the basic ways Windows 8 will use the UEFI. (If your PC doesn't support a UEFI, Win8 should still work fine.)

The article shows how current text-based, boot-time options, such as system repair store and image recovery, can be made more usable with a new graphical interface. The story goes on to describe how system startup could go, in seconds, from power-on to Windows Desktop without so much as flickering the screen. It also shows how dual-boot will work with a graphical face-lift.

The changes appear to be largely cosmetic, but they're long overdue and a welcome improvement to the constrained, DOS-era recovery environments under which Windows operates.

The second article (<http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx>), "Protecting the pre-OS environment with UEFI," shows how the UEFI secure boot — using Public Key Infrastructure (PKI) digital certificates — validates programs, peripherals, and OS loaders before they can run. The system can go out to the Internet and check whether the UEFI is about to run an OS that has had its certificate yanked.

If it sounds a lot like Secure Sockets Layer protection — no stranger to controversy, there certainly are similarities.

Microsoft states it will let the hardware manufacturers struggle with the difficult question of who controls the digital-signature keys. "Microsoft supports OEMs having the flexibility to decide who manages security certificates and how to allow customers to import and manage those certificates, and manage secure boot. We believe it is important to support this flexibility to the OEMs and to allow our customers to decide how they want to manage their systems."

Still, Microsoft is ensuring that anyone buying a certified Windows 8 PC can rely on a certain level of protection from rogue OS loaders. "For Windows customers, Microsoft is using the Windows Certification program to ensure that systems shipping with Windows 8 have secure boot enabled by default, that firmware not allow programmatic control of secure boot (to prevent malware from disabling security policies in firmware), and that OEMs prevent unauthorized attempts at updating firmware that could compromise system integrity."

The controversial side of dual boot

When those details first hit, the Linux community flew up in arms. Dual booting between Windows 8 and Linux might

Continued from page 4

require a digital signature from a recognized certificate authority. That authority might be Microsoft, through its Windows Certification program, and Linux folks would have to pay the piper.

That controversy went on for a while but eventually died down (though it never disappeared) when it became clear that putting together the signature is relatively easy and not very expensive.

Then another conflagration started last week. To understand why, you have to understand that UEFI secure boot has two bail-out options. First, most PCs let you turn off UEFI secure boot entirely. You have to be sitting at the computer and do it manually, but it's easy enough. In one of the Microsoft postings mentioned previously, the company acknowledged that hardware manufacturers could "allow customers to ... manage secure boot."

Second, there's a provision for something called "custom secure boot mode" in which you, as a customer, can sit at your computer and type in a signature for any OS loader you like. This manually created whitelist overrides the Windows 8 or third-party check, letting the UEFI run OS loaders unhindered.

You must also understand that Windows 8 will run on two entirely different hardware platforms — Intel/AMD platforms spanning the range from tablets to full-size desktops, and the tablet-friendly ARM platforms. If you use Win8, one of your first decisions will be which platform you choose.

The Linux world was taken aback when researcher Glyn Moody and the Software Freedom Law Centre announced last month in a blog that Microsoft is making specific demands from hardware manufacturers who intend to sell Windows 8 bundled with their ARM machines — that is, those lightweight Windows 8 tablets. The Microsoft restrictions prevent hardware manufacturers from disabling secure boot and also prevent hardware manufacturers from implementing "custom secure boot" whitelists — but again, only on ARM hardware.

In other words, if at some point in the future you buy an ARM-based tablet with Windows 8 preinstalled, you won't be able to dual-boot with Linux or any operating system other than the ones that pass the security check. Presumably that could mean Windows 8 or some later version of Windows that Microsoft might ordain in the future.

Aside from the fact that the restrictions fly in the face of what Microsoft specifically said in September, it's hard for me to get too worked up about them. If you buy a Win8 (ARM) tablet, you won't be able to root it (<http://en.wikipedia.org/wiki/Rooting>), and you may not be able to upgrade it. You'll just have to take that into account when you think about buying one — assuming Microsoft is up-front about the limitation and mentions it to consumers.

Intel-based Windows 8 machines — even tablets (including tablets that run only the Metro interface) — aren't hobbled by those ARM restrictions. At least at this point, Intel/AMD machines are, in fact, required to allow multi-booting (with signed operating systems) and even to replace Windows 8 with an OS of your choice. It remains to be seen whether Microsoft's going to change its mind about that distinction.

