

# COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud Newsletter. We hope you find the contents helpful. As always, if you need any fraud advice please reach out to your Local Counter Fraud Specialist. You'll find our details in your organisation's Anti-Fraud, Bribery and Corruption Policy.



## **Who are the Counter Fraud Team, what we do, and how we can help**

As part of the NHS standard contract, all NHS service providers must have somebody responsible for preventing, detecting and investigating allegations of fraud, bribery and corruption (collectively known as economic crime).

The person who does this role is known as a Local Counter Fraud Specialist (LCFS). LCFSs must undertake training and be accredited with the NHS Counter Fraud Authority before they can be formally nominated to work at each NHS organisation.

The Counter Fraud Team comprises 7 members of staff and is part of the Internal Audit consortium, Audit Yorkshire. We provide a counter fraud service to 17 different NHS organisations.

Different areas of the NHS face different fraud risks, but every single area is at risk of some kind of fraud taking place. Examples include fake invoices being sent in, staff calling in sick then working elsewhere or patients evading charges. Staff themselves may also be at risk of being a victim if they receive a phishing email or phone call encouraging them to share information which can be used by a fraudster.

The Counter Fraud team aim to raise awareness of fraud by issuing these newsletters, delivering training sessions and sending information and alerts out. We're happy to chat to any staff member or drop into a team meeting if you'd like to get to know us better.

We would much rather prevent a fraud than deal with the aftermath of one being successful. We constantly horizon scan to keep up to date with the latest scams, as the NHS is an attractive target for criminals and their methods of trying to extract money constantly change.

If something looks amiss, don't worry about whether it is fraud or not, just let us know about it. If it isn't a fraud, or needs referring elsewhere, we can still help with that. We'd rather receive a referral where everything turns out to be ok than miss the opportunity to prevent a financial loss. During 2024/25, we received 333 referrals and 78 of these required a formal investigation.

Details of how to contact us can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.

## Fraud Awareness Alert: WhatsApp “HR” Scam Calls

The Counter Fraud Team has received reports of NHS staff receiving scam phone calls.

### What's Happening:

- Scam calls are being received on mobile phones.
- A pre-recorded message says HR needs to discuss an issue and requests you add a number to WhatsApp.
- Once the number is added, the fraudster may attempt to:
  - Steal personal or financial information.
  - Gain access to your WhatsApp account via verification codes.
  - Send malicious links to install harmful software on your device.



One staff member who received this call advised that it came to his personal mobile. When he answered, it was a pre-recorded message in a female voice which simply said there was a HR issue and asked that he add the number to his Whatsapp.

### What You Should Do:

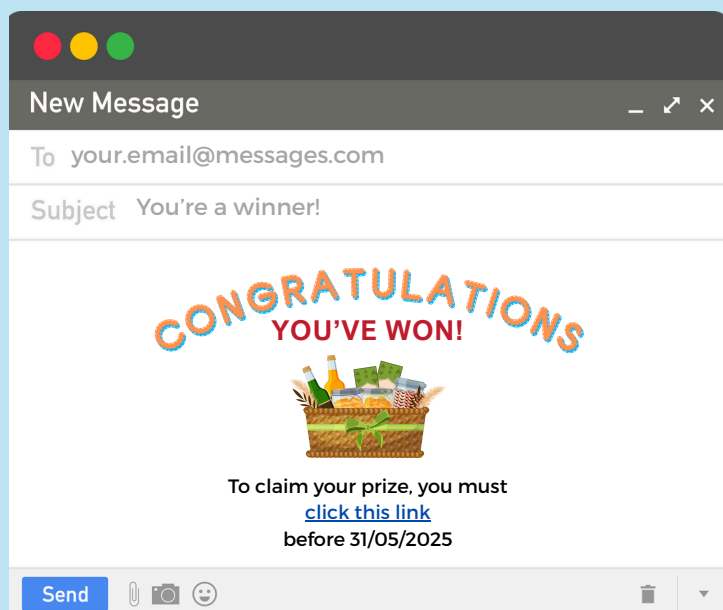
- Do not add the number to WhatsApp.
- Hang up and block the number immediately.
- If you are unsure if HR have genuinely tried to contact you, please get in touch with them using contact details from your organisation's intranet.
- Never share personal or financial details through WhatsApp or over the phone unless you've independently verified the contact.

