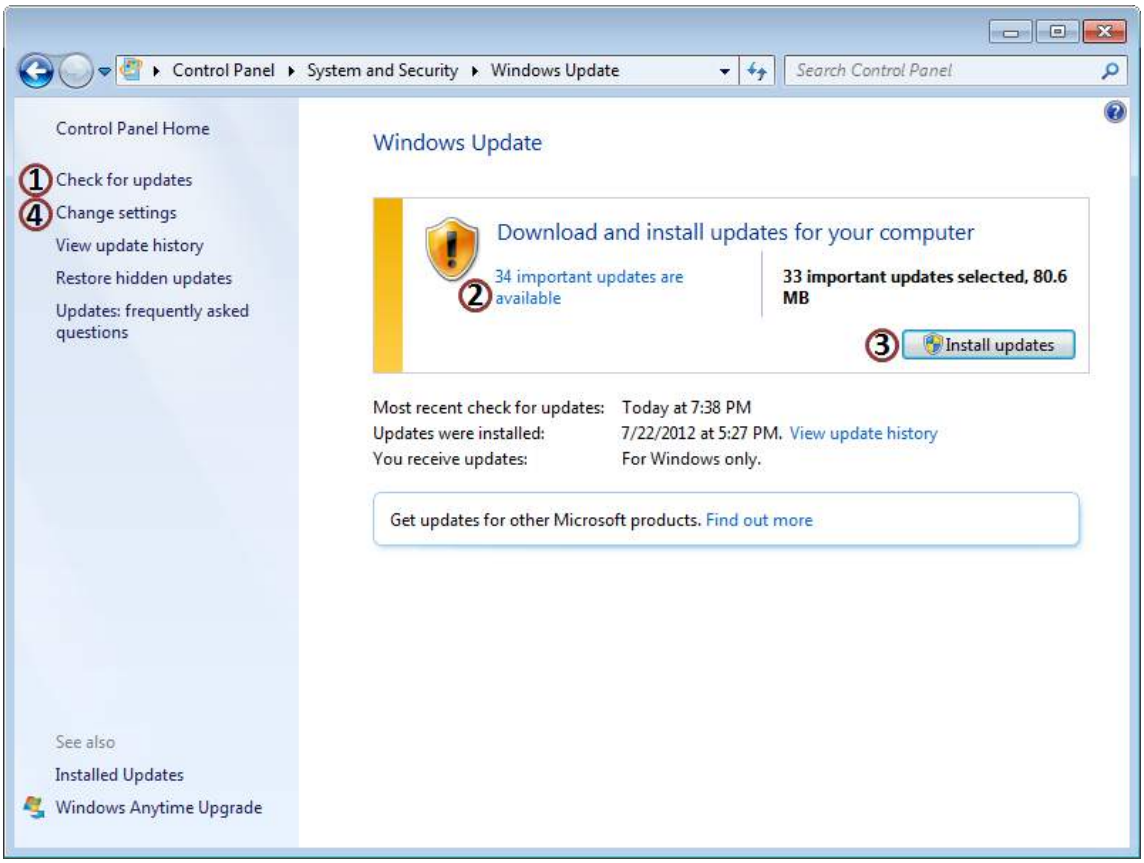
9 Keeping Windows 7 secure, up to date and virus free

As soon as you connect your computer to a network, especially a public network like a wireless hotspot, there is a risk of the computer becoming infected by unwanted software. Historically this software would have been a virus. Nowadays, there is a lot of unwanted software out there which may infect your computer like a virus does, that is not classified as a virus. This software may include spyware software which records the sites you visit and software that displays unwanted popup ads on your computer. This chapter shows you how to keep your computer secure and protected from harm, by ensuring updates are installed, a firewall is configured and anti-virus software is kept up to date.

Windows update

New vulnerabilities are discovered in computers all the time. These vulnerabilities may be discovered by Microsoft, a third party and in some cases by someone who deliberately writes malicious software. Sometimes vulnerability may be found but no one has discovered a way to exploit that vulnerability as yet. Think of it like leaving a Window open on the tenth floor of a building. It is possible for someone to access the building through that Window, but until they work out a way to get to the tenth floor they cannot make use of the open Window. This is why it is important to keep Windows up to date with the latest updates. Keeping your system up to date will mean your system may already be protected from the latest malicious software even before it is created. In order to keep your Windows system up to date you need to ensure that Windows Update is configured and setup correctly.

