



BW Data Designs

# Home Computer Security Suite



*Advice and useful Internet website  
addresses for providing affordable  
security on Home Computers*





---

# Home Computer Security Suite

*Advice and useful Internet website addresses for providing affordable security for Home Computer users.*

*Presented by BW Data Designs*

## Computer Security

The threats encountered during the use of the Internet today are not just the technological ones such as virus infections and the like, but more recently the threats against personal liberty, the real possibility of identity theft and even more worrying the threat to younger users from people with “less than honourable intentions”.

Identity theft can lead to fraud on a massive scale and the modern home computer, which used to be seen as a repository for such personal information such as addresses and even bank account details can no longer be regarded as safe for storing such information. The Internet Explorer address book is often attacked to try to gain information about users and their contacts, avoid using this facility.

The very worrying threat to younger users has been well covered in the news media over recent months; even so, with the increased use of such websites as “FaceBook”, “MySpace” and “Bebo”, the problems seem to be on the increase. The only way to stay safe online is for users to recognise the threats and to ensure that their actions are appropriate. Parents need to make it their responsibility to exercise some level of supervision over the use of home computers. Those parents who claim that they don’t understand the newer technology need to take steps to learn about computing for their own benefit as well as other family members.

Users must also be aware that no personal information should ever be transmitted over the internet, and in some cases that means not even a user’s real name, and most definitely not the real home address or age.

Many threats to PCs and the data they hold exist, particularly if the computer is connected to the Internet, and even though there are software solutions to most of these threats, the main weapon in a user’s armoury is continued vigilance and a cynical attitude towards everything “offered” to them.

A healthy attitude to adopt is one of **“If it looks too good to be true, then it probably is”**.

---

As users are becoming more “net-savvy”, so are the writers of malicious codes, so called malware or scumware. Methods employed to deliver and deploy viruses are becoming ever more sophisticated and although the basic method remains the same as it’s always been, an attachment to an email, there are indications that some infections originate from infected websites; the so-called “drive-by” infection method. In the early years of the Internet many of those malicious codes were written by young computer enthusiasts out to prove that they could find ways around the rudimentary security applications that existed at the time. Nowadays the spectre of world wide organised crime is responsible for many of the threats.

These days, most viruses are written to be able to read the contents of an infected computer’s address book and send itself to those addresses, the clever bit is that they can also “spooft” the sender’s address, making it look as though the infected email is coming from someone known to the recipient. Scanning of attachments for viruses before opening them is of the utmost importance. Many ISPs who provide email services will have a plug-in for their email programs that will prevent known viruses being delivered.

There has also been a rise in so-called “Phishing” recently. This practise usually involves trying to gain information relating to a user’s personal details such as bank account numbers, PIN numbers, passwords and so on. This is based on the method of sending official looking emails to a recipient, often threatening that a particular account such as PayPal, email accounts, bank accounts, etc. will be terminated within a short period unless all the relevant details are supplied. The question one must ask is “Would that service actually use email to ask for such details?” If in doubt, do not reply to the email, but go to the website of the service involved and research the questions yourself, or better still use the telephone or even a letter. It’s only at that site will you find the necessary secure transaction systems for information such as passwords. It’s often a reasonable course of action to email, or otherwise, contact that service and voice your concerns; they might be unaware that their customers are being targeted. Of course, the biggest giveaway is an email from Barclays Bank requesting security information when you know that you bank with HSBC.

Spam, junk email, call it what you like, but it is still unwanted electronic communications and is a “fact of life” on the Internet, especially if your email address is published on a website. Users can reduce the volume of spam by adopting a healthy cynicism towards it. Check your email program’s mail filters and set them appropriately. However, not even the best filters will keep it all out. It’s important that you never reply to spam, although it is tempting to click the box at the bottom, which says something like “To unsubscribe .... Etc” **do not do it**, the sender will become aware that he has found a live inbox and will send even more spam. The best option is to block the sender’s address in your email filters and delete the email.

