Session -7: Phishing, spamming & spoofing

Firstly, what is spam? (And what it isn't?)

Like the junk mail that's pushed through your letterbox, spam is worthless information that you haven't asked to receive. You should however **never** "unsubscribe" from a spam email as this only confirms your email address is valid and you'll get even more spam.

Spammers send messages all over the internet from loads of different addresses and they often "spoof" these addresses to hide who actually sent them and trick you into thinking they may be from a reliable source.

What isn't spam is a marketing email you might get from a reputable company you have dealt with, like a utility company or retailer. Although you might not want it, it is legitimate marketing information and it should come with an "unsubscribe" option so you can remove yourself from the distribution list.

What is Phishing?

Phishing is a type of online identity theft. Scammers use messages designed to look as if they are from a genuine company to try and trick you into giving out private information like your BT ID username and password or even your bank details.

Think before you click

Never click on any links in a suspicious email

- BT (and most reputable companies) will never ask you for private/personal details or banking information out of the blue
- BT will never send you an email with an attachment

What is Spoofing?

Spoofing is a technique used by spammers where an email is sent with a forged "From" address, in this case yours. With spoofing, emails are made to look as if they come from you, when in fact they don't.

This often happens when your account has been compromised. The spammer may have stolen your contacts and then sent emails to them by forging the sending address to look as if it's come from you.

Unfortunately, spoofing isn't something that can be stopped. Your best protection against spoofing and spam is to protect your email address:

- Be particularly security conscious if you use a public or shared computer
- Remember, each time you exit your email you should sign out completely by clicking the **Sign Out link** at the top of the page. This means anyone using the computer next won't be able to access your account
- Email accounts are now regularly compromised by people checking emails on smartphones using unsecured wi-fi networks. The smartphone stores your account details so each time you log in both the username and password get sent, allowing anybody using the open network to see your details
- If you believe that your account has been spoofed, the best option is to create a new email address (sub-account) within your existing email account. You can then tell your contacts to use that email address instead of your old one. Unfortunately, deleting the old email address won't stop the spoofing activity on that account, so you should also tell your contacts that any email received from the old address will be bogus and should be deleted