JULY 2025

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud Newsletter for NHS staff. 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.

Fraudsters in Disguise

Welcome to the July 2025 edition of the Counter Fraud Newsletter, where we shine a spotlight on some of the latest tactics fraudsters are using to try and slip under the radar. A common thread through many of the issues we cover this month is deception by disguise – where criminals go to great lengths to appear legitimate, trusted, or familiar in order to manipulate their victims.

One example is the increasingly sophisticated use of Cyrillic characters in web addresses. At first glance, these can appear identical to trusted sites but lead to malicious phishing pages. Similarly, we explore the rise of CAPTCHA scams, where fake security checks are used to trick users into unwittingly giving fraudsters access to their own devices.

We're also seeing cases where phishing emails claiming to be from His Majesty's Courts and Tribunal Service are sent out pressuring recipients into making payments, sharing sensitive data or clicking on malicious links.

On the clinical side, we look at how you can help prevent imposter workers who pose as legitimate staff from entering NHS premises. These scams highlight just how important it is to verify ID and credentials for anyone working within the organisation.

Lastly, if you want to test your knowledge, you'll find details of a Scam Awareness Quiz towards the end of the newsletter.

In this issue, the message is clear: fraudsters are masters of disguise. By staying alert and informed, we can all play a part in unmasking fraud and protecting our NHS.

Look Closer: Cyrillic Letters in Web Addresses

A new twist on fake web addresses and emails is making it even harder to spot scams. Fraudsters are now using characters from the Cyrillic alphabet (used in languages such as Russian) to create web addresses that closely resemble trusted sites — a tactic known as "homograph spoofing."

For example, a fake version of the popular messaging platform WhatsApp was recently found using Cyrillic characters that look almost identical to the Latin ones used in English. The trick works because several lowercase Cyrillic letters are visually indistinguishable from Latin letters or numbers — giving scammers a new way to disguise malicious links.

This kind of mimicry isn't limited to social media platforms. Fake banking sites, email addresses, and login pages are all being crafted using these subtle substitutions, with the aim of catching users off guard.

To stay safe:

- Never click on links if you're unsure about the source.
- Bookmark trusted websites or type the address manually into your browser.
- Be cautious of online ads that claim to "improve" or "unlock" special features on well-known sites — these are often scams in disguise.

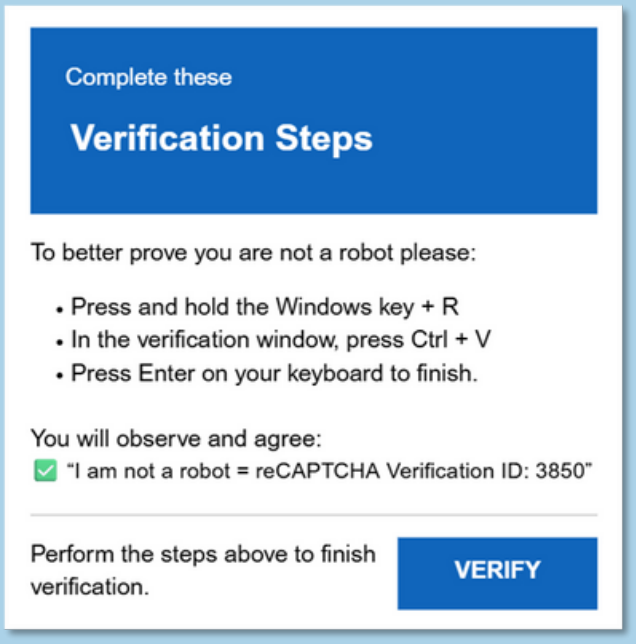
When it comes to fraud, if something feels off, it usually is. A careful second look could make all the difference. You can read more about this particular scam on the Computer Active Magazine website.

Fake CAPTCHA Scams

When you visit some websites they ask you to prove you're human and not a robot. These tests are called CAPTCHA and are designed to be easy for humans but difficult for machines. They often take the form of a series of photos where you're asked to select which of them show traffic lights / motorbikes / boats etc.

In the last few months malicious versions have been spotted, prompting warnings from various institutions – including the University of York.

Instead of asking you to pick the right photos, a dodgy CAPTCHA has been seen that asks you to follow a series of instructions to "prove you are not a robot". If you follow the steps directed, malicious software is installed onto your device, compromising your data and accounts.



Remember, genuine CAPTCHAs will not ask you to:

❌ Run commands on your device (such as by pressing Windows + R),

❌ Copy and paste content,

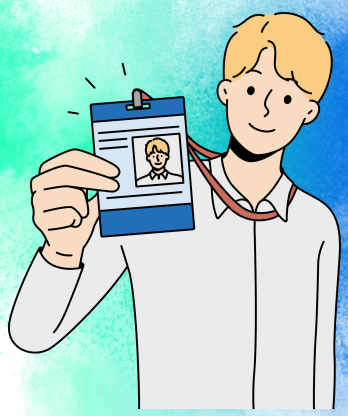
❌ Download attachments or follow links,

❌ Enter passwords.

