Protect yourself from email phishing

Email phishing is a method in which the scammer sends an email pretending to be a person, company or trusted site in order to steal passwords or sensitive information. Scam emails can become spam or junk and may also have a link or file attached for you to click on or open. Opening these links or downloading the files may harm your device.

How to spot a phishing email

- **Were you expecting it?** If the message comes from a person or entity you don't know, think twice before replying, clicking on any link or downloading any attached files.
- **Who sent the message?** Is the email address what you expected? Check whether the sender's email address is spelt correctly, the domain is trustworthy and, if it matches the name of the person who sent the email.
- **Is it asking you to do something?** Phishing emails usually ask you to carry out an action such as clicking a link, downloading an attached file, replying to the message or providing personal information. They often try to create a sense of urgency to look for an immediate and irrational reaction.
- **Is it poorly written?** Does it contain poor grammar, spelling errors or an unusual style of writing.
- **Sense of urgency.** It may request a quick response or a threat that unless you act now, a deal will expire, or your account will be closed. Or even trick you into thinking you've won money or a prize.

What to do if you think you've received a scam email?

- **Ignore attachments and all links.** Don't open any attachments unless you know they're from someone you know and trust. Don't click on links within the email - always search for the website or company yourself instead.
- **Don't reply.** Never reply to scam emails, even to say 'No'. This will let the scammer know that your email address is active, and they'll send you more emails.
- **Think twice before sharing any details.** Organisations shouldn't contact you unexpectedly asking for your password or for financial information. Never be pressured into sharing any personal or financial details.
- **Double-check.** If you get an unexpected request for payment from someone claiming to be a trusted company, look up their phone number and give them a call to check.
- **Stay protected.** Make sure you have updated anti-virus software installed on your device to protect it from viruses.
- **Mark the email as spam through your email provider.** This will delete the email and will stop emails from that address from entering your inbox in the future.
- **Report and delete.** Report scam emails to Action Fraud, then make sure you delete the email.

DID YOU KNOW?

Spear phishing uses personalised messaging to trick a specific individual or organisation into believing they are legitimate.

HOW TO IDENTIFY A PHISHING EMAIL OR SMS

Have you received an unexpected message?

YES / NO

Is there anything strange about the sender?

YES / NO

Are you being asked to share data, click on a link or download a file?

YES / NO

Can you verify with the sender, through a separate communications channel, that the message is legitimate?

YES / NO

Report it directly to the person or company, through their official telephone number, email address or website page.

Remember, think before you click or reply.