The threat to your personal details, such as bank account numbers, PIN numbers, your address book contacts and so many other snippets of information can continue even after you’ve disposed of your computer. Deleting files and folders in the normal fashion does not remove the information from the hard disk, nor even does re-formatting the disk. The data remains on the hard disk and that information can be recovered by those with less than honourable intentions sometimes resulting in fraudulent use of that information. Software is available to completely erase all previous data and programs from a hard disk drive prior to disposal of an old computer. If you are unable to locate or use such software tools, you would be well advised to remove the hard disk drive from the computer and physically destroy it before disposing of the computer.

BW Data Designs can advise and assist you with these extremely important security issues.

---

•  
•  
•  
•  
•  
•  
•  
•



## Home Networks

Home PCs and laptops are becoming cheaper and more easily available and along with broadband internet connections and easily configured routers the possibilities for new threats abound. The new home network can pose major security risk.

It is even more important that each computer on the home network is protected against all of the threats examined in this document, anti-virus, anti-spyware, and so on. If an infection is found on one machine, it will migrate immediately to all the other machines on the network. Removal must be carried out on all the machines, individually while they are disconnected from the network. It is not sufficient to think that one computer is protected so all the others will be too.

A firewall is essential on all machines on the home network too, although the router might be fitted with a software or hardware firewall, it will have to be set up to prevent access to the network from known IP addresses, whereas the firewall on your computer, such as Zone Alarm works in the opposite way, it prevents access from all IP addresses unless you give permission. The router firewall can however be a useful tool in your security armoury. Provided you know the address of the website you want to deny access, then it will be denied to all computers on the network.

Modern laptops are designed for wireless internet connection, either using a local hotspot, such as a café, restaurant, hotel, some motorway service areas or at home. Wifi internet routers for home use are rapidly becoming the norm in home networks, and even though you have all the security measures in place, there are still threats to be considered.

Many of the cheaper broadband connections are “limited bandwidth”, that is users are allowed to download up to a given, agreed maximum amount of data in a given period of time. This might be 2GB, 5GB per month, or whatever download limit is quoted on your contract with your ISP. Incorrect setting of the wireless router can allow other people to use your connection, and your download limit without your permission, effectively stealing what you have paid for. It can come as somewhat of a shock to find that your bandwidth allowance has been used by someone else.

Almost all wireless routers allow users to set up some sort of password protection on their connection, which while it won't prevent others from “seeing” your network; it will require a password to connect to it. These passwords can be set for either 64 bit or 128 bit encryption. 128 bit encryption will require a password containing 26 digits in the range 0 to 9 and A to F. An awesome level of security, one might think. However, there are electronic devices that can be purchased quite cheaply that can crack these passwords fairly quickly. It is therefore essential that they are changed at regular intervals if you don't want to find yourself having to wait until next month to download those pictures from the family overseas.

An open wireless network can also allow unauthorised access to any folders on a computer that have been set for sharing between other machines on the home network. BW Data Designs can assist in setting up Small Office/Home Office and wireless networks.



## Anti-virus software

Security software specialists estimate that the number of malicious programs and viruses released to the Internet is running at something like 300 a week, fortunately most are variants of previously identified viruses and their products are quickly updated to meet the threat, but users of computers must realise that their own security software must also be regularly updated to take advantage of the improvements.

Computer suppliers will often “bundle” an anti-virus program with other loaded applications upon purchase. These programs are usually of the licenced variety and good for one year of free updates; however continued safe operation will require that you purchase another year of updates. The fee is often in the region of £10, paid by credit card over a secure web connection.

To the new user, this can appear as a “good deal”, but why pay for something that you can get free?

