IT Security Advice on Scam Email

There are many email scams in regular circulation, often purporting to come from genuine organisations such as banks, government departments and the post office.

Examples include:

- Inland Revenue to say you are due a tax refund
- Post Office to say you have a parcel
- Banks and building societies asking you to verify your account
- Justice.gov.uk to say your vehicle is parked illegally
- Scotcourts.gov.uk to say you are due in court

The list is endless.

The purpose of such emails is to fool you into giving out personal financial information, or to compromise your computer by introducing nasty software.

The first thing to be aware of is that the sender's address will have been spoofed to make it look as though the email has come from a legitimate organisation. Such organisations would never contact you in this way.

No bank or building society would ever ask you for information such as usernames, passwords, credit card numbers, account numbers, etc. Any email asking you to 'verify your account', 'confirm your sign in details', or using a similar form of words, is almost certainly a scam, even if it appears to come from your own bank.

For your own protection

- Always log on to your own bank's website directly by typing the web address directly into your browser and never via a link in an email

- Check out what your bank has to say in their section on security; most of the major banks and financial institutions have very useful security information and guidelines on their websites, and they tell you what to look for in a genuine communication.

- If you find you have received an email which looks unusual in any way at all, or comes from a source that you are not expecting or have never had dealings with before, or that is similar to those mentioned above, do be wary.

    - Do not open it
    - Do not reply to it
    - Do not forward it to anyone
    - Do not click on any links contained within the email
    - Do not open any attachments
    - **DO delete it**