If you are trying to access a website and a pop up like this appears, it's best to close the page. Use a search engine to find the genuine website or use the organisations app (if they have one).

If you are worried that you have interacted with a pop up like this on a work device, please contact your IT department for support.

Check that ID! Protecting Our Wards from Imposter Fraud



Did you know one of the simplest — and most effective — ways to protect patients, staff, and NHS resources is by checking ID?

Imposter fraud is when someone pretends to be an NHS employee, agency worker, or contractor to access wards, equipment, or sensitive information.

Fraudsters may pose as:

- Agency or locum staff.
- Substantive staff (in particular they may choose to impersonate maintenance / cleaning / IT / security staff due to their access privileges).
- Contractors or equipment suppliers.

Once inside, they could steal staff and patient's details or belongings, NHS equipment, or gain access to restricted areas and items such as controlled medication.

What to Watch Out For
🪪Individuals without a valid NHS or agency ID badge.
❌Someone refusing or making excuses not to show ID.
🤔Unexpected or unannounced visits from unfamiliar faces..
⌛Unknown individuals hovering around access points, potentially looking to tailgate through secure doors.

Remember: All legitimate NHS, agency, or contractor staff should carry valid photo ID and be happy to show it when asked.

Your Responsibilities

✓ Always ask to see an ID badge if you don't recognise someone on your ward.
✓ Check the details carefully — name, photo, expiry date, and organisation.
✓ If you're unsure, contact your manager or security team immediately.
✓ Never allow unauthorised persons into staff-only areas.

If You Suspect a Fraudster
Contact your security team and make sure to contact your Local Counter Fraud Specialist.

Fraud on Paper

Not all scams arrive by email or pop-up. Some come neatly presented on headed paper, complete with logos, official-sounding language, and even forged signatures. Fake documents — including invoices, contracts, letters, and credential packs — are still being used by fraudsters to try and gain trust and deceive NHS staff.

These documents may appear to come from known suppliers, agencies, or government bodies, and often include just enough detail to pass a quick glance. They may ask for urgent payments, confirm changes to bank details, encourage you to scan a QR code or direct you to visit a malicious website.

What makes these scams effective is the effort fraudsters put into making their documents look genuine — they disguise themselves in paperwork that appears trustworthy.

To protect yourself:

- Always verify changes to payment details or supplier information directly using known contact points — not those provided in the document.
- Be cautious of urgent or unexpected requests, especially those involving money or sensitive access.
- If something doesn't feel right, check before you act. You can contact your Local Counter Fraud Specialist for advice.

Spotting and Avoiding HMCTS Scams

In recent years, the prevalence and sophistication of scams have grown dramatically, with fraudsters frequently targeting individuals by impersonating trusted organisations. One concerning trend is the rise of HMCTS (His Majesty's Courts and Tribunals Service) scams. These scams prey on the authority and legitimacy of the justice system, often causing significant distress and financial loss for their victims.

HMCTS scams are fraudulent communications (such as emails, text messages, phone calls, or letters) that falsely claim to be from His Majesty's Courts and Tribunals Service. Scammers design these messages to trick recipients into revealing sensitive personal information, making payments, or clicking malicious links.

The scams can be emails, texts or phone calls and will claim you owe money for court fines, have missed a court date, have been fined for failing to attend jury service, have an outstanding warrant, or owe a fine.

The caller may pressure you to provide payment details immediately, often using intimidating or aggressive tactics.

Here are some telltale signs that a message or call claiming to be from HMCTS might be a scam:

- Unexpected contact: you receive unsolicited communication about a court case, jury service, or fine that you were not aware of.
- Requests for immediate payment: the message demands urgent payment to avoid arrest or legal action, often by bank transfer or gift cards.
- Requests for personal information: you are asked to provide sensitive details such as bank account numbers, National Insurance number, or passwords.
- Suspicious contact details: the message comes from a generic email address (e.g., Gmail, Hotmail) or phone number, rather than an official .gov.uk address or recognised government phone number.
- Unfamiliar links: you are prompted to click on a link that appears strange, overly long, or does not end in .gov.uk.

If you suspect you have received a scam communication claiming to be from HMCTS:

❌ Do not respond to the message or caller. Do not provide any personal or financial information, and never make a payment unless you are completely certain the contact is legitimate.

❌ Do not click on any links or open attachments. These could contain viruses or lead to phishing websites.

✅ Contact HMCTS directly using official channels. If you're in any doubt, use contact information found on the official government website to verify the legitimacy of the message or call.

🏦 Contact your bank immediately to report any unauthorised transactions or if you've shared your financial details.

Test Your Knowledge

To help us all be more aware, the BBC, in collaboration with the Open University, has devised a quiz aimed at gauging our ability to identify potential scams.

It's a great exercise to ensure we're all better prepared and more likely to recognise an attempt.

If you'd like to try the quiz, you can find it halfway down the page through the following link:

https://connect.open.ac.uk/science-technology-engineering-and-maths/scam-interceptors/

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.