

Online Security Mini Primer

This PDF is designed to give you a few pointers to aspects of online security. It's unfortunately a massive issue which will not go away and I can only skim the surface here.

Since technology moves on so quickly, there may be some aspects of this PDF which become outdated. Sorry about that, I'll try to update when necessary, but feel free to comment via the website at www.woodcom.co.uk

Topics included;

| | |
|---|---|
| What you need to know for online security | 2 |
| Viruses and Trojans | 3 |
| Hackers and Crackers | 5 |
| Prying Eyes | 5 |

Online Security Mini Primer

What you need to know for online security.

When you are connected to the Internet, you can give all kinds of secrets away to people who know where to look. If you are confident of your security, or want the fright of your life, go to Gibson Research Corporation and allow them to 'Test your Shields' by clicking on the links to 'Shields Up'. The results are eye-opening. All they do at this site is find information that anyone with the right tools could find out, directly from your computer. The problem is that these hacking tools are available on the internet, if you know where to look and what to look for.

Although this is worrying (if you're not concerned, you haven't understood), there is something you can do. Go to Zone Labs and click on the button to download their excellent firewall software Zone Alarm. This is free for personal and non-profit use, but you can buy Zone Alarm Internet Security Suite , which is even more capable, for reasonable cost. Once installed, what it will do is protect the connections available from your computer over the internet, both in and out, through your modem or broadband link. Although we consider Zone Alarm to be the best, in the spirit of fairness McAfee and Norton and others also sell firewall software.

For businesses there are a whole bunch of very powerful, very complex, and very expensive options, such as Symantec Raptor, and Microsoft ISA Server. There are also much cheaper but very competent Linux-based firewalls which can be run on older redundant computers. We cannot go into detail here, but if you are interested, email us.

Online Security Mini Primer

Viruses and Trojans.

So what's the difference?

Trojan Horse: Normally shortened to just "Trojan", they used to be a program that either pretended to have, or was described as having, a set of useful or desirable features, but actually contains a damaging payload. However now Trojans will be programs that open systems up to hackers by stealth, creating 'open doors' for them to gain control of the systems.

Virus (plural viruses): A software program that self-replicates (creates copies of itself). Viruses may damage or destroy data, cause the computer to crash, display messages, either immediately or on a specified date. Normally require human intervention in running a program or opening an email attachment. The notable exception being boot sector viruses, which are spread via disks simply being 'booted up'.

Worm: A program that is designed to copy itself from one computer to another over a network, including the Internet itself. Can be spread by e-mail, IRC chat or copy themselves over the Internet as an open system is found. Because the worm doesn't need human intervention, worms spread much more rapidly than computer viruses.

It would be easy to find fault with these simple definitions, and the way they operate, and what they do, are becoming increasingly blurred. The point is however, they are going to be around for a while. So which is the worst? Simply whichever one your computer contracts! With the increasing sophistication of what is generically termed 'malware', not running anti-virus software is almost suicidal. It is also not good enough to buy the software, load it, and forget it. AV software that is not kept up to date (a minimum of once a week at the moment), is almost worse than none at all, since it engenders a false sense of security. It is also a good idea to subscribe to new virus warning services from your anti-virus software vendor.

Online Security Mini Primer

One side effect of the tremendous upsurge in malware, is that as newly produced worms look for computers and Web Servers to infect, the enormous amount of Internet activity generated, actually slows down the Internet for everyone else. If you have a firewall running, all those attempts to communicate with HTTP or port 80 (amounts to same thing), are probably worms attempting to find a server running Microsoft's Web Server software, so they can infect it.

For details of the most recent threats, go to our [Virus News](#) page. For software to help prevent or deal with threats, go to our [Solutions](#) page.

Online Security Mini Primer

Hackers and Crackers.

Historically hackers were people who loved nothing more than getting inside someone else's computer system, just because they could. As the sophistication and use of computers increased, so did the challenges facing the hackers. At some point the idea of just getting in changed, and as large businesses became increasingly dependent on their computer systems, the Law took an increasingly dim view of hacking.

The theoretical distinction between hackers and crackers, is that hackers do it for the challenge, whilst crackers will invariably try to damage or control systems for their own gain or simply to vandalize. If there is someone in their bank's database, most people won't stop and wonder what the intent is, they will just want them out.

Prying Eyes.

Something people tend to forget in all the 'Mission Impossible' gadgetry, is that someone may just be simply watching using no more than their eyes. If someone were to use a work, library, Internet cafe, etc computer, any passwords or usernames could be seen. OK, we could get excessively paranoid at this point, but how many of us try and shield the keyboard when we input our pin number into the cash machine? Same thing really.

Particularly at work, if we use the Internet, the passwords can be cached by the computer, and retrieved with the use of a simple program. The advice really has to be, think before you click that dialogue box that helpfully offers to remember your passwords for you.