Counter Fraud Newsletter – March 2023

AUDIT YORKSHIRE

Welcome to the March 2023 edition of the Counter Fraud Newsletter for NHS Staff. We hope that you find this information helpful. If you have any questions or feedback, you'll find out contact information on the last page.

Fraud in Numbers 2022

The rise in fraud in the UK has led to the Government to classify the crime as a national security threat and it must be dealt with by law enforcement agencies as a top priority. Here are some statistics:

Fraud is under reported but is believed to account for **40%** of crimes in the UK

In 2022, **£4 billion** was lost to fraud in the UK. This is two thirds more than was lost in 2021.

Around **60%** of fraud is cyber enabled.

Only **2%** of police resources are dedicated to combatting fraud.

Our top tips to prevent yourself from becoming a victim are:

- Remain vigilant.
- Don't be afraid to challenge something which doesn't seem right.
- Keep passwords safe.
- Don't click on unexpected email links.
- Read our monthly newsletters to find out about the latest scams.

Fake Voucher Scams

Social media users are being warned about fake vouchers which are being posted online. The latest example is for a non existent "Marks and Spencer (M&S) Golden Ticket". The scammers claim that 500 people can get their hands on a golden ticket worth £100-£750 just by liking and sharing their post. The victims are encouraged to click on links which then steal their credentials or infect their devices with viruses. A spokesperson from M&S has confirmed that the posts are fake. M&S did previously run a gold ticket scheme when they opened new stores – and it appears that the scammer is using photographs from these events to make their posts look more realistic.

As household budgets remain under pressure, there are likely to be lots of different versions of this scam online. You may come across voucher "giveaways" for supermarkets, high street retailers, and energy companies being shared on social media. Please remember that if something seems too good to be true, it probably is. The best way to check if something is a genuine offer, is to contact the company using their customer service contact number or webchat.

Charity Scams

Fraudsters are quick to take advantage of any disaster situation to steal money that you kindly donate to a good cause. Charities receive over £76 billion a year and so it is a sector which scammers are keen to tap into. To ensure that your money is used for it's intended purpose, only support registered charities who are regulated and held accountable in accordance with charity law. Here are some top tips to help you spot the scammers amongst the genuine charities.

- You can check whether a charity is formally registered here - The Charity Commission - GOV.UK (www.gov.uk).
- If a small charity claims affiliation with a more recognisable one, it is safer to donate via the well known option.
- Fundraisers which have only received small amounts. Genuine charities are likely to raise a significant amount.
- Find the charity you want to donate to and visit their website. Do not respond to emails or click on links within an email which have been sent to you which you have not requested.
- Check that images used in appeals have not be lifted from elsewhere – you can find out how to do this in an article in the February 2023 edition of our newsletter. Even if the image has not been used elsewhere, look closely at it. Some pictures used are not photographs taken at the scene, but they have been created using Artificial Intelligence.
- If you are approached by a street collector and wish to donate, check that the person has formal identification and that their collection tin / bucket is properly sealed and not damaged.
- Never be made to feel pressured to make a donation either inline or in person. Take your time to do research to make sure that your money goes to the cause you intend it to.

Cyber Security

How safe is your secure word?

Historians have found that we've been using our mother's maiden name as a security question since 1882. In this digital age where we are using multi factor authentication it may well become obsolete in the near future. However, many official organisations (such as banks) still use this traditional security question.

Has this stood the test of time to remain fool proof? Unfortunately not. One of the Counter Fraud team was able to find the maiden name of 5 out of 6 of her colleague's mothers in less than 20 minutes thanks to the public digitalisation of births, marriages and deaths.

Read any advice on passwords and it will all say to make them unguessable. Some advice on the security question is to make one up (was anyone else's mum called Miss Squarepants before she married your dad?). We advise to take care if you do this. Although most don't, some organisations will check this against official records. You also have to remember what answer you gave or risk being frozen out of access to services.

We cannot avoid using a mother's maiden name in some situations, but if you get options for what your security word is, use the option that the answer cannot be easily found on the internet. Whilst we're on the subject, just a reminder that the 'games' you often see on social media where you can get your fairy goblin name by combining the name of your first pet with the street that you grew up on, are nothing more than phishing exercises used by fraudsters to capture your details.

Twitter Removing Text Based Two Factor Authentication

You may have heard that Twitter is taking away the text message based Two Factor Authentication (2FA) option for users who are not subscribed to Twitter Blue. 2FA is an additional security protocol, where you must provide two forms of identification when logging into an account. For example, you are asked to enter your password plus a one time access code which has been sent to you by text or email.

In March 2023, Twitter are taking away the option to have a one-time access code sent via text to your phone – however, there are other options you can use. If this change affects you, you can read more about your options on the National Cyber Security Centre blog and on the Wired website.

Remote Access Scams

Have you ever had a call out of the blue from someone claiming to be from Microsoft? The caller will usually say that they have been alerted to a problem with your device, and that they need to carry out urgent repairs. The situation is so worrying that in fact, they need to log into your computer NOW.

They encourage you to allow them to access your computer via a Remote Access programme – such as AnyDesk, Team Viewer, Microsoft Remote Desktop etc. These are genuine tools with a legitimate purpose and you may have used some of these when on the phone to IT.

