PC Security and Your Protection.

Garry Henwood

Get the Latest Security Udates and Patches

From time to time, weaknesses are discovered in programmes running on your computer. These weaknesses can be exploited by virus writers and hackers to gain access to computers. As such, publishers will release 'patches' from time to time to correct these weaknesses.

To check for patches and updates you should visit the publisher's website, typically their 'Download' section. Generally, the latest versions of an operating system family (like Microsoft Windows) or browser (like Internet Explorer, Firefox etc) is the most secure.

Microsoft users can visit: http://windowsupdate.microsoft.com , which can automatically check what is required for both your operating system and browser and then download it at your request.

Install anti-virus software

You may already be using anti-virus software but to be effective, the software should be updated on a regular basis with the latest virus definition files. If you are unsure how to do this, you should refer to the program's 'Help' function.

Any file with no extension or a double extension, eg wow.jpg.pif is almost certainly a virus and should never be opened. Also, never open an e-mail attachment that contains a file ending with .exe, .pif and .vbs as these are commonly used with viruses.

There are many effective programs to choose from, but the most common commercial products include McAfee, Trend Micro, Sophos, Symantec and F-Secure. It is also possible to obtain free anti-virus protection from Microsoft Security Essentials, Grisoft AVG Anti-Virus, Antivir, ALWIL Avast and ClamWin. However, be sure to visit the genuine site as there are many fake products claiming to protect your computer but which may actually infect it with viruses.

Use a personal firewall

A personal firewall is another small program that helps protect your computer and its contents from outsiders on the internet. When installed and correctly configured, it stops unauthorised traffic to and from your computer.

There are many effective programs to choose from. Common commercial examples include Windows Firewall and Check Point Zone Alarm (free), McAfee Personal Firewall and Norton Personal Firewall.

Use Anti-spyware program

Spyware is the term used to describe programs that run on your computer which monitor and record the way you browse the internet and the sites you visit. It can also be downloaded without your consent or knowledge and used to see personal information that you have entered online, including passwords, telephone numbers, credit card numbers and identity card numbers.

Anti-spyware programmes currently available include AdAware, Microsoft Defender (free), Spyware Blaster, Spy Sweeper and, Sunbelt Software Counter Spy. Again, be sure to visit the genuine site as there are many fake products claiming to protect your computer but which may actually infect it with viruses.

Block spamm email

Check with your ISP Provider and your Email Settings.

Be alert to fraud

Be aware that there are fake websites designed to trick you and collect your personal information. Sometimes links to such websites are contained in e-mail messages purporting to come from financial institutions or other reputable organisations. Never follow a link contained in an e-mail - even if it appears to come from your bank.

Keep your passwords safe and secure

All your Software programs and accounts rely on good strong password authentication, especially Banking. When creating passwords, remember the following things:

- Keep them to yourself
- Dont give them out to Website officials
- Make them hard to guess
- Vary them: Try to use different passwords for different services
- Change your passwords regularly
- Never write them down or encrypt them yourself keep them safe

Be careful on line

Avoid using sites that require passwords eg banking at an internet café, libraries or any other public sites to avoid the risk of information being copied and abused after you leave.

Ensure Privacy

Dont risk people looking over your shoulder seeing you keying in passwords

Always log off

Remember to log off from your Websites and close your browser when you have finished your session. Settings in the browsers allow removal of history and form filling, clearing all traces of your visit from the computer's memory.

Password protect your PC phone laptop

This will prevent other people from using it if it is left unattended or stolen newer technology allows finger print authentiation.

Disable auto complete

The 'AutoComplete' function on your computer stores information that you have previously entered, eg: addresses and passwords. Typically, the browser's own 'Help' function will tell you how to do

Admin mode

It's a good idea not to use your computer in administrator mode because anyone who gains access to it will then have almost unlimited rights to see stored data or download software - including viruses. It's far better to make a user account and log in with that for day-to-day use.

Secure wireless network

A wireless network allows you to connect your computer to the internet without having to use a cable. It typically contains a wireless router, which uses radio signals to transfer data to computers within the network.

Wireless routers come preset to very insecure settings to help users connect to them for the first time - but this also means that other people could access your internet account quite easily. For this reason, you should always consult your manual or online guide to find out how to connect more securely through your wireless network - usually by creating a password.