

Microsoft Windows 7

15 – Security and protection



SECURITY AND PROTECTION

INFOCUS

Keeping your computer and valuable data safe from harm is an ongoing problem for most computer users. For all the joys and benefits that the internet brings us, internet security remains a major issue. Every day, anti-virus programs, spyware protection and firewalls are working hard to protect our computers from possible threats, such as malicious software (viruses) and attempts by 'hackers' to gain access to our computers and collect our personal and other sensitive information.

Windows 7 has several features available to help to ensure your computer and data remains secure.

In this booklet we will show you how to:

- view the Action Centre
- check Windows Firewall settings
- view spyware settings
- check automatic update settings.

UNDERSTANDING COMPUTER SECURITY

Although we cannot always avoid threats, we can certainly take steps to minimise the associated risk. This applies not only to our lives, but also to our computers. We can

take steps to ensure that we protect our computers and keep them secure, and minimise the threats they face on a daily basis.

What Are The Threats To My Computer?

If you use the internet and email, share files with others or allow others to use your computer, then it is essential that you keep your computer secure to prevent harm. This is because computer criminals (also known as 'hackers') are constantly writing viruses and other forms of malicious software in an attempt to access your computer and steal your personal information, or to cause your computer to stop working as it should.

For all the benefits and advantages of the internet, internet security is still a major issue. For the most part it's because users are generally not educated on what they can do to keep their computer secure when using the internet.

How Can I Keep My Computer Secure?

There are a number of things you can do in Windows 7 to ensure your computer stays secure.

Windows Firewall

Hackers attempt to gain access to your computer by looking for vulnerabilities in your computer's security. This is where the firewall comes in. A firewall is a software program or hardware that checks incoming information (such as from websites) and blocks malicious software or attempts by hackers to gain access to your computer through a network or the internet. A firewall will also stop you from spreading viruses to other computers. In Windows 7 a firewall is installed and turned on by default.

Use Anti-Virus Software

Viruses, worms and Trojan horses (all types of programs designed to infect computers) are created by hackers in an attempt to erase information on your computer or to cause it to stop functioning as it should. Viruses can also be spread from computer to computer without the user being aware they are spreading a virus (such as through email and files on your computer). Installing anti-virus software and keeping it up-to-date is a must for internet users. Although Windows 7 does not include anti-virus software, there are free programs available to download (see www.microsoft.com), or you may already have virus protection software installed. Ensuring that **Windows Automatic Update** is turned on means that updates will be detected and installed automatically.

Maintain Spyware Protection

Spyware programs are designed to collect information about you, such as websites you visit, or they may display pop-up advertisements and the like. You are not usually aware that spyware has been installed on your computer, but if odd toolbars appear on your web browser, your default home page changes, or your computer starts running slower, there's a chance it's spyware. Spyware can be installed on your computer through free software that you download and install, and/or websites you visit. Windows 7 includes **Windows Defender**, designed to protect your computer from spyware. Again, ensuring that Automatic Updates is turned on will protect your computer from spyware.

Back Up Your Data

Make sure you regularly back up the data on your computer. If a virus or other type of malicious software does somehow find its way onto your computer, you can then restore your computer's data and settings to an earlier time, that is, before the virus infected your computer.

Playing It Safe

Although Windows does its best to keep your computer secure, it really does come down to you being aware of the types of threats that exist, how they can end up on your computer, and what you need to be aware of and can do to ensure that your computer and valuable data stays safe.

CHECKING THE ACTION CENTRE

The **Windows Action Centre** is your one-stop-shop to view messages and alerts about any outstanding security and/or maintenance issues. If a security or maintenance issue requires your attention,

the Action Centre notification, which appears as a flag in the **Notifications** area of the **Taskbar**, will display pop-up messages or appear with a cross.

Try This Yourself:

Before starting this exercise ensure you are viewing the desktop...