To configure Windows Update, open the control panel and then select the option System and Security. Once you have opened System and Security, select the option Windows Update. You can also open Windows Update by typing Windows Update from the Start Run box. Either way, you should get the screen shown below.

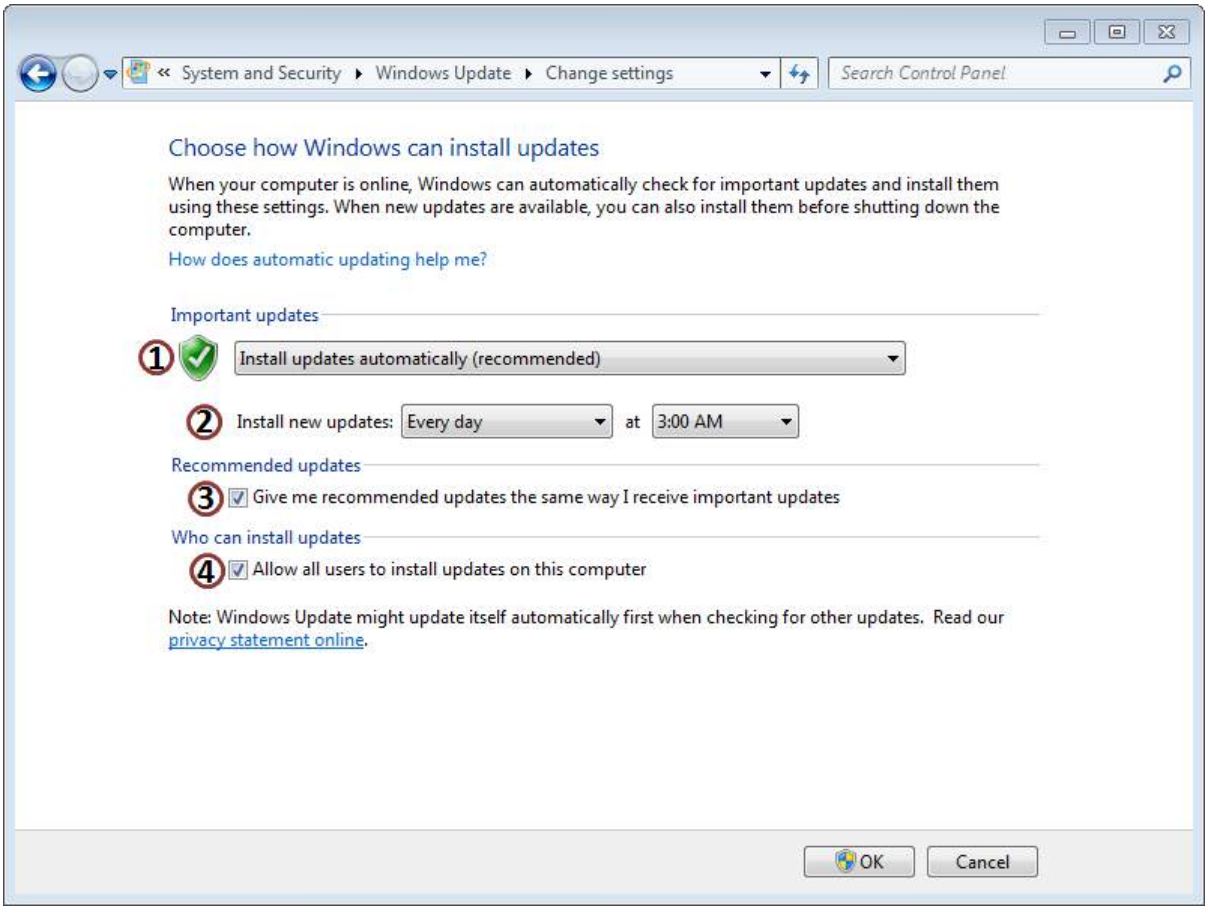


1. Option 1 shown above, "Check for updates," will force a manual check to see if any updates are available. This can be done at any time.

2. Point 2 above shows you how many updates are available but have not yet been installed. If you select this, you can choose which updates to install or install all of them.

3. The button "Install updates" will installs the selected updates. After updates have been installed, Windows Update may ask for the computer to be rebooted.

4. When you select the option, Change Settings you will get the screen shown on the next page.



1. The top option determines how updates should be installed. There are four options you can choose from.

Install updates automatically (recommended): This option automatically downloads updates when they become available and installs them. You should select this option if possible to ensure your computer is automatically kept up to date.

