Fraud Information Alert 4

MIAA Anti-Fraud Service

December 2019

Ongoing Active Threats

Vigilance Reminder!

Four recent fraud attempts aimed at North West health bodies have been thwarted by vigilant staff. This is a reminder of active fraud threats and how spot and report them.

Email Spear Phishing Attempt
A senior member of staff was targeted by criminals. HR received the following fraudulent email message -
"I have recently changed banks and would like to have my direct deposit changed to my new account, I need your prompt assistance on this matter."
The email address that this message originated from caused concern, verification with the member of staff involved via existing contact details revealed this to be an attempted fraud.

Attempted Invoice Fraud
A Trust recently ran a tender exercise. Following the tender award they published the award notice on Contracts Finder Database. A fraudster obtained the supplier name and contract details from the Contract Finder website and sent a fake invoice in an attempt to receive payment for the work. Again the email address used be the fraudster caused concern. A verification call to the supplier via existing contact details confirmed that the invoice had not been sent by them and the fraud was prevented.

IT Phishing Attack
The following email including a clickable link was sent to NHS.net account holders -
"Our ongoing effort to update our databases and electronic mail systems requires the removal of all unused accounts. If you still use the address that received this warning, please immediately verify identity and confirm that this email address remains active by clicking here. Anyone using an NHS email account who doesn't verify an active email address within seven days after receiving this warning will lose all messages currently saved in that account upon its deletion."
NHS Net administrators will never send you this type of message. If you have any concerns about emails that you receive report them to your local IT Team or Anti-Fraud Specalist. (AFS details on this alert.)

Attempted Banking Scam Call
We also aware that a health body has recently been contacted by an individual claiming to be from their bank and advising them that he wanted to send them an email link to download a banking software update. Finance staff suspicions and vigilance resulted in checks via their existing banking contact who confirmed this wasn't genuine and was an attempted scam. The phone call element of this attempt would seem to be a step up from just issuing unsolicited scam emails containing dubious links.

If you have any doubts about an email or phone call, 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. Examine the originating email address closely to see if it's genuine.
For more tips see **MIAA Fraud Information Alert 3.**

ACTION REQUIRED

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

NHS STAFF for ACTION & AWARENESS

MIAA IA 19/20 4

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

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