

Doctors Orders

Welcome

Welcome to the latest edition of the Computer Doctors Newsletter. Those of our customers that have visited our Northampton workshop in the last few weeks, can't have failed to notice large amounts of MDF and pots of paint cluttering up the place.

Yes, it's that time of year again! Our front office is slowly morphing into our customer waiting room (we like to call it the Doctors Surgery, but then we were always a bit corny).

The intention is for customers to have a cup of tea or coffee and check their emails, while we work on their computer. Obviously, some jobs take a lot longer than others, but there are many small jobs where the fault is obvious and can be rectified while the customer waits, (if this is their choice). Also fitting extras such as more RAM memory or an additional hard drive can be done in a few minutes.

We are also hoping to stock more parts and accessories and we will be introducing some pre-Christmas offers to get the ball rolling.

Many of our local Northampton customers have asked us to stock more parts and accessories. With the demise of a number of local computer shops the only alternative is to go into town to the big superstores. We're a bit limited for space, but we will try to keep a few of all the most popular items, on display. So please feel free to offer your suggestions and we promise to take them on board if at all practicable.



Inside this issue

- [Microsoft warns of new security attack](#)
- [Flash player update problems](#)
- [Create your very own Virtual Private Network](#)
- [Tame those annoying e-mail read-receipt requests](#)
- [Misplaced backup file clogs hard drive](#)
- [Use a sandbox to improve your security online](#)
- [Merge your Outlook contacts with your iPhone](#)
- [AVG upgrade problem](#)

Microsoft posts emergency defence for new attack

With little warning, Microsoft, released an unscheduled or "out-of-cycle" patch for a highly critical vulnerability that affects all versions of Windows. Security bulletin MS08-067 (patch 958644) was posted to warn of a remote-code attack that could spread wildly across the Internet.

Microsoft says it found evidence two weeks ago of an RPC (remote procedure call) attack that can potentially infect Windows machines across the Internet with no user action required.

Windows Server 2003, 2000, and XP (even with Service Pack 2 or 3 installed) are particularly vulnerable. Vista and Server 2008 gain some protection via User Account Control, data-execution protection, and other safeguards.

While firewalls are a first line of defence against this attack, don't think you're secure just because you have a firewall. Malware and viruses use many different techniques to wiggle their way into our systems.

For example, our office's network is protected by firewalls on the outside, but inside the network, PCs have file and printer sharing enabled. If a worm got loose inside the office network (and the patch hadn't been installed), the attack would spread like wildfire.

Many antivirus vendors have already issued definition updates that protect against this attack. Your antivirus program, however, may not protect you completely even if your AV definitions are up-to-date. Early reports indicate that there are already nine different strains of viruses trying to take advantage of this vulnerability.

"infect Windows machines across the Internet with no user action required"

MS Download Centre

We thought that everybody new about the Microsoft download centre, as we use it on a daily basis. But we were wrong. When asked, lots of our customers have never heard or it!

If you are looking for trial versions of Microsoft software or free fixes this is the place.

Categories include, games, Internet, Windows security, Windows media, drivers, home & office, mobile devices, servers, Mac & other platforms and lots more.

Although Windows Update automatically updates your Windows installation, it doesn't automatically update the rest of your Microsoft software, plus the download centre has lots of non-essential software that is just there to make your life easier.

<http://www.microsoft.com/downloads/Search.aspx?displaylang=en#>

We can expect more to come, so even the best AV application may not be able to update fast enough.

We've tested this patch and have had no problems applying it. If you are at all concerned that you may not have received this update, we strongly urge you to download and install this patch manually. Restart your PC before installing any patch to verify that your machine is bootable. Then be sure to reboot again after installing the patch, so the patched binaries completely replace the vulnerable components.

