

# Doctors Orders

## Welcome

Hello welcome to the February edition of Doctors Orders. We had a nurse ring up last month to tell us that she read halfway through last months newsletter before realising that it was not a medical journal. "Just as incomprehensible" she said.

Well that caused a ruck, I can tell you. The boss went on a "Geek" hunt and rounded up everybody with white socks, protruding teeth and glasses and gave them a lecture on speaking to the rest of humanity in plain English.

When I made my usual monthly collection of articles for the newsletter, it consisted of a picture of a computer, drawn in crayon, a page with stick on letters cut from newspapers, much like a ransom note, saying "TIP: DON'T GET VIRUSES" and a piece of folded paper that when you put your thumbs and forefingers in it and wiggled it back and forth, it told you if your hard drive had failed! Call me suspicious if you like, but I sensed a bit of tension.

Still it all came good in the end and hopefully there will be something for everybody in this months edition.

The late breaking news last week was that our software suppliers told us "no more Windows XP after January 31st"!

We all stood around aghast at the news. Half the PC's we sell have Windows XP home or Pro and Microsoft has stopped supply of a product that is selling like the proverbial hot cakes.

Microsoft will allow us to downgrade Vista Business or Vista Ultimate to XP Pro, using the Vista licence, so for businesses wanting a PC with XP Pro to match their existing equipment, this will be an answer. Not so easy for home users who will have to make do with Vista until Windows 7 is released later this year.  
(Page 2)

If you are adventurous and want to try something completely different, see page 6 and install the totally free Ubuntu the Linux based, open source operating system. It doesn't need a powerful PC so will revitalise that old PC in the loft and give it a new lease of life.

Craig



---

## Inside this issue

---

- [Online backup, is it worth the Hassle?](#)
- [Vista Doomed!](#)
- [Start Patching Windows 7 beta](#)
- [Search links redirected to Spyware downloads](#)
- [There's more in that download than meets the eye](#)
- [Dual Boot Ubuntu to make your Windows PC safer](#)
- [Three Quality Laptop Deals](#)
- [Virgin Media Special offer](#)

# Online backup, is it worth the Hassle?



Copies of backed up data on-site are very use-

ful, as they enable you to restore lost files quickly, but they don't cover you against physical drive failure or disasters such as theft, fire or flood. It's well worth factoring in the failure rate of some media. Remember that CDs and DVDs are easily scratched. External hard drives can fail, as can USB flash drives and any of the above can be lost in a moment of carelessness. This is why an off-site backup is important. In times gone by, this would mean sending tapes or discs away once they've been recorded, but thanks to the internet, it can now all be done online. Your backup is stored in a secure, remote location so that should the worst happen, valuable data doesn't add to the list of things lost. The ideal scenario is to have two back-up plans in place: one backup to external disks on-site, which are useful and convenient, and a second backup to a remote location, which adds an extra layer of security. Better still, it won't break the bank to do so.

There are several useful online backup services, many of which provide free trials or a limited amount of free storage to tempt you in to try. Three worth checking out include Mozy (<http://mozy.com>), Humyo ([www.humyo.com](http://www.humyo.com)) and Carbonite ([www.carbonite.com](http://www.carbonite.com)).

Mozy provides 2GB free storage space so you can get to

grips with the system before deciding if you

want to upgrade: unlimited space costs \$4.95 (around £3.40) per month. Carbonite doesn't provide any free space, but does give you a 15-day trial and then unlimited space for \$50 (about £34) per year. If you're looking for the ability to back up, synchronise and collaborate with a single tool, then Humyo is well worth considering. The Business solution starts at £9.90 per month or £99.90 per year for 100GB storage space. Use the following tips to help make the most of these and other online backup tools.



## 10 tips for setting up secure online backups

### 1 - USE YOUR OWN ONLINE STORAGE

If you've got access to secure off-site storage as part of your internet access or hosting plan, you can use that. Programs like Genie Backup Manager ([www.genie-soft.com](http://www.genie-soft.com)) can be configured to back up via FTP.

### 2 - GET IN THE MESH

Microsoft's Windows Live Mesh offers 5GB of free online storage space that can be shared across multiple computers, enabling you to both synchronise and back up at the same time. It's still in beta, so beware – check it out at [www.mesh.com](http://www.mesh.com).