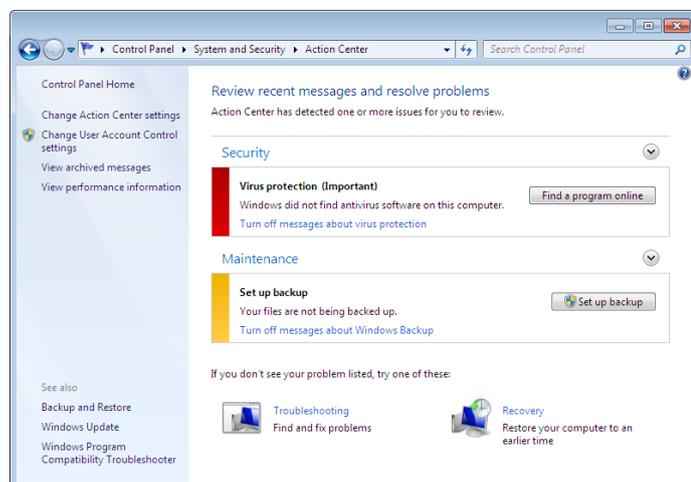
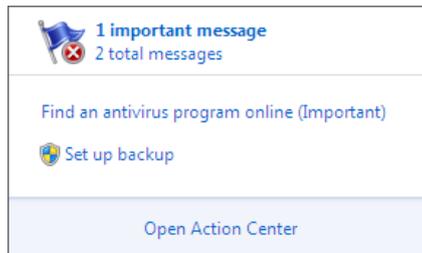
- 1 Click on the flag  in the **Notifications** area of the **Taskbar** to display a pop-up menu

If any issues require your attention they will be listed here...

- 2 Click on **Open Action Centre** to open the **Action Centre** window

The Action Centre window displays any alerts or messages that require your attention. In this picture shown, the Action Centre advises that no virus protection is installed, and that a backup schedule has not been set...

- 3 Click on **close**  to close the **Action Centre** window



For Your Reference...

To open the **Action Centre**:

1. Click on the flag  in the **Notifications** area of the **Taskbar**
2. Click on **Open Action Centre**

Handy to Know...

- To open the **Action Centre** window, select **Start > Control Panel**. Click on **System and Security** and then **Action Centre**.

CHECKING WINDOWS FIREWALL SETTINGS

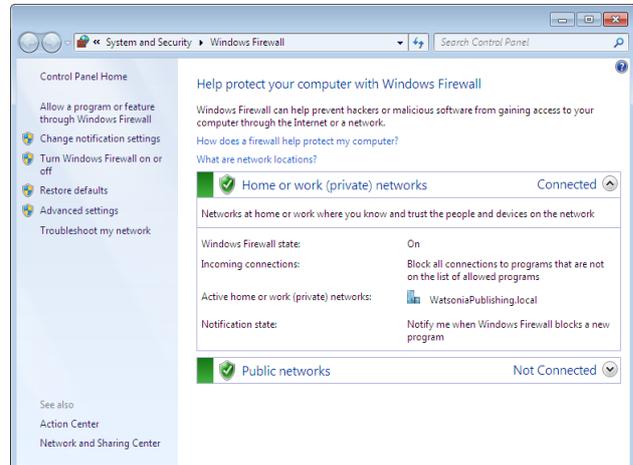
A **firewall** acts as a guard between your computer and a network or the internet, and stops any attempts by hackers to gain access to your computer. It also blocks any malicious software from installing on your

computer, and likewise, will stop you from inadvertently spreading viruses and the like to other computers. **Windows Firewall** is turned on by default.

