

# Computer Doctors Newsletter

So here we are again, three and a bit weeks to Christmas and I'll bet you're like me and haven't bought any Christmas presents yet. There are a few well organised people among us that have been planning Christmas since July and have presents wrapped and labelled and Christmas cards stacked and stamped, ready to go.

Fortunately, all my relatives are the well organised variety, so all their presents for me are almost certainly ready to be dropped into my sack on Christmas eve. Ready for Santa to claim all the credit.

**But what to buy them, that's the question! I usually end up on Christmas eve, raiding the Computer Doctors parts bins in desperation. (My boss lets me pay monthly for the rest of the following year at a very advantageous interest rate. He says the experience will stand me in good stead for when I'm old enough to get a mortgage).**

Last year I got my brother a 2Gb pen disk and the year before that a web cam. This year I've got him a really good set of PC speakers so that he can listen to all his music. I just hope, this year, someone finally buys him a computer!

So this is me, Craig the trainee, wishing all our customers a very merry Christmas and a happy, healthy and prosperous new year.

## Audio and Video Conversion Programs

The ready availability of audio and video material in digital format has allowed all of us to have access to a huge range of content with an ease and accessibility never before possible.

This wonderful blessing has, however, been tarnished by the proliferation of different audio and digital media formats. The existence of so many formats has meant that seemingly simple tasks, such as transferring a YouTube video to your iPod or making an MP3 file from a DVD soundtrack, can end up being complex tasks, so complex that they become nearly impossible for non technical users.

In response to this situation we have seen the market flooded by expensive commercial media conversion programs, some costing up to £100. The good news is that there are many free media conversion programs available that will do the job just as well as their commercial cousins.

My long-time favourite has been "Super" [1]. It's really no more than a user friendly interface for a variety of command line conversion programs.

It has two great strengths: first, it's reasonably easy to use, and secondly it handles a large number of different file formats. For example, with video files it handles 3gp/3g2 (Nokia, Siemens, Sony, Ericsson), asf, avi (DivX, H263, H263+, H264, Xvid, MPEG4, MSmpeg4, etc), dat, fli, flc, flv (used in Flash), mkv, mpg (Mpeg I, Mpeg II), mov (H263, H263+, H264, MPEG4,

etc), mp4 (H263, H263+, H264, MPEG4), ogg, qt, rm, ram, rmvb, str (Play Station), swf (Flash), ts (HDTV), viv, vob, and wmv. It also handles audio file format conversion including ac3, amr, mp2, mp3, mp4, ogg, ra, wav, and wma.

The download link for Super on the author's site is quite hard to find so I've listed an alternative download site [2].

An alternative to Super is MediaCoder [3]. It has the advantage of being open source and, arguably, is a little easier to use. It doesn't handle some of the formats handled by Super but is being continuously expanded by its authors. iPod and PSP owners will appreciate the special features for these devices that makes usage particularly straight-forward.

If you are mainly interested in just video conversion then check out "Any Video Converter" [4]. It has a better interface than either Super or MediaCoder and is very fast as well. Input formats include DivX, XviD, MOV, rm, rmvb, MPEG, VOB, DVD, WMV and AVI. It's set up to make MP4 conversion as simple as possible, but it can handle other output formats if you are prepared to delve into the options.

[1] [www.erightsoft.net](http://www.erightsoft.net)

[2] [www.afterdawn.com/software/video\\_software/video\\_encoders/super.cfm](http://www.afterdawn.com/software/video_software/video_encoders/super.cfm)

[3] <http://mediacoder.sourceforge.net/>

[4] [www.download.com/Any-Video-Converter/3000-2194\\_4-10611989.html](http://www.download.com/Any-Video-Converter/3000-2194_4-10611989.html)

### Special points of interest:

- Demand for low cost high spec Viper PC, breaks all records.
- Microsoft finally give security advice to home users too
- Storm Worm and friends have control of one in four PC's!
- In depth technical look at managing your PC without collecting Viruses and Spyware
- MSCONFIG essential tool for budding computer geeks



### Inside this issue:

Audio & Video Conversion.	1
Storm Worm Latest	2
File search utilities	2
Office 2007 security guide	2
Font Frenzy	3
Windows Home Server	4
An Internet PC with no viruses or spyware.	5



## Search Files Without Using a Desktop Search Utility

Desktop search programs like X1 or Google Desktop Search allow you to quickly find any file on your PC by filename or by any phrase contained within the file.