### Freeware

- Download: **AVG Anti-Virus** [www.grisoft.com](http://www.grisoft.com) AVG is a free anti-virus package that is loaded onto your computer so that you can scan for and remove virus programs. Free licence for personal use only. Check weekly for updates to the definitions list. The latest version, AVG2011 (AVG 10.0) can be set to check for and update automatically every day.
  - Download: **Avast Anti-Virus** <http://www.avast.com> Avast is another well respected anti virus application that is free to use for home users. The current version is 5.0.677. Like AVG, it also provides free definitions updates. Other versions can be purchased for “Enterprise” and business use. Avast also operate an online virus scanner
  - On-line scans: **Housecall** [www.trendmicro.com/housecall](http://www.trendmicro.com/housecall) A free scanner, which operates on-line. You log into the site and start the scan. “Housecall” can automatically remove any virus it finds. This scanner can take some time for larger drives. There is no need to update since “Housecall” is not actually loaded onto your machine, although some of the software will load on your computer before the very first scan. BW Data Design’s own website provides a direct link to the Housecall service.
  - **Microsoft Malicious Software Removal Tool.** The latest version is downloaded to a user’s computer once a month, during the update process from the Microsoft Updates website. The removal tools is installed and run once automatically. The removal tool can be downloaded manually from the Microsoft download centre. It is configured to remove many of the more serious threats noted in the last few years including the “Blaster” and “MyDoom” worms. The Microsoft Malicious Software Removal Tool is updated automatically on a monthly basis with the operating system updates.
-



**Licensed (purchased)** *The two most well known are detailed but others are available*

- **McAfee** virus scan. [www.mcafee.com](http://www.mcafee.com) This virus scanner loads to your machine. Supplied on CD-ROM, about £30 from PC World. The licence must be renewed annually and costs about £10. Virus definitions are updated regularly and automatically.
- **Norton Anti Virus.** [www.symantic.com](http://www.symantic.com) This anti-virus software is very similar to that supplied by McAfee in that the main system is loaded from a CD to your machine and regular updates of the virus definitions list are automatic. An annual licence must also be renewed to maintain full protection.

Both Norton Anti-Virus and McAfee have shown signs in the past of slowing the operation of a computer owing to the high demand placed upon memory resources, especially during the start-up process.

Some ISPs offer their own versions of an anti-virus application, usually a “re-badged” version of McAfee or Norton. In many cases, there is an option, albeit well hidden, to opt out, rather than to opt in to the program. Among the most notable ISPs operating this technique is AOL.

Conflicts can occur if more than one anti-virus application is installed on your computer. If a “second opinion” is required, then you would be advised to use an on-line scanner.

One major advantage of freeware over purchased solutions is concerned with updates, often issued on a daily basis. A purchased program will most likely be configured to download and install any updates automatically, with no intervention from the user. However, once the licence has expired, usually after one year, a further licence purchase is required to be made to continue receiving updates.

Updates for freeware will continue for the life of the program, often automatically too. So no matter how new the threat, a freeware anti-virus program, while being a few hours late in supplying an update to combat the threat, will supply an update to protect you. A purchased licence will only protect your computer if you remembered to renew the licence.

Neither Norton Anti-Virus nor McAfee can be removed easily from Add/Remove programs in the Control Panel. Both will require the use of the correct removal program, either of which can be found at Major Geeks [www.majorgeeks.com](http://www.majorgeeks.com)



## Firewalls

### Freeware

A firewall is strongly advised for those users on a dial-up connection and essential for users with a broadband connection. Firewalls prevent unauthorised activity such as crackers gaining access to your computer from a remote location or your computer sending data to the Internet without your knowledge. In a very small number of cases, a firewall has to be disabled for an application to run correctly, notably PC Pitstop might not execute properly while Zone Alarm is active.

- **Zone Alarm** [www.zonelabs.com](http://www.zonelabs.com) This firewall, unlike some of the purchased applications is easy to set up once it has been downloaded to the computer. It can be set for your own personal web activities by asking very simple questions such as “This is a new website, do you want to access it?” All you have to do is just click on the “yes” button.

### Licensed (purchase)

- **McAfee Firewall.** [www.mcafee.com](http://www.mcafee.com) This firewall is usually bundled with the McAfee virus scan and is available from such outlets as PC World. It is not the easiest firewall to set up.

