

How to:



**Friends of
the Earth**

protect your computer a guide to trouble-free computing

As use of computers both at home and work continues to grow and grow, so unfortunately do the risks. Friends of the Earth's Community Site Manager Jonathan Nichols shares some simple precautions that you can take to make cyberspace a safer place to be

Computers and the internet can be fantastic tools to help your local group with its campaigning. Your computer allows you to send letters and mailings, produce newsletters, keep the accounts, design posters, contact other campaigners, look up facts and figures on the internet and all manner of useful things. And most local groups will have at least one person amongst them who knows their way around a computer...

If your group would benefit from access to a computer, or from updating an existing system, **Friends of the Earth's Local Groups Support Fund** may be able to help buy computer equipment. Contact Naomi Hunt on 020 7566 1677, or localgroups@foe.co.uk to ask for an application form.

You can also download the form from: http://community.foe.co.uk/local_groups/running_your_own/resource/fundraising/index.html



General information

References to software included in this guide may well go out of date quickly – I recommend occasionally looking at computer magazines available in newsagents for up-to-date information.

You may also like to share your tips on safe computer use, or ask for advice from others, in the Computers discussion forum at <http://community.foe.co.uk/discussion>

People using Windows can also visit Microsoft's Home User Security Centre at <http://www.microsoft.com/athome/security/>.

The Government has recently launched <http://www.itsafe.gov.uk/> – a regularly updated website with advice for home and business computer users. The site also lets you sign up to receive alerts and updates by email.

Speak the lingo

the low-down on commonly-used computer terms

1. Virus

Simply speaking, a computer virus is a small piece of code which infects your computer – the term comes from its ability to spread from one computer to another. The type of ‘infection’ and its effect varies widely – many viruses cause minor inconvenience (such as making your computer run slowly, or popping up messages on the screen), while others can cause serious damage, such as deleting files or stopping you from using your computer completely.

Trojans and **worms** are types of programme which can harm your computer. Where I use the term virus here, I will often mean trojans and worms as well.

How to detect a virus

A wide range of anti-virus software is available at a range of prices (some is even free, and can be just as effective as paid-for software). One essential thing to remember though is that whichever you choose, **it is only effective if it is updated and used regularly**. Anti-virus software checks files on your computer against a list of known viruses, and so regular updates are needed to keep this list current. See page 14 for examples of anti-virus software. I suggest running a full virus scan of your computer once a fortnight. You should also scan any discs or CDs given to you with files on before opening the files.

Mac or Linux?

Historically, the vast majority of viruses were written for the Windows system, and so Macs (and computers running other operating systems such as Linux) have always been considered safer in this regard. However, as Mac usage becomes more and more popular, virus creators are targeting them more – and so you should still take these precautions. Some of the software is PC-only, but alternatives should be available either by searching the internet or looking in a Mac-users magazine available in most newsagents.

2. Spyware

Spyware is software which hides on your computer and literally spies on what you use the computer for – eg recording which websites you visit or the passwords that you enter. This information could be used for criminal activities, such as accessing your online bank account, or is sold to companies for marketing purposes. As well as invasion of privacy, spyware can also cause your computer to run slowly. It can get on to your computer in many ways, so check for it regularly.

Tools for checking spyware

Adaware –

<http://www.lavasoftusa.com/software/adaware/>

SpyBot – <http://spybot.safer-networking.de/>

Microsoft / Giant –

<http://www.microsoft.com/athome/security/spyware/software/>

Win Patrol – <http://www.winpatrol.com/>

3. Firewall

A firewall essentially acts like a wall between your computer and other computers/the internet – it will stop any unwanted transfer of information between them. Windows XP has a built-in firewall, but you may need to switch it on – if you use XP look in the help section for more information. Free firewall software is available from <http://www.zonelabs.com> or <http://smb.sygate.com/>

4. Spam

This is the common name used for unsolicited email messages, which are a huge problem. They clog up email inboxes, and can be offensive and/or fraudulent.



5. Power surges

Occasional power surges can damage your computer via the power cable or phone line. You can buy a **surge protector**, which is usually built into a multi-way adaptor, fairly cheaply. Many now come with a limited amount of insurance for equipment which is plugged into it.

During a lightning storm, you should unplug as much electrical equipment as possible anyway – not all surge protectors can cope with lightning strikes.

6. Backups

There are several ways you can lose important information stored on your computer – even without viruses, your hard drive can still get corrupted. If you do a **regular** (say monthly) back up you will minimise any loss.