It's a brave new world out there, with Win8 tablets going up against the iPad 3 later this year. Stay tuned!

Viper lowers PC prices as Hard Drive prices stabilise

Viper, one of the few companies to just as quickly put their prices down when parts cost fall, have made price cuts in their range across the board.



From **£100** slashed from the price of the top of the range Viper SuperSnake, to **£30** off the Viper "G" series, the whole range has had price cuts to make them even better value for money. Considering that all vipers now have a 3 years hardware warranty, the Vipers slash whole life costs to a fraction of that of the big named brands.

Even our most popular PC tower, the **No Frills** has had a revamp.

The No Frill Plus is no more, but the good news is, the new **No Frills Tower** has the full specification of the old No Frills Plus.

So you can now get an Intel 2.6MHz dual core processor, 250Gb SATA hard drive, 2Gb of superfast RAM and Windows 7 home premium 64 bit all for just **£250** inc vat.

A quality PC at supermarket prices, and the backup of the Computer Doctors.

<http://www.computerdoctors.co.uk/shop/desktop.htm>

Welcome to the 64-bit era of Windows

In the brave new world of huge software packages and gigantic memory requirements, capacity counts.

Here's what you need to know about upgrading from 32-bit to 64-bit machines — because sooner or later, upgrades will happen to you.

The new norm: 4GB of RAM and 500GB hard drives

The average PC sold today, desktop or notebook, has a 500GB hard drive, 4GB or more of RAM, and a blazing graphic processor — and costs less than the horse-and-cart systems of the pre-Windows XP days. The escalating demand for hard-disk space and processing power is driven by the powerful software we now use and by ever-larger data files — especially digital images and video. Mindful of the need to let users adjust to change yet still have the option of upgrading legacy 32-bit machines, Microsoft offered both 32-bit and 64-bit versions of Windows 7 on the same retail installation disc, right from launch.

Although many Windows XP users still cling to their 32-bit systems as if they were life jackets on the Titanic, many more are moving to Windows 7 — and a surprisingly large number of those machines are 64-bit editions. Here's why that change is good.

The move to 64-bit and Win7 goes hand in hand

Unlike any previous version of Windows, the use of a 64-bit operating system is tied closely with the rapid uptake of Win7. In July 2009, for example, Amazon.co.uk had more pre-orders for Win7 in just eight hours than it had had for Windows Vista in that OS's first 17 weeks, according to a July 2009 BBC report. (<http://news.bbc.co.uk/1/hi/technology/8151342.stm>) Windows 7 quickly became the fastest-selling OS in Microsoft's history.

And a lot of those sales were Win7 x64. A Microsoft blog stated that by June 2010, 46 percent of all PCs were running a 64-bit edition of the OS. It went on to report that only 11 percent of Vista PCs were using the 64-bit edition — three and a half years after that OS launched. The blog noted that 77 percent of April 2010 retail PC sales were Win7 x64 machines. That's an astounding change.

Using 32-bit software: apps, yes; hardware, no

The first rule of using 32-bit code on Win7 x64 is that hardware drivers won't run. You must use 64-bit hardware drivers for all internal and external devices.

Fortunately, the same is not true for applications. Just about any 32-bit Windows app that runs on XP will run without a snag on a 64-bit Windows system. That's because of an integrated technology called Win32 on Win64 (WOW). This Win7 subsystem converts 32-bit API-call executables into 64-bit APIs. But the technology isn't perfect. Although these converted executables work most of the time, they can fail if a particular application relies on proprietary, legacy 32-bit device drivers.

Another problem: On first look, it doesn't seem that 32-bit apps have Registry entries. They do, but they're buried in a subkey of a subkey. To maintain the integrity of the 64-bit Registry, Windows redirects 32-bit installed apps to the Wow6432Node key located below the primary Software key. You have to expand this key to see the 32-bit keys and values. For more on this, see Microsoft's "32-bit and 64-bit application data in the Registry" page. (<http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072%28v=VS.85%29.aspx>)

The ease of finding 64-bit hardware drivers has improved greatly since Win7 was first released. Peripheral manufacturers have even updated many older, legacy hardware with 64-bit drivers. The two best resources for 64-bit drivers are the hardware vendors' websites and Microsoft's Windows 7 Compatibility Centre (<http://www.microsoft.com/windows/compatibility/windows-7/en-us/default.aspx>).