(Continued page 3)

## Vista Doomed!

**It seems that the not so loveable Vista is to be replaced in the second half of 2009 with Windows 7 full product. As nearly all Microsoft's products eventually get delayed by at least a year, we'll take this date with a pinch of salt.**

**The Microsoft hype machine is so full of Windows 7, we have had customers asking for it on new PC's, not realising that the recently released beta (test) version is as holey as a 1978 Austin Allegro and just about as reliable.**

**Still when it hits the streets, Windows 7 will be faster, more secure, more stable, in fact all the things that Vista was supposed to be.**

## Start Patching Windows 7

Steve Ballmer's (CEO of Microsoft) announcement at this year's Consumer Electronics Show that the Windows 7 beta would be available for download on Jan. 9, 2009, caused a buzz. In fact, the huge demand for the public beta forced Microsoft to delay the release until the company could ensure that its servers could handle the crush.

If you're one of the millions of folks who downloaded the Windows 7 beta, there's already some patching required. The patch described in Knowledge Base (KB) article 961367 fixes a problem that mangles MP3 files. The update also applies to Windows Media Centre and Windows Media Player. As with all beta software, things may not work as you expect them to, and some devices may not connect as they should.

If you're the adventurous type and download the beta, make sure you don't use the Checked Build version. This is a special build that developers use to expose raw errors for debugging. If you install this version, you'll get more Dr. Watson errors than you've ever imagined. Unless you're a code developer working on a special project, the Checked Build version is meant to be run only after a Microsoft support person asks you to do so.

### 3 - PICK THE RIGHT PRODUCT

If choosing a dedicated online backup solution, make sure it meets your needs. Both Carbonite and Mozy Pro charge per computer being backed up, but Humyo's Business accounts support four or ten users depending on the package selected.



### 4 - WHAT TO BACK UP

You'll need to manually choose which files and folders to back up – which means you'll need to know where your email is stored, for example. Mozy makes things easier by allowing you to define "backup sets", which lets you pick specific file types to back up rather than files or folders.

### 5 - LIMIT BACKUP SPACE

Humyo and Mozy Pro both allow system administrators to limit how much backup space is made available to end users, keeping you firmly in control of your storage space.

### 6 - BE PATIENT

Uploading gigabytes of data will test even the fastest internet connection, so be prepared to wait days or even weeks for all of your data to be backed up on to your online backup server. Once done, only new or changed files are uploaded, so the process will be much quicker.

### 7 - THROTTLE BANDWIDTH

Online backup tools are designed to try and work around your schedule, uploading when your connection is idle, but if you find them interfering with your day-to-day work, look for an option to limit the bandwidth (it's called Low Priority Mode in Carbonite, for example) to wrest back control of your internet connection.

### 8 - RESTORE FILES

You should be able to not only pick and choose which files to restore when the time comes, but also select an alternative location to restore them to if you need to.

### 9 - RESTORE OLD VERSIONS

All three solutions keep multiple versions of your backed up files, so if you need to rollback to an older version of a file you can do so – snapshots are typically taken daily.

### 10 - HOW SECURE?

All reputable online backup services encrypt your data before it's backed up – some like Carbonite will even allow you to store the encryption key yourself, perfect if you're the paranoid type.

## Search links redirected to Spyware downloads

For at least the past four months, an Internet attack has been under way that transforms the links in search results into browser hijackers. Known as the go.google, go.yahoo, or go.msn virus, it infects systems to redirect certain Google, Yahoo, and MSN search-results pages to hacker-operated sites.

Even worse, the virus takes several steps to prevent you from removing it. The infection blocks access to certain antivirus sites and shuts down many antivirus tools. The go.google virus in particular appears to be widespread: a quick search of Google for go.google virus turns up no fewer than 4 million pages where people discuss this piece of malware.

Getting this nasty off your computer is a two-step process. First, scan your system with a malware-removal tool. If you're unable to open and download updates for your regular antivirus and anti-malware software, use a non-infected computer to download to a flash drive a program such as the free Malwarebytes Anti-Malware ([www.malwarebytes.org/mbam.php](http://www.malwarebytes.org/mbam.php)) and SuperAntiSpyware ([www.superantispyware.com](http://www.superantispyware.com)). Finally, plug the flash drive into the infected computer and run the antivirus program from that device.

Note that even if you are able to download a malware-removal tool on the virus-laden PC, the virus may prevent you from running it. To get around that problem, rename the anti-malware tool's executable file. For example, change SuperAntiSpyware.exe to mytool.exe. Now you should be able to launch the program.