However, these programs carry a high overhead. Creating and maintaining the indexes eats up a lot of processor power, and the indexes themselves take up a lot of disk space.

If you only occasionally need to search all the files on your PC for a specific phrase, you don't need a full desktop search program. You can achieve the same result in other ways and avoid the unnecessary overhead.

The first option is to use the search feature built into Windows but it's agonizingly slow. So slow that you would only ever use it as a last, desperate resort. Besides, it's a resource hog as well. That's why many experienced users turn off the automatic Windows indexing service.

The second option is to use a Grep style search tool. Grep is a famous UNIX command line utility but there are several free versions for Windows, including BareGrep [1] and GNU Grep for Windows [2]. Both, however, are rather too technical in their usage and not suitable for average users. Rather more friendly is the GUI based Wingrep [3] program. It's a fast and very powerful product, but unfortunately it's shareware, not freeware.

The third option is to use a dedicated non-indexed search utility such as the freeware program Agent Ransack [4]. Ran-

sack is a great product but it has somewhat limited search features compared to its shareware "big brother" called File Locator Pro. However, if you can live with its reduced feature set it's a great freeware solution.

A final option is to use the search feature built into some File Managers. Among the best of these is XYplorer [5]. XYplorer can search for both file names and file contents and has powerful search specification options, including the ability to limit the search to specific drives, folders, file types, creation dates, size, file attributes and more. Furthermore, the speed of the inbuilt search is simply amazing.

XYplorer is shareware but you can get the last free (for personal use) version from here [6]

Overall XYplorer gets my recommendation as the best free non-indexed solution to finding files and file content quickly and easily. As a bonus you'll also get an outstanding file manager and a great replacement for Windows Explorer as well.

[1] [www.baremetalsoft.com/baregrep/index.php](http://www.baremetalsoft.com/baregrep/index.php)

[2] [www.steve.org.uk/Software/grep/](http://www.steve.org.uk/Software/grep/)

[3] [www.wingrep.com](http://www.wingrep.com)

[4] [www.mythicsoft.com/agentransack/](http://www.mythicsoft.com/agentransack/)

[5] [www.xyplorer.com/product.htm](http://www.xyplorer.com/product.htm)

[6] [www.321download.com/LastFreeware/page22.html#XYplorer](http://www.321download.com/LastFreeware/page22.html#XYplorer)

## Microsoft Security at home

Microsoft publishes various online guides to security, and finding all the information you need can often be confusing. But here's one page that brings together lots of useful facts and links for home users and it's well worth adding to your web favourites. In addition to containing details about the latest patches and fixes that Microsoft has issued, and advice on how to download and install them, there are also topical tips such as how to prevent your neighbours from borrowing your wireless Internet, how to handle suspicious email messages, how to avoid online donation scams and how to stay safe when you're using a public computer.

[www.microsoft.com/protect/default.msp](http://www.microsoft.com/protect/default.msp)

## MS Office 2007 Security Guide

Microsoft has published an excellent set of documents aimed at helping you ensure that Office 2007 is configured for optimum security. If you use Office 2007 at home or at work, and you want to ensure that your computer and your files remain out of the reach of hackers and viruses, this is well worth reading.

[www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.msp](http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.msp)

## Storm Worm Gets Even Sneakier

A particularly nasty piece of malware called the Storm worm (also known as Dorf and eCard) is believed to have infected up to 50 million PCs worldwide. The infected machines form a huge botnet (<http://en.wikipedia.org/wiki/Botnet>) under the control of the criminals behind Storm. This turns **your PC into a "Zombie" and uses your Internet connection**, without you knowing, to send spam, Trojans, viruses and all manner of other malware to other poor unfortunates.

One of the nastiest aspects of the worm is that it is constantly being updated on the infected machines to avoid detection. According to Sophos analyst Richard Cohen the latest trick in its ever increasing defensive repertoire is to neutralize a wide range of anti-virus software products but instead of killing the antivirus, it leaves it running. Users thus think they are protected while in reality they are infected. The worldwide estimate of one in four computers being a Zombie, doesn't surprise us in the least. Some users never scan their **PC's for viruses or spyware or would even know what to do if** their antivirus program found something. Fortunately, our customers are much more knowledgeable, as the number of calls we get on virus/spyware matters proves.