Download updates but let me choose whether to install them: This option will download Windows Updates automatically but will not install them. In order to install the updates the user will need to choose which updates to install. Use this option if you want control when updates are installed or if you want to choose which updates are installed.

Check for updates but let me choose whether to download and install them: This option will still check for updates but lets the user decide which updates to download and install. If you have a small amount of bandwidth you may want to use this option. This way, large updates will not be downloaded when using a slow connection. The user may decide to download the updates when a faster network connection becomes available or in off-peak times.

Never check for updates (not recommended): The last option switches off checking for updates. This is not recommended. Updates will not be installed and the user will not receive notifications telling them when new updates are available. In order to download and know if updates are available the user must manually check for updates.

This option allows the user to decide when updates should automatically be installed. By default this will be done every day at 3am. If the computer is not on at 3am, the updates will automatically be installed when the computer starts up next. When Windows first starts up a lot of software needs to be loaded by the operating system and the user many decide to open some applications straight away. To make the computer more responsive, the installation of Windows updates will be delayed after start up to allow software on the computer time to start up.

Option 3, "Give me recommended updates the same way I receive important updates,", this downloads other updates from Microsoft that are recommended but not considered as important and do not affect the security of the computer. These include program updates and device driver updates. It is a good idea to install these updates even though they may improve your Windows experience but will not affect the security of the computer.

The option "Allow all users to install updates on this computer" allows users that are non-administrators to install Windows updates. Since Windows updates come from a trusted source, in most cases you will leave this option on as it is better for a user to install an update than it is not to install the update at all.

For information about Windows Update, see the following link for the Microsoft FAQ.
http://windows.microsoft.com/en-us/windows-vista/Updates-frequently-asked-questions