Another way to get around the inability to access your antivirus program is to check your system for the presence of a particular rogue device driver:

- Step 1: Click Start, Control Panel, Performance and Maintenance (in Categories view), System.
- Step 2: Select the Hardware tab and click Device Manager.
- Step 3: Choose the View menu and select Show hidden devices.
- Step 4: Scroll to the Non-plug and play drivers section and expand the tree.
- Step 5: If you see an item labelled TDSSserv.sys, right-click it and select Disable.

After you reboot your computer, you'll be able to access your antivirus program and browse to anti-malware sites to remove the pest from your PC. Once you've cleaned your system, make certain that you update your antivirus software every day to avoid re-infection.

# There's more in that download than meets the eye

Most PC users have a distorted view of the nature of the security risks they face. Conventional wisdom holds that the three biggest threats come from (1) criminals exploiting flaws in Windows and other software products; (2) e-mail-borne viruses; and, more recently, (3) visits to malicious Web sites.

These threats, though real, are relatively minor players: each accounts for only a few percent of home PC infections. No, folks — the biggest threat doesn't come from any of these exotic sources but from something much more common and pedestrian: downloading infected programs.

The people who make their living cleaning up infected PCs have known this for years. When they ask users when their problem started, the answer is all too commonly "after I downloaded and installed a new program."

Tech-support personnel in corporations will tell you the same thing, and they'll often single out senior managers as particularly susceptible to malware-bearing downloads.

This practical experience is borne out in the statistics. Security research company Trend Micro recently reported that of the top 100 infections in 2008, approximately 63% were caused by downloading and running programs. E-mail-borne infections accounted for only 3%, while the exploitation of security flaws in products was responsible for a tiny 1.7% of PC infections.

## **Software thieves get more than they bargained for.**

So, what are these infected programs that users are downloading?

They include free games, utilities, toolbars, and just about any other program a malicious site can entice a user into downloading. An even-greater threat are pirated software and pornography.

Pirated software is particularly dangerous, because such programs are used widely and are often crawling with viruses.

In fact, when we're looking for a new set of malware for a security tests, we go straight to pirated-software sites and cracked-software sources on BitTorrent.

The last time we did this, 39 of the 61 illegal programs we downloaded from BitTorrent were infected. Most of the infections are in the key generators ("keygens"), but in seven of the 39 cases, the infection was in the pirated program itself.

Even scarier was how few of these infected downloads had been noted by users in their comments on the BitTorrent search sites. I'm not sure why, though I do

know that some malware infections disable your security software, so the commenter's were likely unaware of the viruses.

I suspect many users of pirated software are smart enough to download a fresh copy of the program from the vendor's site and use only the pirated serial number or keygen they lifted off BitTorrent. Whatever the reason, be assured that you cannot rely on program ratings given by BitTorrent users.

Now, all of this sounds very scary, but I don't want to alarm you unnecessarily. Most downloading is perfectly safe. Indeed, downloading and trying new programs is one of the great pleasures of the Internet.

However, you do need to be smart about what you download and install. That, as we shall see, is not too hard at all.

In the last few years, I've downloaded and installed hundreds of programs onto my PC and it's never been infected by malware. Not even once.

This is not due to any technical genius on my part nor to the quality of the security software I use. It's the result of adopting safe downloading practices. If you develop the habit of using these practices, your computer will be just as safe.

## **Rule 1: Download only from reputable sources**

Following this single rule will cut your risk of infection dramatically. So, what is a "reputable source"? Certainly the following:

- 1] Any major download site, such as Download.com, Softpedia.com, and MajorGeeks.com.
- 2] Any site of a reputable developer or vendor, such as Microsoft, Google, HP, and Dell.
- 3] Any open-source software hosted on Sourceforge.net, Mozilla.org, and other large open-source hangouts.
- 4] And of course our own download page which links to the software vendors own site or one of the above.

There are many more "reputable sources." The problem is knowing which sites to trust. McAfee SiteAdvisor is a free plug-in for Internet Explorer ([www.siteadvisor.com/download/ie.html](http://www.siteadvisor.com/download/ie.html)) and Firefox ([www.siteadvisor.com/download/ff.html](http://www.siteadvisor.com/download/ff.html)) that rates sites based on a number of security criteria, including whether the downloads from the site are free from malware.

If a site has SiteAdvisor's "Green" rating, you can be pretty sure it's safe. Conversely, you can count on any site with a "Red" rating as being unsafe.

