Simple steps to avoid being phished

Phishing is an increasingly common type of spam that can lead to theft of your personal details such as credit card numbers or online banking passwords.

Phishing attacks work by the scam artist sending "spoofed" emails that appear to come from a legitimate website that you have online dealings with such as a bank, credit card company or ISP - any site which requires users to have a personal identity or account. The email may ask you to reply with your account details in order to "update security" or for some other reason.

The phishing email may also direct you to a spoofed website or pop-up window which looks exactly like the real site, but has been set up for the sole purpose of stealing personal information. Unsuspecting people are then often fooled into handing over credit card numbers, passwords or other details.

According to the Anti-Phishing Working Group, phishers are able to convince up to five per cent of recipients to respond.

How to protect yourself:

- **Never respond to emails that request personal financial information**
  Banks or e-commerce companies generally personalise emails, while phishers do not. Phishers often include false but sensational messages ("urgent - your account details may have been stolen") in order to get an immediate reaction. Reputable companies don't ask their customers for passwords or account details in an email. Even if you think the email may be legitimate, don't respond - contact the company by phone or by visiting their website. Be cautious about opening attachments and downloading files from emails, no matter who they are from. Sophos uses SPF (Sender Policy Framework). This is an anti-forgery solution which involves publishing a list detailing which servers are allowed to send Sophos emails.

- **Visit banks' websites by typing the URL into the address bar**
  Phishers often use links within emails to direct their victims to a spoofed site, usually to a similar address such as mybankonline.com instead of mybank.com. When clicked on, the URL shown in the address bar may look genuine, but there are several ways it can be faked, taking you to the spoofed site. If you suspect an email from your bank or online company is false, do not follow any links embedded within it.

- **Keep a regular check on your accounts**
  Regularly log into your online accounts, and check your statements. If you see any suspicous transactions report them to your bank or credit card provider.

- **Check the website you are visiting is secure**
  Before submitting your bank details or other sensitive information there are a couple of checks you can do to help ensure the site uses encryption to protect your personal data:

  Check the web address in the address bar. If the website you are visiting is on a secure server it should start with "https://" ("s" for security) rather than the usual "http://".

  Also look for a lock icon on the browser's status bar. You can check the level of encryption, expressed in bits, by hovering over the icon with your cursor.

  Note that the fact that the website is using encryption doesn't necessarily mean that the website is legitimate. It only tells you that data is being sent in encrypted form.

- **Be cautious with emails and personal data**
  Most banks have a security page on their website with information on carrying out safe transactions, as well as the usual advice relating to personal data: never let anyone know your PINS or passwords, do not write them down, and do not use the same password for all your online accounts. Avoid opening or replying to spam emails as this will give the sender confirmation they have reached a live address. Use common sense when reading emails. If something seems implausible or too good to be true, then it probably is.

- **Keep your computer secure**
  Some phishing emails or other spam may contain software that can record information on your internet activities (spyware) or open a 'backdoor' to allow hackers access to your computer (Trojans). Installing anti-virus software and keeping it up to date will help detect and disable malicious software, while using anti-spam software will stop phishing emails from reaching you. It is also important, particularly for users with a broadband connection, to install a firewall. This will help keep the information on your computer secure while blocking communication from unwanted sources. Make sure you keep up to date and download the latest security patches for your browser. If you don't have any patches installed, visit your browser's website, for example users of Internet Explorer should go to the Microsoft website.

- **Always report suspicious activity**
  If you receive an email you suspect isn't genuine, forward it to the spoofed organisation (many companies have a dedicated email address for reporting such abuse).