Windows Security Essentials

Andrew Bovett
Bovett Computer Services
7th July 2005

These days there are many threats to your PC and the information on it. Most of these come from the Internet – it's useful but also dangerous. Problems can range from the inconvenience of a PC that runs a bit slower than it used to or being bombarded with pop-up adverts, to major problems like credit card fraud and “identity theft”.

There is no single solution to these problems, but you can guard against them, and this article aims to give you the basics in a concise format. Please remember, though, that PC security is an ongoing thing – it's not “fit and forget”. For example, many of the PCs I am asked to help with are full of viruses even though an anti-virus program is installed, because the owner didn't check it was up to date or run any scans.

Basic security measures

Here is a brief list of the basic measures you can take. I'm not going to explain the details of how to do each one here – there's plenty of information on this on the web (including my web site at http://www.abovett.co.uk), or you can contact me at pcsupport@abovett.co.uk for more help.

1. Install **Anti-Virus** software and update it regularly – preferably at least once a week. If your anti-virus program has an automatic update feature, by all means use it, but *don't* depend on it, as they don't always work reliably – particularly with dial-up Internet connections. Get into the habit of checking for yourself that the program is up to date.

   You should also use the scan feature in your anti-virus program to scan the whole system for viruses on a regular basis, to catch any that “got past it” on the way in.

   If you don't yet have anti-virus, there are some free ones available. AVG from http://www.grisoft.com is free for personal use on a single computer.

2. Install a **firewall** program and learn how to use it. A firewall stops intruders getting into your PC, and most also stop unauthorised programs “phoning home” with your personal information. Windows XP includes a basic firewall, but there are better ones available, and some are free for private use, such as ZoneAlarm from http://www.zonelabs.com. Learn how to understand the alerts it generates and *don't* just blindly click on buttons until the alert goes away!

3. Use **Windows Update** to load the latest fixes for Windows. Later versions of Windows include an automatic updates feature which will help if you turn it on, but you should still check for yourself periodically – preferably about once a month.
4. Install one or two reputable **spyware/adware** detection programs, and use them to scan your PC periodically. As with anti-virus programs, you must remember to update them regularly.

   Spyware and Adware are programs which target you with (usually unwanted) adverts and often sends information about you back to the programs authors. Some come disguised as useful programs to persuade you to install them, whilst others are picked up whilst browsing the web.

   Beware about which programs you use, though, as some so-called spyware blockers are themselves actually adware or spyware! Two good free ones are “SpyBot S&D” from http://www.safer-networking.org and Ad-Aware from http://www.lavasoftusa.com (free for personal use).
5. **Be Careful** when opening e-mails or browsing the web. Just because an e-mail comes from (or appears to come from) someone you know doesn't mean that attached files or web sites are safe. If in doubt, check it out – a good first step is to type the name into Google and see what you find.

   You will find many apparently useful programs being advertised on the web, and many claim to be free. Again, check them out – they may well be spyware or worse. If you're not sure, then don't install them.

Going Further

The points in the above section are basic essentials for safe Windows computing. However, there are several things that you can do to further improve your security. Some suggestions are presented below, starting with the more straightforward ones. These won't be for everyone, but at least the first one or two are worth considering for most people.

Change your web browser

Internet Explorer (the big blue “e”) is the most popular web browser, because it comes free with Windows, and it's easy to use. However, it's also generally the least secure. The newest versions are better, but it's still the case that more “malware” (viruses, trojans, spyware etc.) is targeted at Internet Explorer than any other browser. Consider switching to **Mozilla Firefox** or **Opera** – both offer more features than Internet Explorer, and are more secure. They can both be downloaded freely from the Internet. Opera has an ad-bar at the top, but if you purchase an (optional) registration code it goes away.

Note that you don't have to remove Internet Explorer to use an alternate browser – they will happily run side by side. In fact you will need to keep

Internet Explorer for things like Windows Update and the odd web site designed specifically for it.

Change your E-mail client

As with Internet Explorer, Microsoft's Outlook and Outlook Express e-mail clients are the most popular but the most vulnerable. Changing e-mail client is a little more work than changing web browser as you will probably want to transfer your old e-mails and account settings to the new program. However, some of the e-mail programs available include features to help you do this. **Mozilla Thunderbird** is free and easy to use, and includes some useful extra features, and other free programs are also avalable. For best security take a few minutes to work through the preferences screens and choose the most suitable settings.

Use “Limited Accounts” on Windows XP

By default, Windows XP sets up the user account or accounts you create when you install it as full system administrators. The problem with this is that any virus or spyware which gets onto the computer whilst using that account has full run of the computer. It's a good idea to create “Limited” accounts, especially if you have children – not so much to restrict what they can do (though it does limit the damage they can do if they get something wrong) but to protect the system if they accidentally download a virus or spyware. You may even wish to create a limited account for yourself for day to day use, and just use a full (“administrative”) account when you need to install software etc.

Use password protected Windows accounts

Windows does not insist that you use a password on your account, and you may find it inconvenient. However, it does improve the security of the system. I would recommend that at least all administrative account users have a password set.

You may not know that by default there is a hidden “Administrator” account with full access rights and no password. There is also a Guest account, which can be a security weakness even when disabled. These are of particular concern if you use a network. I have written a separate article, titled **Setting Administrator & Guest passwords on Windows XP**, which gives information on how to protect these accounts.

Disable unneeded services and startup programs

Most Windows PCs have a number of programs which run at startup. Not all of these are always needed. Also, by default Windows XP starts a lot of “system services” which are not required for most people.

The details of how to determine which ones to disable is beyond the scope of this article, but there's plenty of information on the web (remember to check it out before depending on it though). You can also get some good

books on computer security which will help with this.

Switch to Linux!

For those who don't know, the Linux (or more accurately *GNU/Linux*) operating system is an alternative to Microsoft Windows. It has several features which make it more secure by design than Windows, and viruses and spyware for Linux are almost unknown.

There are many variants (or *distributions)* of Linux, and the features and ease of use vary widely. Cost also varies, but is a lot less than Windows, and many distributions are free. Some versions worth checking out include **MandrakeLinux** and **Ubuntu**.

Switching operating systems is not something done lightly, as you would also need to change most of the programs you use. However, for those who are interested, it's possible to run Linux alongside Windows (you choose which one you want each time you switch the computer on). It's even possible to get versions of Linux which run entirely from a CD and don't change you system at all – ideal for checking out what Linux is all about without any commitment. These are known as *Live CDs*. Both MandrakeLinux and Ubuntu have live CDs available.

Andrew Bovett

Bovett Computer Services providing various PC related support services in the Cheltenham/Gloucester area, including:

- Software troubleshooting (including virus removal)
- Internet and e-mail support
- Hardware repair and upgrades
- Network installation and administration support
- Security advice
- Computer training
- Web site design and administrative support
- Supply of computers, peripherals and software

If you have questions or comments on any of the items in this article, or would like help with any of the areas listed above, please get in touch.

E-mail: pcsupport@bovett.co.uk

Web: http://www.bovett.co.uk

Tel: 01684 298896 (fixed)
07801 747068 (mobile)