Fraud Counts Newsletter

International Fraud Awareness Week 2023 – Edition 3

Introduction

Welcome to our latest edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on current scam trends including fraudulent calls to NHS staff impersonating the NHS, how to use QR codes safely, information on how to protect your online profiles, fraud cases currently in the press, a reminder on reporting fraud concerns, and how to contact your Local Counter Fraud Specialist.

Current Scam Trends

The Scam

Since the start of the financial year, we have seen a surge in fraudsters trying to divert salary payments by impersonating NHS staff. The fraudsters have set up fake email accounts and have contacted HR, Payroll and Finance departments asking for changes to employee bank details to be made.

But how have the fraudsters been identifying the names of NHS employees? A review of the attempts that had been made found that in **100% of cases**, the person who was being impersonated had a publicly visible LinkedIn profile. In 70% of cases, the fraudster made direct contact with a named Payroll, HR or Finance employee at the same organisation who **also** had a visible LinkedIn profile.

All of these LinkedIn profiles had low privacy settings, meaning the person's full name, job title, and place of employment could be viewed via search engine results. This meant that the fraudster didn't need their own LinkedIn account to get hold of this information.

Prevention Advice

- On LinkedIn you can stop your profile details from showing up in search engine results. Instructions on how to do this can be found on the LinkedIn help site.
- If you have an inactive or rarely used LinkedIn account, it is best to delete it.
- Never share personal or financial information with someone you have met on social media. Make sure you use a strong and unique password for each account.
- Always use Multi-Factor Authentication when it is available, this lowers the chance of your account being hijacked.
- Be wary of unsolicited contact and offers that are too good to be true.
- You can read more about job offer scams on the Which? website.

LinkedIn has been the subject of several reports around security issues such as fake profiles, account hijacking, and the site being used to carry out fraud by offering fake job offers or phony investment opportunities. These same concerns also apply to other social media platforms, so even if you don't use LinkedIn it's important to review your privacy and security settings.

©ASW Assurance

The Scam

We've heard reports recently about fraudsters posting QR codes in car parks. When the codes are scanned, instead of taking the drivers to a site to pay for their parking, it takes them to a site controlled by fraudsters who take the car parking fee – and then continued to make debits every day until it was cancelled.

What are QR Codes?

A QR code is simply a shortcut to a website. They are increasingly used by many businesses. For example, some restaurants no longer have a paper menu, instead they provide a QR code which visitors scan to view the menu, place orders, and pay for their meal. This was a particularly popular tool for shops and other services during the Covid-19 pandemic as it limited the number of surfaces customers needed to touch.

Using a QR is simple - open the camera app on your phone, point it at the code when your camera detects the site the code is linked to you can see which internet address it will take you to. If you are happy to continue, you simply press the link which will have appeared.
The QR code itself cannot be hacked; the fraud risk is in relation to the site the code leads you to.

In short, QR codes are a great way to quickly access information and the majority are legitimate. However, other than using them to check what you will be having for dinner, or reading back issues of the counter fraud newsletter, please stop and think before you enter information into websites which have been accessed via a QR code. If in doubt, look for alternative ways to contact the company.

Prevention Advice

- Look at the QR code before you scan it to make sure that a sticker hasn't been placed over the top.
- Use the camera app on your phone to scan codes – you do not need to download a QR app.
- Check the internet address the code wants to take you to. Once you are in the website, it may look legitimate, but the address (URL) will not match the official website in suspicious cases.
- If you have accessed a website through a QR code, don't put any financial details, personal information or username / passwords into the site it has taken you to.
- If you receive an email with a QR code telling you to access this to make a payment, double check with the company or access their website in a new browser.

You can find more information and advice on the Credo website.
Here's a legitimate QR code, try it to see where it takes you: -

©ASW Assurance

The Scam

Our Counter Fraud colleagues have made us aware of a scam call which was made to a patient in Yorkshire. The fraudster claimed to be from the NHS and said they were calling to confirm the patient's appointments. They asked for the patient's name, address, date of birth, national insurance number, and bank details.

When the patient refused to share their bank details, the caller stated that all their appointments would be cancelled and ended the call.

The patient attended their local hospital where they were reassured that their appointments had not been cancelled.