If the fraudster gets access to your device, they may install viruses or other malware which then steal your data. Some particularly unpleasant criminals may even impersonate your bank's fraud team, and claim that a problem with your device or internet connection has led to money being stolen from your account. This gives them an excuse to ask you to log into your online bank whilst they are remotely connected to your device. They will then encourage you to move your money into a "safe" account which is under their control. These fraudsters are very persuasive and persistent.

- If you receive a call claiming to be from your bank's fraud team, end the call, and either wait 30 minutes or use a different phone to call the official customer service number (you'll find this on the back of your bank card).

- If you receive a call claiming to be from IT, ask for the call reference number and end the call. Wait 30 minutes or use a different phone to call the IT team using their usual number. Microsoft do not call people out of the blue.

You can read more about this type of scam on the Which? website.

Can you spare 2 minutes to complete a quick survey on NHS Fraud?

It would really help the Counter Fraud Team if you could take the time to respond. There are only 10 questions and it is estimated that completing the survey should take less than 2 minutes. Thanks very much for your help.

To provide your response, please follow this link: https://www.surveymonkey.co.uk/r/K7KZ7MX

In the Press

Grandmother foils fraudsters who were impersonating her grandson

A woman in Ontario, Canada, received a phone call from a tearful young man who claimed to be her grandson. He explained that he was in jail and needed help paying his bail – to the tune of $9,300. This was the third time she'd received one of these scam calls, so this time Bonnie decided to play along. Her quick thinking enabled the police to intercept the fraudsters, who were arrested and charged. You can read more on the BBC news website.

Which? publish their top 5 weirdest scams of 2022

Consumer website Which? have put together an article exploring the five strangest scams that had been reported during 2022. The article includes some creative methodologies that have been used by fraudsters, but please do remember that a lot of fraud is very convincing and can be difficult to spot. Have a look at the weirdest scams on the Which? site.

7 year prison sentence for fake psychiatrist

Those of you who have been on the Recruitment Fraud Prevention Masterclass will recognise the name Zholia Alemi. Alemi was first brought to police attention after she had herself appointed as Power of Attorney for an 84 year old vulnerable patient, and attempted to change the victim's will to list herself as the beneficiary. When this came to light, an investigative journalist did some digging into Alemi's past, and it was identified that despite working as an NHS psychiatrist for 22 years, she had never passed the first year of her medical training. Alemi was sentenced to 5 years imprisonment for her conduct against the vulnerable patient.

A trial looking at fraud offences against the NHS has recently concluded that Alemi presented a forged degree certificate and a fake "letter of verification" when applying for NHS roles. She has benefited by an estimated £1.3 million in wages. She has been sentenced to a further 7 years in prison. You can read more on the BBC news website.

Counter Fraud Training

Fraud Prevention Masterclasses

Our Fraud Prevention Masterclass Programme is drawing to a close for this financial year. We would like to thank everyone who has attended and we hope that you found the information you were given useful.

In 2022/23 we covered the following topics:

- Recruitment Fraud
- Cyber Enabled Fraud
- Payroll Fraud
- Creditor Payment Fraud
- Fraud Awareness for Managers
- General Fraud Awareness

We will be publishing a new timetable of Masterclasses in Spring. If you have any suggestions for topics you would like to see covered, we would love to hear from you. Please drop one the Local Counter Fraud Team an email with any feedback or suggestions (our contact details are on the next page).

In the meantime, if you would like to arrange a bespoke fraud training session, or if you'd like us to pop along to your team meeting for a less formal chat about the world of NHS fraud, please don't hesitate to get in touch. You'll find some further details below.

Open offer for bespoke training/fraud awareness input

The counter fraud team is always happy to put together bespoke training for your specific role or department. If your team would benefit from a Fraud Prevention Masterclass on the topics listed above, this can be arranged outside of the planned Masterclass training schedule. We are also happy to attend any team meetings to introduce ourselves and talk about NHS Fraud. If you would like to arrange a session for your team, please contact one of the Local Counter Fraud Specialists (our details are on the next page).

You can view previous editions of the counter fraud newsletter on the Audit Yorkshire Website by scanning this QR code.

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS

You can **contact the Counter Fraud team** using our details below. You can also report your concerns to the **NHS Counter Fraud Authority** via their online reporting tool or hotline. If you making an anonymous report, **please give as much detail as possible** as we won't be able to contact you for more information.

I have a concern that fraud may be being committed against the general public

These concerns can be reported to **Action Fraud** (0300 123 2040). If someone has been actively defrauded, it may also be appropriate to report to the **police**. If it is suspected that the victim's bank account has been compromised, they will need to **speak to their bank as a matter of urgency**.

I have received a suspicious email to my NHS.net email address.

Do not click on any links or attachments.

Forward the suspect email **as an attachment** to **spamreports@nhs.net**. To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".

I have received a suspicious email to another email account (not NHS.net)

Do not click on any links or attachments.

Forward the email to **report@phishing.gov.uk.** You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

I have received a suspicious text message

Do not click on any links in the text message!
Forward the text message to **7726.**

I have come across something and I'm not sure whether it is fraud-related

You are very welcome to contact the **Counter Fraud team** for advice and support, our details are below.

How to Contact your Local Counter Fraud Specialist

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
Rich Maw Local Counter Fraud Specialist	R.Maw@nhs.net 07771 390 544
NHS Counter Fraud Authority	0800 028 4060 https://cfa.nhs.uk/reportfraud