



Fraud Information Alert 2

MIAA Anti-Fraud Service

JULY 2019

Phishing attack aimed at ESR credentials

NHS Digital's Cyber Security Operations Centre has been closely monitoring a spear phishing campaign targeting NHS organisations in order to steal Electronic Staff Record (ESR) credentials.

Spear phishing is a type of fraud where a phishing attempt is targeted against specific individuals or organisations. Attackers attempt to steal sensitive data such as passwords or credit card numbers. Attackers may gather personal information about their target to increase their probability of success. Spear phishing can be performed via e-mail, phone calls or other communication channels.

It has been reported that staff in some NHS organisations have received emails that claim to be from their Human Resources (HR) 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. When the user clicks on the link, they are directed to a fake NHS ESR login page, which appears exactly the same as the genuine ESR front page except that it does not offer smartcard login.

These 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. **Please be vigilant and report any such emails or activity to your organisation's IM&T helpdesk.**

NHS retirement fund scams

Scammers are known to be currently targeting pension pots of all sizes, including those of NHS employees and retirees. They can be articulate and financially knowledgeable, with credible websites, testimonials and materials that are hard to distinguish from the real thing. Scammers design attractive offers to persuade you to transfer your pension (or to release funds from it).

The warning signs

Scam offers often include: Free pension reviews; higher returns than normal; help to release cash from your pension; high pressure sales tactics; unusual investments; complicated structures where it isn't clear where your money will end up; long-term pension investments.

Four simple steps to protect yourself from pension scams

Step 1 - Reject any unexpected offers 'out of the blue'

Step 2 - Check who you're dealing with (Check the [FCA's Financial Services Register](#))

Step 3 - Don't be rushed or pressured Step 4 - Get impartial information or advice – from [The Pensions Advisory Service](#), [Pension Wise](#) and Independent Financial Advisers

More information can be found at: www.fca.org.uk/scamsmart & www.fca.org.uk/scamsmart/how-avoid-pension-scams Report to Action Fraud - If you suspect a scam you should report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

ACTION REQUIRED

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

**NHS STAFF
for
ACTION &
AWARENESS**

MIAA IA 19/20 2

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



Counter Fraud Authority

