

Firewalls

July 2007

If your PC connects to the Internet without one of these in place - you are taking a grave risk, even more so if you use a Broadband connection.

Our E-Business Advisers discuss this essential security item:

1. What is a Firewall?

The term firewall relates to either a piece of equipment (hardware) for larger networked PC systems, or (often for standalone PCs) a software application, which filters traffic entering or leaving a computer.

When a PC is connected to the Internet, information is flowing to and fro, in a near-constant stream, through a "port". This is, in essence, a gate enabling information to go in and out.

A firewall controls the communications to and from your PC through these ports. It permits or denies the flow of information and communications based on a Security Policy (i.e. permissions which can be configured to meet your needs).

2. So how does a firewall help to stop unwanted access to a PC?

The most basic and important functions it carries out are:

- A good firewall makes your PC invisible to the Internet. The ports don't just appear closed -

they just don't appear at all to the outside world.

- It automatically blocks suspicious incoming traffic – e.g. a hacker attack.
- It alerts you every time a program on your PC tries to send information to another computer or Web site.
- This stops any Spyware and Trojans that you may have (see below) from sending potential hackers your confidential and personal information – e.g. credit card details or passwords.

3. What could happen if I don't use a firewall?

If you don't have firewall protection for your single PC or networked system, then as soon as you connect to the Web - **before you even start your browser or email** - you are **open to serious attack**. Some or all of your ports will be open, unmonitored - and prime targets.

The kinds of thing that might happen if you haven't got a firewall are various - but all are unpleasant, damaging or dangerous:

- **Port Scanning:** Hackers scan the ports on your PC to figure out if they are open or exist at all. If your computer reports an open port, a hacker can send a worm or virus to it. They can even use an open port to take control of your PC.

Fact Sheet

- **Viruses:** Programs or pieces of code that "infect" one or more of the programs on your PC could be placed on your system. Basically, your PC "gets sick" and starts performing in weird ways, leading to data damage and loss.
- **Worms:** Malicious programs that propagate over a network, reproducing as they go. Worms can cause the same effects as viruses but they are more dangerous since they spread by themselves.
- **Trojans:** Programs that appear legitimate but do something illicit when run. Just like the wooden horse the Greeks gave Troy as a "gift", users mistake the Trojan for a useful or interesting program that they choose to download.

Once installed and run, Trojans can secretly open remote access channels to hackers, relay passwords and credit card data or destroy user files. It's similar to a virus but generally does not replicate itself.

- **Your PC could be hijacked and used in Denial Of Service (DOS) Attacks:** This kind of attack happens when a hacker places a program on your PC, and probably several thousand other undefended PC's. They become "zombies", effectively under the hackers control.

At a given time or on a certain signal, your PC's and the others infected all try to repeatedly connect to a well known web site.

The huge amount of data means that the target web site is unable to accept all the requests for connection, the system resources exhaust, and the system crashes and denies service access to the web site.

Criminal gangs have utilised this technique in extortion attempts against companies such as www.bluesquare.com, a gambling web site based in London.

The site was subjected to repeated DOS attacks, meaning that they would be losing money as gamblers couldn't place bets, unless they agreed to pay the extortionists demands.

Fortunately, the criminals, (based in Moscow), were caught, but this technique has been used repeatedly on many well known sites, sometimes for monetary gain, but often just for "kicks".

To avoid the above, firewall protection is **absolutely crucial** for your systems.

4. Broadband Users – beware!

A firewall is especially important if you have a high-speed broadband Internet connection.

Hackers love to take over high speed broadband-connected PCs. They then have your speed and "always on" connection to increase their possibilities to send malicious code and collect the sensitive personal information they desire.

Machines with broadband connections also make DOS attacks a lot easier to run for hackers too.....

5. I'm convinced! How do I get a firewall?

There are plenty of excellent firewall software applications available. Some are free to download, some have to be purchased. These may be more suitable to ensure the level of security is high enough.



Fact Sheet

P.S - you'll also need anti-virus software too - see our "Computer Viruses" Fact Sheet in this series.

6. Useful Links

www.zonelabs.com - Zone Alarm is a good, free firewall which can be downloaded directly from the above web site.

www.symantec.com or www.mcafeestore.com -

web sites of two of the major anti-virus software companies, who both also offer good and inexpensive firewalls.

Disclaimer: we have no commercial links with these companies or their products, and their appearance in this fact sheet is not an endorsement