



On-Site PC Support Services, Bespoke PC Design & Upgrade Services

Home Computer Security

This home computer security article was written for the purpose of helping users secure their home computers against viruses, worms, and backdoors and specifically against the blaster worm and worms like it.

Terms

To help you protect your computer, it is helpful to understand how you get viruses, worms, trojans, and other bad software. First I would like to provide some terms which will speed this process.

- **Attack** - An attempt to gain unauthorized control of someone's computer.
- **Vulnerability** - Typically, a software bug or misconfiguration which affects the operation of an operating system or other program run on a computer allowing it to be more easily accessed. Hackers, worms, viruses, and trojans use vulnerabilities to gain access to computer systems without the user's knowledge.
- **Virus** - Malicious software that spreads by attaching itself to files or creating files that may be executed in some way. Usually it is sent to users as an email attachment. It may require a computer software vulnerability to spread depending on the type of program it uses to spread.
- **Worm** - Spreads without the user taking any action and usually exploits a bug (or vulnerability) in an operating system or some other program that may be running on a computer. This requires a computer software vulnerability to spread.
- **Trojan** - A program which is usually given away for free which has a hidden purpose. It may be some type of file such as a video that user's may be interested in. The user would normally install and run this program although the installation would be so simple the user would be unaware of it. This program may or may not use a vulnerability to spread.
- **Hacker** (for this discussion) - A person who deliberately attempts to manually break into other systems and use them without the knowledge of the owner. Usually hackers exploit computer software vulnerabilities on the victim's computer, however once they have control of a system it is not possible to be sure they are denied access again without reformatting the hard drive and re-installing the operating system.
- **Spyware** - Spyware is not as serious a security concern as viruses, trojans, worms, and even hacker attacks, but many free programs contain spyware such as the current popular freezip program. Spyware is mainly a privacy concern than a security concern. Spyware does not take control of a computer system, but sends information to the spying entity about how the computer system is being used such as what web sites are being visited. The biggest concern with spyware or any other potentially malicious software is that it may download other code and install it on the user's system. Additionally it may hide itself from the user to prevent it from being removed.
- **Firewall** - Firewalls in simple terms are used to limit remote access to specific parts of the operating system or programs running on the system. They may block incoming attempts to connect to an application or exploit a vulnerability. Firewalls remove many of the possible methods of breaking into a computer without permission. It will help prevent hackers, viruses, worms, and trojans. It may also block spyware from contacting the spying entity.





On-Site PC Support Services, Bespoke PC Design & Upgrade Services

Backdoor - A program which allows an unauthorized user to have access to a victim's computer.

Solutions

These are basic and simple security requirements which must be followed in order to have a computer be anything close to secure.

1. **Every computer that connects to the internet in any form MUST have a personal firewall** or be behind a corporate firewall. The type of connection is not important. A personal firewall is required for dial in connections, cable modem, DSL, ISDN, T1 and others. The ONLY exception is when there is some type of firewall already existing between the computer and the internet. Get a personal firewall and configure it according to the maker's instructions.
2. **Every computer must have virus protection** and updates to the virus list database should be done at least twice a week. A full virus scan should be done at least once per week.

If you do not at least take the two measures listed above then you should not connect your computer to the internet. In the past I believed that I could just keep my system updated with security updates and did not need a personal firewall. This was a perfect formula for getting trojans, viruses, and backdoors and I ended up with four of them and had to reformat my hard drive and re-install my system.

There are also other security recommendations but the two above requirements are critical to all systems. The other security practice that should be done includes:

- Updating your systems with security updates and service patches when they are considered stable, but this can be a technical decision. See the below paragraph about updating your system.

It is best to read a e-mail discussion group postings to determine the state of current patches and vulnerabilities. Microsoft and other vendors issue postings about security patches and vulnerabilities when they come out. One of the best mail listings to subscribe to for learning about Windows vulnerabilities and patches is at <http://www.ntbugtraq.com>

A couple of additional practices related to your computer which may be lifesavers are:

- Back up your data - This should be done regularly to one or more of another computer, a writeable CD ROM drive, a zip drive, or tape drive. Remember if you should lose your data, everything you have done since your last backup will be lost. If you should find it necessary to re-install your system in the event of a security breach you will be glad you have done this. Also I have seen several hard drives fail and cause complete loss of data to users.
- Create an emergency boot floppy for your operating system - You should learn how to do this for the operating system you are using. Instructions in this area are beyond the scope of this document.