Microsoft has posted several versions of the patch that apply to different operating systems:

- [Windows 2000 with Service Pack 4](#)
- [Windows XP with Service Pack 2 or 3](#)
- [Windows XP 64-bit Edition](#)
- [Windows Server 2003 with Service Pack 1 or 2](#)
- [Windows Server 2003 64-bit Edition](#)
- [Windows Vista with or without Service Pack 1](#)
- [Windows Vista 64-bit Edition with or without Service Pack 1](#)
- [Windows Server 2008 32-bit Edition](#)
- [Windows Server 2008 64-bit Edition](#)

Flash Player update problems

Flash player is used to view and interact with many web-sites.

Lots of our customers are having Flash trouble these days, with the new patches and with just getting the updates to install. Worse, Adobe's own site is contributing to the problem: you type the correct URL for Adobe's page on fixing installation woes, but, that URL currently generates only a "Sorry, this page is not available" message.

First off, here's the correct Flash troubleshooting page. http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_19166&sliceId=1

The officially sanctioned steps listed there may not help, however: message boards are abuzz with frustrated users for whom the authorized fix doesn't work.

There's an unofficial workaround that seems to do the job in many cases, but it's definitely extreme. Read all the way through these next steps before you decide whether it's worth trying:

- **Step 1:** Uninstall all current versions of the Flash Player by downloading and running Adobe's Flash Player Uninstaller (warning: clicking this link actually begins a download of the tool). http://download.macromedia.com/pub/flashplayer/current/uninstall_flash_player.exe
- **Step 2:** Reset your PC's security to its default settings using Windows' built-in Secedit utility. Full instructions for resetting security in both XP and Vista are given in Microsoft Knowledge Base article 313222. (You'll find more information about the Secedit tool in this Technet article.) <http://support.microsoft.com/kb/313222/en-us>

Note that resetting your PC's security to default levels changes many, many settings. For example, it turns off Print and File Sharing and affects the permissions for local and network file, system, and resource access.

If you've altered your bootup process in any way, the security reset will revert your bootup to the default settings. Logins may also change; for example, a Guest account you'd deactivated may come back to life. Restoring the factory security defaults can be a sweeping change if, you've customized many settings on your PC.

So, is the process worth it? I liked Flash when it was small and simple, but it's neither now. When a non-essential tool such as Flash starts to require playing with Windows' security settings just to get it to run, I personally think it crosses into the "not worth it" side of the ledger. But that's just me. You may feel differently.

Create your own VPN with Hamachi

If you work for a large company, you may access your corporate e-mail or other systems remotely via a virtual private network. VPNs tunnel and encrypt your data so no one can read it until it gets to its destination.

But what if your company doesn't have a VPN? Or what if you want to connect to your home network securely? That's where LogMeIn Hamachi comes in. This amazingly simple tool lets you create a secure connection between any combination of computer locations, a task that would otherwise require a special router and/or complex configuration tools.

For example, you can install Hamachi on your desktop computer at home and join your laptop to the home network from the road. Or give family and friends secure access to your home network for sharing folders or even playing songs from your iTunes library.

While remote-access programs let you control an individual computer, Hamachi actually joins the remote computer to the network, which may contain any number of other computers. The program is not logging into your home computer, though you can do this using Windows' Remote Desktop along with Hamachi.

When you install Hamachi, you're assigned a permanent IP address for that machine. You can create any number of VPNs or join existing ones. You might create two or more networks for different purposes — family and work, for example — with different member computers and then log in and out of them with a right-click. Your unique Hamachi IP address works anywhere, including from behind NAT routers.

When you create a network in Hamachi, you give it a name and a password, which you can then send to other people so that they can join your network. (They will also need to install Hamachi.) For added security — in case you're worried about the password being compromised — the paid version of the program lets you prevent anyone you haven't approved from joining.

While Hamachi is great for sharing folders remotely, the program also provides secure Internet access from public Wi-Fi hotspots. All traffic is encrypted between your computer and your home network, which is behind your router firewall. Hamachi can also be used to set up online gaming networks, private torrents, and access to your FTP server. Free version available or paid for with more features \$5/month or \$40 year.

