

# Something new...



To keep your computer safe you need to know the dangers and the steps you can take to stop them. Find out how right here...

Without regular maintenance of the information contained on your computer, you'll find it will gradually become slower.

Music and photography files occupy lots of space, but just regularly adding and deleting files will mean they become spread over your hard disk, or fragmented, so take longer to load. For many reasons it's important to perform a regular computer health check.

## Health check

Defragmenting your disk will gather together all your files and you'll find lots of magazines and books that explain this process.

Making regular backups and creating a 'restore' disk is vital

unless you're happy to lose all your key data in the event of an unexpected computer failure!

When you're surfing the internet, the need for protection and maintenance routines is much greater - even if you're only sending emails. Most of these routines can be automated and will operate quietly in the background.

There are about 450,000,000 internet surfers around the world, and if you take precautions to stay safe it's an amazing place to discover. The technology's there to contact all these people and there's still 93% of the world's population to get on board!

There's a minority, however, who use the internet maliciously.

Viruses were once a bit of a prank but are much more money-oriented and malicious now, so you need to develop your computer's immunity.

## Prone to infection

According to security company Sophos, an unprotected computer is on average infected with malicious software, or **malware**, within 12 minutes of being plugged into the internet! It is also estimated that over 90% of the world's computers have an infection of some sort. But don't let this put you off, because you can stop this happening to you.

**Malware** is software that's been designed to intercept or take partial control of a computer's

## Your quick guide to a healthy computer...

- **Install and turn on a Firewall** - It's the most effective way to prevent others accessing your machine. Most operating systems such as Windows XP will have one installed. Make sure yours is turned on!
- **Install anti-virus software** - And make sure it's regularly updated. Good examples are McAfee, Sophos, Kaspersky and Norton. At Stitchlinks we use the powerful AVG Antivirus.
- **Install an anti-spyware program** - Run it regularly and keep it up to date. Find out more on our Freestuff section of the website where you'll find a short report on Spyware and what you can do about it.
- **Beware of downloading** - From unknown sites. They can harbour trojans (see jargon). If you do - and we do it, too - try to make sure you have a recent backup just in case you need to reinstall everything.
- **NEVER open** - Email attachments from unknown sources - even if they appear innocent. It's a classic way of spreading viruses or trojans. If you don't know the person, don't open the attachment.
- **Beware of 'banks'** - Emails from your bank, ebay or PayPal will contain your name in the header. Bonafide Banks never ask for full sets of passwords on the internet. Never click on the links included.
- **Don't respond** - To emails asking you to confirm financial details as part of an upgrade or security check unless your name is included in the message. Better still confirm by post.
- **Check website addresses** - On links, as trojans can direct a computer to a bogus address to collect your details. Instead, type the URL (web address) in yourself rather than click on a link.
- **Check page security** - Any page that collects financial details needs to be secure. Secure sites now advertise the fact with a little padlock sign, which you'll find at the bottom right-hand corner. This is normally a good indicator. Continue to take the precautions above as well.

operation without the informed consent of the owner. It can be grouped into the two general categories; **viruses** and **spyware**.

**Viruses** are programs that can reproduce themselves many times, or run to cause damage to your computer when a pre-programmed set of circumstances comes about; **spyware** are small, malicious programs that get into your computer and gather information about you that can be remotely accessed. Each of these processes will also add more background activity to your computer, which will inevitably slow it down.

While the effects of spyware and viruses could just be a slower computer, or the appearance of irritating adverts, they could be more serious. For example, they could send a copy of themselves to everyone on your email Contacts list, or your computer could be opened up to allow someone to access personal information. At

worst, your computer may be turned into a **zombie** – controlled from the outside and used to spam other users all over the world.

### Building up immunity

It's something you need to take seriously, but the good news is that armed with this knowledge you can take action to stay safe and enjoy the tremendous benefits of the internet and it's potential to introduce you to the rest of the world. Whatever you do – don't stop using it; you still have 449,999,999 friends out there to contact ! And there will be at least another 64,000,000 next year (that's about two every second)!

In August 2006, Google announced that it will introduce warnings to notify users about websites which are known to distribute 'badware'. Google search users will be warned before they enter suspect websites: "The site you are about to visit may

harm your computer!" Along with Lenovo and Sun Microsystems it has also sponsored a StopBadware project, in which researchers from Harvard and Oxford Universities are creating a clearing house for information on malicious software and the ways they're circulated.

As far as you're concerned it's all about being aware and installing effective antivirus and spyware programs, which will keep you safe. It's like everything else in life; you gather the knowledge, take precautions to stay safe, then go out and enjoy the new experiences!

New malware is developed daily, so it's important to regularly update your antivirus programs. This can be done automatically; here at Stitchlinks our protection is updated every time we switch on our computers at no extra cost , so we know we're as safe as we can be against the latest viruses.

Take a look at how to go about improving computer safety, below.



## Your quick guide to a healthy computer...

- **Use a different browser** – Internet Explorer is a huge target for spyware. Try a different browser. At Stitchlinks we use Mozilla Firefox, which can be downloaded free.
- **Install from a CD** – CDs can't be tampered with, so if you can install software from a CD rather than as a download, do so. Make sure it's not an illegal copy, because they just may have some trojans on them.
- **Take regular backups** – And make sure you have kept a separate record of any settings that you will need if you do have to reinstall software that may have become corrupted. You won't lose data this way.

### Jargon

Making it easier to understand those technical terms

- **Antivirus software** – A computer program that identifies and eliminates viruses and other malicious software.
- **Firewall** – Helps to screen out attempts to access your computer via the net. Switch on before surfing!
- **Phishing** – The practice of illegally trying to get hold of personal details. Examples are fake bank, PayPal and ebay sites.
- **Spyware** – A program that watches what computer users do and reports back over the internet. Less harmful versions will simply track what types of websites you visit and send this information to an advertisement agency. Malicious versions can record what you type to intercept passwords, credit card and personal details.
- **Trojan horse** – Malicious software disguised as, or hidden in legitimate software. Only buy from recommended sources!
- **Virus** – A program that inserts copies of itself into other programs or documents. These will damage files on your computer and can be passed on to others.
- **Worm** – A worm can multiply by itself without any intervention. It uses a network to send copies of itself to other systems. They slow down networks.