[www.sophos.com/security/blog/2007/10/682.html](http://www.sophos.com/security/blog/2007/10/682.html)



## Microsoft Security Updates

November's set of security patches from Microsoft contains just 2 fixes, one of which is described as important and the other as critical. If your PCs are set to download and install updates automatically then you should already be protected, but it's always a good idea to visit Microsoft's security website occasionally and opt for an automatic check to ensure that you're not missing any important updates.

The "critical" rated patch, MS07-061, finally fixes a problem that has been known and exploited since mid-year. The flaw meant that a Windows user who clicked on a carefully crafted malicious URL could have his or her PC compromised by a hacker. The problem was originally blamed on Firefox but Windows was the real culprit. The flaw affects all recent

Windows versions.

The "important" patch, MS07-062, affects only Windows Server 2000 and Windows Server 2003. Microsoft says that a spoofing vulnerability exists in Windows DNS Servers and could allow an attacker to send specially crafted responses to DNS requests, thereby spoofing or redirecting Internet traffic from legitimate locations.

Further details of the Microsoft November updates can be found here [1]. All the updates are distributed automatically via the Microsoft Update Service. Dial-up users in particular need to be aware that these updates are large files and will require a considerable period of time online to be successfully downloaded. If you are

not certain that you have received the updates, then visit the Microsoft Update Service [2] now.

[1] [www.microsoft.com/technet/security/bulletin/ms07-nov.msp](http://www.microsoft.com/technet/security/bulletin/ms07-nov.msp)

[2] <http://update.microsoft.com>

## Free tool for managing shared computers

Looking after a shared computer, in either a domestic or business environment, is never easy. Every time others use the machine, they create lots more temporary files, cached internet pages, registry entries, and possibly introduce spyware or adware or viruses which can affect subsequent users. If you've ever used a PC in an internet café and have been jealous of the way that those machines manage to reset everything after each user has accessed the machine, you need SteadyState. It's a free add-on for Windows XP, from Microsoft, which locks down the machine so that all changes made by a user are deleted when they log off.

[www.microsoft.com/windows/products/winfamily/sharedaccess/default.msp](http://www.microsoft.com/windows/products/winfamily/sharedaccess/default.msp)

## Don't get in a frenzy with your fonts

A customer recently contacted us to talk about a problem he'd been having with the fonts on his PC. As he rightly pointed out, whenever you install a program it often comes with a bundle of new fonts and you rapidly end up with hundreds of them on your machine, which can slow down the computer and take up valuable disk space. So he had decided to have a clear-out and managed to remove around 250 unwanted fonts. It was then that he discovered he had another problem. He'd inadvertently deleted a key Windows built-in font, so some of his programs would no longer run. He found the solution to his problem in a neat little freeware program for Windows XP called FontFrenzy. It's a font manager with loads of additional features, such as being able to restore any of the default Windows fonts if you accidentally delete them. It also helps you view, manage, install, delete and preview your fonts.

[www.sdsoftware.org/default.asp?id=5929](http://www.sdsoftware.org/default.asp?id=5929)



## Viper Christmas Special breaks all records for pre-orders

Our flabbers were well and truly gasted with the number of pre-orders received for the Viper "Christmas Special". We had to check with Viper to make sure they were on track with the numbers they had promised us and they are working flat out to keep up with demand. Its not surprising really, with a dual core Pentium processor, DVD dual layer re-writer, 250GB hard drive, 1Gb of RAM memory, Windows Vista Home Premium pre-installed (and disk supplied) and all this for only £299 inc vat. We put it through its paces in last months newsletter and it passed with flying colours. Do not confuse this with machines from Tesco or Asda, this is Viper build quality at supermarket prices. Stock available from 1st December.

[www.computerdoctors.uk.net/shop/vcs.htm](http://www.computerdoctors.uk.net/shop/vcs.htm)



## MSCONFIG—Who He?

MSCONFIG is an extremely useful free utility supplied with Windows that provides an easy way to find out which programs, utilities and services are configured to run in the background every time you start your PC. Even better, it allows you to easily disable programs that you don't need, which in turn can speed up your PC and help to prevent system crashes. Most people know that the more programs you have running on your computer at once, the more likely it is that your computer will either run slowly or even crash. What most people don't know is that every time you boot your computer

a whole mess of "hidden" programs load in the background. Some of these hidden programs are essential, but most aren't. Turning off some of these hidden programs can significantly increase your computer's performance and reliability. Click the links below for your version of Windows and see a step by step guide in using this extremely useful tool.