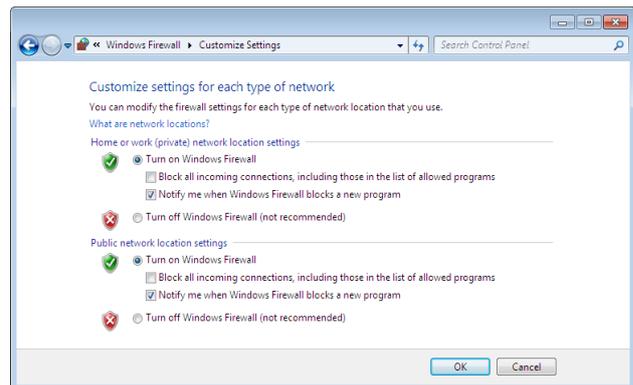
Try This Yourself:

- 1 Select **Start** and type **firewall** in the **Search** box
- 2 Click on **Windows Firewall** in the search results listing to open **Windows Firewall**
The Firewall window displays the status and details of any current network connections...
- 3 Click on **Turn Windows Firewall on or off** in the left pane
The Customise Settings window is displayed. Here you can view the current status of your firewall. You will leave the settings as they are...
- 4 Click on **Back**  to return to the previous window
- 5 Click on **Allow a program or feature through Windows Firewall**
This is a list of Allowed programs and features, and note most of them are turned off (unchecked). It is best to leave these as they are unless you know which programs you want to allow...
- 6 Click on **close**  to close the window

2



3



For Your Reference...

- To check **Windows Firewall** settings:
1. Select **Start** and type **firewall** in the **Search** box
 2. Click on **Windows Firewall** in the results listing

Handy to Know...

- **Windows Firewall** will allow you to view most websites and download programs, however, if Windows isn't sure about the security of a website or program, it will notify you before it blocks it and ask you whether you want to allow access or add it to the list of allowable programs.

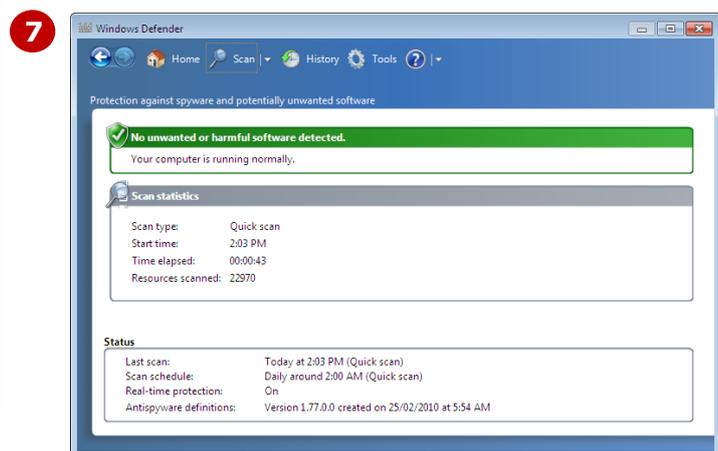
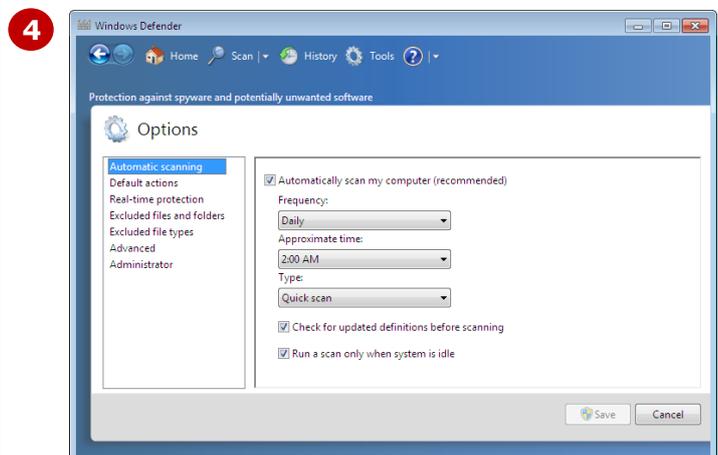
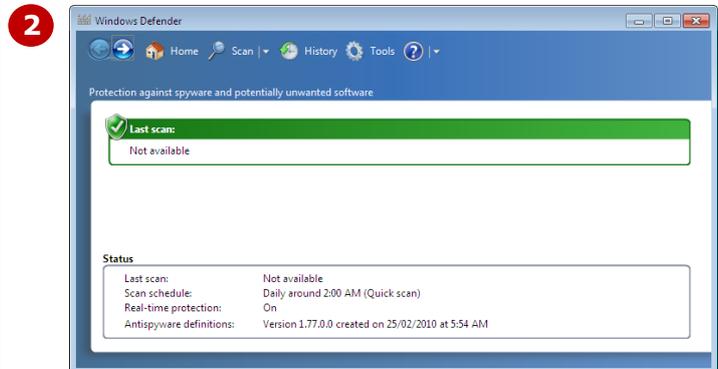
CHECKING SPYWARE PROTECTION SETTINGS

