COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence

July 2021

Welcome to the July 2021 edition of our newsletter. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, you will find our details on the last page.

Current Scam Trends

Nursing and Midwifery Council (NMC) Impersonated by Fraudsters

The Nursing and Midwifery Council (NMC) has been made aware of a fraudulent call which is being made by someone who is claiming to work for them. The caller asks a payment to be made and for confirmation of personal details in order to "progress a registration application". The NMC are reminding everyone that they will never contact you to ask for payment over the phone. If you do receive a call and you're unsure if it is genuine, please hang up without sharing your personal or financial details. The NMC advise that if you want to check a call claiming to be from them is legitimate, you should call their contact centre on 020 7637 7181. Further information can be found on the NMC website here: Beware fraudulent registration calls - The Nursing and Midwifery Council (nmc.org.uk)

Scam Call: BT regarding a problem with broadband

In June 2021 Counter Fraud were approached by a Trust department regarding the receipt of phone calls from a caller claiming to be from "BT." The mobile number used was noted: 07442429024. The caller stated that there was a serious problem with broadband and asked that the call taker opened up certain windows/sites on the internet so the issue could be fixed. The call taker did not engage further with the caller and ended the call- a wise course of action.

The incident was reported to Action Fraud/City of London Police (national lead force for fraud) and full details given. Please be vigilant if a caller purports to be from a service provider, financial institution or government department .

Attempted Mandate Fraud Impersonating an NHS Employee

Staff at an NHS Trust received an email this month which requested a foreign payment to be made. The email looked at first glance as though it had come from a Trust employee. However, when the full details were checked, the email had been sent from a German email account. The email also contained some grammatical errors. Please be vigilant if you process requests for payment. If you receive any requests which appear to be unusual, please contact your Local Counter Fraud Specialist.

Cyber Security Tips - Multi Factor Authentication

Any site, device or application which is accessed purely via a password can be vulnerable. Adding another layer of protection, such as entering a code or scanning a fingerprint is known as Multifactor Authentication (MFA). By entering more than one factor (evidence of your credentials), the risk of somebody unauthorised accessing systems is greatly reduced.

Using MFA requires you to prove your identity using two of the following categories:

Something you know: such as a pin code or password
Something you have: like a mobile phone, QR code or smart card
Biometric authentication: such a fingerprint scan or use of a voice or facial recognition feature.
Location: a specific computing network or GPS location

It is recommended that MFA is used wherever it is available. Passwords can be stolen, guessed and leaked. If your password is compromised, computers cannot differentiate between a legitimate user and an imposter.

Remember to create a strong password (or passphrase), and change it often. You should also make sure that you do not use the same password for multiple accounts and never share your password with anyone. For further advice and information, please contact your Local Counter Fraud Specialist.

NHS Procurement Fraudster Who Stole £800k Jailed

Barry Stannard, a former IT manager at Mid Essex Hospital Trust, has been sentenced to five years and two months in prison for fraud offences against the NHS.

Stannard had siphoned off over £800,000 from the Trust by setting up fake companies which he used to submit phony invoices. As a senior manager, Stannard had authority to sign off invoices as long as they were for less than £7,500.

Stannard ensured that each of the hundreds of fake invoices he submitted was for less than that amount. He was the managing director of each of the fake companies and was therefore able to pocket the money for his own use. He carried out this ruse for at least 7 years.

Stannard had not declared any Conflict of Interest to the Trust regarding his role as director of the two companies. Stannard is also believed to have created false identities, which he used to contact his colleagues at the Trust to make his fake companies appear to be legitimate and the invoices genuine.

The courts are now considering a confiscation order which would allow the NHS to recover some of the proceeds of Stannard's crimes.

GP Practice Manager Sentenced for £184,000 Fraud

Kirsty Whawell admitted carrying out a series of fraud offences against her employer, a GP practice in Leicestershire. Whawell was employed as Practice Manager, a role which gave her access to practice finances. Whilst employed there, she awarded herself several unauthorised pay increases and pushed through overtime payments despite claiming to her colleagues that she never claimed for extra hours.