Windows Vista

[www.netsquirrel.com/msconfig/msconfig\\_vista.html](http://www.netsquirrel.com/msconfig/msconfig_vista.html)

Windows XP

[www.netsquirrel.com/msconfig/msconfig\\_xp.html](http://www.netsquirrel.com/msconfig/msconfig_xp.html)

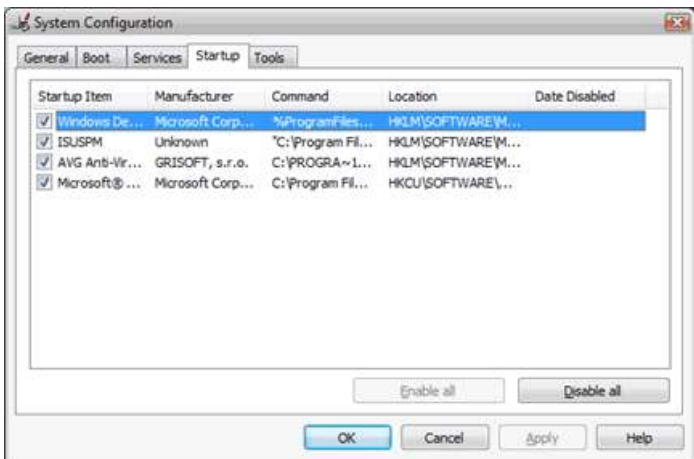
Windows 95, NT or 2000

[www.netsquirrel.com/msconfig/msconfig\\_95\\_NT\\_2000.html](http://www.netsquirrel.com/msconfig/msconfig_95_NT_2000.html)

Windows 98, 98SE or ME

[www.netsquirrel.com/msconfig/msconfig\\_98\\_and\\_ME.html](http://www.netsquirrel.com/msconfig/msconfig_98_and_ME.html)

Tip: There are no spaces in web addresses (URL's). If you are typing the web address manually and you see a space, its an underscore ( \_ ) hidden by the URL's underline. They are meant to be typed all on one line. We break them in half, in the newsletter, to get them to fit in the column width.



## Windows Home server—First impressions

Microsoft is finally shipping Windows Home Server, the latest addition to the Windows family. However, it's an OEM-only product, which means that you can't easily go out and buy a copy to install on an old PC that you happen to have lying about. You can, though, buy it pre-installed as part of a dedicated WHS box, which various companies such as Viper are developing.

Windows Home Server is a superb idea, aimed at the growing number of households that have more than one PC. It's a cut-down version of Windows Server 2003 (no sign of Vista here, thankfully), that helps to ensure that your digital household runs smoothly and efficiently. It'll stream your collection of music and video files to other PCs, for example, as well as to devices such as your Xbox 360. It can even act as a Web server, allowing you and others to browse your pictures and other files via the internet from anywhere in the world, which is just wonderful if you want an easy way to keep in touch with relatives around the world.

In fact, all aspects of Home Server are accessed via a web browser so there's no need to have a monitor or keyboard connected to the machine itself. Just hide it in a cupboard somewhere, plug it into your network, and access it from wherever you wish.



Perhaps the best feature of Windows Home Server is that it provides an easy way to ensure that all household PCs are backed up. Install the client software on all your machines, and they get backed up to your Home Server every night. If anyone loses a file, or even an entire PC, it can be recovered from the Home Server. So is this the backup solution we've all been waiting for? Not entirely.

If you're going to go to the trouble of backing up every machine in your household, you need to be confident that you can recover data after just about every conceivable problem that might occur. Windows Home Server doesn't fully deliver, in my opinion, because there is no off-site backup. So a disaster at your house, like a flood or a fire or a robbery, could mean that you lose all your precious data files and all your backups too.

Still, we're going to give it a fair crack of the whip. We will be evaluating it over the next month or so, on a Viper PC specially built for Windows Home Server. So as they say, "watch this space".

[www.microsoft.com/windows/products/winfamily/windowshomeserver/default.mspx](http://www.microsoft.com/windows/products/winfamily/windowshomeserver/default.mspx)



## An in depth look at how not to get viruses and spyware

After spending years trying to get viruses and spyware off **customers PC's, I've learned an important lesson.**

Don't get infected by malware!

In other words, put maximum effort into preventing infection rather than detecting and removing infection.

This statement may seem bland and unremarkable but there's more to it than you think.

