Martin Bradshaw

COMPUTER SECURITY

The purpose of this guide is to try to amount useful information relating to general computer security and Internet use.

Please check the specification of your PC and the programs you are downloading before installing them. This guide is not intended to be a comprehensive list of all the issues or threats that exist on the Internet. There is however, enough information to get your PC protected and ensure that you can surf in relative safety.

If you are surfing the Internet, or using email, then the recommendation is that you have, at the very least, a firewall and an anti virus program. These products are essential for protecting your PC from harm.

Please read the descriptions if you are unsure of why you might need a particular product. All the programs you will need can be downloaded for free, so there is no reason to not protect yourself!

FIREWALLS

A firewall protects your PC from unwanted Internet traffic. The primary function of a firewall is to let good traffic pass through and block 'bad' traffic - to stop it entering the protected (or 'trusted') network. 'Good' traffic can be defined as that required by your PC to operate applications, such as email and web browsing. 'Bad' traffic relates to worms, Trojans, scanning applications etc.

The most important part of a firewall is its access control features that distinguish between good and bad traffic. Larger commercial firewalls tend to run on dedicated hardware. For personal protection, software firewalls are sufficient for most users needs. Both commercial and personal firewalls operate in basically the same way.

Software firewalls are programs that run on your computer and nestle themselves between your network card software drivers and your operating system. They intercept attacks before your operating system can even acknowledge them. The firewall lets you request web pages, download files, chat, etc. while making sure other people on the internet cannot access services on your computer such as file or print sharing. These firewalls are designed for users with little or no technical experience. They will self-install and take you through a series of guided steps to configure the firewall.

ANTI VIRUS SOFTWARE

Anti virus (AV) software is a class of program that searches your PCs memory and hard drives for any known or potential viruses. AV software contains thousands of virus definitions and patterns known as signature files. These files will usually be updated automatically (as and when a new virus becomes known). In the past, updating AV signature files once a month was seen as sufficient, today, signature files may well be updated every day.

There are many commercially available programs that vary in cost and competence. Free AV software for home (non-commercial) use is now available. Many thousands of new viruses are discovered each year, so it is essential that you have an AV program that will automatically update its virus signatures. These free programs may lack some of the extra features found in the commercial products, but they are no less effective. For some examples of antivirus software, Windows Security Essentials is a recommended free AV program developed by Microsoft, or you can trial some of the demo versions of antivirus programs such as Avast, Mcafee or AVG.

Also note: contrary to popular belief, while the same viruses that affect Windows might not affect Mac OS, Mac operating systems **ARE** still vulnerable to viruses and Trojans. Try AV programs such as ClamXav or Mcafee to ensure the security of your machine.

I THINK I HAVE A VIRUS, HELP!
First thing to do is don't panic. Visit the website of any of the major AV vendors and they should have 'stinger files' available. These are mini antivirus programs designed specifically to remove certain viruses. Normally these are new viruses or common ones known to cause problems. Follow the instructions and run the program.

Many vendors now offer online scans of your PC to check for viruses.

Once the virus has been removed, make sure that your existing antivirus program is up-to-date (or install one if you don't already have one) and run a full system scan. This could take an hour or so, depending on the size and number of files on your hard drive.

SPYWARE / TROJANS
Spyware is any technology that aids in gathering information about a person or company without their knowledge. Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get into a computer as a software virus or as the result of installing a new program.

The majority of websites use cookies to track users. In many cases, the use of cookies is totally legitimate and perfectly acceptable (Scoobynet, for instance, uses cookies to remember your username and password). However, some cookies can and do track your Internet usage. Cookies are easy to delete and control, usually through a setting within your web browser (Try looking for browsing history or privacy options on your browsers preferences). Many forms of spyware are much more advanced and require specialist programs to remove them.

Trojans are normally malicious programs contained within or masquerading as seemingly legitimate software. They can also infect your machine as part of a virus. Trojans often contain ‘backdoor’ access methods to your PC or might try and collect sensitive information such as passwords. A combination of good antivirus software and a decent firewall will help to protect your PC.

PARENTAL CONTROL
if you would like to control what your kids can access on the Internet, there are a number of programs that can help. These programs can restrict access to certain types of website, based upon defined categories. Categories normally include such things as sexually explicit sites, gambling etc. These control setting are now often found within operating systems or network devices for easier management.

WIRELESS SECURITY
If you are considering installing a wireless network in your home or at work, please do some research first. There are well-documented weaknesses in WEP (Wireless Equivalent Privacy) - the most common wireless encryption protocol, but that does not mean it should not be used. Even basic encryption is better than none at all. Newer standards such as WPA (Wi-Fi Protected Access) and WPA2 offer a much stronger encryption method and provide much higher levels of security. Wireless networks should never be installed without basic security and encryption measures. Please seek professional advice if you are unsure.

OTHER TIPS
make sure you keep windows patched and updated - use the Auto Update feature within windows update to ensure that you are protected against the latest vulnerabilities. Check emails carefully and discard anything that you think is suspicious. Be wary of any email that has an attachment – even if it comes from someone you know, and especially if it comes from someone you don't.

ALWAYS KEEP BACKUPS of important information. Most PCs now come with either CD or DVD recorders. Use these to make backups, or use a separate external hard drive. Try to keep backups on separate devices to allow redundancy in case of drive corruption or faults.

Windows XP Service Pack 2 features a surprisingly effective firewall. This is enabled by default, when you install SP2. This firewall has been credited with a noticeable reduction in the number of attacks seen on the Internet. It is well worth running this program.

Don't run as 'Administrator' - Most viruses and Trojans require admin rights to actually install and execute their payloads. Most users configure their PC with a single account that will normally be given full admin rights. You don't need these rights to perform the normal day-to-day functions on your PC. Set your main login as a normal user account and create a separate admin account.

Computer security is a serious issue, but it does not have to be overly complicated. Please don't ignore it.