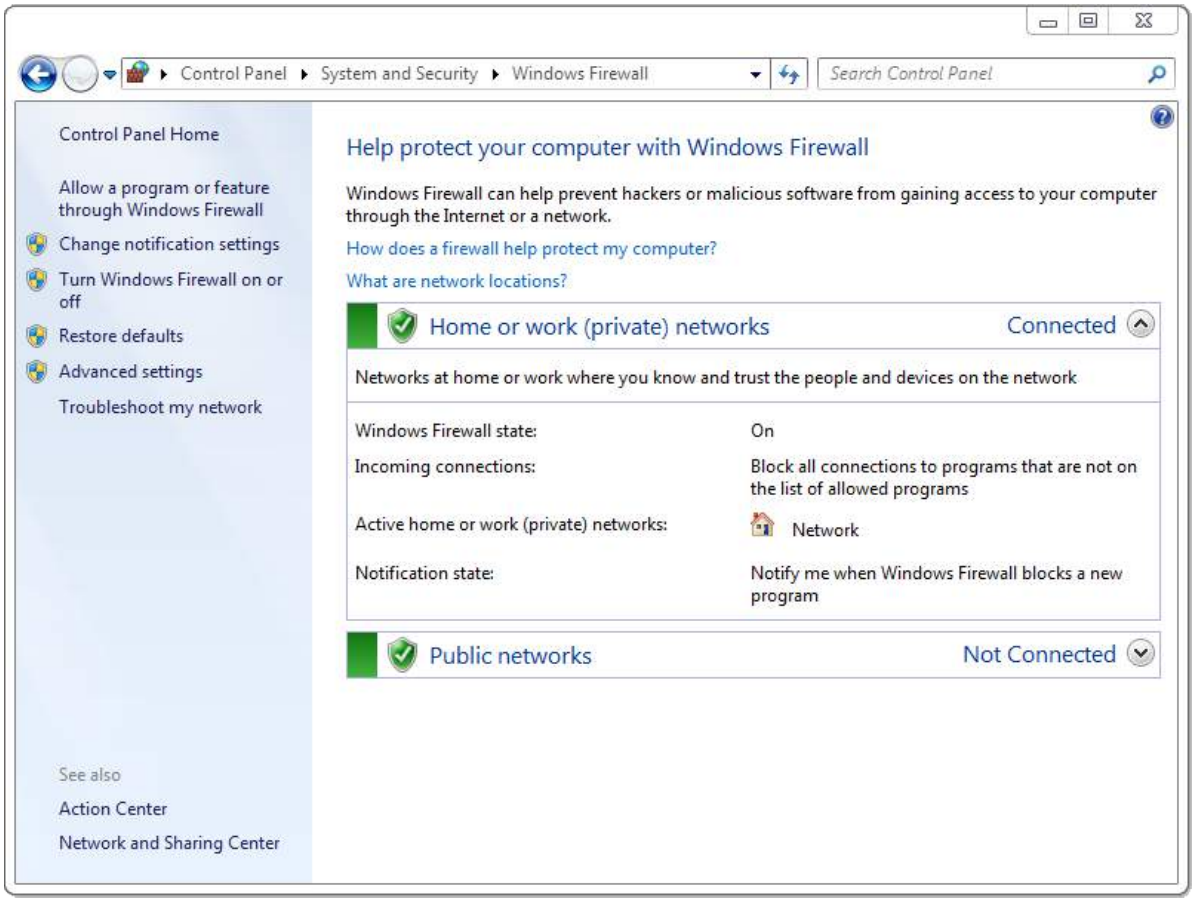
Firewall

A firewall is software or hardware that is designed to keep a network or computer secure. It does this by stopping unwanted or unasked for traffic. In many cases your connection to the internet will already have a firewall. For example, home DSL devices often have a firewall included and if you are connect to a company network they will have a firewall. Other times there may be no firewall, for example when you are using a wireless hotspot. There is also another case that you may want to consider. This is when your computer is on the same network as another computer that is infected. This is why it is important for an operating system like Windows 7 to have a firewall to protect the computer from local threats and threats from public networks like a wireless hotspot. A firewall is considered essential in modern computing. If a vulnerability exists in the operating system, the firewall may stop an attack trying to use that vulnerability and prevent your computer from becoming compromised.

Windows Firewall

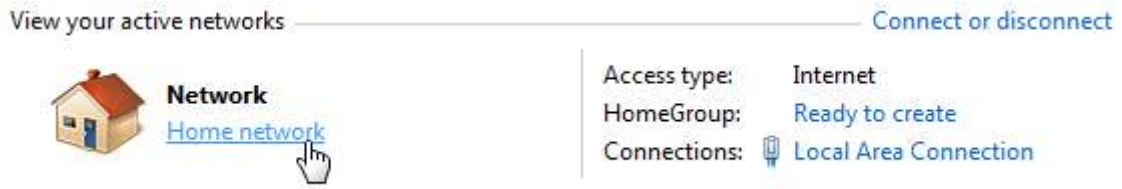
The Windows Firewall is included with Windows 7 and is regarded as quite a secure firewall by many computer users. The firewall was originally added to Windows in 2004. Since the Windows Firewall has been around such a long time, it is quite a secure robust product with good software support. For these reasons, many Windows 7 users will use the Windows Firewall rather than installing a firewall from another manufacturer.

To access the Windows Firewall type in Windows Firewall from the search box in the start menu. The Window Firewall can also be accessed by opening the control panel from the start menu, selecting System and Security and then selecting Windows Firewall.



The control panel for the Windows Firewall is shown above. The Windows Firewall has two groups of settings. One group of settings is used for home and work networks, while the other group of settings is used for public networks. The control panel for the Windows Firewall will show you which network locations are in use. In this case, only the home or work location is in use. The public network location is currently not connected. It is not uncommon to use wireless adapters to use the public network location and wired adapters used for a home or work location. If you want to change the location that the Windows Firewall is using, select the option at the bottom left, Network and Sharing Center.

Network and Sharing Center allows you to configure additional options for networking including the network locations used for each connection. As shown below, you should be able to see a list of the active networks. In this case, the active network is connected to the home network. To change it, it is a simple matter of selecting home network and then selecting the network you want. There are three options given – home, work or public. Essentially home and public use the same setting so it does not matter which one you choose. This allows a work computer to be easily used on a home network.



As shown above, there are a number of settings inside the Windows Firewall control panel that can be configured.

1. Allow a program or feature through the Windows Firewall: This will allow you to configure which applications and traffic will be allowed through the firewall.

2. Change notification settings and Turn Windows Firewall on or off: Both these options take you to the same screen. Here you can switch the firewall on or off. By default, the Windows Firewall will prompt you when it blocks network traffic from an application. This allows you to know that traffic was blocked and gives you the option to allow the traffic through the firewall. If you do not want Windows to do this, you can switch this option off in here. There is also an option to block all incoming network traffic. You would normally use this option on insecure network like a wireless network to give your computer additional security.

3. Advanced Security: The advanced settings option opens Windows Firewall and Advanced Security. This is an advanced tool that gives you a lot more control over what traffic is allowed and blocked by the firewall. In most cases the standard Firewall control panel should have more than enough options for the average user.