The traditional way of adding additional protection

For a long time I've advocated the best way of protecting your PC was by using multiple security layers based on anti-virus, anti-spyware, anti-Trojans, HIPs and other security software.

It's still a sound approach but I've come to believe that for most folks, the cost is too high and the additional protection afforded too little.

The cost here is not so much financial though that is an issue, but rather the serious impact adding many security layers can have on the performance of your PC.

There is also a cost in complexity. The more security programs you run the more chance they will either interfere with each other or with other programs.

Each additional layers you add increases your protection but by an incremental amount only. A good anti-virus program may offer 95% protection. Adding a good anti-spyware utility may increase this to 97%. The addition of an anti-Trojan may take it to 98%.

This is because today's security products overlap in function much more than they used to. A modern anti-virus program will detect a lot of spyware while a modern spyware program will detect some viruses, worms and Trojans as well.

Although the protection achieved only goes up incrementally with each layer added, the processing load on your PC will rise more or less in proportion to the number of layers. So using adding an anti-spyware layer to your anti-virus layer will double the load on your PC. Adding in an anti-Trojan as well may well triple it.

So folks, while layering is a good thing we are faced here with a law of diminishing returns.

But that's not the only problem with the traditional layering approach to protection. If an aggressive malware program is allowed to run on your PC it may disable all your layers of protection rendering them useless.

I've seen it happen many times and it is a frightening sight to see all your security programs icons disappear from the system tray

Thankfully some security programs resist termination by hostile agents but the majority don't. And even those that do resist may well prove vulnerable to new, more advanced termination methods yet to be developed by malware programmers.

My approach these days is simple: if you allow malware programs to run on your PC don't expect your security programs to fully protect you. If you are lucky they will but with security, you shouldn't rely on luck.

So how do you prevent infection?

The basics

Ensure you keep Windows and MS Office completely up-to-date by applying the latest fixes from the Microsoft Update Service ( <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en>)

Make sure your other software products are also fully updated, particularly popular products like Firefox, Opera, the Adobe Reader, Sun Java, Flash plug-ins and media players. The easiest way to do this is to use the free Secunia Software Inspector ( [http://secunia.com/software\\_inspector](http://secunia.com/software_inspector))

Be careful where you surf. In particular stay away from sites offering commercial software serial numbers, keygens and other hacked material. Avoid accidentally wandering to hostile sites by installing McAfee Site Advisor ( [www.siteadvisor.com](http://www.siteadvisor.com)) a free browser plug-in that appends site security ratings to search engine listings.

Never click on email attachments from un-trusted sources however tempting and attractive such attachments may seem. Similarly, never click on links in email from unknown correspondents.

Never install programs unless you are fully confident they are clean. In particular, only download files from trusted sources and never install programs that friends give you on removable media unless you have verified that are clean by submitting them to free web based testing services such as Jotti ( <http://virusscan.jotti.org>) and Virus Total. ( [www.virustotal.com/flash/index\\_en.html](http://www.virustotal.com/flash/index_en.html))

Install a robust firewall to ensure worms can't secretly enter your PC via the internet. My current favourites are the free Comodo firewall and ZoneAlarm Pro but there are several other excellent choices including Jetico and Netveda to name but two.

These basic measures are surprisingly effective in keeping your PC free from infection. Indeed, I've known users who follow these rules and don't use any additional security products yet have never had a malware infection.

However, sticking to these rules is not easy; it requires a level of discipline most users don't have. Who hasn't been tempted to open a funny PowerPoint email attachment or install a free game?

And it's not only a question of discipline. These days you can get infected simply by innocently surfing to a hostile web site or opening a "loaded" MS Office document. You need more protection that the basic security rules can provide.

Protection is better than cure

The best way to increase your level of protection is to make sure that if a malware program sneaks its way on to your PC that it is never allowed to run on your PC in a normal Windows environment.

A normal Windows environment is a user account with full administrator rights. It's probably what you are using right now as it is the default setup in all recent versions of Windows up to but excluding, Windows Vista.

There are three way you can keep malware well away from your normal Windows account.

1. Use a Windows limited user account for your daily work
2. Run all high risk programs with limited rights



### 3. Run all high risk programs in a sandbox or virtual machine

Each method has its pros and cons so let's look at them individually.

#### Option 1: Use a Windows limited user account for your daily work

Using a limited user account can be very effective in preventing malware infection as most malware products need full administrator rights to install themselves. In a limited account they just can't get a foothold.

