

DO YOU SMELL A PHISH?



POPULAR PHISHING EMAILS:

- You have voice mail
- Payment / invoice notification
- Resume / CV
- Flight or hotel booking

BEWARE OF SPEAR PHISHING

Did you know that most security breaches happen not through sophisticated hacker attacks, but because people click on bad links in phishing emails?

SPEAR PHISHING - FRAUDSTERS ARE ACTIVELY LOOKING FOR YOU!

 **80%**

of malicious software attacks are as a result of phishing.

 **11%**

of people open malicious attachments or click on bad links in phishing emails.

SCARY STATS

Spear Phishing means criminals personalise their attacks specifically for you. They find out things about you and create a tailored scam that looks legitimate, even calling you by name.

WATCH OUT FOR FAKE EMAILS

- F Feeling:** Does the message trigger an emotional reaction such as curiosity or fear, or does it try to pressurise you?
- A Action:** Does it ask you to click on a link, open an attachment or provide personal information?
- K Know:** Do you know the sender? Hackers sometimes spoof a sender's email address to make the mail look like it comes from someone you know.
- E Expect:** Were you expecting the email? Verify suspicious emails immediately.

Remember - always think before you click!



- 1 Take part in our cyber hero training
- 2 Check your inbox for details
- 3 Watch a short clip and answer 5 easy questions



Popcorn
Training