Oxford Home IT Support
...computer services direct to your door
01865 594020
www.homeitsupport.biz

Newsletter | Viruses, Spyware & Fake Anti-virus | April 2011

**A free newsletter provided by Oxford Home IT Support**
**To get your free copies visit www.homeitsupport.biz/news**

# Viruses, Spyware & Fake Anti-virus

## Welcome

Welcome to the April 2011 Newsletter. This month we are going to revisit protecting your PCs against viruses and spyware and covering a few hints and tips to keep yourself safe as we're seeing record levels of infections at the moment.

## What's the difference between viruses and spyware?

Essentially **Spyware** is designed to be installed and run covertly on your PC so that you're not even aware that it's there. This kind of software is becoming very popular and is dangerous as it can be doing lots of harm to you without you even being aware that it's there.

Spyware will be watching what you're doing on the internet, looking for login details to capture, online banking and email systems etc., as well as a whole host of other activities.

Generally **Viruses** are used in order to spread spyware and other malicious software, often to do damage to your systems and files or to send Spam from your PC.

## What is malware?

**Malware** is a term used to describe any software that is used to do harm to your system. For the rest of this newsletter we'll refer to spyware, viruses and other malicious software as malware, as they are essentially the same for the recipient.

## How do I get malware?

The majority of malware arrives on your PC via the internet. It's the quickest and easiest way for a hacker to get it across the world to you and relies on the fact that most people do not protect themselves correctly and are not careful enough online.

Malware will be sent out via email and via web pages, often from the most innocent of looking websites. Always be aware of downloading anything from any website unless you can fully trust the site and the files you are downloading. Always virus check any files you download before you run them and never just double click on a file that has just arrived by email or from a web page. Even a Word document or PDF file can contain a virus, so don't assume anything is safe unless you have checked it first.

## What is a Trojan?

**Trojans** are simply a way of getting some malware to you easily. They are software programs which pretend to be something innocent, whilst hiding malware inside, just like the traditional Trojan and equally as dangerous. For example, someone will send you a file saying

it is a video of your favourite pop group. It came from a friend, so without checking it first you trust it and just double click on it. A video plays and it *was* your favourite pop group. However, it ran a video for you to watch whilst at the same time installing some malware on your system.

It relies on the fact that most people don't check what they are downloading, they just run it.

## Fake anti-virus sites


At the moment the most common way to spread malware is coming from **Fake anti-virus** websites. You visit a website and get a pop-up window that says you have viruses and need to download the full version of some software, such as "Windows Anti Virus 2011" or "Super Anti Virus" or “System Cleaner”.

You get worried, think you are infected, even though the messages are just simply web pages, so download and run the "free" anti-virus software. You end up downloading some spyware and viruses and infecting your machine. We see this very frequently now.

If you see messages like this, restart your web browser and ignore any messages that are not coming from the security package that you have installed, such as AVG. If you are ever unsure then just ring us and we'll assess it for you. Never download any "security" package from the internet as a result of any message that pops up on your PC.

Avoid downloading the so-called "Spyware Doctors", "Registry tuners", "PC tuners" and so on that are often just malware. It can be difficult to spot a real one from a fake one so it's best to avoid them.

## What is a firewall?

A **firewall** is a piece of software designed to protect you from a direct attack from another computer on the network or internet. Once you are connected to the internet you are then potentially making your computer available to every other computer connected to the internet and can, therefore, become a target for millions of hackers all over the world who would like to get direct access to your machine.

In order to avoid someone being able to connect directly to your machine, your machine should be running firewall software. This should keep out unsolicited traffic and allow in only what you requested, such as a web page or an email from your account.

Windows XP/Vista/7 and Mac OSX all have firewall software built in, so make sure they are turned on.

In addition, if you connect to the internet via a router, such as a BT Homehub or similar, those routers too will have firewall software built in. If you use a USB modem, switch at the earliest possibility to a router and connect via a network cable. This will give you a quicker connection to the internet and be much safer.

## So what software do I need?

The software we have been using and recommending to all our customers on Windows for many years is from AVG. This software is the best we have found and used and the one we use on all our Windows machines.

Their Internet Security package provides protection against spyware and viruses and runs very efficiently, without affecting performance like some other packages can.

It also monitors the results from search engines, providing you with instant notification of any websites that are known to contain malware that could be downloaded.

AVG Silver Reseller

The full version can be purchased directly from us at:

www.homeitsupport.biz/buyavg

There is also a free version of AVG, available at http://free.avg.com, which will give you basic protection, which we still advise over any other system for good protection. You do not get support or all features with the free version.

## What else should I do?

You should make sure the firewall software is turned on and set your machine to download and install system updates automatically. One thing hackers tend to rely on is people using out of date software, especially web browsers.

If you are using Windows under no circumstances should you be browsing the internet using Internet Explorer 6 (IE6), it is too vulnerable and insecure. Go to http://www.microsoft.com/windows/internet-explorer and click on the link to download Internet Explorer 9, the latest version for maximum security and compatibility for Windows Vista or Windows 7, or IE8 for Windows XP.

If you are using a Mac, allow the Software Update procedure to run and your browser will be kept up to date automatically.

## And finally?

Your bank, PayPal or eBay etc., will not send you an email with a link in it to login and "reset" your security details or anything of that nature. If you think you need to login to your online accounts, go to them via their normal address from your web browser, do not follow a link to them from an email.

**Never** use Google or any search provider to reach a website when you know the web address. For example, if you need to login to your HSBC account, don't put HSBC or hsbc.co.uk into Google or any search box. Put it directly into the address bar. Only then can you be sure you are visiting the correct site.

Lots of people visit spoof websites by searching for them in Google only to find that hackers also have a site listed in Google that responds to the keywords for your bank, and it's the new way hackers are using to lure you to the wrong site.

If you need help on any issues raised in this newsletter, email us at help@homeitsupport.biz.

**Thanks for reading,**
**See you next issue!**