For the majority of Windows users the Windows Firewall provides the basic network protection required to protect your computer. There are also other firewall products on the market, some are free and some come at a cost. Regardless which product you choose, you should ensure that a firewall is installed and configured on your Windows 7 computer.

Anti-Virus and Malware

The major of people have heard the term virus. A virus is a piece of software that infects the computer without the user's knowledge. Once the computer is infected it may do things like waste ram, create random data on the hard disk or worse delete or corrupt your data files. Over the years malicious software has been developed that is simpler in nature to a virus and does not work in the in same way as a traditional virus. Malicious or unwanted software is often grouped together and can be referred to as Malware. Listed below are a few examples of software that come under the Malware heading.

Spyware

Spyware is designed to infect your computer without your knowledge like a traditional virus. Spyware reports back information about your computer usage to a third party. For example, it may upload your entire web browsing history to a third party. It is not designed to cause harm to your computer like a virus but may unintentionally do so. The harm can come from slowing down your network traffic when it is uploading data to the third party, using extra memory and processing power and in some cases crashing the computer. Since spyware installs on the computer without user knowledge, it will often bypass correct install procedures and forces its way onto the operating system. The Spyware is often not compatible with different software versions and operating systems or just poorly written and for this reason can cause computer crashes.

Trojan Horse

A Trojan horse is different from a lot of other Malware software in that it is a standalone piece of software that is often attached to another piece of software. The name Trojan horse comes from Greek mythology. In Greek mythology a wooden horse was built so that soldiers could hide inside. A Trojan horse in computing is software that will often present itself as something useful that the user may want. Since the user may feel the software is useful, they may run the software and unknowingly run the Trojan horse software that is contained within. Since the user has run the software, the Trojan software has tricked the user into allowing it to run on the computer and thus gain access to the computer.

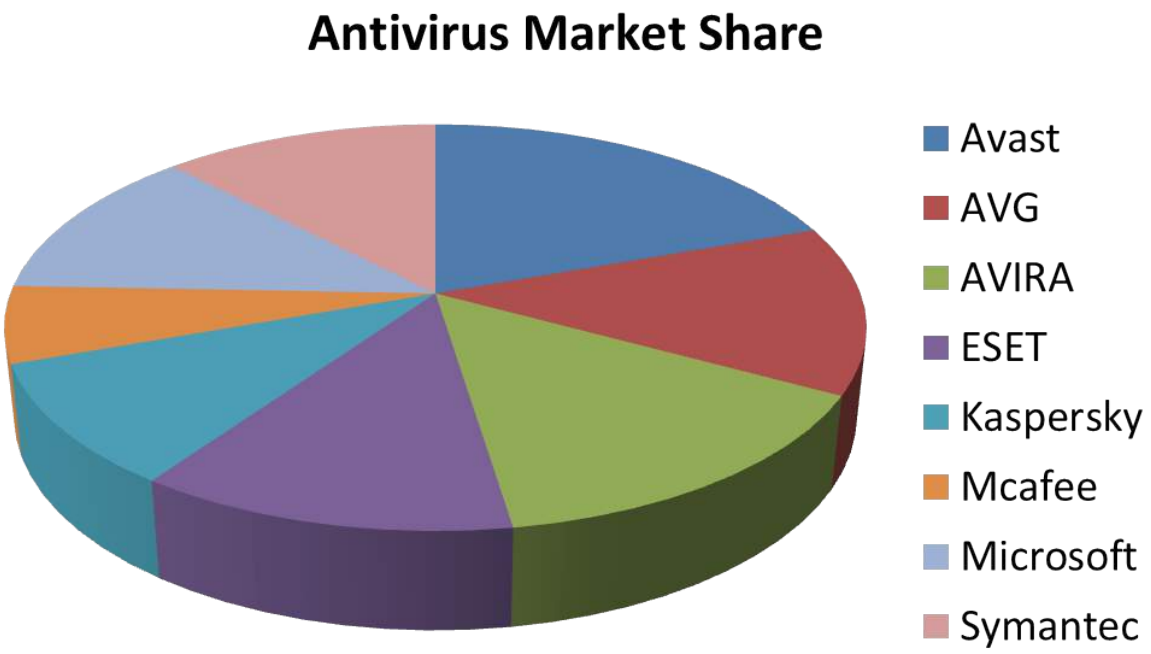
Once the Trojan horse software has run, it may do anything from creating a back door for a hacker to access the system, data theft or record keystrokes on the computer. An example of a Trojan Horse may be a free screensaver. Once the screen saver is installed it also installs a number of hidden programs. In a lot of cases the software will appear to install correctly. The user will get a fully functionally screen saver but be unaware that additional software was installed. For this reason, it is important that any software that you install comes from a trusted source.

