AUGUST 2025

AUDIT YORKSHIRE

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,

Fraud in the UK

The National Crime Agency (NCA) include fraud within their national strategic assessment, as it remains the most common offence in the UK - a recent independent review puts it at 43% of all crime in England and Wales.

Only 14% of cases were reported to Action Fraud or police. The reasons for not reporting varied - some people felt it was not necessary once their bank had refunded them, others didn't know how to report what had happened.

The majority of frauds are cyber-enabled, often involving social media, online marketplaces, or email scams. Investment and romance fraud remain high, while courier and payment diversion fraud still cause significant harm despite being below pre-pandemic levels.

Criminals are also adopting new tactics, including deepfake videos and voice cloning, to impersonate company leaders and trick victims — in one case, costing a business £20 million.

Fraud is not just an individual issue — public sector and business fraud remains a serious problem. In 2022–23, £3.5 billion of the UK's £39.8 billion tax gap was linked to criminal attacks. The cost-of-living crisis has also driven increases in refund and return fraud.

For the NHS, the risks are real. Criminals often exploit busy environments, target staff through phishing emails or fake payment requests, and use sophisticated tools to bypass security measures.

Stay alert to suspicious messages, especially those urging quick action or requesting sensitive information. If something doesn't feel right at work please report it to your Local Counter Fraud Specialist. Outside of work, you can report concerns to Action Fraud : https://www.actionfraud.police.uk/

Key Statistics

43% of crime in England and Wales is Fraud

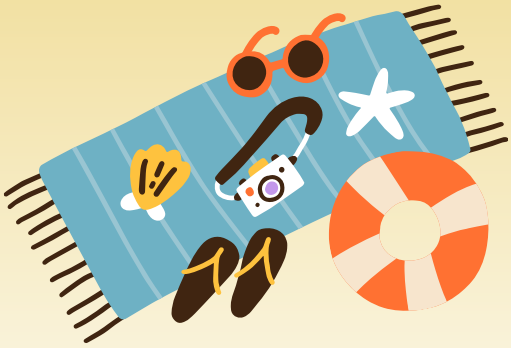
14% of fraud is reported to Action Fraud or police

3.2m estimated victims of fraud in England and Wales

9% of victims could give info on the fraudster*

*lack of knowledge about the fraudster is more common when fraud occurs online

Holiday & Ticket Scams on the Rise



With summer in full swing, many of us are busy booking getaways, weekend trips, or making plans for concerts and festivals. Sadly, fraudsters are just as busy – and they're getting more inventive in finding ways to trick people out of their money.

From fake villa rentals to bogus tickets for sold-out events, these scams can be convincing and costly.

Holiday scams often involve adverts for dream getaways – such as private holiday homes, bargain packages, or discounted flights – that turn out to be completely fake. Victims may only discover the truth when they arrive to find there's no booking at all.

Ticket scams target fans of high-demand events like concerts, theatre shows, or sports matches. Fraudsters sell tickets that are counterfeit, cloned, or entirely imaginary, leaving buyers stranded at the gates.

The growth of online marketplaces and social media has made it easy for scammers to appear legitimate. Many set up professional-looking websites and post fake glowing reviews to lure in victims. The result can be more than just a financial hit – often hundreds or thousands of pounds – but also the huge disappointment of ruined plans.

How to Protect Yourself

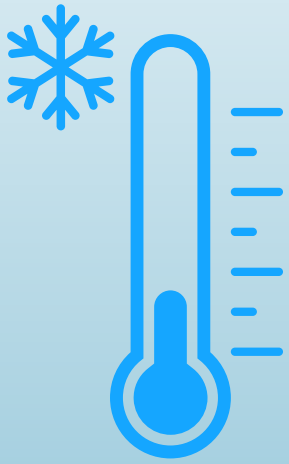
- Stick to trusted sellers – book holidays through reputable travel companies that are ABTA or ATOL members. For events, only buy tickets from official box offices or approved agents.
- Check the website carefully – fraudsters often copy well-known websites, changing only small details in the address.
- Be wary of "too good to be true" deals – especially if found through social media links or unfamiliar sites.
- Research sellers – check independent reviews and confirm the company exists before parting with money.
- Pay by credit card when possible – it can offer stronger protection if something goes wrong.
- Don't be rushed – scammers love to pressure you into a quick decision. Take a moment to think before buying.

