NHS
North West London

RE: Warning: Phishing and Mobile Phone Message Scams

Dear Colleagues,

We want to alert you about the increasing number of phishing and mobile phone message scams, including those on WhatsApp. These scams can trick you into giving away personal information or money. Here’s what you need to know to stay safe.

What is Phishing?

Phishing is when scammers send fake emails, messages, or websites to steal your personal information, like passwords or credit card numbers. Phishing attempts can occur via:

- Email
- Text message
- Through other messaging apps
- Phone calls

What is a Mobile Phone Message Scam?

These scams involve receiving fake messages on your phone, including SMS and WhatsApp, that try to trick you into clicking on malicious links or sharing personal information. There is an increasing number of WhatsApp phishing scam targeting NHS in addition to emails.

Common Signs of Scams:

1. **Unexpected Messages**: Be cautious of messages from unknown numbers or unexpected messages from known contacts.
2. **Urgent Language**: Scammers often use urgent language to make you act quickly, like "Your account will be locked!" or "You’ve won a prize!" or “Need Urgent Action”
3. **Suspicious Links**: Avoid clicking on links that look suspicious or are shortened URLs.
4. **Requests for Personal Information**: Legitimate companies will never ask for sensitive information like passwords, credit card details or money via message.

How to Avoid Scams:

1. **Verify the Sender**: Always check the sender’s information. If it seems suspicious, do not respond.
2. **Do Not Click on Links**: Avoid clicking on links in messages from unknown sources. Instead, go directly to the official website.
3. **Report Suspicious Messages**: Report any suspicious messages to your mobile carrier or the platform (e.g., WhatsApp).

4. **WhatsApp - Enable Two Factor Authentication**: Add an extra layer of security to your account by requiring a PIN. Refer to WhatsApp guidance but the setting is commonly found in WhatsApp, settings, account, Two-step verification, turn on and set a pin.

What to Do if You Suspect a Scam:

1. **Do Not Respond**: Do not reply to the message or provide any personal information.
2. **Block the Sender**: Block the number or contact that sent the message.
3. **Report the Scam**: Report the scam to your mobile carrier, WhatsApp, or the relevant authorities.
4. **For NHSMail**: Report all suspected spam, fraudulent or malicious emails to NHSmail for analysis and blocking. See the NHSMail reporting cyber threats.

If you have any concerns, please contact the service desk on 020 3350 4050 or email nhsnwl.servicedesk@nhs.net@nhs.net

NWL ICT and Cyber Security Team
NHS NWL ICB