There are two main firewall types; software and hardware. Software firewalls, often referred to as “Personal Firewalls” are designed to close all routes into the central processor from the external network and then to seek permission to allow an operation to be undertaken. Hardware firewalls usually operate in the opposite way; that is they will allow all operations or addresses unless that address has been previously blocked. Hardware firewalls are most often found as an integral part of a network router device.

### Microsoft Windows

Following the introduction of Windows XP Service Pack 2, all Windows operating systems have incorporated a Personal Firewall, which following initial teething troubles can now be regarded as efficient and able to provide a minimum level of security. Users who want to install enhanced security levels can install any third party firewall application they wish. Users are advised that there could be conflicts between the installed firewalls and the Windows application should be disabled.

---



## Anti spyware and advertising ware.

Spyware is the generic name for codes that are placed on your computer usually for underhanded marketing purposes. These small codes, usually called cookies are normally designed to allow users to set their own preference when regularly visiting a website, but some are written to monitor your Internet use and report activity back to the cookie owner so that your machine can be targeted with pop-ups and advertising that you might be interested in. For the most part, they do no real damage to your machine, unlike viruses, but they can block up and consequently slow down your computer.

There are some potentially dangerous consequences of having some spyware hidden on your computer hard drive, one of the most worrying aspects involves the use of keyloggers; small programs that actually track a user's keyboard use and report the operations to the program owner, not what a computer user needs when accessing secure sites to use a credit card, for instance. Another growing trend is to automatically re-direct an Internet connected computer to another "Service Provider" by installing an unauthorised dialler. These diallers are usually configured to connect the computer to premium rate numbers, often overseas. The cost implications are quite horrendous, some charges have been reported as many tens of pounds per minute! Fortunately, such re-diallers are not such a problem for broadband users.

Since these programs are usually correctly written code, and not a virus, the many anti-virus scanners will not be configured to locate and eradicate them, and finding and removing these cookies is not the easiest operation for a user. Fortunately, there are programs that can do this for you.

### Freeware

- **MalwareBytes Anti-Malware** [www.malwarebytes.org](http://www.malwarebytes.org) is a well respected program which can stop any malware from running and then clean out the offending program. This program is particularly effective when run with the computer in Safe Mode.
- **SUPERAntiSpyware** [www.superantispyware.com](http://www.superantispyware.com) is another very well respected anti spyware program which can clean out almost all bad software. It is most effective when used in conjunction with MalwareBytes Anti-Malware.
- **SpyBot S&D** [www.safer-networking.org/en/download/](http://www.safer-networking.org/en/download/) SpyBot Search and Destroy scans your computer storage looking for these "tracking cookies" and then presents you with a list with the option to retain or remove them. The Spybot opening screen gives a link to "Spyware Blaster" which can be run together with Spybot to offer an increased level of protection. Spybot can recognise and eliminate many keyloggers.



- **Ad-Aware** [www.lavasoft.de](http://www.lavasoft.de) The latest version is Ad-Aware 8.3.3 which can locate and remove tracking cookies associated with advertising. Removal of these cookies can often mean that many pop-ups will not actually find your computer.
- **SpywareBlaster** [www.javacoolsoftware.com](http://www.javacoolsoftware.com) This is a useful utility that can be run in the background quite safely alongside other spyware products. Its main function is that of an anti spyware firewall, in that it prevents most attempts of a remote website planting tracking cookies on your computer. It does not remove spyware already resident on the machine.
- Pop-up stoppers can play a part in the efficient and enjoyable web experience. Be warned, many pop-up stoppers are themselves some kind of spyware, often loaded as a part of say “A funky new toolbar”. The Google ([www.google.co.uk](http://www.google.co.uk) or [www.google.com](http://www.google.com)) toolbar is an excellent search facility that does incorporate an effective pop-up stopper. Internet Explorer 8 includes a pop-up stopper.
- **Spychecker** [www.spychecker.com](http://www.spychecker.com) contains a useful list of the top Internet security applications with links to the downloadable programs. They list freeware, shareware and trial versions.