If you believe you have already been targeted or have shared any information:

- Report it to Action Fraud on 0300 123 2040
- Contact your bank immediately if financial information may have been compromised.

You can also contact the Counter Fraud Team by emailing [yhs-tr.counterfraudyork@nhs.net](mailto:yhs-tr.counterfraudyork@nhs.net)

HR will never contact you via WhatsApp to discuss work-related issues. Legitimate communication from HR will always be through the usual channels such as work email, phone calls, or in-person meetings.



### Fake prize scams

If you've ever looked in your personal email "spam" folder, you'll probably have seen emails like this.

Having just checked my own emails, this LCFS can report she has apparently won a Marks and Spencer's letterbox afternoon tea, several Shein mystery boxes, and a complete set of luxury pillows. And all without entering any competitions. Lucky me!

These emails are sent out in their thousands, and will usually include brand names for companies we know and trust. Common ones include Marks and Spencer, Screwfix, Dyson, and Amazon.

If you click on the link in these emails, you'll be told that to receive your gift, you need to cover the cost of postage. You're asked to enter your personal details and card information.

The fraudster might then use your card details to sign you up to expensive subscription services. They could also use your details to work out who you bank with, then call you pretending to be from the bank's fraud team.

Remember - if it looks too good to be true, then it probably is! Be very wary of these sorts of messages. You can forward suspicious emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk). If you think your bank details have been compromised, please contact your bank and let them know as soon as possible. You can read more on this topic on [the Guardian website](#).

## Cryptocurrency – what it is and what the fraud risks are.

Cryptocurrency, or crypto, is digital money that exists only on the internet.

You can't hold it like cash, it only exists online. Just like you can send an email instantly, you can send cryptocurrency to anyone, anywhere in the world, without needing a bank.

People use it to make online purchases, invest, or send money across the world quickly. Unlike regular money, it isn't controlled by a bank or government.

Cryptocurrency transactions are recorded using blockchain technology which is a secure and transparent way to track transactions. It is like a public record book or digital notebook that keeps track of all transactions. Imagine a notebook where each page is a "block" that records transactions (who sent what to whom).

Once a page is full, you move to the next one, linking them together—this creates a "chain" of blocks. Once a page (block) is written and approved by many computers, it cannot be changed. Instead of being stored in one place (like a bank's database), it's shared across many computers.

Some people see cryptocurrency as the future of money as it may be profitable, while others think it's risky because prices go up and down a lot.



### Protecting cryptocurrency.

Cryptocurrency is stored in a hot or cold wallet. Hot wallets are software based, or online, and are accessed via the internet. Cold wallets are hardware based, or offline, and come in the form of a physical device, such as a USB stick. They are much safer from online attacks. It is generally advised to use cold wallets for long term or high value investments and to use hot wallets, which are quicker and more convenient to use, for short term low value investments.

A seed phrase is a sequence of random words that stores the data required to access or recover cryptocurrency in your hot or cold wallet. Seed phrases are generated to secure digital assets. Keep seed phrases safe and private as it can be used to regain access to a crypto wallet. It would be better to store it on good old fashioned paper hidden in your home than keep it in a note app online.



Cryptocurrency is designed to be secure, but there are still fraud risks.

### Crypto Scams

There are lots of fake investment platforms out there. They will promise high returns, take your money then disappear.







Phishing emails are also sent pretending to be from a genuine cryptocurrency company where a link in the email takes you to a fake website where log in details can be stolen.

Scammers may pretend to be famous people and ask for or endorse cryptocurrency.

Fake giveaways may also ask you to send cryptocurrency first to receive more in return.



### Avoiding Cryptocurrency Scams

-  If it looks too good to be true, it probably is.
-  Only download apps from official sources (Google Play, App Store, or verified websites).
-  Bookmark official websites and never click on random links.
-  Do your own research before investing.
-  Use a strong, unique password for each cryptocurrency account.
-  Avoid public WiFi when accessing cryptocurrency wallets (use a VPN if needed).

# 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 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.

## 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**

## 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.