Fraud Information Alert 5

MIAA Anti-Fraud Service

March 2026

Business Email Compromise

The NHS Counter Fraud Authority (NHSCFA) has been alerted by the NHS Cyber Security Operations Centre (CSOC) to identified incidents involving the compromised and fraudulent use of nhs.net email addresses.

How the fraud operates

The modus operandi involves a malicious email being sent to nhs.net users with a hyperlink attached requesting a log in. Examples of this threat involve staff being requested to log into their shared drive (used commonly for online working). Once complied with, staff credentials are harvested and access is then gained via the Cloud. (Obviously this scam can be perpetrated against any email domain.)

Reports indicate that these compromised accounts have then been used to open online shopping business accounts, in some cases being granted invoice-based credit lines (in one case £12,000). When items are ordered, the cost of these items has been subsequently invoiced to the NHS organisation and paid resulting in a loss to the NHS. We understand that many NHS departments use online shopping platforms, and we ask that this risk is highlighted to ensure that invoices are thoroughly and frequently checked.

In addition to the cyber security prevention advice contained here, NHS organisations should ensure they have appropriate controls in place to prevent invoice fraud.

Prevention advice and action

- This guidance outlines key prevention measures to help staff identify and prevent these types of cyber enabled frauds. However, other controls may also be appropriate depending on local risk assessments. By staying vigilant and following recommended steps, organisations can reduce the risk of financial loss. To protect against this type of fraud, please consider the following:

Organisational cyber security controls

- Staff should be alert to unusual emails sent to their nhs.net accounts (as well as other domains) welcoming them to an online shopping business account or confirming that a credit line or invoice-based purchasing facility has been opened in their name. Any staff receiving such an email must report it immediately to their IT security team and Local Counter Fraud Specialist (LCFS).

Continued on page 2

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to: NHS STAFF for ACTION & AWARENESS

MIAA IA 25/26 5

For further information on MIAA's Anti-Fraud Service visit miaa.nhs.uk

- The National Cyber Security Centre (NCSC) publishes a broad range of advice and guidance, particularly for large organisations.

- NHS organisations should follow NCSC's '10 steps to Cyber Security', and in particular:

  o Take a risk-based approach to this identified fraud risk to secure data and systems.

  o Ensure cyber security policies are fit for purpose, endorsed by senior leaders, and are communicated effectively across the organisation.

  o Ensure employees are equipped to manage cyber security within their own environment by raising awareness of this fraud risk and providing training as necessary to employees in identifying and managing incidents.

  o Provide clear reporting lines for suspicious emails to their IT and/or fraud teams.

Recommendations for employees

- Creating a strong individual password for different systems by using three random words, including a combination of upper and lower-case letters, symbols and numbers, is a good way to protect yourself online. Further guidance on strong passwords and how to stay secure online is available via the National Cyber Security Centre website.

- Clicking links or replying to suspicious emails, as even 'unsubscribe' links can be traps.

- Be alert to emails demanding immediate action, threatening account closure, asking for financial information, or indicating a business account has been opened.

- Be mindful of junk email inboxes, ensure they are checked regularly, and emails are deleted if not of use.

- If fraud is suspected, follow the organisation's escalation process immediately and contact the IT team and/or LCFS for advice.