On-Site PC Support Services, Bespoke PC Design & Upgrade Services

Why do I need a firewall?

It would seem that if you keep your anti-virus definitions update with your virus protection program and you keep your system patched with the latest updates you would not need a personal firewall. Viruses would be immediately caught by your antivirus program, and your vulnerabilities would not exist since you always patch them immediately. This does not work for the following reasons:

1. Viruses begin to spread before they are identified. The only way they are identified is when someone discovers their computer is behaving incorrectly and then they realize they have a virus. Then the virus updates are posted to anti-virus vendor websites such as Symantec. Therefore the virus can spread to you before it is identified and your system may be compromised and other unwanted items such as hacker backdoors may be placed on your system before the virus is removed. A firewall can also help prevent additional items from being placed on your system if you should get an unknown virus.
2. Firewalls typically block most of the routes that viruses, trojans, worms, and hackers will try to use to gain access to your computer. A computer with a firewall is thereby much better protected than one without.
3. It is likely that some vulnerabilities may not be patched before the attack occurs.
4. Vulnerabilities like viruses must also be discovered. If a hacker discovers the vulnerability or someone writes a virus program to use an undiscovered vulnerability, a firewall may still be able to prevent the attack.

Even with all these measures there is no guarantee that your system cannot be compromised by a virus, worm, or hacker, but it is very likely that you will have much less trouble. Remember there is no guarantee that your hard drive will not break tomorrow so you should also back up your data to another computer, tape, or CD periodically when possible.

Firewall Recommendations

There are many personal firewalls that should work well, but it may be worth reading personal firewall reviews to find the best one when you are choosing one. Go to <http://www.google.com> and type "personal firewall reviews" to find sites that provide these reviews. I use Norton Personal firewall from Symantec, but zonealarm personal firewall is free for individuals and non profit organizations. It is available at <http://www.zonelabs.com> Please do not violate license laws when using this product. Since antivirus software is also an essential requirement to have a reasonably secure computer a nice convenient package is Norton's Internet security package from Symantec which can be found in many stores. It comes with both antivirus software and a personal firewall. The commercial version of ZoneAlarm's personal firewall also is very well recommended.

Configure your firewall before connecting to the internet. Most users should at this point read their documentation or run the provided firewall tutorial. You may get alerts while configuring or in one case I got an alert indicating that a specific program wanted to act as a server on the internet. Before answering the question I used another computer and went to <http://www.google.com> and looked up the name of the program the alert had specified. At this point I realized the computer had a virus. If you are told by the alert that a program wants to act as a server the likely answer to this question should be no, but it is best to look up the program name on Google to be sure. Also keep in mind any actions you may be taking which may prompt a program to access the internet to determine whether an action you took caused the internet access request to occur.

SupportTech,
15 Crawford Street, Newport, Gwent. NP19 7AY
✉ rob@supporttech.co.uk
☎ (01633) 783315 \ (07763) 603088
www.supporttech.co.uk





On-Site PC Support Services, Bespoke PC Design & Upgrade Services

Updating Your Windows System

- Windows 95 - If your operating system is Windows 95, you should update it to Windows 98, 2000, or XP because Windows 95 is no longer supported by Microsoft.
- Windows 98/Me - Use the web site at <http://windowsupdate.microsoft.com> to get your updates. It is said on the NTBugtraq email group that this is not always reliable however. Also you should update your Internet Explorer browser to version 6 or above by using the site at <http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp>
- Windows 2000 - Download and install Windows 2000 Service Pack 3 at <http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp> Service Pack 4 is now out but still has some unresolved questions that administrators are dealing with but it can be downloaded at <http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp> Update your Internet Explorer browser to version 6 or above by using the site at <http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp> Review the critical updates at <http://www.microsoft.com/windows2000/downloads/critical/default.asp> and install them. Windows 2000 Also has an autoupdate utility which can be configured from the control panel. It is said on the NTBugtraq email group that this is not always reliable however.
- Windows XP Home - You can find out about updates at <http://www.microsoft.com/windowsxp/pro/downloads/>
- Windows XP Professional - You can find out about updates at <http://www.microsoft.com/windowsxp/pro/downloads/>

SupportTech,
15 Crawford Street, Newport, Gwent. NP19 7AY
✉ rob@supporttech.co.uk
☎ (01633) 783315 \ (07763) 603088
www.supporttech.co.uk