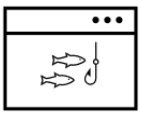
In addition, she tricked partners into signing off invoices and cheques to suppliers and locum doctors. Once the documents were signed, Whawell would alter them by erasing the payee details and diverting the money into her own bank account. The cheques and invoices added up to over £126k. When added together with the pay rises and overtime claims, Whawell managed to fraudulently take £183,391, as well as stealing £687 from another practice during the process of a merger.

Whawell was also found to have presented a forged DBS certificate to hide a previous conviction for stealing from an employer. This information should have been disclosed during her application to work at the practice but Whawell deliberately concealed her past.

In court, Whawell pleaded guilty to six counts of fraud by abuse of position and one count of fraud by false representation. She was sentenced to one year in prison and a confiscation order is being considered.

If you want to learn more about Recruitment Fraud, including how to spot forged documents, you'll find details of our Recruitment Fraud Prevention Masterclass on the next page.

Audit Yorkshire Cyber Security Checks



As you will no doubt have noticed from the newsletters we have shared over the previous year, the NHS continues to be targeted electronically by criminals.

Cyber criminals target the NHS for several different purposes - to divert payments (whether these are invoice payments to suppliers, or payroll payments to individual members of staff), to spread malicious software (such as ransomware which encrypts your files and charges a fee to unlock them) or to harvest sensitive data (such as information about employees or patients, or credentials that are needed to gain access to finance systems and email accounts).

Audit Yorkshire are able to arrange for cyber security exercises to be run at your organisation to help look for any potential weak spots. There are currently two different exercises we can arrange:

Mock Phishing Exercise – to detect any cybersecurity weakness in your organisation. Our targeted campaigns help organisations understand the level of vulnerability across its workforce. The results can be used to tailor training and awareness effort to improve workforce susceptibility.

Penetration Testing – to test the security of your networks, systems, websites and web apps. For this exercise, accredited NHS employed experts will perform tests to safely identify any security weaknesses and make practical recommendations to address these issues.

If you would like to discuss arranging either of these exercises, please contact tom.watson6@nhs.net

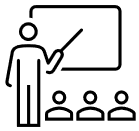
Counter Fraud Training

NEW - Fraud Prevention Masterclasses

The LCFS team are currently scheduling a series of Fraud Prevention Masterclasses, covering key fraud risks within different areas. The masterclasses are delivered via Microsoft Teams and will last around 45 minutes to 1 hour.

The sessions are being delivered on a monthly basis, and cover some key areas that have very specific fraud risks. They include an overview of the various risks which may be encountered, real life case studies and practical advice on the prevention of fraud risks.

If you have an interest in any of the topics below and would like to sign up for a session, please get in touch with Rosie Dickinson (rosie.dickinson1@nhs.net)



Recruitment Fraud

Ideal for staff with responsibility for pre-employment checks.

5th August 11-12
3rd September 10-11
11th October 10-11
5th November 10-11
4th February 10-11

Payroll Fraud

Ideal for payroll staff who are new or would like a refresher.

10th August 2-3
9th September 10-11
15th October 11-12
10th November 11-12
12th January 2-3
11th February 10-11

Creditor Payments

Ideal for staff in accounts payable or who deal with invoices/suppliers.

20th August 2-3
10th September 10-11
15th November 10-11
10th December 11-12
14th January 11-12
18th February 10-11

How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:

Steve Moss, Head of Anti-Crime Services	Steven.moss@nhs.net 07717 356 707
Marie Hall, Assistant Anti-Crime Manager	Marie.Hall15@nhs.net 07970 265 017
Rosie Dickinson, Local Counter Fraud Specialist	Rosie.dickinson1@nhs.net 07825 228 175
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Local Counter Fraud Specialist	R.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060 https://cfa.nhs.uk/reportfraud