## So, what files are definitely unsafe to download or install?

Topping the list are files a site offers to you unprompted or via a popup window. If the site asks whether you'd like to install a toolbar, video viewer, download manager, or whatever, always say no. Such files are the riskiest of all downloads, so never be tempted. Make no exception here; this is seriously dangerous territory.

Other unsafe sources are file-sharing services. Never download software from BitTorrent and other file-sharing networks unless you can verify the authenticity and integrity of the download with 100% certainty. For most people, it's best to play it safe and never download from these services.

The same prohibition applies to software provided to you by friends and colleagues. Unless it's on the original manufacturer's CDs, there's no way you can verify the authenticity and integrity of the program.

### Rule 2: Scan all downloaded files

Normally, you don't have to worry about scanning files you download, because most of the top antivirus and antispyware programs automatically scan a file when you download it. If you're unsure whether your security product scans downloaded files automatically, you can usually initiate a manual scan by right-clicking the downloaded file and selecting the "Scan this file" option.

Unfortunately, even the best AV scanners have a less-than-100% detection rate; a downloaded file may scan as clean yet still be infected.

You can further reduce the chance of a file's being infected by making use of a free Web-based scanning service, such as Jotti (<http://virusscan.jotti.org>) and Virus Total ([www.virustotal.com](http://www.virustotal.com)). These sites run your downloaded file through a dozen or more antivirus and anti-malware programs.

Of course, there's still a chance your download is infected, even if it passes all the tests at Jotti or Virus Total. However, the protection these services offer is good enough to keep most PCs safe.

### Rule 3: Run suspicious programs in a sandbox

If you have the slightest doubt about a program or e-mail attachment you downloaded, install the program or open the file in a sandbox or other virtualized environment before you load it on your PC.

My favourite sandbox app is the excellent free program called Sandboxie ([www.sandboxie.com](http://www.sandboxie.com)). This and other virtual environments allow you to install and run programs in an area of your PC that's been specially corralled off.

If the program you install happens to be infected, the infection is confined to the sandbox and cannot affect your PC. Any infection can be removed by simply deleting the sandbox or its contents.

A good feature of sandboxing is that your security soft-

ware can see what's happening in the sandbox and can warn you of any problem. In fact, it's much easier for your AV scanner to detect an infected program that is actually running than to detect an infection simply by scanning the file before installation.

If you install a downloaded program in a sandbox and get no warnings from your security software, it's unlikely that the file is infected. You can then delete the sandbox and install the program with confidence on your real PC.

### Rule 4: Read the software licensing agreement

Of my four rules for safe downloading, this one is most likely to be ignored. That's a pity, because perusing the end-user licensing agreement (EULA) is a surprisingly good way of determining whether the program you're installing contains any unwanted components.

Now, no hacker or Internet criminal is going to tell you in a licensing agreement that they have malicious programs in their software. However, most adware purveyors and spyware vendors will disclose the contents of their "services."

That's because adware is quite legal. Indeed, some AV and antispyware programs won't pick up particular adware programs because they're legal.

Spend a couple of minutes reading the EULA rather than just automatically clicking the "I have read this and agree" button.

If you find reading EULA's too tedious, have Javacool Software's EULalyzer program read it for you and flag for your attention any worrying paragraphs. EULalyzer is free for personal and educational use ([www.javacoolsoftware.com/eulalyzer.html](http://www.javacoolsoftware.com/eulalyzer.html)).

In addition to reading the EULA, you should also be vigilant about what you agree to during the program's installation routine. Quite often, software vendors will slip into the install wizard a default selection permitting the installation of a third-party's product.

A common example of this practice is the otherwise excellent and highly recommended disk-cleaning program CCleaner ([www.ccleaner.com](http://www.ccleaner.com)). Embedded in the utility's install is a default option to add the Yahoo search toolbar to your system. If you don't want the toolbar, you need to uncheck the option.

Now, the Yahoo search toolbar is a legitimate product and quite a good one, in fact. But do you really want it? I don't, and I suspect most other users don't want it, either. The next time you install a program, read before you click.

So there you are. Of all the security threats you face, downloading and installing programs is statistically your highest risk. There's four simple rules for downloading that anyone can follow. Just stick to these rules and you're on the way to a malware-free 2009.

# Dual Boot Ubuntu to make your Windows PC safer



If you'd like to know how it feels to be ignored by viruses and spyware, add Ubuntu to your existing Windows installation.

