AUDIT YORKSHIRE

November 2026

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.

International Fraud Awareness Week 2026

Spot it. Stop it. Protect the NHS.

To mark International Fraud Awareness Week 2026, the Counter Fraud Team has produced a series of short awareness videos to help staff avoid common fraud risks, recognise the warning signs, and know what to do if something does not feel right.

Each video is only a few minutes long and you do not need sound on your computer to play them.

Take a few minutes to explore the series and help protect the NHS from fraud.

Video Library

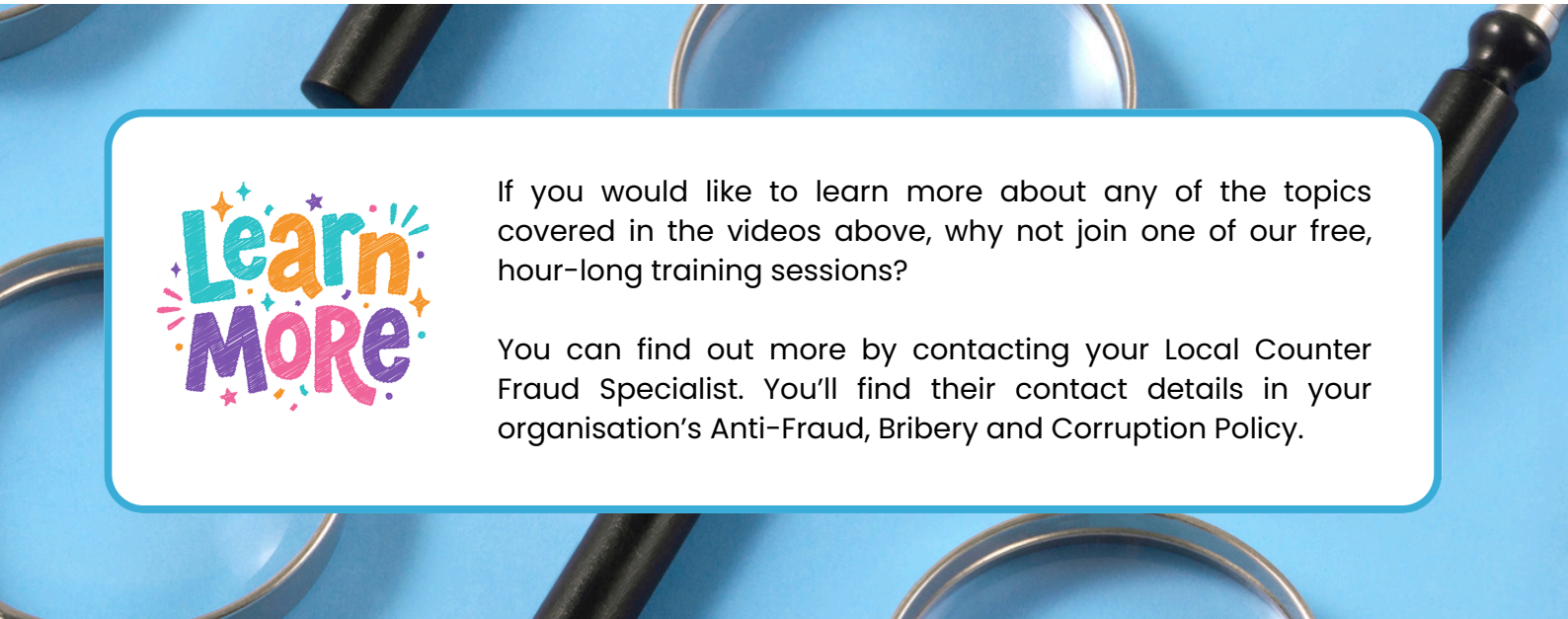
Could a fraudster steal your salary?

Phishing emails - would you take the bait?

Is your candidate really who they say they are? - Recruitment fraud

Right name, wrong person - imposter frauds

Second job - here's what you need to know.



If you would like to learn more about any of the topics covered in the videos above, why not join one of our free, hour-long training sessions?

You can find out more by contacting your Local Counter Fraud Specialist. You'll find their contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.



💷 £100 Energy Payment: Don’t Let Fraudsters Cash In

The Government has announced a £100 Household Energy Payment to help with rising energy costs. In England, households in Council Tax Bands A–D will be eligible, with payments due to begin from January 2027.

If you pay your Council Tax by Direct Debit, you won’t need to apply. Your council already has the details needed to make the payment automatically. Those who pay by another method will need to provide their details through arrangements made by their local council.

Unfortunately, schemes like this can provide the perfect opportunity for fraudsters. Be wary of unexpected texts, emails or phone calls telling you that you need to “claim” your £100, particularly if they ask you to follow a link or provide bank or personal details.

How to Stay Safe

- If you pay Council Tax by Direct Debit, you do not need to apply.
- If you pay another way, your local council will arrange how you can provide the necessary details.
- Don’t follow links in unexpected messages claiming to offer access to the payment.
- If you are unsure whether contact is genuine, go directly to your council’s official website or contact them using details you have independently verified, rather than those provided in a message.

“Cash Traps” at ATMs

Cash machine says “money dispensed” but there's no cash? It might not be a faulty ATM. Police are warning people across Yorkshire about “cash traps”, concealed devices fitted to cash machines by criminals.

Here's how the fraud works: you request cash as usual and your bank account is debited, but your money doesn't appear. Instead, the notes are caught by a hidden device fitted to the ATM. The offender returns later and retrieves the trapped cash.