Spyware is malicious software generally designed to collect information about you. It is common for spyware to be found in free software that you might download, such as screen savers. To prevent

spyware, Windows 7 is packaged with **Windows Defender**, a software program designed to scan your computer for spyware and remove any threats. Defender is turned on by default.

Try This Yourself:

- 1 Select **Start** and type **spyware** in the **Search** box
- 2 Click on **Windows Defender** in the search results listing to open **Windows Defender**
- 3 Click on **[Tools]** in the toolbar to display **Tools and Settings**
- 4 Click on **Options**
Automatic scanning shows that an automatic scan schedule has been set up...
- 5 Click on the drop arrow for **Approximate time** and select another time (one that will be when the computer is turned on so it can run the scan)
- 6 Click on **Real-time protection** in the left pane
This shows that real-time protection is turned on, which means that Defender will notify you when spyware attempts to install itself and asks you what action to take...
- 7 Click on **[Scan]** in the toolbar to begin a manual scan of your computer
This might take a few minutes, and hopefully you are advised that no harmful software was detected...
- 8 Click on **close**  to close the window



For Your Reference...

To open **Windows Defender**:

1. Select **Start** and type **spyware** in the **Search** box
2. Click on **Windows Defender** in the search results listing

Handy to Know...

- If **Automatic Updating** is turned on and set to notify and/or automatically install updates, updates for the latest spyware definitions (threats) will be downloaded and installed automatically. That is, you really don't have to do a thing when it comes to checking for and removing spyware!

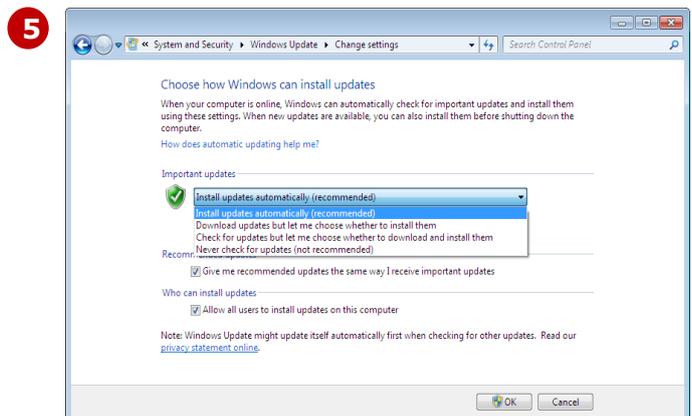
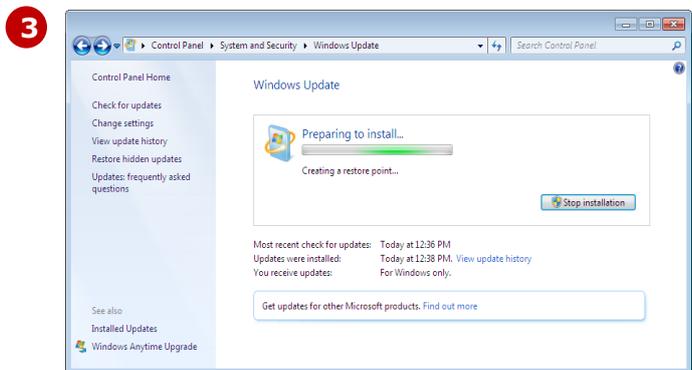
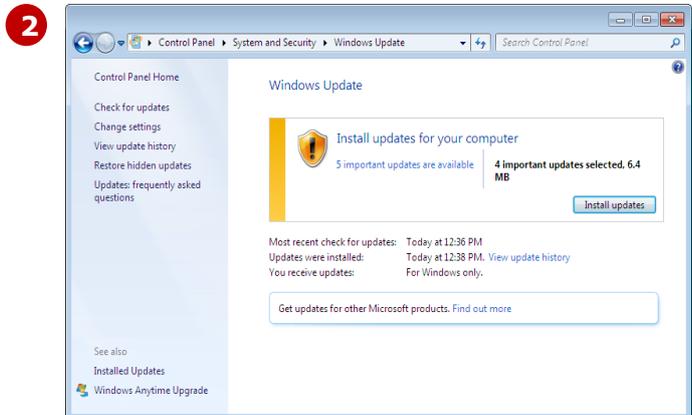
CHECKING AUTOMATIC UPDATE SETTINGS