A free utility makes creating a dual-boot Windows/Ubuntu machine fast, simple, and safe.

Get the best of both Linux and Windows worlds

Many of us have been using Windows for more than two decades, and we know the operating system's ins and outs. Windows runs the programs we love, it's fairly stable, and it supports our printers, media players, and other hardware devices. Sure, you (or your boss) have to pay for the pleasure of using Windows, but the price is insignificant compared to these benefits.

Here's the other side of the coin, though: Windows' popularity has made its inevitable flaws the juiciest target for malware authors, resulting in a ceaseless stream of critical security advisories and patches.

Although you certainly can use the Internet safely on a Windows PC, doing so requires a lot of effort these days just to ensure that your copy is properly patched and secured. Like it or not, Windows has become the Ford Pinto of operating systems.

Now imagine that your PC is suddenly free of this ever-present threat, and you can use a browser to surf the Web without fear of drive-by downloads.

Alternative operating systems such as Linux and Apple's OS X are in some ways fundamentally more secure than Windows. These OSes aren't entirely immune from software flaws and the resultant attacks, but successful malware infections in Linux and OS X are rare.

Of course, a big reason why you're safer using Linux and OS X is that they present a much smaller target for malware authors: the vast majority of PCs connected to the Internet run Windows. Now it's easier than ever to reap the benefits of both Windows and non-Windows environments.

## **Painless way to add Ubuntu to your Windows PC**

You can install OS X on your PC, but doing so is neither easy nor permitted by Apple's license, which requires all installations to be on Apple hardware. There are hundreds of free Linux distributions, however, that will work. Canonical's Ubuntu 8.10 — code-named Intrepid Ibex — is arguably the easiest Linux distro (Distribution) for Windows users to install, configure, and use.

In addition to the major revamps that appear each year in April and October, Ubuntu receives updates and patches almost daily. The free OS also comes with an enormous library of free, downloadable applications and utilities.

Installing most Linux distributions requires you to download and burn to a CD a several-hundred-megabyte .iso file and then boot your PC from that disc. Ubuntu supports this installation method, but it also provides an alternative, brain-dead-easy approach: Wubi, a free Ubuntu installer that works entirely within Windows (<http://wubi-installer.org>).

Rather than repartition your disks, Wubi downloads and installs Ubuntu's files to a virtual disk stored on your existing Windows partition. Wubi's download is still a daunting 700MB, which can take a while if you lack a fast connection. (Of course, you can keep using your other Windows programs while Wubi does its thing in the background.)

Once the download is complete, Wubi prompts you to reboot, after which you'll see a new boot menu listing as options your existing Windows installation and Ubuntu.

Wubi obviously isn't the right tool for every situation. If you plan to install Ubuntu on multiple machines or would like to preview how well it supports your PC's hardware before installing, you're better off downloading, burning, and booting the live CD version of Ubuntu ([www.ubuntu.com](http://www.ubuntu.com)). The live CD is also the only way to install Ubuntu to its own partition.

Dual-booting Windows and Ubuntu is not your only option. If your system has sufficient RAM, you can run Ubuntu within a Windows virtual machine. If you use this method, I recommend that you have at least 1GB of system memory under Windows XP and at least 2GB on Vista PC for acceptable performance.

## **Where to find Ubuntu device drivers**

In the past, the first time you booted Linux often resulted in a mixture of joy and sorrow. The joy is in having a free, non-commercial operating system that boots and runs so well. The sorrow is in realizing that many of your hardware devices simply don't work as well under Ubuntu as they do under Windows — if they work at all.

Ubuntu 8.10 and other current Linux distros have dramatically improved hardware support, compared with previous versions. As a result, you may find that Intrepid Ibex recognizes and enables all the peripherals on your system. Wireless networking remains a weak area, however. If Ubuntu doesn't support your wireless adapter, install a Windows driver using the Ndiswrapper utility

(<https://help.ubuntu.com/community/WifiDocs/Driver/Ndiswrapper>).

Makers of display adapters and other hardware often provide Linux drivers for the devices. However, unless the drivers are open-source, they won't be installed by default in Ubuntu.

To enable proprietary hardware drivers in Ubuntu, choose Add/Remove Applications on Ubuntu's Applications menu, search for hardware drivers, check the box next to the Hardware Drivers application in the search results, and click Apply Changes. Next, choose System, Administration, Hardware Drivers. Follow the instructions that appear for activating the driver.