Think about what is on your computer which is either irreplaceable or would take a lot of effort to replace. If you **organise** your files tidily (eg if you use Microsoft Windows, save all your personal files in the c:\my documents folder) things are much easier – you can simply back up one folder. You also need to find out where your emails, email addresses and favourites are saved – each email package saves them in a different place. In Outlook, addresses are in C:\Windows\Application Data\Microsoft\AddressBook and email messages in C:\Windows\Application Data\Microsoft\Outlook.

✓ **Avoid** copying files into another folder on the same drive. If the hard drive corrupts you'll still lose them.

✓ **Don't** use floppy discs. They aren't reliable and in any case don't hold many files.

✓ **Remember** – if something bad happens to your hard drive, you'll need to reinstall the operating system and all of the programs before you can retrieve your backed-up data. You can do this either from the original CD-ROMs (which you should keep in a safe place, together with any serial numbers) or you could use **ghosting** software to create a snapshot of your whole system which can be recovered later – search the internet to find suitable software.

7. Phishing

Emails which claim to be sent by well-known companies, and which ask you to reply with personal information such as your credit card number or account password, are a major problem.

These deceptive emails are called spoof emails because they fake the appearance of a popular website or company – they are also known as hoax or phishing emails.

Reputable companies will not ask you for sensitive personal information (such as your password or bank details) in an email. The best thing to do is to delete these messages – never reply to them. Never click on links in suspect emails either – if it appears to come from a website that you do use, login to that website in your usual way rather than following a link.

8. Browsers

Chances are you use **Internet Explorer** to access (or browse) the internet – it is by far the most popular software for doing this, but it is also the browser most easily susceptible to spyware. There are alternative free internet browsers available – such as **Firefox** (<http://www.getfirefox.com/>) or **Opera** (<http://www.opera.com/>) – which have several features built-in to help protect your privacy.

9. Windows update

If you use Microsoft Windows, you should install all the latest **Critical Updates** as they are released. See <http://windowsupdate.microsoft.com/>.

Depending on the speed of your internet connection, this could take some time, but it's a fairly simple process and one which should be done regularly.

Top tips for ...

...avoiding viruses

✓ Don't open email attachments if you don't know exactly what they are and who they are from. Even if you recognise the name of the sender, the attached file may not be safe. Some types of virus use email programs to quickly forward themselves to someone's entire email address book.

... avoiding spam

✓ **Never reply** to spam emails – this only confirms that the address is a real one and will lead to yet more spam.

✓ **Use different email accounts** for different purposes – eg one for friends and family only, one for signing up to mailing lists, and one for using in discussion forums.

When you register your details on a website, read the smallprint carefully and tick or untick any relevant boxes to make sure your address isn't added to a mailing list.

✓ Your email software should include **filters** – use these to filter out messages containing certain words which you don't want to read.

... making back ups

✓ If you have a CD/RW drive, you can make backups to **CD-rom**. You may even have software already installed which makes the whole process

easier. CD-roms are relatively cheap, but are fairly limited in the amount of data that they can hold. Obviously you need to then keep these CD-roms in a safe place.

✓ You can make backups to a separate **hard drive**, either internally placed in your computer, or externally linked by a cable which can be unplugged. This backup method is more expensive but more reliable than using CD-roms.

✓ There are several companies which can back up the contents of your computer **online**. These services cost money, but do provide the assurance that your data is backed up by professionals and at a remote site. You'll need a broadband connection to make this a realistic option

... choosing passwords

✓ Use different passwords for different purposes, eg online banking, email, discussion forums.

✓ Use eight characters or more.

✓ Use a combination of letters (upper and lower case) and numbers.

✓ Change your passwords frequently – say every six months.

✓ Don't use information easily obtained about you, eg child's name, your street name.

Examples of anti-virus software

AVG anti virus <http://free.grisoft.com/>

AVAST <http://www.avast.com/>

AntiVir <http://www.free-av.com/>

McAfee Anti-Virus <http://www.mcafee.com/>

Norton Anti-Virus http://www.symantec.com/product/index_homecomp.html

Sophos Anti-Virus <http://www.sophos.com/>

F-Secure <http://www.f-secure.com/solutions/home.shtml>

Some websites such as <http://housecall.trendmicro.com/> also offer an online virus scan of your computer – these are useful, but don't replace the need to install anti-virus software.