Fraud Information Alert 3

MIAA Anti-Fraud Service AUGUST 2019

NHS ESR Spear Phishing Attack – Active Threat

Suspicious Emails & Clickable Links

ESR Users have been receiving emails that claim to be from their Human Resources (HR) or ESR service, but are sent from accounts outside the NHS. These emails typically say that the user's salary has been increased and invite them to click a link to access related documents. Links direct them to a fake NHS ESR login page, which appears exactly the same as the actual login page. The malicious emails are customised for each organisation they are sent to.They typically contain the organisation's logo and the phishing links include their website domain within the URL. Example email subject lines: August Salary Details; Salary Raise Confirmation; Salary Review Letter; Update Bank Details.

Most cyber frauds against the NHS are aimed at defrauding the health body; these latest attacks are directed against NHS staff themselves. **Would you click on this link in an email?**

You have been awarded a pay rise.
Click https://my.esr.nhs.co.uk to see what it is.

The real ESR website is actually my.esr. nhs.uk What the fraudster wants you to do is enter your Username and Password details to login to their fake website so they can record your key strokes and capture your information. They will then use those details to login to the real website and change your bank account details to one they control.

Personal pay rises and significant changes to pay will never be communicated to any NHS employee via an email.

Some other things to think about:

- **Do you recognise who the email is from?** Is it the genuine email address you're familiar with?
- **If an email starts impersonally,** with just "Hi" or "Hi + your email address or full name", be wary of the email's provenance.
- **Are the contact details at the foot of the email genuine?** Is there a real link to a website? Type the website address into a search engine to see if it is real – don't click the link offered.
- **Does any branding contained in the email look professional and clear?** Is it up to date branding?
- If you are being asked to **update or re-enter personal information over email,** it is likely to be a scam.
- If there is an **error in the email,** like a misspelled word or poor grammar, beware.
- 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 the genuine company or the genuine person via an established/known number to verify. Take your time and have a think about what links you are clicking on. It may affect you personally as well as the wider NHS.

ESR Users are advised to forward suspicious or spam emails as an attachment to spamreports@nhs.net - step-by-step instructions can be found here. All successful phishing attempts should be reported to the National Fraud & Cyber Crime Reporting Centre (better known as Action Fraud).

ACTION REQUIRED

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

NHS STAFF for ACTION & AWARENESS

MIAA IA 19/20 3

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:
Kevin Howells
Anti-Fraud Specialist
0161 743 2008
07825 732629
kevin.howells@miaa.nhs.uk
kevin.howells1@nhs.net

MIAA ASSURANCE