COUNTER FRAUD NEWSLETTER

April 2021

Welcome to the April 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

The following scams have come to the attention of the LCFS team during the last month. Please remember that fraudsters rarely stay still, and they will use variations of these tactics to try and avoid detection.

HMRC Investigation Calls

The HMRC Fraud Investigation Scam Call is not new but certainly continues to be popular. In the last month, several colleagues have reported receiving these calls (including a member of the Local Counter Fraud Team).

When picked up, an automated message plays stating that the recipient is under investigation by HMRC for fraud offences, and that a warrant has been issued for their arrest. The victim is advised to press 1 or face imminent arrest. If they do press 1, they will be transferred to a fraudster who will seek personal and financial details.

These calls can be reported directly to Action Fraud. You should make a note of the phone number which was used and roughly what was said in the automated message, so that Action Fraud can add this to their intelligence. Please do not press 1 as there is a risk that doing so could connect you to a premium rate number or flag your mobile number as a potentially viable target for fraudsters.

NHS and National Insurance Number Fraud Calls

In a similar scam, there have been recent reports of colleagues and members of the public receiving calls which state their NHS Number or National Insurance Number has been used in a fraud.

The automated message encourages the call recipient to press 1 in order to speak to “an officer”.

As there are still a lot of people are waiting to access their Covid-19 vaccination, there is a risk that people may panic that this call is genuine and that it will impact their ability to get an appointment.

Action Fraud have published an article about the National Insurance Number scam after receiving a flood of reports about calls which had been received. You can read their article here.

These calls are very similar to the HMRC scam but instead of threatening to have the victim arrested, they are designed to sound helpful. In reality, they are computer generated and will be the first step in trying to trick information out of the victim. These calls should also be reported to Action Fraud.

Ticket Fraud

As lockdown restrictions begin to ease, people have begun looking ahead to summer events such as festivals and concerts. Unfortunately, fraudsters are making the most of this by trying to trick customers into using phishing websites or buying fake tickets. In February, Action Fraud received 216 reports about this type of fraud.

Action Fraud have released an article explaining how you can protect yourself from this type of scam.

A Focus on Cyber Scam Techniques - Fleeceware

Fleeceware Apps

Avast (a Cyber Security organisation) have identified a number of Fleeceware Apps which are being downloaded by mobile phone users. The apps are often serve a genuine purpose (e.g. a QR code reader or a fun camera filter) and attract users by offering a short “free trial” period.

However, once the free trial ends, the user is stung with repeated subscription fees, even if they have already deleted the app. The only way to cancel the subscription is to go into the app settings and cancel it from inside the app. These apps appear to be targeting younger mobile phone users who may be unaware of the hidden costs. Parents tend to discover the charges later after numerous fees have already been paid.

To avoid fleeceware, Avast highlight that you should be very wary of apps that feature short free trial periods. You should also be sceptical of viral adverts for apps and look closely at the small print to make sure you know if automatic charges will apply and how to cancel any subscription.

It is also good practice to secure the ability to make payments behind a biometric lock (e.g. fingerprint) or password.

11 Year Prison Sentence for NHS Fraudster

Stephen Day has been sentenced to 11 years and 5 months imprisonment after being found guilty of a string of fraud offences, including defrauding the NHS by over £80,000.

Day provided false information to two employment agencies in order to be appointed full time Director of Finance for three different NHS organisations at the same time. This resulted in Day receiving three separate full time salaries - one from a Commissioning Support Unit, one from a CCG and one from a Trust, despite being physically incapable of properly fulfilling his responsibilities.

He deliberately failed to declare his multiple job roles, and used a web of lies and careful tactics to try and cover his tracks. He refused to use NHS devices and lied about requiring time off for a family bereavement which had occurred 9 years earlier. He also claimed he needed time off in order to access cancer treatment.

Day's offences weren't exclusively against the NHS. He also managed to gain high level employment at several companies where he then proceeded to empty their bank accounts. He made £1.4 million through this activity. In addition, he persuaded a friend to transfer £4,500 to him using a romance scam.

Day spent his money on luxury holidays, expensive furniture and car accessories.

Day was sentenced to 11 years and 5 months in prison, and has been banned from acting as a director for 9 years. A Proceeds of Crime Act application is now being explored to try and recover money for the victims. You can read the BBC article here.

NHS Sick Leave Fraudster Sentenced

In February, a member of staff at Mersey Care NHS Foundation Trust was found guilty of lying about her sick leave from the NHS. The member of staff had gone onto sick leave after an alleged assault at work.

Shortly after beginning her 2 year sickness absence, she began studying for a BNURS Mental Health Nursing Degree. Evidence which was gathered indicated that she was telling the Trust HR team that she was unable to complete her substantive post, but was actually completing the same duties as part of the practical element of her course.

It was calculated that the Trust had overpaid her by over £40,000 as a result of her dishonesty. The nurse admitted the offences in interview and was convicted at court.

She has been sentenced to 16 months imprisonment, suspended by 2 years, and ordered to complete 200 hours of unpaid work. A compensation order has been requested, seeking repayment of the £40,000 and the case has been referred to the NMC for their investigation.

Did You Know? Conflicts of Interest

All NHS staff need to be aware of their organisations policy on gifts, hospitality and conflicts of interest. These topics are covered within your organisation's Conflicts of Interest and/or Standards of Business Conduct Policies.

These policies form part of your organisation's commitment to transparency and integrity. Under the Bribery Act 2010, organisations can be prosecuted if they fail to put sufficient measures in place to prevent bribery from happening.

Understandably, patients and their families may wish to thank staff for the services and care that have been provided. The Conflicts of Interest and/or Standards of Business Conduct Policy explain the steps you should take if you are offered gifts or other forms of hospitality.

Conflicts of interest may arise in many different circumstances. Some basic examples of potential conflicts of interest include:

- Having a family, personal or financial connection to a supplier,
- Potential involvement in the recruitment process where a friend or family member applies for a role
- Offers of gifts, hospitality or donations

You must also make a declaration if you already work elsewhere or if you are planning to seek a second role outside your current post. If you do hold a secondary role, you must ensure that you do not carry out work for your other employer during NHS work time.

It's vital that you make yourself aware of what is expected. There is the potential that the fraud team will be asked to investigate if these policies are not followed. If you're ever in doubt, please seek advice from your line manager or HR representative.

Counter Fraud Training

Training Sessions

A central part of your Local Counter Fraud Specialist's role is to raise awareness of fraud within the NHS. This can take many forms but the most successful and popular method for us to do this is via face-to-face training with staff. Thanks to the range of conference calling software now at most people's fingertips, we're able to offer online fraud training.

Our Fraud Awareness training focuses on:

- How different types of fraud affect the NHS
- Practical advice on what to look out for and methods to protect yourself and your organisation from fraud
- Real life case studies showing how the NHS is targeted
- Information on how to report concerns about fraud

This training can be arranged to suit you and will be delivered via Microsoft Teams. It is part of our normal service and can be delivered to groups of any size. We are also able to design and deliver bespoke training packages based on any fraud related areas of concern that you feel are most relevant for your team.

We are currently running masterclasses on several different topics. These are being delivered remotely on Microsoft Teams and WebEx. The current set of masterclasses cover how to identify and prevent:

- Cyber enabled fraud - phishing and mandate fraud
- Recruitment fraud
- Payroll fraud (designed for new starters in Payroll teams or as a refresher for Payroll staff)

To register your interest in a session, contact one of the LCFS team using the details below.

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 07970 264 857 / 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