Likewise, Ubuntu rejects proprietary software, such as the codecs necessary to play back MP3s, DVDs, Flash animations, and other media. To enable most of these proprietary plug-ins and codecs in one fell swoop, return to the Add/Remove Applications utility and search for and install Ubuntu restricted extras.

### Exploring Ubuntu's wealth of applications

Once you get Ubuntu's basic configuration down, start investigating the OS's interface and built-in applications via the Applications menu. You'll find some familiar faces — both Firefox and OpenOffice.org are installed by default.

If you're feeling adventurous, choose Add/Remove Applications to browse Ubuntu's online software repositories of office, entertainment, and scientific programs. They're all free.

If you take a liking to Ubuntu — or another Linux distribution, for that matter — you may end up replacing Windows entirely. Linux's Wine utility allows many Windows programs — though not all of them — to run under Linux.

In a pinch, you can install a copy of Windows in a Linux virtual machine. Should the installation come under malware attack, just delete it and reinstall Windows in a new VM. Your Linux host installation will remain unfazed.

Operating systems aren't necessarily a one-size-fits-all affair. And anyway, who says you have to choose only one?

At the moment we do not offer tech support for any Linux operating systems. But this may change in the future.

## Three Quality Laptop Deals

### IBM ThinkPad T41.

14.1" screen, 40Gb hard drive, 512Mb RAM, wireless, XP Home.

These have been returned to IBM for re-furbishment after a 18 month business contract with a large company.

All tested and with any scratched panels replaced. Unboxed but with free carry bag. 30Day warranty, ideal first laptop.

**£199 inc vat**



### The all new Fujitsu Siemens mini laptop.

With a 8.9" wide-screen, Intel Atom processor, 60GB hard drive, 1Gb RAM, webcam, XP home.

Only weighs 1Kg! Up to 4 hours battery life. Boxed with 12 months Fujitsu warranty.

**£265 inc vat**



### Toshiba Satellite Pro Dual Core

15.4" widescreen, 120Gb hard drive, 2Gb RAM, Vista Premium. Boxed with 12 months Toshiba warranty.

**£399 inc vat**

## Tip

Software conflicts are the biggest pain in a computer technician's life. They involve hours of trial and error and searching late release notes from many manufacturers and the Internet. More often than not, the fix costs many times the value of the PC, so if you don't want to spend the family fortune on getting your PC fixed, read on.

Many software conflicts come to light when a Windows automatic update installs and other software suddenly conflicts with it. Well known names such as Skype, Zone Alarm and Adobe have all had to bring out fixes in the last few months to keep up with Windows updates. The first thing to do if you have a problem is to hang on for a few days. (Software manufacturers are usually quick to bring out a fix for their software if a Windows update has trashed it). Then check all your software to see if updates are available. Still got a problem? Then its down to Googling it and wading through hours of listings.

If all else fails, ring for an engineer. He'll probably reinstall and add your programs one by one until the problem arises. Still not a cheap option!

## Virgin Media Special offer

Virgin media is currently the only broadband service provider using Fibre



-Optic cable to provide your broadband, rather than squeezing it down your phone line. This means faster, more reliable Internet access, no phone filters and worries about internal phone wiring dropping the connection.

Most people know that in Northants, Virgin brought NTL and NTL were well known for being hard work if you needed to contact them. But our local Virgin rep assures us that Virgin are making big strides to improve the situation. Despite this, we've never had a problem with the product, it works and is good value.

We have been able to negotiate a special deal for new Virgin customers, enabling us to provide a FREE cable wireless router (usually £43.75) with every installation that it booked and installed by us.

The wireless router acts as a firewall, a network hub so that if you have more than one PC, they can transfer files and print to each others printers. Also a wireless enabled PC or laptop can surf the internet from anywhere in the house.

So if you are unhappy with your existing ISP or if your broadband is slow give us a call. We can check with Virgin to see if you have cable to your street, arrange installation and the all important wireless security.

**01604 415984**

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](http://www.computerdoctors.uk.net/pages/newsletter.htm)



Map to our Northampton Workshop  
[www.computerdoctors.uk.net/  
pages/map.htm](http://www.computerdoctors.uk.net/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: 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)

### Email test Facility:

[mail.computerdoctors@keme.co.uk](mailto:mail.computerdoctors@keme.co.uk)