Future-proofing: 64-bit provides power to spare

As Microsoft points out, "A computer with a 64-bit version of Windows can use more memory — 4 GB (gigabytes) or more — than a PC with a 32-bit version of Windows, which is limited to about 3.5GB or less. (Even if a PC comes with 4GB or more of memory installed, a 32-bit version of Windows can use only about 3.5GB of that memory.)"

With the relatively low price for RAM these days, it should be no surprise that 4GB is the default configuration on most new PCs. Although 2GB is the minimum RAM required for running Win7 x64, 4GB is recommended to make good use of 64-bit processors and operating systems. (Up to a point, more RAM installed translates to more apps you can have open without loss of speed.)

There are some limitations to the amount of RAM that a particular version of Win7 x64 can support. For example, Windows 7 Professional, Enterprise, and Ultimate can address up to 192GB of RAM; Home Premium, by far the most common version installed today, supports 16GB; however, Windows 7 Home basic is limited to just 8GB. That's still an impressive — and usually excessive — amount of RAM for most personal computing use.

Better security with a 64-bit operating system

Even the most passionate Windows XP user has to admit that it was a malware nightmare; we survived years of what seemed like endless rounds of patches. Antivirus protection is better in all versions of Windows 7, but even more so in 64-bit versions. While we still get security fixes for the 64-bit operating systems, these fixes are far fewer than on 32-bit systems.

There's a significant reason a 64-bit OS is more secure: malware written as 32-bit software will usually not run on an x64 system. For example, it would be difficult for a 32-bit virus or rootkit to modify the 64-bit Win7 kernel.

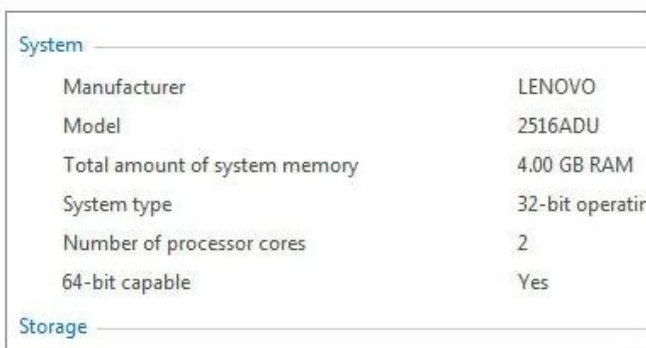
When the time comes to update to Win7 x64



If you've decided to move to the 64-bit version of Win7, you have essentially two options: buy a new PC with Win7 x64 already installed, or add it to your existing system. The former is obviously the easiest route. You'll know that all installed components and drivers are 64-bit compatible.

Whether you can upgrade an existing system depends on the age and design of its components — primarily the BIOS and CPU. Start by running the Windows 7 Upgrade Advisor (<http://www.microsoft.com/download/en/confirmation.aspx?id=20>). Once the advisor app finishes examining your system, its 64-bit report page will tell you whether you can safely install Win7 x64. As shown in Figure 1, you might have to install the OS and then reinstall your apps and data. It's a bit of work, but it should give you a clean system.

Figure 1. Windows 7 Upgrade Advisor's 64-bit report can determine whether your system is Win7 x64-ready.



If you're already running Windows 7 x32 and want to upgrade, use the Performance Information tool already included with Win 7. Click Start/Control Panel/Performance Information and Tools. Under Base score, click the View and print detailed performance and system information link. In the Systems section, you'll see a 64-bit-capable listing, as shown in Figure 2.

Figure 2. If you want to know the system type of your current Win7 installation and whether your system is 64-bit-ready, run Win7's built-in Performance Information tool.

