Security awareness series.

Spam and Phishing

1 Welcome to a short presentation on spam and phishing.

2 Firstly - what is spam? Well it’s also referred to as UBE or UCE - unsolicited bulk or commercial email. It’s unwanted - like the junk mail that comes through your letterbox at home.

3 Why is it a problem? Well, it’s a nuisance - you have to spend time each day reading the messages, hopefully recognising them and then deleting them. And if you get a lot of spam messages, it all adds up. Also you might miss real genuine email - in amongst the mass of spam or you might delete real mail by accident.

   But worse - you might not recognise it and you might treat it as genuine and you maybe click on something you shouldn’t or send back some information. The messages that ask for information are known as phishing emails. They are called that because they fish for details - usually passwords, but other details are also requested.

4 So how can you recognise these messages? Well it’s worth looking at the email headers. Sometimes the message is clearly addressed to someone else or comes from a patently fake source. However, it is important to understand that some headers can be faked so you really need to look at the full email headers to see if it really comes from someone other than who it claims to come from.

   The types of messages that ask for information fall into a category known as social engineering. The messages may appear to come from someone you are expecting to hear from - maybe your bank, your ISP or maybe a supermarket. It’s usually somewhere where you have an account with some personal details and usually a password.

   It’s easy enough to guess that a message coming from a bank is not genuine if you have no dealings with that bank, but at some point, you will receive a message that seems so relevant that you look at it and take it in good faith. For example, before Christmas in recent years, there are waves of phishing emails that claim to be about a parcel you have just sent. They claim the parcel has got lost and ask for personal details. Obviously, they are trading in on the fact that a lot of people send parcels at that time of year and will naturally be concerned if told they have got lost. They will then give details in the hope that their parcel will be found.

5 So how does it work? The messages often ask you to visit a website. These websites are fake and set up so as to exploit loopholes such as vulnerabilities on your machine. Your machine may get infected when you click on the website.

   The machine can then be controlled by the bad guys - maybe used to send out more spam and get the blame put on you. It’s quite cheap to send email, particularly so if you use other people’s machine to do it. And if they have a fast connection to the Internet... even better.

   The message may phish for a username and password and then uses this to impersonate you on a mail server and send out email from your account. This is likely to result in your email account being blocked.
If the server is a College machine, there is the possibility that the College, as a whole, may be blacklisted and all mail from the College would be blocked by other sites.

If you’re in any doubt, ask the IT Service desk.

6 So how can you prevent it? Well, be careful with your email address. Don’t publicise it everywhere. Or, if you need to publicise it, maybe obscure it in some way such as replacing the @ sign with brackets and the word “at”. The spammers use automated tools to “harvest” addresses from websites, so this sort of obfuscation can stop some of the tools.

Keep your machine healthy - keep it patched and keep your anti-virus up-to-date.

Also - be aware of your normal machine behaviour so that you can recognise if it suddenly starts going very slowly. For all you know, your machine may be sending out thousands of spam messages behind your back.

Unfortunately, this is not the whole story - sometimes the bad guys are ahead of the anti-virus guys (the good guys), but if you are not tempted in the first place to do something you shouldn’t, your machine will live to fight another day.

7 You can let others help. Mail clients can try to guess what is spam and flag it for you - but there is always a margin of error. If you filter flagged messages to another folder, it is then easier to spot patterns and recognise spam when looked at in bulk. It also means you can check this folder at regular intervals and not have the spam mixed up with the rest of your email.

Obviously you should always check a folder of suspected spam for genuine messages. Sometimes the presence of a particular word in the subject field may find a message incorrectly flagged as spam.