By default, Windows 7 will turn on the **automatic updates** features. This means that Windows will download and install any authorised updates without you even being aware of it! This is an important feature of

Windows 7, as it ensures that your computer has the latest updates for programs, including installed anti-virus and spyware programs (called virus or spyware definitions).

Try This Yourself:

- 1** Select **Start > Control Panel** to open the **Control Panel**
- 2** Click on **System and Security**, and then click on **Windows Update**
The Windows Update window is displayed, as well as alerts about updates to be installed. This alert will only appear if automatic update settings are not set to download and install automatically...
- 3** Click on **[Install updates]** to begin installing the updates if you have this option
The updates will begin installing and may take a few minutes...
- 4** Click on **Change settings** in the left pane
Here you can choose how Windows manages updates...
- 5** Check that the **Install updates automatically (recommended)** option is turned on
- 6** Change the time that new updates are installed to a time when you are likely to be connected to the internet, and click on **[OK]**
- 7** Click on **close**  to close the window



For Your Reference...

To view **Automatic Update** settings:

1. Select **Start > Control Panel**
2. Click on **System and Security**
3. Click on **Windows Update**
4. Click on **Change settings** in the left pane

Handy to Know...

- Your computer has to be connected to the internet to enable Windows to check for updates and begin downloading and/or installing them.

CONCLUDING REMARKS

Congratulations!

You have now completed the **Security and protection** booklet. This booklet was designed to get you to the point where you can competently perform a variety of operations as outlined in the task list on page 2.

We have tried to build up your skills and knowledge by having you work through specific tasks. The step by step approach will serve as a reference for you when you need to repeat a task.

Where To From Here...

The following is a little advice about what to do next:

- Spend some time playing with what you have learnt. You should reinforce the skills that you have acquired and use some of the application's commands. This will test just how much of the concepts and features have stuck! Don't try a big task just yet if you can avoid it - small is a good way to start.
- Some aspects of the course may now be a little vague. Go over some of the points that you may be unclear about. Use the examples and exercises in these notes and have another go - these step-by-step notes were designed to help you in the classroom and in the work place!

Here are a few techniques and strategies that we've found handy for learning more about technology:

- visit CLD's e-learning zone on the Intranet
- read computer magazines - there are often useful articles about specific techniques
- if you have the skills and facilities, browse the Internet, specifically the technical pages of the application that you have just learnt
- take an interest in what your work colleagues have done and how they did it - we don't suggest that you plagiarise but you can certainly learn from the techniques of others
- if your software came with a manual (which is rare nowadays) spend a bit of time each day reading a few pages. Then try the techniques out straight away - over a period of time you'll learn a lot this way
- and of course, there are also more courses and booklets for you to work through
- finally, don't forget to contact CLD's IT Training Helpdesk on **01243-752100**