NHS
North West London

RE: Heightened Cyber Threat – Stay Vigilant Following Recent Retail Sector Attacks

In light of recent high-profile cyber-attacks on major UK retailers including Marks & Spencer, Co-op, and a national supermarket supplier, we're issuing this advisory to reinforce key cyber security practices and raise awareness across the organisation.

Summary of Recent Events

- Marks & Spencer: Customer data was compromised in a ransomware attack involving malware, SIM-swapping, and exploitation of known vulnerabilities.
- Co-op: Suffered a similar breach, likely linked to the same threat group.
- Third-party supermarket supplier: Targeted in a ransomware attack, highlighting broader supply chain vulnerabilities.

Why This Matters

These attacks reflect a growing trend of cyber threats targeting organisations with access to sensitive data—including NHS partners and suppliers.

What do I need to do?

1. Be Alert to Phishing and Social Engineering

- Do not click on links or open attachments in unexpected emails—even if they appear to come from known contacts.
- Validate requests for sensitive information or payments through established channels (e.g., phone call or direct website access).
- Be cautious of messages via SMS, WhatsApp, or social media that prompt urgent action.

2. **Protect Your Credentials**

- Never enter your NHS credentials into unfamiliar login pages.
- Use strong, unique passwords and enable multi-factor authentication (MFA) wherever possible.

3. Secure Your Devices

- Lock your screen when away from your desk.
- Avoid discussing sensitive information in public spaces.
- Keep mobile devices physically secure and updated.

4. Report Suspicious Activity

- Report all suspected spam, fraudulent or malicious emails to NHSmail for analysis and blocking. See the NHSMail reporting cyber threats or Cyber Security Guide for NHSmail on Collabor8 for more information and how to report these emails.

- Forward suspicious emails as attachments to spamreports@nhs.net for NHS and for non NHS to report@phishing.gov.uk.
- Permanently delete suspicious emails using Shift + Delete.

The most common form of attack is through phishing emails designed to steal credentials or deliver malware.

Thank you for remaining vigilant and doing your part to protect our systems and data.

NWL ICT & Cyber Security Team
NHS North West London