



Beginners: Precautions Using the Internet (1)

Spam

Spam or Junk Mail is unsolicited commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services that you are likely to receive through your email box, just like you would normally get through your letter box! **Spam** might contain inappropriate or **offensive** material. To minimise the amount of junk mail you receive:

- whenever you register with a company or web site, **do not give them permission** to pass your details on to third parties or to send you a regular newsletter.
- **Use different email accounts** for different purposes, for example use one email account for your friends and family, a different one for making purchases online and a third one to be used exclusively on forums, message boards and chat rooms.
- **Never reply** to junk mail. Often spam is sent out randomly; by responding to the email you simply verify that you have a valid email address, and you will be targeted even more.
- Most email accounts include free spam protection tools; use them to **report** spam and even to **block** senders.



Viruses

A **virus** is a computer program, usually disguised as something else, designed to cause damage by either deleting or corrupting files on your computer. Their effects can vary from displaying irritating messages to stealing data or giving other users control over your computer.

You can receive an infected file in an email attachment, in a download or from a diskette or CD. A virus programme has to be run before it can infect your computer—this happens when you open the infected file.

Many of the most prolific viruses are spread by email; usually they are activated by a user opening an attached document which is infected.

To minimise the risks of introducing a virus to your system:

- **Use a firewall** to prevent viruses from sending out information.
- **Install antivirus software** and update it regularly.
- **Don't open** but delete emails from senders you do not recognise.
- **Delete attachments** that you were not expecting, without opening them, especially if they have two file extensions (e.g. LOVE-LETTER-FOR-YOU.TXT.VBS or ANNAKOURNIKOVA.JPG.VBS)
- **Don't run unsolicited programmes** or documents, including screensavers and joke programmes, from the Internet.

Internet Security: Virus protection and Firewalls

Antivirus software can detect viruses and either **disinfect** (remove the virus code) or **delete** the infected files.

Antivirus software scans a computer system and looks for viruses that might have infected it by comparing it to a list of all known viruses. This means that antivirus software is only effective on the viruses it already knows; it is therefore imperative to keep the antivirus software up-to-date by regularly downloading up-to-date lists of known viruses.

There are many antivirus software available on the market, from companies like Symantec and McAfee, which offer a yearly subscription. All Hillingdon Libraries PCs use Sophos antivirus.

When a computer is connected to the Internet it uses communication ports to send and receive data. Malicious individuals or organisations can use these ports to access your computer without your knowledge to delete information from it, steal your personal information (like passwords or credit card numbers) or spread spam or viruses from it. A **firewall** acts like a bouncer, it's designed to keep unauthorized users from tampering with or accessing information on your computer.

Only authorised users such as those with a key or access card will be able to enter or exit your system.

