Fraud Counts Newsletter

Spring 2023

Introduction

Welcome to the Spring 2023 edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on current scam trends including fake voucher scams and charity scams, cyber security, fraud cases currently in the press, a quick guide to reporting fraud concerns, and how to contact your Local Counter Fraud Specialist.

Current Scam Trends

Fraud in numbers 2022

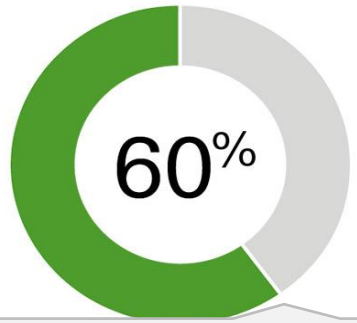
The rise in fraud in the UK has led to the Government to classify the crime as a national security threat which must be dealt with by law enforcement agencies as a top priority. Here are some statistics:



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.



It is estimated that around 60% of all fraud is cyber enabled.



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

©ASW Assurance

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

- Be fraud aware everywhere – this can apply just as much in your personal life as well as work!
- Don't be afraid to challenge something which doesn't seem right.
- Keep passwords safe.
- Don't click on unexpected email links.
- Keep up to date with our newsletters and other communications to find out about the latest scams.

Fake voucher scams



This Photo by Unknown Author is licensed under CC BY

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.

Suspicions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence - 0800 028 40 60 or www.reportnhsfraud.nhs.uk



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 your money is used for its intended purpose, only support registered charities (they 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.
- 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 online or in person. Take your time to do research to make sure that your money goes to the cause you intend it to.
- Check that images used in appeals have not been copied from elsewhere – you can find out how to do a "Reverse Image Search" in the How to help box below. 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.

How to help box - reverse image searches

Fraudsters who post fake listings on selling websites will usually lift photographs of the item from somewhere else.

To check whether a photo has been lifted from somewhere else, you can run a reverse image search. To do this:

1. Save the images which have been shared on the suspicious advert.

2. Open the image search on Google (images.google.com)

3. Click on the icon shaped like a camera to run a search using an image.

4. Upload the image that you've saved. You will quickly see if the image has been posted elsewhere.

5. You can also do the same thing to search videos. Just take a screenshot of a distinctive part of the video and run that image through the Google image search.

©ASW Assurance

Cyber Security



This Photo by Unknown Author is licensed under CC BY-ND

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're using multi factor authentication it may become obsolete in the near future. Yet 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. If you think a fraudster won't go that far to get your personal information, think again.

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 took 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.



If you have any suspicions or concerns,
You can call us anonymously on

0800 028 40 60

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information
The NHS Counter Fraud Authority leads on fighting fraud, bribery and corruption in the NHS and the wider health group

NHS
Counter Fraud Authority

Department of Health & Social Care

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? published an article exploring the five strangest scams that had been reported during 2022. The article includes some creative methods that have been used by fraudsters. Always 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
Zholia Alemi first came to the police's 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 showed that despite working as an NHS psychiatrist for 22 years, she had never passed the first year of her medical training in New Zealand as she claimed. Alemi was sentenced in 2018 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.

©ASW Assurance

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 overleaf. You can also report your concerns to the NHS Counter Fraud Authority via their online reporting tool https://cfa.nhs.uk/reportfraud or **via their free** 24hr confidential fraud reporting hotline powered by Crimestoppers on 0800 028 4060. If you are 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 already been defrauded it may also be appropriate to report to the police. If the victim's bank account may have 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 or not it is fraud related

- Your Local Counter Fraud Specialist is available for advice and support, our details are overleaf.

©ASW Assurance

Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS.

Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact one of our team below.



Gareth Cottrell – Counter Fraud Manager

✉ gareth.cottrell@nhs.net ☎ 01872 258057
07814 002364



Tracy Wheeler – LCFS

✉ tracy.wheeler2@nhs.net ☎ 01752 431378
07789 868568



Byron Kevern – LCFS

✉ byron.kevern@nhs.net ☎ 07775 417508



Sarah Smith – LCFS

✉ sarah.smith337@nhs.net ☎ 07467 685609

©ASW Assurance