It's easy to set up a limited user account. Just go to the Control Panel, select User Accounts and create a new user account as a limited user. Then sign in to this account for your normal computer work rather than the account you are currently using.

Setting up a limited account may be easy but using it can be a real pain. For example you won't be able to install most programs. You won't be able to update others. You won't be able to access any part of the PC other than your own documents and the shared documents area. Plus, you won't even be able to change the system date!

Some folks can work with these limitations or work-around them by swapping to a full privilege administrator account when they need to install programs or do other more advanced tasks. Others use the Windows "Run as" command and similar utilities to temporarily elevate their privileges when needed.

Most users though, find using a limited account to be simply too awkward and inconvenient. Agreed, their computer is safe but that's little comfort if their PC is only barely usable.

That said using a limited account is an excellent solution for advanced users prepared to tolerate the inconvenience or ordinary users with basic computer needs. If Granny never does anything but check her mail and browse to newspaper sites to read the headlines than setting her up with a limited account is a good way to go. Do expect phone calls though; one day even Granny is going to need to do something that requires administrator privileges.

#### Option 2: Run all high risk programs with limited rights

This is a more practical strategy. Run as a full administrator user but restrict the rights of all programs such as your browser and email client that can be sources of malware infection.

Getting this to work could be a complex business but thankfully there are some free utilities available that were written to perform this exact task.

The best known of these is DropMyRights. (<http://msdn2.microsoft.com/en-us/library/ms972827.aspx>)

It allows users to easily create special versions of their browsers, email clients IM client, media player or other internet facing programs that run from a full administrator account but with the restricted rights of a Windows limited user.

It's a simple and neat solution that provides good protection from infection yet doesn't inconvenience the user in the same way as working from within a limited user account.

The approach however has some weaknesses perhaps the worst of which is downloaded files. Yes you are safe from infection while using a browser but if you run any files you download then you can easily be infected if those files contain embedded malware.

There's no easy way of getting around this either. However our next solution provides the perfect answer.

#### Option 3: Run all high risk programs in a sandbox or virtual machine

The strange name "sandbox" derives from the Java world where it refers to the highly contained and restricted environment in which Java programs (applets) are allowed to run. They are allowed to "play in the sandbox" but not go outside it. The important point is that while running in the sandbox, the programs have no access to your PC.

So it is with sandbox security programs. While browsing or engaging in any computer activity within the sandbox you are totally corralled off from your other parts of your PC. Any files you download are isolated to the sandbox. Similarly, any programs that are executed only do so within the sandbox and have no access to your normal files, the Windows operating system or indeed any other part of your PC.

That means that if you get infected by malware while using the sandbox your "real" computer is not affected. Furthermore you can close the sandbox and all that's within it is erased including any infections, leaving your real PC in a pristine state.

Sandboxing is a great security solution for preventing infection. There are also some excellent sandboxing programs around including my favourite, the donation-ware utility "SandBoxie." (<http://sandboxie.com>)

There are some downsides. Sandboxing creates a two-worlds view of your computer and this confuses some users. It is not necessarily always clear whether at a given moment you are working in the sandbox or not. Overcoming this potential confusion requires users to be attentive and disciplined. If they get it wrong and think they are surfing in the sandbox when they are not it's possible to become infected.

This confusion is particularly evident with downloaded files. Files in the sandbox are not really permanently on your computer unless you deliberately move them from the sandbox to your real PC. If you shut the sandbox without moving them they will be lost forever.

This two-worlds view is simply too confusing for some users. With sandboxing, a confused user can be an unsafe user.

There are other problems too. Sandboxing is only available for PCs running Windows 2000 and later. Furthermore sandboxing can create problems on some PCs. Indeed I've known PCs to seize up totally with a sandbox installed. Luckily though, this is not common.

Virtual machines such as VMWare (<http://vmware.com>) and Microsoft's Virtual PC ([www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx](http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx)) are similar to sandboxing but take the idea one step further by completely separating the virtual machine from the real PC at a conceptual level. Rather than have a sandbox as part of your real PC you have a virtual PC that is notionally fully distinct from your PC.

This difference aside these two virtualization models have a lot of similarities. Infections that are incurred in the virtual machine cannot affect the real PC. Similarly shutting down the virtual PC removes all trace of infection.

Unfortunately they also share the same user confusion: "Am I in my real PC or the virtual one?"