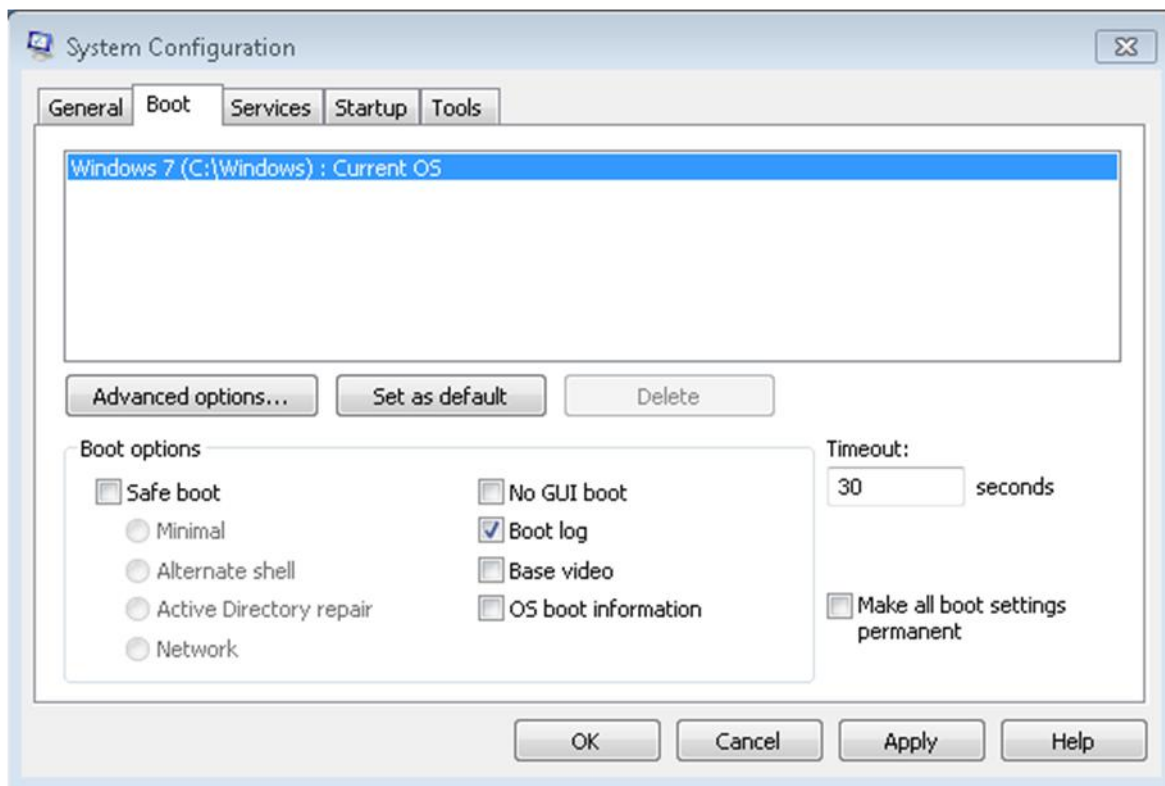
Finally, I recommend you check out Microsoft's Windows 7 Compatibility Centre for a list of compatible third-party hardware and software. (<http://www.microsoft.com/windows/compatibility/windows-7/en-us/default.aspx>)

Windows 8, now available as a developer's preview download, comes in 32-bit and 64-bit flavours. (It currently has the same system requirements as Windows 7.) Given the proliferation of 64-bit hardware and, more slowly, 64-bit apps, it will be interesting to see who's not using the 64-bit version of Microsoft's next OS.

Using Windows “Safe Boot” To Diagnose and Repair Problems

When something goes wrong with Windows it can be very difficult to diagnose or repair, and there are times when booting your computer into Safe Mode just isn't good enough. Safe Mode, a special diagnostic mode built into Windows strips the OS of all drivers and start-up software and presents you with a very limited version of Windows in which to diagnose what might be causing a problem, and repair it. Many Windows features simply won't operate in Safe Mode so there's not very much you can do.

Fortunately though there is an alternative and it's in every version of the operating system (XP, Vista and Windows 7). This is called “Safe Boot” and you can find it in the MSConfig panel. To open this type **msconfig** into the Start Menu search box in Vista or Windows 7, or run **msconfig** from the run option in XP.



Under the Boot tab in the MSConfig window you'll see the Safe Boot option as a tick box. Turning this on, will make Windows use the Safe Boot option every time thereafter. When you want to stop using Safe Boot and return to starting Windows normally you'll need to return to the MSConfig panel and untick this option. There are also several other options here including Minimal Boot, which will take you into the full Safe Mode, but the standard option will normally be enough for most people.

The Safe Boot screen, is a half-way house between the full Windows desktop and Safe Mode. What you will find though is that most of your hardware drivers will be installed and working though your startup software will still be disabled.