Adware

Adware is software that installs itself without the user's knowledge. It may attach itself to useful software or silently install itself when a user visits a website using a system vulnerability. Once installed, the software will display ads on the user's computer. The person who wrote the software are attempting to generate revenue for themselves by displaying the ads. Adware can fast become very annoying to the user with endless popup ads appearing while the user is trying to work.

Anti-Virus and Malware Software

Nowadays when attempting to keep your computer secure, you should understand that you are no longer looking for just anti-virus software. Software should be able to stop and remove adware, spyware, Trojan horses and viruses. There are lots of free products on the market as well as commercial products. Some software offers a complete solution while other software may only address particular types of Malware. Some software comes with additional features like a firewall and webpage screening.



There are a lot of different products on the market that offer anti-virus and Malware features. Shown below is the current market share for each of the main products. In this chapter I will have a closer look at Microsoft Security Essentials, AVG, Avast! and Norton Antivirus.

Figures from OPSWAT. http://OPSwat.com

Microsoft Security Essentials

Microsoft Security Essentials is a free product for the home user. If you run a small business, you can use it on up to 10 PC's for free. Since its release in late 2009, Microsoft Security Essentials has received a lot of positive reviews. According to The Security Industry Market Share Analysis report of June 2011, published by OPSWAT Inc., Microsoft Security Essentially is in the top 4 most used antivirus products used in the world.

For business, Microsoft Security Essentials lacks centralized management features. This makes it not a good choice for large businesses that want to manage their software from a central point. Microsoft provides another product called Microsoft System Center 2012 Endpoint Protection which provides centralized antivirus software.

Microsoft Security Essentials is an easy product to install and is available for download from the following web address. http://windows.microsoft.com/MSE

AVG

Anti-Virus Guard better known as AVG was first released in 1992 in the Czech Republic by Grisoft. AVG offers a free edition of their software as well as two commercial versions. The first commercial version offers the same features as the free editions and also offers additional protection if you are sharing files. There is also a commercial AVG version called AVG Internet Security. This version has the same features as the other two, but also includes an email spam blocker and the AVG firewall. The free version is very functional and is used by a large part of the anti-virus market. It is available for the home user but not for business or organizations. AVG does however offer discounts for government, education, charities and churches. AVG also offers a centralized management tool which is useful for businesses that want to control anti-virus from a central location.

Avast!

The Avast! product is a free antivirus product which in its official name includes an exclamation mark at the end. The free product offers good protection from viruses and Malware. There is also a Pro version which offers additional features to protect you while buying products online and a sandbox feature. The sandbox features allows you to conduct web browsing and run programs in what is referred to as a sandbox. A sandbox is a virtual machine that runs separately from the rest of the operating system. If the sandbox was to become infected, the sandbox is destroyed when the application closes. This is a great feature as even if a virus or malware is downloaded, it is isolated from the rest of the operating system, preventing it from being infected. There is also an internet security version, which includes a firewall and email spam protection.

Norton AntiVirus

Norton AntiVirus is sold by Symantec Corporation and has no free product. It is however often bundled with new computers giving the user a trial period in which to try out the product. If they are happy with the product they can buy a subscription later on. According to AV-Test.org (independent antivirus software testing website) functionality of Norton AntiVirus base product is similar to free products like AVG and Avast! Norton also offers two additional products called Norton Internet Security and Norton 360. Norton Internet Security offers additional features like identity theft protection and paternal controls to manage which website your children can browse. Norton 360 offers all the features of the other two products plus the ability to backup the computer and a PC turner. The PC Tune feature is meant to speed up the running of your computer.

Summary

A lot has been covered in this chapter. To summarize in order to keep your computer secure ensure that Windows updates are being installed on the computer. This will ensure that any known vulnerabilities in Windows 7 will be fixed by installing updates as soon as they come out. Also by installing and activating a firewall, this will help protect your computer from attack. Lastly ensure that antivirus software is installed and kept up to date at all times and enabled. There are many free and commercial products available. For a lot of users many of the free products available are more than capable at protecting a computer. If you are considering buying a commercial product though, consider which additional features you will get. Besides the basic features of antivirus the free products, the commercial products offer additional protect like protecting you while making online transactions and protecting your e-mail from spam.