AUDIT YORKSHIRE

November 2025

Counter Fraud Newsletter

Welcome to this month's edition of the Counter Fraud Newsletter for NHS staff. You will find contact details for your Local Counter Fraud Specialist in your organisation's Anti-Fraud, Bribery and Corruption Policy.

Did you know that NHS fraud costs millions of pounds every year – and that you can help to prevent it?

This International Fraud Awareness Week, which runs from 16 – 22nd November, your Counter Fraud Team wants to remind everyone of our shared responsibility to protect NHS resources and taxpayer money. Click here to watch a video version of this article.

Fraud is when someone deliberately deceives others for personal or financial gain, causing a loss to someone else.

In the NHS, this can take many forms, such as:

- A staff member falsely calling in sick while working elsewhere.
- A supplier charging for goods or services that were never delivered.
- A cyber-criminal pretending to be a contractor and asking for payments to be sent to a different bank account.

New Failure to Prevent Fraud Offence

New legislation means that organisations can be prosecuted if they don't have reasonable procedures in place to stop staff, agents, or associates from committing fraud for the organisation's benefit.

This makes it more important than ever to report any suspicions of fraud.

How You Can Help

You must report any suspicions, evidence, or knowledge of fraud to the Counter Fraud Team.

Every report helps us find and fix weaknesses in our processes—even if the concern turns out to be unsubstantiated.

Reports can be made anonymously, and the person you're reporting about won't be told unless the concern is verified.

We'll work with you to make sure you're comfortable with any actions taken. For more details, see your organisation's Whistle Blowing policy.

Let's work together to keep the NHS safe from fraud—every action counts!

Beware of Black Friday Scams

It's that time of year again! The busiest shopping period is here, and many of us will be heading online to try and snap up some bargains.

Black Friday is one of the biggest shopping events of the year—but it's also prime time for online scammers. With inboxes full of tempting offers and social feeds overflowing with "too good to be true" deals, it's easy to get caught out. Black Friday can be a great opportunity to save money—just make sure cybercriminals don't get a share of your budget.

One of the most common tactics is phishing, where criminals send emails or texts pretending to be trusted retailers or delivery companies. These messages often use urgent language—"your parcel is on hold", "limited time offer" or "low stock - act now" —to push you into clicking malicious links.

Social media ads can also be misleading. Some promote heavily discounted products that are faulty, fake, or simply don't exist. These ads can also land you on fake websites for trusted brands, the sort that harvest your personal information and card details.

How to Stay Safe

- Verify websites before entering any details - check the site matches the company's usual web address. It can be safer to purchase from their **official** app if they have one.
- Don't click links in unexpected emails or text messages.
- Research unfamiliar retailers before purchasing. Check TrustPilot and try Googling "[company name] + scam".
- Be wary of social media posts and adverts where the comments have been turned off.
- Watch out for manipulation tactics - messages claiming your order cannot be completed, that your parcel won't be delivered, or that you have limited time to act.

In The Press : NHS Credit Controller Pleads Guilty to Fraud

A former Credit Controller at Guy's and St Thomas' Foundation Trust had pleaded guilty to fraudulently taking £218,000 and attempting to take a further £84,000 from the Trust.

Edias Mazambani, in his role of a Credit Controller, abused his position of trust to access secure financial databases at the Trust. He created fake refund requests for money which was held on behalf of patients and clients.

The money Mazambani took from these fake refunds was sent to four different bank accounts, two of which belonged to other members of NHS staff. These four accomplices then moved money between themselves and back to Mazambani. The two other NHS staff members have been found guilty of Money Laundering.

They are expected to be sentenced by the Courts in January 2026.

Typo Traps

After seeing a warning on social media that a fake email with a slightly amended address was doing the rounds, the Counter Fraud Team did a bit of digging.

The email which had been flagged was pretending to be from microsoft.com, but the first 'm' had been changed to an 'r' and an 'n', making it rnicrosoft.com.

At a glance, this will look pretty convincing to most people. We've seen other examples in the past where the letter 'l' is replaced with a number '1'.

This tactic is so commonplace now that it has its own term – typosquatting.

It is also known as URL hijacking, and is a form of cybercrime where fraudsters register email addresses and domain names that closely resemble legitimate websites.

As well as using similar looking numbers and letters to closely resemble a recognised contact, fraudsters also rely on common typing errors.

For example, a user intending to visit nhs.uk might accidentally type nsh.uk. In 2014, this domain name had been bought by somebody in the Czech Republic hoping to cash in on people landing on this malicious site in error.

Just to add yet more terminology to it, fake websites are sometimes referred to as domain doppelgangers or evil twin sites.

Typosquatting / domain doppelgangers can lead to:

🚨 Phishing attacks targeting anybody.
🔑 Credential theft through fake login portals.
👎 Reputational damage if users are misled by fraudulent sites.

How to spot and prevent this cybercrime:

✅ Check email addresses and look closely at the characters used.
✅ Double-check URLs before clicking or entering credentials.
✅Check your spelling - even the best typists can fall prey to an attack of sausage fingers.
✅ Use bookmarks for frequently visited sites.
✅ Be vigilant to the risks and signs of typosquatting.

Don't let one wrong letter ruin your day.

QUICK TIP CORNER

Spot Suspicious Links Fast

Before clicking any link, hover your cursor over it to preview the real web address.

Look for subtle misspellings, extra characters, or unexpected endings that don't match the organisation's official site. If something looks odd, don't click.

Please note this doesn't work on touch screen devices like phones and tablets. It is always best to type in the address of the website you want to visit instead of clicking links in emails or texts.

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please notify your Local Counter Fraud Specialist. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.

You can also report your concerns to the NHS Counter Fraud Authority using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.