Dealing with Suspicious Emails

What is Phishing?

“Phishing” is when a scammer attempts to encourage you to disclose personal information, such as financial information or login details. Phishing emails try to get you to reveal sensitive information or infect your machine, by pretending to be from someone else i.e. your bank, utility provider or a colleague/friend etc.

What other types of emails should I be aware of?

A scammer could send an email containing an attachment or link, which you are invited to click on. Clicking on them could install harmful software on your device.

What should I do?

If you receive a suspicious email, such as an unexpected message from a colleague asking for payment, please take a moment to confirm whether it is genuine before proceeding any further. This may include checking with the sender; however, you must not reply to the message directly. If in doubt, ignore the email and report it to the IT Department by emailing ITSupport@joh.cam.ac.uk.

What if I click on a link or open a file?

Tell the IT Help Desk. This is nothing to be embarrassed about. The point is that a seriously malicious piece of software (for example an app that quietly copies all of your passwords and bank details to a scammer) will not give any indication it is present. Inform the IT department, who can do something about it.

Tips

✓

- Check the sender’s email address matches who they say they are
- Treat links with caution, by hovering on the link to reveal if there is a fake link
- Look out for noticeable spelling/grammatical errors as well as unusual formatting. This can be a sign of a phishing email

✗

- Do not open attachments from a suspicious email
- Do not enter any login details or personal information into a site that arouses your suspicions
- Don’t hesitate to contact the IT Department if you are suspicious about an email. It is better to be safe than sorry