Winter Fuel Payment scams

Winter Fuel Payment scams typically involve fraudsters sending out texts, emails, or even letters claiming to be from the UK government. These messages often state that you need to apply for a winter fuel payment, heating subsidy, or cold weather payment.

The messages usually contain a link to a fake version of the GOV.UK website, which asks for your personal and financial details. These phishing sites are designed to mimic the official GOV.UK branding, making them harder to spot. The goal of these scams is to steal your information and potentially drain your bank account.

Most people who are eligible do not need to apply for their payments. Details of who needs to apply can be found on the official Government website here - Winter Fuel Payment: Overview - GOV.UK



We are aware of text messages doing the rounds which say that you need to urgently complete a form or you will not receive the benefit. The messages put you under pressure by saying this needs to be done the same day or by the next day. The government will never ask for this information via text or email.

If you have input personal details into a link about Winter Fuel Payments, **please contact your bank immediately**. This can be done by calling 159 and stating the name of your bank. If you are asked to describe why you are calling, say "fraud" if you have noticed any unusual transactions from your account, or "account security breach" if you have shared details but not had any unexpected debits. Your bank will be able to advise further.

If you know anybody of state pension age who may be eligible for payments please make them aware of this type of scam.

Stay Safe on Public Wi-Fi

Free public Wi-Fi is widely available in places like cafés, hotels, train stations, and on public transport. Although it's convenient, it can also pose serious security risks—especially if you're accessing sensitive information.

A recent study by cybersecurity company NordVPN found:

- 70% of UK commuters use at least one device during their journey.
- 28% of UK commuters are using their travel time to do work related tasks.
- 13% of UK commuters take no steps to protect their data on public Wi-Fi.

Fraudsters can easily create hot-spots which are designed to look like legitimate free wi-fi networks. If you connect to one of these in error, your data and device can become compromised.

If you're accessing work systems or information on public Wi-Fi:

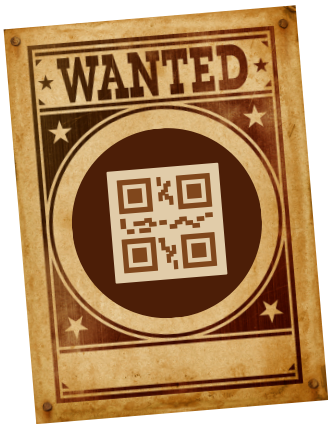
- Make sure you are following your organisation's policies and procedures. If in doubt, contact IT before connecting to an unknown network.
- Check that your work device has an approved VPN installed and make sure you know how to activate it. If you're unsure, contact your IT team.
- Avoid logging into confidential NHS systems or work platforms unless absolutely necessary. Consider whether it's appropriate to access that information in a public setting where someone could see it.

If you're using your personal devices:

- Avoid sensitive transactions: don't log into your online banking, personal email accounts, or health apps on public Wi-Fi unless you're using a VPN.
- Use a reputable VPN. Download a trusted VPN app from your phone or tablet's official app store for added protection.

In all circumstances:

- Add two-factor authentication to your accounts for extra protection.
- Make sure you install the latest security updates for your devices.
- Some devices automatically connect to any available Wi-Fi without asking permission. You can turn this feature off in the settings menu.
- Use strong passwords: create unique, complex passwords or use a password manager.
- Lock your device: use a password, PIN, or biometrics to protect your device



Quishing: QR Code Scams

We have reported on this type of scam in previous newsletters. We're publishing a reminder as Action Fraud have recently revealed that they received 784 reports about 'quishing' in the last financial year, and £3.5 million was lost to this type of scam.

Quishing is a form of phishing attack that uses fake QR codes to direct victims to malicious websites, steal credentials, or deliver malware. When a user scans a QR code, they are usually redirected to a website or prompted to download an app.

Attackers create a QR code that links to a malicious website or payload. These codes may be printed on stickers and placed over legitimate codes in public spaces, sent via email, posted on social media, or embedded in flyers and posters.

Many individuals are not in the habit of scrutinising QR codes before scanning, making them an attractive target for cyber attackers.

Be cautious when scanning QR codes in public spaces. Look out for QR codes that are on stickers or look like they've been tampered with.

Check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.

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.