FIREWALLS AND ANTIVIRUS - ESSENTIAL SECURITY

Firewall and *antivirus* are your main technology defence mechanism - it is the virtual equivalent of securing the doors and windows of your office. However, these two pieces of software cannot stop all types of attacks so, on top of this, you need extra layers of protection. Two options exist: software and *hardware*. Hardware firewalls are more costly and are suitable for slightly larger organisations. *Software* firewalls protect each computer individually and can follow a laptop around.

Keep up-to-date

Antivirus software relies on *virus definitions* to detect the latest viruses. Hundreds of new viruses are released daily and definitions are needed to catch these newcomers. Make sure you update virus definitions frequently; all the major antivirus software does this automatically (daily or more often).

Allow only what you need

Computer ports are virtual doors to your computer, think of it as closing all the windows when you go to stop intruders getting in. 65,535 ports exist and most people do not use that many. Configure the firewall so it only allows the ports and services you actually need to do your work. Some of the most common are:

8080 HTTP (hypertext transfer protocol)
443 SSL (secure socket layer)
80 HTTP (hypertext transfer protocol)
110 POP3 (post office protocol, version 3)
53 DNS (*domain name* service)
68 DHCP (dynamic host control protocol)
20 *FTP* data (file transfer protocol)
21 FTP (file transfer protocol)
22 SSH (secure shell)
143 IMAP (*internet* message access *protocol*)

Infections

If you think you have been infected by malware you should disconnect the internet to stop any spread to other computers on the network. Some crafty viruses will disable antivirus programmes so you might need to install another one – use a USB stick or use an online scanner (such as Trend Micro's Housecall). Some will disable and hide all data and programmes, especially the fake security suites.

Use a trusted product

There are so many antivirus, firewalls and security suites available and also some rogue ones. Rogue ones will install and disable genuine software and maybe even hide your data. Before you download and buy anything, check reviews elsewhere to ensure it is genuine. Rogue products will often ask for a payment to fix a 'problem'.

Change the defaults

Some software and hardware firewalls come with defaults like: username, password, management *URL* and remote access. Enabling these opens you up to more problems. Also remember to change and disable these on software and hardware products.

Enable logging

Most firewalls and antivirus products can log activity and this may be useful to spot a problem after it has happened. Do not log everything since this will slow the computer down and waste space. Only log medium to critical security events.

Scan frequently

As well as ensuring your antivirus product is up-to-date, you need to scan your entire computer frequently. Scan your computer at least once a week and make sure it scans everything including: all folders, all drives, *registry*, memory and emails. This can be set to run automatically - you might want to set it for a time when the PC won't be used to intensively such as lunchtime.

Filter websites

Viruses can be caught through your website browser. Occasionally genuine websites are hijacked and infected with viruses with the aim of infecting your computer. Some antivirus and firewall vendors include this as standard so make sure it is enabled. Website browsers such as Internet Explorer, Firefox,Opera and Maxthon come with their own URL checker to ensure you do not visit black-listed websites.

Firewall and antivirus are not the be-all and end-all

This is what most home-users and business owners think and it's a big mistake. Many simply install a *firewall* and antivirus system and think they are now bullet-proof and impregnable. No firewall or antivirus systems are 100% accurate and this is why large companies often have two antivirus systems installed so one might catch what one might miss. A firewall will not protect data that is on the move... i.e. if someone steals a laptop or *USB* drive.

Block pings and port scans

Pings are a response given to show the system is working and happy but a large amount can cause a DOS (denial of service) attack. Set your *ADSL router* and software firewall to block these externally. Port scans are used to see what *ports*are open but sometimes this can be someone planning an attack. Block port scans to reduce the information revealed.

Apple antivirus

Many diehard Apple Macintosh fans say their Macs are totally bullet-proof - and virus resistant. While it is true there are fewer threats and that they are more reliable, you shouldn’t assume anything. The reason there are fewer threats is because of market monopolies but, as more Macs are bought, threats will increase. One of the first ever Mac viruses dates back 30 years. As Mac antivirus software is so not easy to sell, Sophos, a leading IT security vendor, has started to offer it for nothing (for home users).

Enable attack blocker

When a firewall detects an attack it can automatically block the attacker's *IP address*. By default, most vendors block it for 60 minutes but it is a good idea to increase this.

Monitor all ports

As mentioned before there are 65,535 computer ports, think of it as a building with 65,535 windows and doors ... unlikely unless you work in a massive office block! Certain ports, like 1243 SubSeven, are more vulnerable than others so make sure your firewall is set to *monitor* all possible ports.

Password protect settings

Hardware and software security suites can normally be protected by a password. This stops children, rogue employees or criminals editing or disabling your firewall. Enable this, it only takes a minute to do.

Auto-scan everything

Malware can penetrate in various forms: email, website, browsers, CDs, DVDs and USB devices. Ensure your antivirus scans all possible methods to increase the chance of capturing malware.

Source : http://www.ictknowledgebase.org.uk/firewallsantivirus