

# Suspicious Links

**Do not click on suspicious links in messages or emails.**

**Why?** They could be scam Emails – aka Fake Emails – aka Phishing (pronounced fishing)

**What?** People (criminals) pretending to be someone they are not. They will try and replicate genuine emails (with copies of brand logos, style of email etc) of companies who you may use, or your employer may be interested in. They will often include a link to a fake website that tricks you into giving sensitive data such as bank details or passwords. Or the email may have an attachment that when clicked will upload malware on to your computer system.

**Who?** They will target anyone with money or data. These scams work on the basis that if they send thousands of fake emails then a few will work. Even with that success rate they can still make a lot of money or get access to data that can then be sold to other criminals.

**Be suspicious** – look for the common signs:

- Is the email asking for money, often urgently?
- Is the email addressed to 'valued customer', or 'friend' (as opposed to using your name)?
- Does the email have an attachment that you aren't expecting?
- Does the email ask you to change or input login details? If someone asks for your password it is a scam.