5 tips to avoid being hooked in a Phishing attack

1 Please ensure staff **don't browse the web or check emails from an account with Administrator privileges**. This will reduce the impact of successful phishing attacks.

2 Scan your devices for malware and change passwords **as soon as possible** if you suspect a successful attack has occurred.

3 Check for obvious signs of Phishing, like **poor grammar and spelling** or low-quality versions of recognisable logos. Do you know if the sender's email address looks legitimate?

4 **Use multi-factor authentication** on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account.

5 Criminals use publicly available information about you to make their phishing emails appear convincing. Please look over **your privacy** settings, and think about what you post.