NHS
North East London

Dear Colleague,

You may have heard news about the number of cyber-attacks taking place across small and large organisations. The NHS is sadly not immune, and faces a myriad of attacks daily, as these devious criminals seek to undermine the integrity of the NHS IT systems and remain unconcerned by the damage inflicted by these attacks. As reported in the news (04/06/2024) the latest cyber-attack effecting several South London Hospitals and partners.

NEL ICB are committed to blocking these types of intrusions which impact on everyone who use NHS (staff and public) services, disrupting the provision of, and endangering the life of service users who are unable to receive care in a timely way because the effect these cyber-attacks have on NHS digital services.

NEL and EMIS have been undertaking a specific piece of work across NEL practices with auditing your server and updating active directory users, to remove both **generic and individual Microsoft Windows user accounts** of staff who no longer work at your site.

It is imperative that this work is completed to ensure unscrupulous persons with unauthorised access and nefarious intentions are stopped. Removing potential exploits such as dormant accounts, takes away a means of gaining access to your practice network.

Please can you work with NEL and EMIS IT staff if approached during this time.

This message also aims to serve as a reminder of the need for practices to inform their local IT service desk (NEL or EMIS) of any leavers, so that their accounts can be disabled and or removed.

Local IT support contact details in table below:

NEL ICB IT Service desk	itservicedesk.nelicb@nhs.net
NEL ICB IT GP service desk Telephone:	0330 303 6780
EMIS self-service portal	https://www.emisnow.com/csm
Email – EMIS/Egton:	mysupport@emishealth.com / support@egton.net
Telephone Number: City & Hackney	0330 053 1721
Telephone Number: Newham	0330 053 1722
Telephone Number: Tower Hamlets	0330 053 1723

We also ask that staff remain vigilant when accessing emails particularly from unknown sources, to refrain from clicking on embedded links and URLs in emails that you are unsure of their origin. If in doubt think about sending a separate email or calling the individual and asking if they sent you the email before opening.

If you have any questions or concerns regarding cyber security, please contact your local IT service desk who will be able to provide answers or direct you to an appropriate person who can.

How can you spot malicious emails?

These emails can vary in sophistication - some are obvious, and easy to spot, whereas others may be more difficult. As a rule, if you receive a suspicious email, you will be able to ascertain whether it is genuine by following these steps:

- Hover over the sender's name and take careful note of the email address. Check that the domain name is correct, and there aren't any misspellings
- Be wary of attached files. If the message has a ".exe", ".scr", ".zip", ".reg" or ".bat" file attached, consider this a red flag
- If you receive an email from an organisation requesting urgent payment of an invoice, consider first whether this is something you expect
- If in doubt, contact the sender by phone or email (ensuring the email you're replying to is correct) to confirm whether the email is genuine

What action is required when you receive malicious emails?

If you believe you have received a malicious email, please follow the guidance below to assist NHS Mail in improving it's filtering processes:

Using the NHSmail Portal (Outlook Web App):

Step 1 – Forward the email to spamreports@nhs.net as an attachment for virus analysis and central trend monitoring:

1. Click on the Spam Email in the reading pane to select it
2. Click on the New mail icon in the top left of the screen
3. Drag and drop the spam email from the email list into the body of the new blank email
4. Type **spamreports@nhs.net** in the To: field
5. Enter the appropriate subject text
6. Note: It is recommended that you use spam, phishing or malicious depending on the type of email you are reporting
7. Click send

Step 2 – Permanently delete the suspicious email (bypassing the deleted items folder)

1. Select the suspect email from your email list.
2. Hold down the ‘Shift’ key and press the ‘Delete’ key.
3. Click ‘Yes’ to confirm if a warning dialogue appears.

Using Microsoft Outlook:

Step 1 – Forward the email to spamreports@nhs.net as an attachment for virus analysis and central trend monitoring:

1. Select the suspect email from your email list.
2. In the Outlook ribbon in the respond area, select ‘More’ and then select ‘Forward as Attachment’.
3. In the email window that opens add **spamreports@nhs.net** as the recipient in the ‘To field’.
4. Click the ‘Send’ button.

Step 2 – Permanently delete the suspicious email (bypassing the deleted items folder)

1. Select the suspect email from your email list.
2. Hold down the ‘Shift’ key and press the ‘Delete’ key.

Click ‘Yes’ to confirm if a warning dialogue appears.