## Microsoft Windows Defender

[www.microsoft.com/athome/security/spyware/software/default.msp](http://www.microsoft.com/athome/security/spyware/software/default.msp)

Following the introduction of Windows Vista, Windows operating systems have incorporated an Anti-scamware scanner called Windows Defender. It can be manually updated or can update automatically during the operating system update procedure at the Microsoft Update website. Defender can only be installed on genuine validated copies of Windows XP SP2 or Windows 2000.

## Combined solutions

**The combination of MalwareBytes Anti-Malware and SUPERAntiSpyware is recommended to ensure that your computer is kept as clear of these malicious codes as possible since each program is designed to target a specific type of threat. Both MalwareBytes Anti-Malware and SUPERAntiSpyware must be manually updated regularly.**

Many security programs, including those listed above and other useful utilities can be found at a very good download website called **Major Geeks** at [www.majorgeeks.com](http://www.majorgeeks.com). Some of the security and cleaning programs found here can be very aggressive in their operation; consequently users would be well advised to seek further assistance in choosing the correct solution to a particular problem.

---



Many of the programs offered at Major Geeks are “freeware”, but some are of the “shareware” variety; that is a payment is usually required to fully activate the product.

## Rogue anti-virus programs

Some anti spyware tools are offered on the Internet that will scan your computer for malicious codes and after finding some offending programs will demand a subscription before the removal process can begin. Obviously, when there are fully functional free programs available, there is little to be gained from purchasing any of these applications. Some even go as far as indicating the presence of a threat when none really exists. This type of “marketing” is designed to play upon the lack of knowledge and insecurities of some computer users.

Many of the later versions of this type of malicious programs can “take over” your computer, often starting before the operating system and consequently not allowing the user to do anything. Very often this kind of software has its own protection to prevent users trying to remove it. Removal of this kind of program is often very difficult and can be extremely time consuming. There is no guarantee that the presence of this kind of program will not cause further damage to the operating system and Program Files, particularly if incorrect removal methods have previously been tried.

**It is extremely important to remember that any security software is only as good as the last update. Update all security software regularly.**



## Anti parasites

Some of the utilities you might at some time download from the Internet can contain small codes for other than reasonable uses. These codes are hidden in the main code and can in some cases slow down or even damage your computer files.

- **DoxDesk** [www.doxdesk.com](http://www.doxdesk.com) can scan your machine and if any parasite is found it will offer advice on how to deal with the invasion. SpyBot S&D and Ad-Aware can remove many, but not all of these parasites. One notable recent parasite was “Hotbar”.
- **Hijackthis** [www.hijackthis.com](http://www.hijackthis.com) is a useful piece of software that can be employed in the fight against some invasions of a particular piece of scumware called the “Browser Hijacker”. The typical indication that a browser hijacker is present is the user’s own homepage, as set in the Internet Explorer settings changes to another page without the permission or intervention of the user. The main drawbacks with the Hijackthis software are first, it needs to be loaded to a disc and run from that if a user intends to run it regularly and secondly, interpreting the results can take a greater degree of knowledge of computer systems to identify any untoward software in the list.

## Computer diagnostics and performance

Maintaining your computer in tip-top condition can take time and knowledge. To help the less experienced user, there is a useful site at [www.pcpitstop.com](http://www.pcpitstop.com) where your computer’s “internal workings” can be checked and evaluated. Any deficiencies will be notified and often the site will offer fixes to repair the problem online and unlike many utility sites, most fixes are free.

The site can be set to scan your machine free and anonymously or you can set up a free account where comparisons between the current scan and previous scans can be made, so enabling you to track changes in your computer’s performance.

