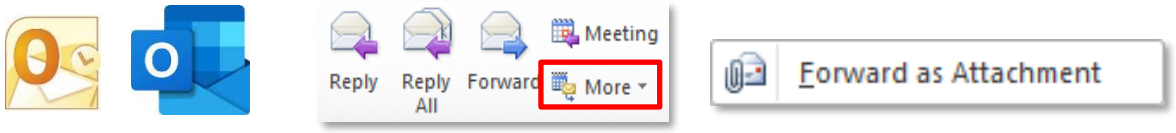
Forwarding emails to spamreports@nhs.net

The NHS Spam Reports team will take action to block malicious email accounts. The team rely on reports from NHS colleagues, which they need to receive in the correct format. They request that you forward the suspect email **as an attachment**.

Forwarding as an attachment on the desktop Outlook app

If you open your emails by clicking on the Outlook icon on your desktop or tool bar, please follow these instructions.

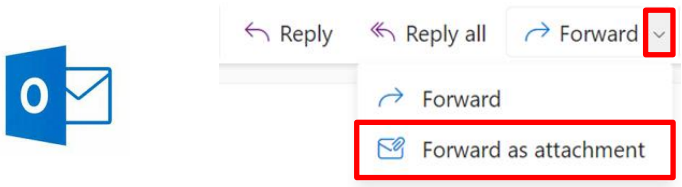
1. Click on the suspicious message within your inbox.
2. At the top of your screen, you should see the various response options – Reply, Reply All, and Forward.
3. Just to the right of the main response options, you should see a small button which says “More”.
4. If you click on “More” you should see a drop down menu, which gives you the option to “Forward as Attachment”. Choose this option.
5. Forward the suspect message as an attachment to spamreports@nhs.net



Forwarding as an attachment from Outlook Webmail

If you open your emails by opening a web browser and going to the NHS Portal, please follow these instructions.

1. Click on the suspicious message in your inbox.
2. At the top of your screen you should see the various response options, Reply, Reply All and Forward which are represented by arrows.
3. Just to the right of these options you should see a little drop down arrow.
4. If you click on the drop down arrow you should see the option to “Forward as attachment”.
5. Forward the suspect message as an attachment to spamreports@nhs.net



Did you know?

The Local Counter Fraud Specialists run a rolling programme of Fraud Prevention Masterclasses. This includes Cyber Enabled Fraud, where we look at the different phishing tactics which are used to target the NHS and the serious damage cyber-fraudsters can cause. The session covers signs of phishing that you can look out for, how to safely check a suspicious email, and practical advice on keeping your account safe.

For details of the next Cyber Enabled Fraud Masterclass, please check the Counter Fraud Newsletter or contact your Local Counter Fraud Specialist.