The greater separation provided by the virtual machine approach does offer more robust security model than sandbox-

ing but it comes at a cost. Virtual machines consume a lot of memory and have a fair degree of processing overhead compared to sandboxing. And moving between the real and virtual machines can be more awkward than with sandboxing. Like sandboxing virtualization can be troublesome on some PCs.

Security wise both offer excellent protection from malware infection. The protection is so good that disciplined users don't really need many other security products to protect them.

Indeed all you need is a good firewall and a good anti-virus program. Combine these with a good sandbox and you will have better security than other users who employ five or more different layers of active security software protection.

Even better your PC will run fast; a complete contrast to machines running multiple security products.

What about on-demand scanning?

OK I've come out heavily against running multiple active security products but what about passive security products like on-demand scanners?

An on-demand scan is one you manually initiate. It may be an anti-virus scanner, an anti-spyware scanner, a rootkit detector or a key-logger scanner.

I'm all for on-demand scans as, unlike using products that employ active monitoring, they don't impose an on-going overhead on your computer. The only computer power they consume is while they are actually performing a scan.

Take for example a good anti-spyware scanner like the free version of AVG Anti-spyware or the excellent free Panda Anti-rootkit detector. Both available from: [www.computerdoctors.uk.net/pages/links.htm](http://www.computerdoctors.uk.net/pages/links.htm)

They consume virtually no computer power unless you actually run the programs. And because they are not constantly running they are less inclined to cause any problems with other programs.

So by all means runs on-demand scans periodically: weekly, monthly whatever. They are a good backstop to your Anti-virus program.

#### Conclusion

When it comes to today's aggressive malware programs, preventing malware from ever getting on your PC is a better strategy than trying to intercept it when it tries to run.

You can prevent malware getting on your PC by combining safe computing practices with other techniques such as reducing the privileges of high risk programs, sandboxing and the use of virtual machines.

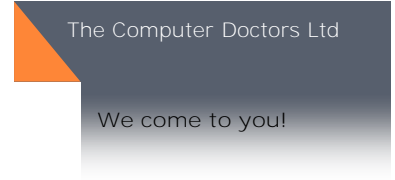
Reducing the privileges of high risk programs is a simple workable solution for

most users. Sandboxing and virtualization offer a more complete solution but are not entirely free of practical problems. For those who can work with these problems, sandboxing and other virtualization solutions offer the best way currently available to prevent malware installing itself on your PC.

With these elements in place the only active security software you really need are a good firewall and broad spectrum anti-virus program. That said you can, indeed should, supplement these with periodic on-demand scans of your PC with a good anti-spyware product and a good rootkit detector. These on-demand products won't impose the on-going overhead you would incur with security software that uses active monitoring.

None of this comes without cost. Defensive computing requires time and discipline. Users not prepared to put in the effort are advised to stay with a layering strategy using multiple security products.

But your Grandmother was probably correct, an ounce of prevention is worth a pound of cure.



*The views of individual contributors to our newsletter, are not necessarily those of The Computer Doctors Ltd. All suggestions are made in good faith and customers should ensure that they fully understand the implications of any changes they make to their computers*

Check out our website  
[www.computerdoctors.uk.net](http://www.computerdoctors.uk.net)



The Computer Doctors Ltd have been in business since 2001 and we enjoy an excellent reputation among customers and suppliers alike, for being fair minded and willing to go that extra mile to make sure that they are happy with the way we do business.

We are UK distributors for the Viper range of **desktop PC's and are resellers for IPC laptops**. We choose our suppliers carefully and not just based on price.

We are members of the Guild of Master Craftsmen who provide an arbitration service in the unlikely event that we cannot satisfy a customer.

We cover all of Northants and nearby areas of Milton Keynes, Leicester, Coventry and Peterborough.

Our customers include domestic and business clients and we tailor our service to encompass the most important requirements of each.

To find out more about what makes us tick, contact customer services at [sales@computerdoctors.uk.net](mailto:sales@computerdoctors.uk.net).

#### 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](mailto:sales@computerdoctors.uk.net)  
Shop: [www.computerdoctors.uk.net/shop](http://www.computerdoctors.uk.net/shop)

Technical Support  
Free: [tech@computerdoctors.uk.net](mailto: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](http://www.computerdoctors.uk.net)  
Skype: Compdocs or Tel: 020 8133 4144

Unit 12 Blackthorn Ind. Est.  
Blackthorn Road  
Northampton  
NN3 8PT