Fraud Information Alert 4

MIAA Anti-Fraud Service February 2022

Salary Diversion Fraud – ACTIVE THREAT

We have recently received reports again from a of number clients about fraudulent attempts targeting payroll staff in an attempt to divert NHS staff salaries into fraudsters' bank accounts. This type of salary diversion fraud was previously reported in 2019 and appears to have resurfaced.

In a recent instance, payroll staff received an email from a fraudster impersonating a member of staff at a Trust, advising that their bank account details for salary payment had changed.

This was not a sophisticated fraud attempt. The original fraudulent email came from an unusual gmail.com email address and contained a spelling error. Payroll staff initially responded to the email informing that they couldn't change the details on the individual's behalf and querying if they had access to ESR.

The fraudster responded to this email stating that they did not have access to ESR and requesting *'how can you help me out?'* This second email was received from an obviously fraudulent email address. The payroll team verified the request with the genuine staff member through their official NHS contact details and they confirmed that they had not made the request and that it was bogus.

The NHS has a number of control measures in place to prevent and mitigate against this type of fraud and verification via existing contact details is just one component. These control measures are not publicised in order to ensure they don't assist fraudsters.

Tips to prevent salary diversion fraud:

- Be alert to any requests (emails, voice calls etc) for your ESR log-in details or requests for any personally identifiable information.
- Be alert to any emails which supposedly redirect you to an ESR login page, or similar, which asks you to update or confirm your details, including your account details.
- Be alert to any emails received from unexpected sources inviting you to click on hyperlinks and/or attachments and look out for emails containing spelling and/or grammatical errors.
- Only use existing ESR login arrangements via secure NHS networks to update your personal details, if needed.
- Fraudsters will try and put you under time pressure, by saying you have to do something immediately or by a deadline. Be aware of this tactic.
- If in doubt, phone your payroll provider if you have any concerns or if you think your personal account details have been compromised.

Report Fraud

If you are suspicious about an email you have received, forward it to: report@phishing.gov.uk.
If you believe you are or have been the victim of a salary diversion fraud, contact your Anti-Fraud Specialist via the details on your organisation's anti-fraud policy or intranet.
Report fraud to Action Fraud by calling 0300 123 2040 or visiting: www.actionfraud.police.uk.

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

MIAA IA 21/22 4
For further information on MIAA's Anti-Fraud Service visit
miaa.nhs.uk

CONTACT: Action Fraud to report any suspicious calls or emails.
For further information or to report NHS Fraud contact:
Virginia Martin
Anti-Fraud Specialist
07551 131109
Virginia.Martin@miaa.nhs.uk