Prevention Advice

- NHS services will not ask you to share your bank details over the phone.
- If you receive an unexpected call asking you to share personal information to "confirm your identity", end the call. Wait 30 minutes or use a different phone to call the organisation back on an official contact number to verify if the call was genuine.
- We advise waiting 30 minutes or using a different phone because some fraudsters can jam your phone line. Even though you think you've hung up, they are still on the line and will intercept your next outgoing call.
- Don't rely on your caller display - fraudsters can disguise their number using spoofing software.

In the Press

Man facing £100k bill and Contempt of Court Proceedings after Suspicious Compensation Claim

Sean Murphy had surgery for a torn bicep tendon in 2017, and during the operation his elbow was damaged. Sean claimed that this injury had left him unable to work, go to the gym or play rugby, and that he was dependent on his wife to help him get dressed. He sought compensation of £580,000 from the NHS.

However, a tip-off was then received that Murphy had been dishonest when describing the extent of the impact on his day-to-day life. Solicitors pointed to evidence including videos on his Facebook account which appeared to show him lifting very heavy weights. They also noted that he had returned to work laying decking and tarmac, and that local media coverage of rugby matches included his name in the line-up.

Judge James Healy-Pratt dismissed Murphy's claim and he has been ordered to pay back £50,000 in compensation that he had already been paid. He also faces having to pay the legal costs of the NHS, with the total bill looking to be over £100,000.

Murphy continues to argue that his claim was not dishonest. A further trial for contempt of court proceedings is due to take place. You can read more on the Metro website.

Suspicions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence –

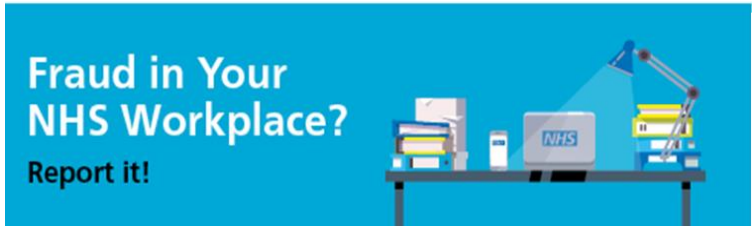
0800 028 40 60 or www.reportnhsfraud.nhs.uk



©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 your local Counter Fraud team using the details overleaf. 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 or not it is fraud related.	You are very welcome to contact your local Counter Fraud team for advice and support using the details overleaf.



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

©ASW Assurance

Looking forward to our next edition of Fraud Counts?

Here's a little preview - Christmas is coming… The fraudsters are getting greedy!



Like it or not, Christmas is just around the corner and, if you haven't already, you may be looking to starting your Christmas shopping and festive preparations. Christmas is a scammer's paradise – lots of people, all looking for bargains to reduce the spend. **Get up to date with some of the likely scams ahead of time.**

Online Shopping Fraud

If you're making a purchase from a company or person you don't know and trust, can you be sure the website is genuine?

- Do some research first, perhaps ask a friend or family member for advice before completing the purchase.
- If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.
- Make sure you install the latest software and app updates. These usually contain important security updates that can protect you against fraud and identity theft.
- Check whether a website is safe using getsafeonline.org

Holiday Fraud

If you spend your Christmas break trying to bag a summer getaway bargain, think before you book.

- Book your holiday directly with an airline or hotel, or through a reputable agent. Check whether they're a member of ABTA.
- If you decide to deal directly with the property owner or a letting agent, ask questions about the booking, room, location and area.
- Don't book on websites that don't have a padlock icon (https) - https://www.getsafeonline.org/personal/articles/online-payments/
- Be extra cautious if you're asked to pay using bank transfer or cash; pay by credit or debit card if you can.

Prevention Advice

- Keep an eye out for news about the latest scams- know how your might get caught out.
- Be in the know – read up about the 12 Frauds of Christmas on the Action Fraud website.
- Learn more about different types of fraud: A-Z of fraud | Action Fraud





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.Smith10@uhbw.nhs.uk ☎ 07467 685609



Sandra Bell – LCFS

✉ sandra.bell19@nhs.net ☎ 07467 685529



Ian Halkerd – LCFS

✉ ian.halkerd@uhbw.nhs.net ☎ 07788 300215



Sammy Donaldson – Trainee LCFS

✉ s.donaldson1@nhs.net ☎ 07467 685529

©ASW Assurance