Top 5 Phishing Tips

To keep you safe

Look but don't click!

Hover your mouse over any links embedded in the body of the email or the sender's email address. If the link address looks weird or is unknown to you don't click on it. If you want to test the link, open a new browser window and type in website address directly rather than clicking on the link from within the email.

Don't give out personal information. Don't download attachments.

Legitimate banks and organizations will never ask for personal credentials via email or text. Also, attached word or PDF documents coming from suspicious sources are most likely to contain viruses which could compromise your personal data or even the entire network if opened from a corporate computer.

Beware of urgent language in the subject line.

Invoking a sense of fear is a common phishing tactic used by hackers. Beware of subject lines that claim your "bank account has been suspended" or that "your password was reset".

Check for poor spelling and grammar.

Read your emails carefully and check for major spelling mistakes or poor grammar. Lack of details about the signer or how you can contact a company representative strongly suggests a phish. Legitimate businesses always provide contact details.

Use additional security.

Go beyond your installed antivirus and utilize email filtering solutions that will scan your inbox for malicious code and viruses found within attachments. Also, using two-factor authentication can help keep your account secure even at the possibility of a password compromise.

To find out more about Cyber Defence Essentials + contact:

Cameron Strange

+44(0)7535 152 393

020 81446916

cameron.strange@9ine.uk.com

Book a meeting in my Calender

www.9ine.uk.com