<https://secure.logmein.com/products/hamachi/vpn.asp?lang=en>

Tame those annoying e-mail read-receipt requests

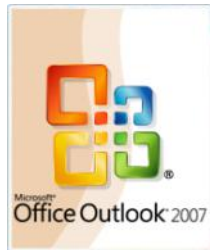
E-mail read receipts have some entirely legitimate uses, but their main purpose today seems to be in sending spam mails. A customer emailed us recently asking :-

"Recently, when Outlook has been emptying my deleted items, a pop-up has come on screen saying that a sender has asked for a read receipt. The senders are always spammers so, of course, I refuse. "The thing is, there's also an option to not be asked again. I was wondering, if you say 'yes' to one particular read-receipt request and then check 'don't ask again,' would you end up sending read receipts automatically in the future and thus accidentally verify your e-mail address as valid?"

Good question! And you're right: spammers use read receipts to determine whether a mailbox is alive and monitored. If their initial spam mail triggers any response at all, they know they've found a live one and can target that mailbox for future spam attacks.

In Outlook, read-receipt requests are normally handled on a message-by-message basis. With the default settings, the answer you give applies only to the current e-mail. Even the "don't ask again" option applies only to that particular message. But there is a way to tell Outlook never to respond to read-receipt requests, or always to respond. It's easy:

1. On the Tools menu, click Options.
2. Under the Preferences tab, click E-mail Options.
3. Click Tracking Options.
4. Select one of the following:
 - **Always send a response** means Outlook will automatically send a read receipt whenever one is requested. This is the setting spammers love.
 - **Never send a response** means Outlook will simply ignore all future read receipts. This is the option I use. If I want someone to know that I've seen their e-mail, I'll tell them myself.
 - **Ask me before sending a response** means Outlook will handle each request for a read-receipt on a case-by-case basis.



Misplaced backup file clogs hard drive

A local business owner was doing the right thing — backing up his system — but the huge file ended up somewhere on his C: drive, almost completely filling it:

"I did a backup with my external device connected and did not change the drive letter in Preferences and ended up with the backup done on my main hard disk. Now I have no more space on my C: drive. I keep getting a message of 'Low disk space on local Disk (C).'

How do I proceed to delete this backup so I can recover my disk space?"

There are several options, depending on whether you want to save the backup file. If you know the name and location of the offending backup file, skip the next two paragraphs.

If you're not sure of the file's name or location on your C: drive, click **Start, Search, All files and folders**. Under What size is it, select the **Specify size** radio button and enter the approximate **at least** size of the file (look at your previous backup files to see about how large they are).

If you don't have easy access to your old backup files, pick a large size. The Specify size function asks for input in KB. For example, enter 250MB as 250000 KB, 500MB as 500000 KB, and so on. (Note that in Vista, use the Advanced Search options to search by size.)

Once you've found the backup file, right-click it. If you simply want to delete the file, press and hold the **left Shift key** and select **Delete** from the right-click context menu; holding the Shift key means the file will be instantly deleted instead of being moved into the Recycle Bin, where it would still occupy disk space.

If your intent is to save the backup file to some location other than your C: drive, select **Cut** from the right-click menu and navigate to an external drive or other location where you wish to store the file. Right-click that location and select **Paste**; the file will be removed from your C: drive and placed where you've indicated.

Timesaver bonus: If you open two folder windows on your screen — one showing your C: drive and the other showing the destination drive — you can just drag-and-drop the files between them. If you drag with the right mouse button, you will get the option to Copy or Move the file, or cancel the action altogether. This cancel option is handy if you've ever dropped a whole bunch of files on your desktop by mistake.

And by the way: top marks to this customer for making backups! I'm still amazed at how many people don't take this simple step to protect themselves and their data.

Use a sandbox to improve your PC security

Sandboxes are a relatively new type of security product that can significantly reduce your chance of getting infected when you surf or when you download and install programs.

I'll explain why sandboxes are so important and show you how to use my favourite sandbox program [1].