Before withdrawing cash, have a quick look at the ATM. Police advise checking for:

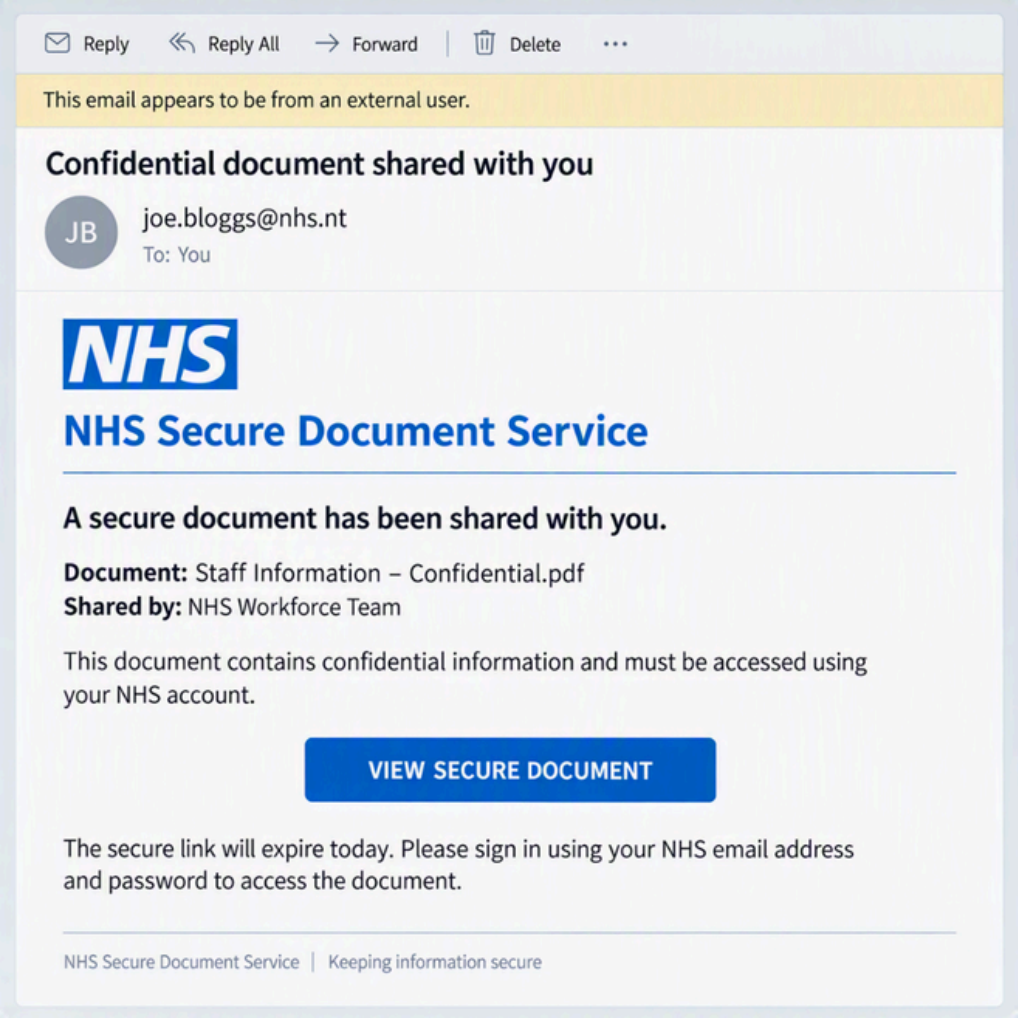
- Unusual attachments.
- Loose fittings.
- Signs that the machine may have been tampered with.

If your account is debited but the ATM doesn't give you your cash, contact your bank immediately, and report what has happened to Report Fraud or your local police force. A few seconds checking an ATM before you use it could save you from becoming a victim. You can read more on the BBC website.

🚩Can you spot the red flags?

Imagine this email lands in your inbox...

It's a busy Tuesday morning when you receive an email about a secure document:



At first glance, it seems reasonable. NHS staff regularly receive shared documents, the subject matter could be relevant, and asking you to sign in doesn't necessarily seem unusual.

But would you act on it?

Before reading on, see how many potential red flags you can identify.

✋ STOP! Have you spotted them all?



The Red Flags

🚩 **1. You weren't expecting the document**
You haven't been given any context about why it has been shared with you.

Ask yourself: Was I expecting this? Do I know who sent it? Is it out of character?

🚩 **2. It creates urgency**
The message tells you the link expires today. That may encourage you to click first and think later.

Ask yourself: Is there really a reason I need to deal with this immediately?

🚩 **3. It wants you to follow a link and sign in**
The aim of a credential-phishing email can be to take you to a convincing fake login page and persuade you to enter your details.

Ask yourself: Where is this link actually taking me?

🚩 **4. The email is from an unknown sender**
Look closely at the email address. It ends @nhs.nt rather than @nhs.net. There is also a yellow banner warning you that the message is from an external source.

Ask yourself: Does the email address look right? *But remember*, even if the sender's email address is correct that doesn't mean it's safe, as their email account may have been hacked.

🚩 **5. The request is plausible**
Perhaps the biggest warning is that there isn't anything obviously ridiculous about it. A good phishing email doesn't need terrible spelling or an unbelievable story. It just needs you to trust it long enough to click.

Ask yourself: Have you got a safe route to speak to the person and check if it's genuine, such as calling their usual work number or speaking over Teams?

What should you do?

🚫 STOP.
🔍 CHECK.
⏳ DON'T RUSH.

If you receive an unexpected request to open a link, access a document or provide login credentials, take a moment to verify that it is genuine using your organisation's established processes.



If you're suspicious, report it using your organisation's usual route for suspicious emails or fraud concerns. If you're not sure where to start, or need some advice on an email you've received, please contact your Local Counter Fraud Specialist.

REPORTING FRAUD CONCERNS

Fraud against 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 Counter Fraud 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 suspicious text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Report 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.