So when might you want to use Safe Boot? Occasionally you will encounter a problem in Windows that you will need to go into Safe Mode to repair. As I mentioned earlier however Safe Mode won't allow you to perform some Windows tasks, and this is where the Safe Boot mode is useful. You may also suspect that your problems aren't being caused by a hardware driver, but by software instead. This diagnostic mode enables you to have a full Windows desktop where nothing loads at startup and where you can run and check programs individually to see what effect they are having on your system.

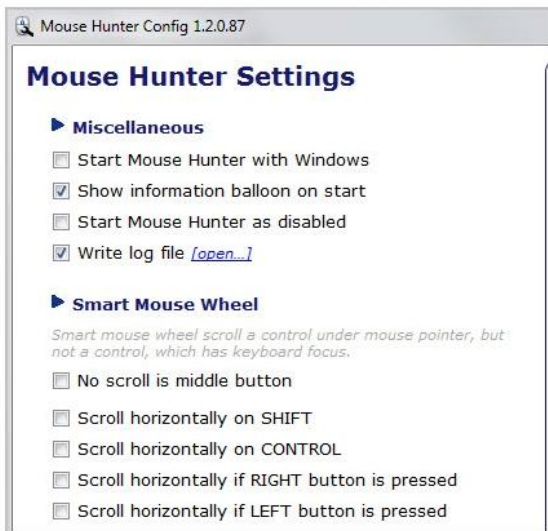
As I have already mentioned Safe Mode is extremely limiting, not just in the very low screen resolution that it gives you. If you need to run full diagnostics on your copy of Windows, to see what's going on inside, or if you need to test individual software packages in a safe environment where they will be able to run properly then Windows Safe Boot is the way to do it.

Remember though that you will need to turn off Safe Boot when you are done, or else Windows will start permanently in this mode. I have found this to be a very useful diagnostic tool in Windows and it's extremely underused because, frankly, many people simply do not know that it exists. Hopefully you will find it useful too.

How To control Non-Active Windows With The Mouse

You can only control the active window with your mouse in a default Windows installation. If you need to do something in another window, you need to activate it first, before you can do so. This can for instance be done with a left-click on the window, the program's taskbar or system tray icon, or a keyboard shortcut like Alt-Tab to bring that window to the front.

Sometimes though you just need to work in that window for a second or so before you continue your work in the other window. This can be you blogging and listening to music at the same time, if you want to skip a song or change the volume for instance. It could also be useful in Windows Explorer when you want to drag and drop files to a folder that is not



visible in the file manager's sidebar. With Mouse Hunter installed and running in the background, you can control some window functions with your mouse even if that window is not active. This includes scrolling the window up or down or using other functionality that is assigned to the mouse wheel. For media players like SMplayer, this could mean going forward or backwards, or changing the volume of the media that is playing currently.

Another application is in Windows Explorer, where I may have selected some files that I want to move or copy to another folder in the sidebar. Once selected, I cannot scroll the sidebar without losing focus on the selected files.

Windows users who like to test the program's functionality can download it from the developer's website. The program is free-ware and compatible with 32-bit and 64-bit editions of the windows operating system.

<http://www.amlpages.com/mousehunter.shtml>

What is the Difference Between Malware, Virus, Root-kits, Spyware, Worm and Trojans

Whenever your computer starts acting weird and makes it difficult for you to work on, the first thing that comes to you mind is whether a virus has affected your computer.

Some of those times, your fears might turn out to be true. Hence it helps to know about these enemies of your computer and get a basic understanding of how they work. That could help you deal with them in a faster & better way.

Malware is any malicious program or software that's designed to exploit a computer user. Malware is basically an umbrella term covering computer viruses, worms, Trojan, spyware, rootkit etc. Some of them attack the computer programs and files while others attack users confidential data. Let's have a detailed look at their mode of operation.

What is a Virus

Just as a biological virus replicates itself in a human cell, a computer virus replicates itself in computer memory when initiated by the user. Not only do they replicate themselves but they may also contain some malicious codes which can affect your files, your operating system or even your master boot records thereby making your computer start slow or not boot at all.

There are different types of viruses, some affect the system adversely and leave it completely unusable while some are just written to annoy the user. Disabling task manager or desktop wallpaper is one of the most common ways that virus creators employ to irritate users.

As a virus always needs a human action to initiate itself, in a computer most of them attach themselves to an executable .exe file because it knows eventually the user will double click on it to run it and that's all it needs to infect the computer. Yes, unfortunately, most viruses are inadvertently initiated by the computer users themselves and hence it is important that when you install and run programs, you know beforehand that you got them from a trusted source.

