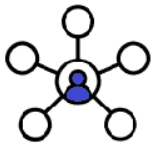
COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence

December 2021

Welcome to the December 2021 edition of our Counter Fraud Newsletter for NHS staff. 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



Omicron Fraud Messages

Throughout the pandemic we've seen that fraudsters are quick to respond to changes in the Covid-19 landscape. This continues to be the case. Warnings have begun circulating about fraudsters sending out emails and text messages claiming that you need to order a free PCR "Omicron" test. If you follow the links and information provided, you will be asked to provide your personal details and/or to make a payment to secure a test.

As in previous versions of Covid-19 scams, the fraudsters are trying to exploit uncertainty and anxiety around the new variant. The Department for Education are concerned that schools and parents may be targeted more heavily due to pupils engaging with testing prior to returning to school in January.

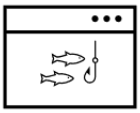
Please remember that the NHS never ask for your financial details. You can find advice about how to access PCR tests on the official NHS website.

Covid Pass Scams

Criminals are using the NHS COVID Pass as a way to target the public by convincing them to hand over money, financial details and personal information.

They are sending imitation text messages, emails and making phone calls pretending to be from the NHS, and offering fake vaccine certificates for sale online and through social media.

If you are contacted about your NHS COVID Pass:



- Be alert to links and attachments in unexpected text messages or emails
- Do not respond to requests for money, passwords or financial details
- Challenge: Could it be fake?
- Use the official NHS COVID Pass website (see below)

The NHS COVID Pass is available to demonstrate your COVID-19 status either in a digital or paper format via the NHS App, the NHS website or by calling 119.

For information on how to get your free NHS COVID Pass, visit www.nhs.uk/nhscovidpass.

If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to spamreports@nhs.net (at work) or report@phishing.gov.uk (at home).

If you are suspicious about a text message, forward it to the number 7726 which is free-of-charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by visiting actionfraud.police.uk or calling 0300 123 2040.

If you have any information relating to NHS COVID Pass or vaccine you can report and anonymously by contacting Crimestoppers online at covidfraudhotline.org or phone on 0800 587 5030.

Covid-19 NHS Staff Grant Emails

Local NHS staff have reported receiving an email which claims that all NHS staff are eligible to access a £2,920 Covid-19 support grant. Unfortunately this is not genuine and the email contains a link which may be aimed at infecting your computer with viruses/malware, or stealing your log in credentials and bank information.

Please be very cautious about emails of this nature. If you receive an email like this, please do not click on any links or attachments contained and forward the message as an attachment to spamreports@nhs.net

Further Scam Trends

“Hello Mum/Hello Dad” WhatsApp Scam

In this scam, fraudsters send messages over WhatsApp impersonating the victim’s family members, most commonly they pretend to be a son or daughter. The first few messages are designed to con you into thinking that they have had to change their phone number. After a rapport has been built, they then move on to ask for help paying a bill or invoice.

WhatsApp have launched an awareness campaign to try and help us all to avoid these scams. If you receive a suspicious message on WhatsApp please follow the advice below:

- Stop—take a minute before you respond. Consider switching on two step verification for your WhatsApp account if you don’t already use it.
- Think—does the request make sense? Are they asking you to share a PIN code which has been sent to you? Are they asking you for money or help paying something? Remember, scammers prey on people’s kindness, trust and willingness to help.
- Call—verify that you are speaking to your friend or relative by calling them directly, or asking them to send you a voice note.

You can find more advice around this scam by visiting the Citizen’s Advice website.

Suspicious “Consulant” Phone Call

A patient has contacted their surgery to advise that a man had phoned, introducing himself as a consultant from a local hospital. The caller knew the patient’s name, DOB and telephone number.

The caller proceeded to tell the patient about a new medication that they thought would suit her and said that she needed to pay him over the phone via card £25 a month. Thankfully the patient did not give any details away. After trying calling back for a further 3 more days the fraudster stopped calling. Genuine NHS staff would not make these calls. If you receive any cold calls like this, please hang up and report the matter to Action Fraud.

Cyber Security—Improving Your Safety at Home

As you will have noticed from reading previous editions of this newsletter, a large proportion of fraud attempts are made via computers, tablets and mobile phones. In fact, Action Fraud reports that 80% of the fraud reports they receive have a cyber-element.

At work, how you are able to use your NHS devices is determined by the security settings that have been set up by your IT team. You will also have policies and procedures to follow that help you to keep your work devices safe.

At home, it can feel overwhelming knowing where to start. You may or may not have anti virus software running, and you may or may not have installed the latest security patches for your various devices.

You might use one password for all your accounts because you find it’s easier than remembering lots of unique passwords.

You might have lots of different devices set up around the house (Alexa/Google Home speakers, video doorbells, smart heating systems, fitness trackers etc.). These devices create an “internet of things” in your home, and each device can present their own cyber security risks. Over the next few weeks, you may also find that you need to set up new devices for yourself or family members.

