Be safe using email

Viruses

Viruses are programs that spread automatically from one computer to another. If your computer is infected by a virus it may cause a lot of damage. A common way for viruses to spread is in email attachments.

Google Mail scans attachments for viruses when they are delivered to your account and again each time that you open a message. The attachments that you send are also scanned for viruses.

Incoming Attachments

Once you open a message, you will notice that Google Mail displays the progress of the virus scan right above the list of attached files. While Google Mail is checking for viruses, you will see a message that says: 'Scanning your attachments for viruses...'

Once the scan is complete, Google Mail will display the results. If an attachment is safe, you can download it by clicking on the link.

If there is a virus in an attachment, 'Virus found' will appear next to the filename and you will not be able to download it.

Outgoing Attachments

If Google Mail detects a virus in an attachment that you are trying to send, you will receive an error message that says: 'Your attachment contained a virus and could not be sent.' Click on the link in the error message that says 'Remove attachment and send.' Your message will then be sent, without the attachment.

Other email programs

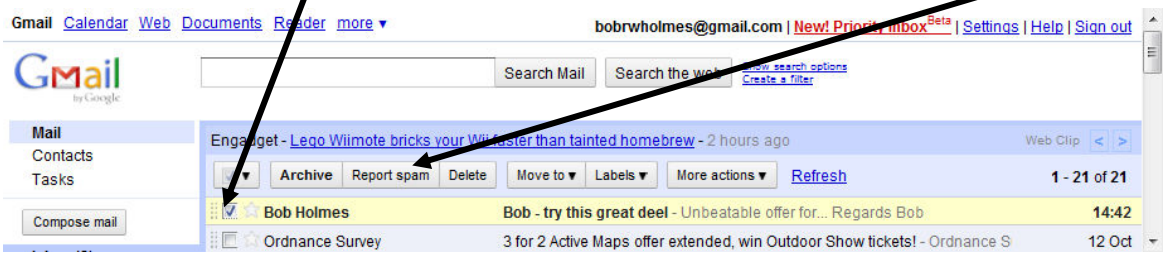
If you use a program like Windows Live Mail or Outlook Express that stores the messages on your computer, it is important to have anti-virus software installed and up-to-date. If you have your own computer the Get Digital Tutor can advise you about suitable anti-virus tools.

Spam

Spam is electronic junk mail; messages sent to millions of addresses. They generally advertise black market goods, unlicensed software, drugs or pornography. They can also be used for financial frauds, e.g. a message offering you a share of some ill-gotten gains if you send details of your bank account (yes, there are some people who fall for this one!). Spam may also be used for Phishing (see below).

The subject line of a spam message will usually give it away. It will be offering the goods or services as above. It may well be obscene. It may also be mis-spelled. This is to avoid automatic filters.

If you receive a spam message, don't open it. Select the message by clicking the check box next to it in the Inbox and then click Report spam.



The message, and all future messages from the same sender, will be moved to the Spam folder. The Spam folder is automatically emptied every 30 days.

Preventing spam

The Google Mail spam filter is fairly effective, but it is still worth taking steps to reduce the risk of spam by restricting the distribution of your email address.

- Never post your real email address on a forum or bulletin board. Spammers use special programs which collect these and use them to build spam distribution lists.
- If you do use forums or bulletin boards, set up an alternative email account just for use on the bulletin board.

Then when the spam becomes a nuisance, just close the account or ignore it so that it lapses.

- If you need to put your email address on a website, for business, or for a club or other organisation, make sure that the website designer takes precautions to prevent the address being copied automatically (this is known as "harvesting".)
- When you register with a website, make sure you do not give them permission to sell your email address, or other personal information, to third parties.
    - Read the text carefully to make sure that you are not accidentally agreeing to this. Websites should make the default to "opt-out", but some, especially those based outside the UK, may not do this.
    - Watch for little checkboxes and make sure to remove any which are checked by default to say that you agree to the website using your details.
    - If you have any doubt, use an alternative address as above.

Phishing

Phishing (i.e. "fishing") is the name given to e-mails that try to fool you into giving personal information, e.g. bank details, passwords for online banking or other websites, credit card numbers.

Phishing e-mails can be very cleverly designed to fool you. They generally have links to fake websites which are almost exact copies of the real website. A recent case used a website which mimicked that of the Inland Revenue!

The thing to remember is that a legitimate bank or shopping site will **never** send out an email to ask you to enter your password or any other sensitive information by clicking on a link and visiting a web site.

If you do receive an email that appears to come from your bank and asks for information, you should contact them by telephone, or by going to their website by typing in the address that you always use, or using the one in your Favorites.

They will almost certainly confirm that the email is a fake.