Phishing /Spam Email Awareness

There are multiple versions of phishing and spam attacks. Each campaign is designed and deployed differently depending on the audience to get the maximum click / responses. It is a form of "Social Engineering"

Normal phishing campaigns are a "spray and pray" approach, send to lots of emails hoping for some responses. However, there are more intelligent and targeted methods in use now.

Deceptive Phishing

The most common type of phishing scam, deceptive phishing refers to any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials.

Those emails frequently use threats and a sense of urgency to scare users into doing the attackers' bidding

For example, PayPal scammers might send out an attack email that instructs them to click on a link in order to rectify a discrepancy with their account. In actuality, the link leads to a fake PayPal login page that collects a user's login credentials and delivers them to the attackers

Spear Phishing

In Spear phishing scams, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.

This requires lots of research into who the victim is going to be, they draw up a company hierarchy and then email employees as if it is their boss, 3rd party supplier requesting payment etc.

The goal is the same as deceptive phishing: lure the victim into clicking on a malicious URL or email attachment, so that they will hand over their personal data. Spear-phishing uses the likes of social media sites like LinkedIn, where attackers can use multiple sources of information to craft a targeted attack email.

Dear Solomon…. Payback to spammer!
https://www.youtube.com/watch?v=_QdPW8JrYzQ

Don't take the Bait !!... Awareness Video
https://www.youtube.com/watch?v=ygON2B9-xTw

See attached "Social Engineering – Red Flags" for what to look for within the email in more detail.

What to check for …..

- **DO NOT** click on any links within emails that are not expected or from unknown senders
- **DO NOT** forward to others, or reply providing bank details or personal information
- **Look out for** generic salutations, grammar mistakes, and spelling errors scattered throughout.
- **Look at the senders email name and address** and validate its authenticity.

  CORRECT Joe.Bloggs <joe.bloggs@jehall.co.uk>
  WRONG Joe.Bloggs < fle3245@wrong.co.uk> or Joe Bloggs < joe.bloggs@wrong.co.uk>

- **Use common sense** if it seems wrong or out of the norm then it probably is
- **If in doubt escalate** to the IT dept to check the email authenticity
- If an email says invoice attached please pay click on the link, open attachment, DONT. Check the email address, contact the sender, to confirm its authenticity before any further action made.