BROADBAND FACTSHEET

Broadband is a term used to describe a range of high-speed connections to the internet.

A broadband connection can send and receive data up to 10 times faster than a standard modem connection (sometimes referred to as a narrowband or dial-up connection).

There are a number of ways that you can access a broadband connection but the common methods are:

- **ADSL**
- **Cable**
- **Satellite links**
- **LMDS**
- **Third Generation Cellular**

Of these, ADSL and cable are the most popular. These connections are described as 'always-on' because they can be permanently attached to the Internet.

Broadband is highly efficient and offers numerous benefits. However, it is important to be aware that if an Internet connection is 'always-on', there are risks that make it vulnerable to attack if appropriate security measures are not in place.

ADSL

ADSL (Asymmetric Digital Subscriber Line) converts a standard telephone line to a high-speed digital link for broadband services. An ADSL modem is connected to a standard telephone socket through a special filter.

This is proving to be one of the most popular methods because (in most cases) there is no need to install a new connection or to change telephone numbers. Internet Service Providers often supply the required modem and filter for their broadband service so that installation can be completed 'out of the box', by the user. For further information about ISPs, you may wish to see our How To Choose an ISP guide, which is available as a PDF file.

In order to use ADSL you must be situated within a certain distance of a telephone exchange. Many web sites have a facility for checking if your postcode is within an ADSL region – for example: **www.broadband1.bt.com/.**

CABLE

Cable broadband uses fibre optic cables, most commonly installed for television services. Domestic users often install broadband as part of a cable television package.

A broadband connection is made via a 'cable modem' which can run up to 40 times faster than standard modem connections. This type of connection requires cable access in your area (you would need to check with whichever cable company you wish to use that it operates in your postal district). Installation needs to be carried out by a cable company.

SATELLITE

Satellite connections use satellites (instead of cables) to provide a communications link via a satellite dish. These connections are most commonly installed for television services - domestic users often install broadband as part of a satellite television package. Initial setup can be expensive but the main advantage is that your location is not a problem because no cables or telephone lines are required.

LMDS

LMDS (Local Multipoint Distribution System) is a wireless broadband technology that provides connections across a few kilometres for multiple subscribers. This can be useful in isolated communities where other mainstream connections (for example, ADSL or cable) are not available.

LMDS is installed using 'cells' which are similar to the radio cells used by mobile telephone systems. However, LMDS can be susceptible to interference from the weather.

THIRD GENERATION CELLULAR

Third Generation Cellular is an emerging technology, sold mostly by mobile telephone companies. It enables users to send high-capacity items (for example, images, e-mail and music) to mobile devices using broadband speeds.

RISKS SURROUNDING BROADBAND CONNECTIONS

Many people are confused about the term 'always-on' and what it means as far as security is concerned.

It does not mean that:

- your computer has to be constantly switched on
- your computer is vulnerable when it is switched off.

It does mean that:

- there is no need to dial out for a connection to the internet
- an Internet connection is always available when the computer is switched on.

If you have a broadband connection and your computer is switched off, there is no risk to your computer. However, if you have broadband and your computer is on, you may be vulnerable to malevolent attacks if appropriate security measures are not in place. The risks to users of broadband services are not new. Most already exist in one form or another but it is the 'always-on' technology and increased communication speed that makes it important for users to be even more aware of these risks.

The most common risks for broadband connections fall into the following categories:

- **External**
- **Single point of failure**
- **System overload**

EXTERNAL RISKS

Computer hackers seek to damage other people's equipment and information just because they can, or because of a grudge. In some circumstances, people gain access to machines and use them as platforms for further illicit activity. Common activities carried out by hackers include:

- Denial of service attack. An attacker will flood a system with messages and data to prevent the target system from operating.

- **Eavesdropping** – An attacker will 'listen in' to network traffic to find information that helps them to break into a system, or to gain valuable information.

- **Network Intrusion** – An attacker attempts to gain control of a system at a very fundamental level, avoiding a range of commonly used control systems and techniques.

- **Port scanning** – An attacker uses a programme that automatically scans the Internet for machines that have certain vulnerable configurations. Once found, the attacker tries to exploit these vulnerabilities for his/her own gain.

SINGLE POINT OF FAILURE RISKS

Smaller companies and individuals often combine their data and telephone lines using broadband. If the connection were to fail for any reason, all remote communication would be affected – hence there would be a 'single point of failure'.

SYSTEM OVERLOAD RISKS

If your organisation has previously used low-speed (narrowband) connections for remote access (perhaps for salespeople or home workers), there is a potential impact when you switch to broadband.

Connecting to the Internet at low speed can be an unattractive option, so usage is kept to a minimum. However, the convenience of broadband may result in more people connecting more often, for longer periods. In turn, this could affect the performance of central servers and networks.

MINIMISING THE RISKS ASSOCIATED WITH BROADBAND

There are a number of steps that you can take to reduce significantly the security risks associated with broadband. These include:

- **Installing a firewall**. These range from large-scale devices for companies to personal firewalls for installation on single machines. A firewall isolates a computer or a network from the public Internet and inspects incoming data to determine whether it should be allowed to pass through or whether it should be blocked.

- **Configuring firewalls to protect ports** (the entry points of a computer used by hackers) so that only authorised parties can gain access.

- **Ensuring that plans and procedures are in place** which detail contingency measures in the event of your broadband service being lost.

- **Avoiding the creation of a 'single point of failure'**. For example, if your telephone system operates through broadband it is a good idea to have a completely separate line that could be used if the broadband connection should fail.

- **Switching off the File and Printer Sharing option in Microsoft Windows** if you only use one computer (i.e. you do not have a network). To do this in Windows 98 you would:
  1. Click the Windows Start button
  2. Select Settings
  3. Select Control Panel
  4. From the Control Panel window, double-click on the Network icon
  5. In this window, click on the File and Printer Sharing button and make sure there are no tick marks in the two checkboxes.

  Note: If your computer is part of a network, you should not switch this option off as it is required to share resources.

- **Using well constructed user names and passwords.**

- **Installing virus defence software** and keeping it up to date.

- **Considering a Virtual Private Network** for highly sensitive information and applications.

For more information on *Achieving best practice in your business:*

- Visit our website at **www.dti.gov.uk/bestpractice**
- Call us on **0870 150 2500** to order from our range of free best practice publications or visit **www.dti.gov.uk/publications**
- Contact your local Business Link adviser by visiting the website at **www.businesslink.gov.uk** or calling **0845 600 9 006**

Published by the Department of Trade and Industry. www.dti.gov.uk