AUDIT YORKSHIRE

February 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.

Don't Get Caught by Payroll Phishing Scams

NHS staff continue to report fraudulent emails, designed to look like they have come from Payroll.

The emails usually contains a link directing staff to a website which has been deliberately crafted to mimic the payroll login page, prompting staff to enter their username and password.

If a staff member enters their details, the sender could:

- Log in to their account.
- Access personal, employment, and sensitive data.
- Change bank account details.
- Redirect salary payments.
- View or amend other Payroll records.

How to Protect Yourself

Emails from Payroll will never ask you to log in via a third-party link. If you want to check where a link will take you, hover your mouse over the link to reveal the real web address. We recommend that you access your payroll systems through your official routes – such as via your staff intranet or saved links.

If you receive a suspicious message

Do NOT click reply, click on links or enter log in details. Instead:

- Report it to the IT team or your Local Counter Fraud Specialist.
- Report it as spam (see page 3 for details on how to do this).
- Delete the email from your inbox and your deleted items folder.

If you have entered your details

Treat it as urgent:

- Change your password immediately.
- Inform IT and Counter Fraud.
- Monitor your payroll account for any unexpected changes.
- Please remain vigilant and report anything suspicious.

Phone Scam Alert: AI Voice Cloning Used to Set Up Fake Direct Debits

Criminals are using AI to clone people's voices and set up unauthorised direct debits over the phone. All they need is a few minutes of your speech, often gathered through fake "lifestyle survey" calls.

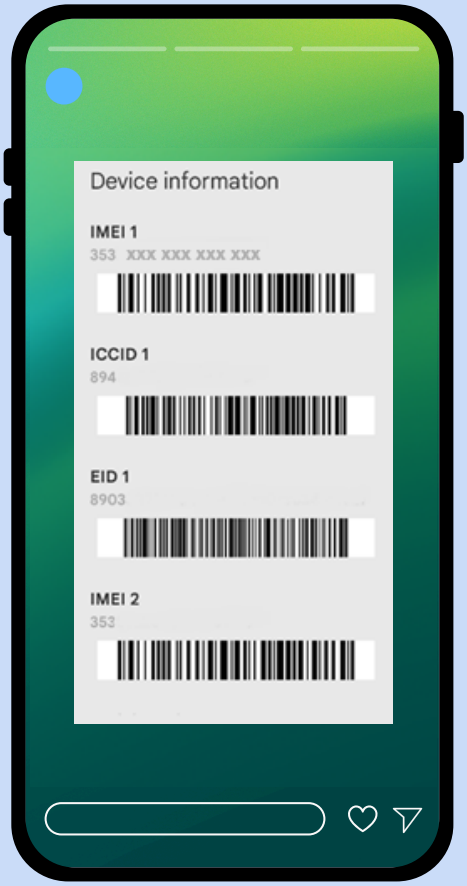
Once they have enough audio, they create a highly convincing copy of your voice and use it to contact banks and authorise payments without your knowledge.

The scam is particularly aimed at older and vulnerable people, and victims often don't realise money is leaving their accounts. The National Trading Standards team warns that scammers may also gather personal, health and financial details during these calls, making the fraud more damaging. You can read more about this scam on the Trading Standards website: Trading Standards Alert : AI Phone Scams

How to protect yourself:

- Don't answer calls if you don't recognise the number. If it's genuine, they'll leave a message.
- Be wary of people asking you to complete surveys over the phone.
- Don't share personal information over the phone, and don't be afraid to hang up.
- Regularly check bank statements, and contact the bank if anything looks wrong.
- Talk to your friends and family about this scam, so that they can spot it too.

Don't let phone thieves benefit - dial *#06#



Typing *#06# on your mobile phone might look like a random code, but it actually serves a very useful purpose.

When you enter *#06#, your phone instantly displays its IMEI number (International Mobile Equipment Identity). This is a unique 15-digit code that identifies your device, a bit like a serial number for your phone.

The IMEI is especially important if your phone is lost or stolen. Network providers can use it to block the handset from accessing mobile networks and if you provide it to the police, they can use this to block your handset making it much harder for criminals to use or resell it.

You don't need a signal or mobile credit to use *#06# — it works on almost all phones, including Android and iPhone. It's a good idea to note your IMEI down somewhere safe or take a screenshot and email it to yourself, so you have it if you ever need it.

A small code, but one that could save you a lot of hassle.

Quick Tip Corner

If you receive a suspicious email, how you report it varies depending on what sort of email account you are using.

The poster to the left explains how to report the suspect message in the correct way.

If you are reporting to spamreports@nhs.net, they will need you to forward the suspicious email "as an attachment".

This is to ensure they get the most information possible about the email. If you haven't forwarded an email as an attachment before, you'll find instructions on how to do this in the box below.

If you are struggling to forward an email as an attachment, please feel free to contact the Counter Fraud Team for support.

You can learn more about how to spot dodgy emails, texts and phone calls by signing up to our Cyber Enabled Fraud Prevention Masterclass.

We currently have a waiting list open for the next run of dates, which are yet to be announced. Contact your Local Counter Fraud Specialist for more information.

The sessions last 1 hour, run on Microsoft Teams, and contain lots of practical tips on how to spot, avoid, and report cyber scams.

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 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 suspect 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.