



Series 5 – How Do I Access the Internet, Securely?

Welcome back to a series of computer related articles brought to you by VistaSol Computer Solutions. Over the coming weeks we are going to be featuring articles based on the theme of 'How do I . . .?'

This week we're continuing our series of articles on the subject of 'How Do I Access the Internet' by offering some advice on how to keep yourself secure. In our previous article we looked at making your passwords more secure. In this article we're going to talk about viruses and your best form of protection.

Part 4 – Virus Protection

What I'd like to cover this week is a brief insight into the various types of malicious programs that are rampaging through cyber space, and some additional steps you can take to protect yourself.

When is a Virus not a Virus?

One common mistake that people make when the topic of a computer virus arises is to refer to a 'worm' or 'trojan horse' as a 'virus'. While the words trojan, worm and virus are often used interchangeably, they are not exactly the same thing. Viruses, worms and trojan horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you better protect your computer from their often damaging effects. Collectively, these malicious programs are often referred to as Malware, and include other nasties such as spyware and adware (more about those next week).

What Is a Virus?

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your operating system, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you inadvertently run it, or open the malicious program. It's important to note that a virus cannot be spread without a human action to keep it going. Because a virus is spread by human action, people will unwittingly continue the spread of a computer virus by sharing infected files or sending emails with viruses as attachments.

What Is a Worm?

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, thereby creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your email address book. Then, the worm replicates and sends itself out to everyone listed in each of the recipient's address books, and the manifest continues on down the line.

Due to the self-cloning nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm had been designed to tunnel into your system and allow malicious users to control your computer remotely.

What Is a Trojan horse?

A Trojan horse is full of as much trickery as the mythological Trojan horse it was named after. The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Steps you can take to protect yourself now

If you've been following our previous articles you should already have most of your security in place e.g. AVG Free (or some other product) and the Windows Firewall. Additionally, you should also accept and apply all the updates offered to you by Microsoft, and keep your anti-virus program up to date.

There's still more you can do to protect yourself, and best of all, it's completely free! What I'm talking about is being security conscious at all times; treat everything as suspicious, especially if it's free, or seems too good to be true, and if you're not expecting it – don't open it, read it or accept it. Apply these common sense rules, and you can't go far wrong.

Think you're already infected?

If you think your computer may already be infected, start by visiting this web site:

<http://housecall.trendmicro.com/uk/>

You should also consider downloading, installing and running a program called 'MalwareBytes' – you can find a link to this on our web site.

Enjoy your on-line surfing experience, but be safe and think about your security at all times.