What is a Worm

Practically a worm is an evolved form of a virus. Like virus, worms too replicate and spread themselves but it happens on a bit larger scale. Also, unlike a virus, a worm does not need a human action to replicate and spread and that's what makes it more dangerous.

A worm always seeks for network loopholes to replicate from computer to computer and thus the most common way of intrusion are emails and IM attachments. As the infection is network-based, a good firewall along with antivirus is necessary to control worm attack. Also, this means that blindly downloading email attachments or clicking the links friends share with you in a chat window isn't recommended. Double-check before you do that.

What is a Trojan Horse

Trojan horse or simply Trojan is a bit interesting. Trojan horse is a program that appears useful by pretending to do certain things in foreground, but in reality they are working silently in background with the only objective of harming your computer and/or stealing valuable information.

Most common way to invite a Trojan horse to your computer is downloading malicious software like keys, cracks, free illegal music, wares etc from an unknown source. Thus the best way to stay away from Trojans is by making sure you install software from trusted sources.

What is a Spyware

Spywares are also malicious computer programs that can be installed on computers but unlike any of the above they don't harm your computer in any way. Instead, they attack you!

Once installed on a system they run in background and keep on collecting user's personal data. These data can include your credit card numbers, passwords, important files and many other personal stuff.

Spywares can track your keystrokes, scan and read your computer files, snoop IM chats and emails. Therefore again it's always advisable to download and install software from trusted sources.

What is a Rootkit

A rootkit, on the other hand, is devious in a different way. This unwanted code on your desktop is used to gain control over your desktop by hiding deep inside your system. Unlike most viruses, it is not directly destructive and unlike worms, its objective is not to spread infection as wide as possible.

So what does a Rootkit do?

What it does do, is provide access to all your folders – both private data and system files – to a remote user who, through administrative powers, can do whatever he wants with your computer. Needless to say, every user should be aware of the threat they pose.

Rootkits generally go much deeper than the average virus. They may even infect your BIOS – the part of your computer that's independent of the Operating System – making them harder to remove. And they may not even be Windows-specific, even Linux or Apple machines could be affected. In fact, the first rootkit ever written was for Unix!

Is this a new phenomenon?

No, not at all. Possibly the most famous case so far was in 2005, when CDs sold by Sony BMG installed rootkits without user permission that allowed any user logged in at the computer to access the administrator mode. The purpose of that rootkit was to enforce copy protection (called "Digital Rights Management" or DRM) on the CDs, but it compromised the computer it was installed on. This process could easily be hijacked for malicious purposes.

What makes it different from a virus?

Most often, rootkits are used to control and not to destroy. Of course, this control could be used to delete data files, but it can also be used for more nefarious purposes.

More importantly, rootkits run at the same privilege levels as most antivirus programs. This makes them that much harder to remove as the computer cannot decide on which program has a greater authority to shut down the other.

So how I might get infected with a rootkit?

As mentioned above, a rootkit may piggyback along with software that you thought you trusted. When you give this software permission to install on your computer, it also inserts a process that waits silently in the background for a command. And, since to give permission you need administrative access, this means that your rootkit is already in a sensitive location on the computer.

Another way to get infected is by standard viral infection techniques – either through shared disks and drives with infected web content. This infection may not easily get spotted because of the silent nature of rootkits.

There have also been cases where rootkits came pre-installed on purchased computers. The intentions behind such software may be good – for example, anti-theft identification or remote diagnosis – but it has been shown that the mere presence of such a path to the system itself is a vulnerability.

Conclusion

Most of the malware that we have discussed have been there probably since the innovation of programming itself and with time, they've become more complex and harder to deal with. That doesn't mean you should worry too much. We have talked about tools like virus scanners and spyware removers before so make sure you keep your computer protected with them. If you are careful enough, most likely you won't have to worry about them.