Block access to system files as you browse

A security sandbox is a program that creates an isolated environment on your PC within which other programs can run. It sets up a kind of virtual PC within your real PC. Programs running in that virtual PC are corralled from the rest of the system.

It's like building a room in the deep interior of your house with no windows or doors. What takes place in that room cannot affect what takes place in the rest of your house. In the same way, what takes place in a security sandbox cannot affect your PC.

Now, this may sound abstract and theoretical, but it has some very practical implications.

First, if you run an infected program within the sandbox, the infection is restricted to the sandbox and cannot get to your real PC.

Second, when you shut down the sandbox, the infection is eliminated from your PC. It will be gone forever without ever affecting your system.

These characteristics make sandboxes ideal for improving your PC's security. And, as we shall see in the next section, sandboxes address the latest type of security threat confronting PC users: hostile Web sites.

Why sandboxes are important to your security

A few years ago, the major risk PC users faced was getting infected by a virus or worm that was contained within an e-mail. You may recall a time when there seemed to be a major virus outbreak every few weeks. Not anymore; with improved ISP e-mail filtering and more extensive use of antivirus products, large-scale, e-mail-borne virus outbreaks have become uncommon. They're not eliminated but are much less frequent.

Today, there is a new threat: infection by visiting a hostile Web site. It works like this:

You go to a seemingly innocent site. While you are viewing the site in your browser, your PC has been silently probed for security vulnerabilities by malware implanted surreptitiously in the site. Once the malware finds a weakness, the site secretly downloads Trojans, keyloggers, and other malicious software onto your PC. You

are not even aware of what has happened.

What does this secretly downloaded malware do? Pretty well anything the criminals behind the scheme want it to. For example, they could take control of your PC and turn it into a remote-controlled slave PC — or zombie — that will do its master's bidding. This may be sending out spam e-mail, attacking Web sites targeted for extortion, or engaging in numerous other criminal and fraudulent activities.

Alternatively, the criminals may install a keylogger on your PC that transmits details of your banking and financial details to some remote computer.

Standard PC security measures aren't enough

At this stage, many of you are probably thinking, "This can't happen to me. I visit only reputable Web sites. Besides, my PC has all the latest Windows security updates installed and I have an excellent antivirus program."

While good security practices will certainly reduce your chances of being infected by a hostile Web site, you can still get infected. Furthermore, the risk is greater than you may think. Here's why:

First, an increasing number of hostile Web attacks are from reputable sites. Criminals may take control of a legitimate Web site via security vulnerabilities in the site's software. They can then use the site to infect unsuspecting visitors.

It may be hours or days before the site owners detect and correct the problem. In the meantime, thousands of unsuspecting visitors to the site could be infected.

The most famous example of this process was the Super Bowl incident in the US last year. The Web sites of Dolphin Stadium and of the Miami Dolphins football team were hacked and used to distribute a keylogger. The sites were infected for over a week before the problem was discovered. In the interim, thousands of surfers who visited the sites looking for football information instead had their PCs infected.

Second, keeping your PC fully up-to-date with the latest Windows security patches may not help, either. Some of these hostile Web attacks use unknown security holes, flaws that even Microsoft doesn't know about. These so-called zero-day vulnerabilities are quite commonly used in hostile site attacks, perhaps because they allow a lot of PCs to become infected in the short time before the site owners discover their site has been hacked.

Finally, don't expect your antivirus and antispyware

software to fully protect you. Yes, your security software will catch some of these Web-based infections, but the chances of zero-day attacks being detected are not high.

Worse still, some of these hostile sites attempt to download software that disables your security software before it gets a chance to warn you of their presence.

Now, all this sounds alarming, but keep in mind that the risk that the average user will encounter a hostile Web site is relatively small. There's no need to get into a panic about this; it's just another security risk that all Internet users face.

However, though the risk is small, the consequences are serious, so putting some protective measures into place is worthwhile. This is where sandboxing comes into the picture.