The good news is, there are places you can find out more about how to improve your cyber security. The National Cyber Security Centre is a part of GCHQ and offers a wealth of advice and information that you may find really helpful.

In particular, they offer a Cyber Aware exercise that you can follow to increase your cyber security at home through taking 6 simple actions. They walk you through each of these actions and explain how they will improve your security. You can even generate a personalised “To Do” list for yourself. That way, you can take a few minutes when you have time to work your way through the various steps.

You can find the Cyber Aware exercise on the NCSC website here.

There is also a really helpful article about connecting smart devices confidently. This could prove to be really helpful if any of your friends or family receive or purchase smart devices over the next few weeks. This article can be found on the NCSC website here.

In the Press

Prison Sentence Following Fake NHS Compensation Claim

Rhys Williams worked as a security guard at Basildon University Hospital in Essex when he claimed he had slipped on some cardboard at work. Williams took three months off work, which he claimed was due to injuries sustained in the fall. He also submitted a personal injury claim, and was awarded £5,010 in compensation.

However, shortly after his compensation claim was paid out, evidence was received which showed that Williams had planned out the "accident". He had even ensured there would be no CCTV coverage to show that he had not actually fallen. He had acted deliberately in a bid to sort out his own finances.

Williams has now been jailed for seven months after being found guilty of contempt of court. You can read more about his case on the NHS Resolution website.

Dentist Sentenced after £74k fraud

Dentist Sheena Lalani has been found guilty of fraud by abuse of position after it was discovered that she had submitted fake claims totalling over £74,000. Lalani held NHS contracts for providing dentistry services at two practices. However, it was later identified that she had submitted 378 fraudulent claims for payments to which she was not entitled. This included claiming to have performed 45 treatments in one day.

Lalani has now paid back over £87k (the amount of money taken, plus inflation). She has also been sentenced to 20 months imprisonment (suspended for two years), ordered to complete 250 hours of unpaid work, and given a rehabilitation order. A fitness to practice hearing is also pending.

You can read the full story on the NHS Counter Fraud Authority website.

Senior GP Sentenced to 3 years 4 months after £1.1m fraud

Dr Rumi Chhapia was recently found guilty of fraud offences after taking £1.1 million in order to fund an online gambling addiction. Chhapia was one of the directors for Portsmouth Primary Care Alliance. He had only been given access to the accounts for 6 weeks, after a colleague who usually looked after the finances was signed off sick.

When the missing money was first noticed, Chhapia claimed that he had been the victim of a cyber attack and continued to move money into his own accounts. Chhapia eventually came clean during a police investigation. He has repaid £238,000 and gambling companies have agreed to pay back £904,000. More on this story can be found on the BBC website.

Man Reported for Fraud after Fake Arm Covid Jab Ploy

In more unusual news, a man has been arrested following an incident in north-west Italy. The man who is in his 50s had attended a Covid-19 vaccination appointment. It was noted that he was wearing a fake arm to try and avoid being vaccinated.

The man appeared to have been wearing a silicone mould over his own arm, and had tried to persuade the nurse administering the jab to turn a blind eye when the deception was spotted. The nurse reported the man to the police. The man is reported to be a health worker who had been suspended due to not having been jabbed. In Italy, the Covid-19 vaccine is a mandatory requirement for all health workers.

More details on this story can be found on the BBC website.

Beware of Charity Scams this Christmas

Action Fraud have published advice around avoiding donating to bogus charities over the coming months. This time of year is often a popular time for people to make donations to various causes.

Unfortunately, there are unscrupulous individuals around who are willing to take advantage of people wanting to do their bit to support others. Over the past 12 months, £1.6 million has been taken by fake charities. This is an increase of 16% compared to the previous year.

The Fundraising Regulator is leading the awareness drive as the festive period approaches, and Action Fraud are also taking part in the campaign. You can read the full article and advice on donating safely by visiting the Action Fraud website.

Counter Fraud Training

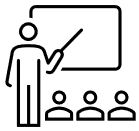
Fraud Prevention Masterclasses

The LCFS team are continuing to deliver our series of Fraud Prevention Masterclasses for NHS staff, covering key fraud risks within different areas.

The masterclasses are delivered via Microsoft Teams and last around 45 minutes to 1 hour.

The sessions have been delivered on a monthly basis, and cover some key areas that have 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.

11th January 2-3
4th February 10-11

Creditor Payments

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

14th January 11-12
18th February 10-11

Payroll Fraud

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

12th January 2-3
11th February 10-11

Cyber Fraud

Tactics used by Cyber Criminals to target us at home and at work.

20th December
11-12

Our Masterclass programme is now winding down for 2021/22, however we will be running more sessions in 2022/23.

If you have any suggestions or requests of other topics you would like us to cover in the next set of masterclasses, please don't hesitate to get in touch with any of the Local Counter Fraud Team (our contact info is 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 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