Our price list

On-Site Rates

Standard call out charge and hourly rate	£69 callout, 1st hour free + £35 per ½ hr (+ parts)
New PC or laptop setup (home users only) + Data transfer from old PC to new (Business Users –all onsite work at hourly Rate - top)	£49 if PC purchased from us, £99 if purchased elsewhere £50 1st user + £25 per additional user

Remote Repair & Support

Remote Repair (max ½ hour)	£19.95 in advance *
Remote Repair Standard Contract	£6.99 per month (£79.95 year)
Remote Repair Plus (Includes 4 free workshop visits per year)	£9.99 per month (£99.95 year)

(Remote Repair is only available to domestic home users, or a business user based as a single user)
(*£10 refund towards workshop or onsite repair if fault not cleared during remote session)

Workshop Rates

Standard rate	£25 per ½ hour
Standard PC & Laptop repair	£79 + parts
+ Data backup (During a PC Repair)	£50 1st user+ £25 per additional user
+ Home setup (On-Site, after repair)	£39
+ standard Security pack & critical updates (During a PC Repair)	£20 (antivirus, anti-spyware & file cleaner)
+ Security pack advanced (During a PC Repair)	£25 (Kaspersky internet security) £40 (Kaspersky I.S. 3 user licence)
Standalone - Backup data from working PC	£50 1st user + £25 per additional user
Standalone - Backup data from non-working PC	£79 1st user+ £40 per additional user
While you wait service (max ½ hour)	£25 + Parts
Automated hardware diagnostic (requires to boot to test CD)	F.O.C.
Manual System diagnostics (not charged if proceeding with repair)	£30
Virus / Malware Removal (from a working PC)	£59 (see standard PC repair for non working PC)
Data recovery standard (memory card, pen disk, hard drive)	from £80 per drive
Data Recovery advanced (e.g. broken hard drive)	from £350 (£30 deposit required)
Engineers Report (for Insurance company)	£25

Laptop hardware Repairs

Laptop replacement screen	£60 + cost of screen
Laptop screen backlight repair	£95 inc parts (£30 deposit required)
Laptop screen inverter repair	£115 inc parts (£30 deposit required)
Laptop power socket replacement	£85 inc parts (£30 deposit required)

We no longer send laptops to a specialist repairer for motherboard repairs. Due to the complex nature of the repair, we are not convinced that this method is proving to be a long term permanent repair. We can supply a contact number if you wish to pursue this method of repair, but we would recommend a replacement motherboard, if available.

For full details of each repair please see our website: www.computerdoctors.co.uk/pages/rates.htm

For full details of Remote Repair see our website: www.computerdoctors.co.uk/care or click support on any page.

vat @ 20% is included in all our prices.

View from the Backside

Best-paid Tube driver is on £61,218 a year



London underground driver, Jai Dev was exposed this week as the "Best paid Tube Driver" in the recent scandal. Unfortunately, his car gave him away. Its not hard to spot a Bugatti Veyron in a works car park full of Rover 200's.

Jai who lives in a 14 bedroom mansion at Greenwich said, "Its not unusual for drivers to earn this amount, especially with our new "smile" bonus".

Apparently, Drivers can also earn a "customer service bonus" of £250, which is paid depending on passenger satisfaction levels. "I give-em a smile and chat-em up a bit and get the bonus every time", said Jai.

Jai's bumper wage is made up of £42,424 basic wage, £13,151 Pension contribution and the rest overtime.

Jai, known to his work colleagues as "Bollywood" because he once had a walk-on part in an Indian movie, makes no secret of the fact that his TfL (Transport for London) job only brings in pin money. "I'm the man to see in my manor if you want a short term loan, popular rates of interest - well we like-em", jokes Jai. "My latest venture is a London based removal business", he said, "if you've got a house and the tenant don't want to move out , me and my colleagues help them decide".

"I'm also big in garden centres", he said, "we've had such a big demand for our plants that we've had to sub contract the growing to other entrepreneurs. You see I believe in spreading my wealth around, that way we all benefit. Some of my sub contractors have converted all the rooms in their houses so that they can grow more plants". "It's a big outlay with the lights and all, but I usually help with a small loan to get them started, so its win, win for me".

Well, it's nice to see someone working hard and getting their just rewards. In these days of penny pinching and austerity, it shows that with a bit of hard work and a job on London Underground, anyone can make their life bearable.

Computer Doctors Ltd
Blackthorn Workshop.
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.co.uk/newsletter



Map to our Blackthorn Workshop
www.computerdoctors.co.uk/pages/map.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: 0872 115 5359

Email: sales@computerdoctors.co.uk

Shop: www.computerdoctors.co.uk/shop

Technical Support

Free: tech@computerdoctors.co.uk

Remote: www.computerdoctors.co.uk/care

Web: www.computerdoctors.co.uk/pages/askthedoc.htm