Using a sandbox for safer browsing

My favourite sandboxing program is Sandboxie [1], which I'll use to illustrate how sandboxes work and how they protect you. Other sandbox programs may work differently.

Sandboxie is a small, 350KB program for Windows XP and Server 2003, both 32-bit and 64-bit. The program currently work with Windows Vista 32-bit but not 64-bit. Sandboxie is free for personal use, though there is a £17.41 registered version with a few more features.

Most folks will be happy with the free version, though I encourage you to register if you can afford to, because this program is the work of a single hard-working individual — Ronen Tzur — not a large corporation.

After you install Sandboxie , you will notice very little that is different on your PC other than a small, yellow sandbox icon in the system tray.

Just because you installed Sandboxie , don't think your browser is now sandboxed.

Unlike ZoneAlarm's £19.95 ForceField [2] and other sandboxing applications, Sandboxie [1] does not set your browser to open in a sandbox automatically. You must do so manually by right-clicking your browser icon and selecting Run sandboxed.

Sandboxie can be set up to isolate your browser automatically whenever you open it. To do so, add the name of your browser's executable file, such as firefox.exe or iexplore.exe, to Sandboxie's list of the programs it always opens in a sandbox.

I use this setting to ensure that my browser always runs in a sandbox, regardless of whether it is started manually or automatically by clicking a link in a document or e-mail.

Some folks like full manual control, while others prefer it to be automatic. With Sandboxie , it's your choice.

Whatever method you use, Sandboxie employs a simple technique to let you know when your browser is running sandboxed: the program places a hash symbol (#) before and after the contents of your browser's title bar.

Security apps see in, malware can't see out

While running sandboxed, you can browse with near-perfect safety to just about any part of the Web. If you get infected by a hostile site, your antivirus and other security programs can still warn you because they can see into a sandbox, even though sandboxed programs cannot see out.

However, be aware that your PC may become infected even if your security programs don't sound the alarm, particularly if you encounter a new zero-day infection.

That's no problem when you're using Sandboxie [1]. When you've finished surfing, simply close your browser, right-click the Sandboxie tray icon, and select Terminate programs to remove any program — including malware — that's running in the sandbox. Then select Delete contents to completely remove any downloaded programs. After that, your PC is completely clean, with all traces of infection removed.

The same technique can be used to ensure privacy. When you clear the sandbox, all traces of your surfing activity are removed, including the sites you visited, the searches you made, and the files you downloaded.

Of course, this can be a mixed blessing: I like to retain my surfing history as well as any saved passwords and bookmarks.

But that's no problem: you can set Sandboxie so that programs running in the sandbox have access to certain nominated files outside the sandbox. If you configure Sandboxie to allow sandboxed programs access to your real Favourites folder, then any new bookmarks you create while surfing in the sandbox will be saved.

However, you are exposing these shared files to any program running in the sandbox — including malware — so be sensible about what you choose to share.

Sandboxing isn't just for Web browsers

You can sandbox any program, not just your browser. This is a great way to check out downloadable apps whose integrity cannot be established. Remember what I said earlier: your security software can see into a sandbox even though sandboxed programs cannot see out.

(Continued on back page)

The best way to merge your contacts with iPhone

Many people find that syncing a new iPhone with their contact and calendar data from applications like Microsoft Outlook just doesn't work easily.

Fortunately, there are techniques you can use to make sure that your devices are sharing data smoothly.

If you're having trouble using iTunes to sync your contact data from Outlook or other sources with your iPhone or iPod Touch, follow these steps to get your data where it needs to be.



Step 1. With your phone connected to your computer, make sure iTunes is running. If necessary, select your phone under the Devices category in iTunes' left pane.

Step 2. With iTunes' Summary tab in front, make sure the Options at the bottom are set the way you want them. I like to control which files are moved and when, so I uncheck Automatically sync when this iPhone is connected. I also select Manually manage music and videos.