**Microsoft (Windows) Update** is a useful utility and should not be disregarded.

This is the Microsoft website specifically for updating and repairing deficiencies in the Microsoft Operating Systems. Windows XP, Vista and Windows 7 can be set to take updates automatically over the Internet. Many of these updates concern security patches (Hotfixes) to repair previously identified problems with Internet Explorer and the Operating System. They should not be overlooked.

The Microsoft Download Centre also offers free updates to all Microsoft products as well as such “toys” as template sets and clipart for Word and Excel. You are also advised to check the “Drivers” section of the Windows Update site for new or improved system drivers.

---



## Registry cleaners

The registry in your computer is not unlike an index of what a program needs to run properly. It is one of the most important parts of the operating system. Users should not make any changes to the registry unless they are fully conversant with the steps they are taking. Errors made while modifying registry entries could result in the computer failing completely.

There are numerous registry cleaners to be found on the internet. Some will say they are free, but when an initial scan is completed will demand money to repair the apparent problems. Some are too aggressive in their operation to be considered as suitable for the general user.

Two programs which include a safe and effective registry cleaner can be found at:

- **Ccleaner** by Piriform [www.piriform.com](http://www.piriform.com) can remove all those bits of files such as useless cookies which get left over from general surfing and eventually clog up your hard drive. It can also be used to safely stop programs from starting when the computer starts.
- **Advanced System Care** by Iobit software [www.iobit.com](http://www.iobit.com) is another program which can safely clean up the registry. It can also optimise the operating system as well as clean some spyware and load anti-spyware protection. Advanced System Care also offers some other novel features.

## Rootkits

There has been a recent increase in installed malware which is almost impossible to locate and eradicate using normal methods. These hidden programs have often been written with the sole purpose of “inviting in” other infections. Cleaning the invited infection is usually a straightforward operation and even though the computer then shows as clean in all respects, new infections appear almost as soon as it is reconnected to the internet. These hidden programs are referred to as “Rootkits”.

One solution is to run a program designed specifically to locate and remove these rootkits such as **F-Secure Blacklight Rootkit Remover** which can be downloaded free from:

[http://www.f-secure.com/en\\_EMEA/security/tools/blacklight/](http://www.f-secure.com/en_EMEA/security/tools/blacklight/)



## Other useful programs

### **Adobe Acrobat Reader** <http://get.adobe.com/uk/reader/>

This program is almost essential these days, primarily for downloading and reading large documents such as tutorials and user manuals. Most government offices now use Acrobat .pdf files for online documents. The latest versions are version 9.4.1 for Windows XP, Vista and Windows 7, and version 6 for Windows 95/98/ME.

### **Adobe Flash player** <http://get.adobe.com/flashplayer/>

Many websites these days use Flash. This is a program to enable you to view animations such as film clips, banner logos and so on. The main drawback with “Flash intensive” sites is the loading time; however, having the viewer loaded can greatly enhance the “experience” of some sites. Macromedia was purchased by Adobe Products during 2006. All older versions of Flash player must be removed prior to installing the latest version.

### **Quicktime** [www.apple.com/quicktime](http://www.apple.com/quicktime)

This is the Apple-Mac equivalent of Windows MediaPlayer. Some web designers favour Quicktime over MediaPlayer often because graphics designers prefer the Apple-Mac range of computers to PCs, and since it doesn't occupy much space on your hard drive (storage medium) then there's little to be lost by having it loaded ready for use. Quicktime will load with some applications you've purchased on CD-ROM.

## Disclaimer

1. The websites listed on this advice sheet are correct at the time of writing, but might, due to unforeseen circumstances close or be otherwise unavailable.
2. The websites listed here are my own preferences. Other similar services might be available to Internet users. Omissions or inclusions on this list are in no way meant to indicate the quality of such services.
3. The decision to install any of the software packages listed here is entirely at your own risk.

For further information please contact:

[security@dragonsegg.com](mailto:security@dragonsegg.com)

Tel: 01656 840746    Mobile: 07787 755463

Copyright. BGW © 2004-2010. All rights reserved.

---