Step 3. Click the Info tab. Select the box at the top of the Contacts section if you want iTunes to sync that information with your phone. Select other settings in that section to control how the data is organized.

Step 4. Repeat the above step for the Calendar and other sections as desired. Click Apply.

That should initiate the syncing process. If it doesn't, wait until the Sync button appears and click it.

No go? Try the official iPhone troubleshooter

If you run into problems while syncing your phone via iTunes, Apple offers several strategies that may solve your problem [2]. Here's a quick rundown of work-arounds to try:

- Make sure you have the latest version of iTunes installed. To test for a newer version, pull down iTunes' Help menu and select Check for Updates.
- Reset the sync history. In iTunes, choose Edit, Preferences. Click the Devices tab and then select Reset Sync History.

- Disable non-Apple add-ins in Outlook by unticking the boxes for each one in the COM Add-Ins dialog box. The steps to opening this dialog vary between Outlook 2003 and Outlook 2007; consult the programs' help files for instructions.

- Use Vista's User Account Control applet to create a new user. Then log off your current account, log into the new account, and try the sync again.

- Uninstall iTunes and then reinstall the program.

If none of the above fixes things, your iPhone syncing problems may be caused by corrupt entries. To test for this, browse through your Outlook contacts list looking for garbled names or other indications of faulty data. (Doing so also helps you eliminate duplicate entries, which are discussed in the next paragraph.) Delete any corrupt or superfluous entries and retry the sync.

One final problem may remain. When merging address books, entries with minor differences are sometimes interpreted as separate entries, resulting in one or more duplicates. Fortunately, a number of products exist to ferret out and deal with such dupes.

A free program I like is Contacts Scrubber for Outlook from TeamScope Software [1]. It searches your contacts and presents duplicates to you one at a time, making an educated guess as to which fields to merge. You can specify which entry is the one to preserve and click inside individual fields to select details to merge, overwrite, or discard.

The free version of Contacts Scrubber can process up to 1,000 items, but TeamScope sells a version for \$29.95 that goes beyond that limit and includes more advanced features. Contacts Scrubber works with Windows NT/2000/XP/Vista and Outlook versions 2000 to 2007.

A phone without stored phone numbers is pretty much useless. Fortunately, the procedures outlined here will solve most iPhone sync problems. Still, you may need to use several techniques until you find the combination that works for you.

[1] <http://www.teamscope.com/otherpro/utilities.asp>

[2] <http://www.apple.com/uk/support/iphone>

AVG Upgrade Problems

As if we didn't have enough upgrade emergencies to deal with this week, a recent update of AVG's antivirus software knocked out some people's Internet connection. AVG's support page indicates that after upgrading to AVG version 8.0.196, your network link may fail!

They suggest "If rebooting your PC doesn't fix the problem, follow the instructions on AVG's support page to download the fixfiles.zip file to your computer. Double-click the .zip file to open it, and then double-click fixfiles.exe in the resulting folder to run the utility". How this is done with no Internet connection is not explained.

If the glitch persists, the company recommends that you run a repair installation of your AVG application.

Our suggestion is to uninstall AVG and install the superior **Avast Antivirus** from our free download site.

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

(Continued from page 6)

Since your antivirus scanner can detect an infected download running in a sandbox, you can simply clear the contents of the sandbox, and all trace of the infection is gone forever.

These days, I never surf without a sandbox. On the rare occasions when I get infected, it's a great feeling to simply clear the sandbox contents and know my PC is safe from harm.

Sandboxing does not replace your antivirus scanner or other security software. Rather, it provides an additional layer of protection. No individual security solution — including sandboxing — is perfect. The more layers of protection you have, the greater your overall security.

I suggest you try the free version of Sandboxie [1], but first a word of warning: sandboxing programs cause problems on a small percentage of PCs, so before you install Sandboxie or any other sandbox program, please make sure your PC is backed up. That way you can recover in the event of a problem.

[1] <http://www.sandboxie.com>

[2] http://download.zonealarm.com/bin/forcefield_x/index.html

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