APRIL 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.

What Does a Fraud Victim Look Like?

When we think about fraud victims, stereotypes often come to mind—perhaps someone elderly, naïve, or unfamiliar with technology. But the truth is far different; fraud victims can be anyone. Age, education, or experience does not offer immunity when fraudsters rely on manipulation and deceit.

Fraudsters are skilled at exploiting and manipulating human emotions - trust, fear, curiosity, sympathy or urgency to name a few. They create convincing stories, use fake identities, sophisticated technology and realistic scenarios designed to bypass your defences. Even the most cautious and informed individuals can become a victim of a scam under the right circumstances.

One important thing to remember is this: falling for a scam is not the victim's fault. Even using the word 'falling' (which I used to make this point), implies that somehow it is the victim's fault, and this perception is something that needs to change. Fraudsters are criminals, and the blame lies squarely with them.

Victim-blaming only adds to the shame and embarrassment people may already feel, which can prevent them from reporting the fraud or seeking support. This is also a contributing factor to why fraud is underreported.

If you or someone you know has been scammed, the most important step is to report it and seek help and advice. Fraudsters rely on silence and shame to continue their operations. By speaking up, you are taking back control and helping to protect others.

Remember, anyone can be a victim of fraud. What matters most is how we respond—by supporting those affected and working together to prevent future frauds.

Beware of Bailiff Scams

Bailiff scams are a growing concern, with fraudsters impersonating enforcement agents to extort money from unsuspecting individuals.

These scams often prey on fear and urgency, making victims believe they owe money and must pay immediately to avoid serious consequences.

A recent article was published by the BBC regarding this type of fraud. Scams: 'Fake bailiffs said they'd take my furniture' - BBC News

How Bailiff Scams Work

Scammers typically pose as legitimate bailiffs (also known as enforcement agents), claiming to collect debts such as unpaid fines, council tax, or other outstanding balances. They may contact victims via phone, email, or even by showing up at their doorstep, demanding immediate payment. Some may use fake ID badges, official-looking documents, or aggressive tactics to pressure individuals into paying.

Common Tactics Used

Unexpected Contact: If you weren't expecting a visit from a bailiff and haven't received prior official communication of an outstanding debt, be suspicious.

Fake Calls and Emails: Fraudsters contact victims, claiming to be from a legal authority, such as a county court, demanding payment.

·**Bogus Paperwork:** Fake court documents or enforcement notices are used to make the scam seem legitimate.

Upfront Payment Demands: Victims are told they must pay immediately, often via bank transfer or cash, to avoid legal action.

No Identification Genuine enforcement agents will always carry official ID and provide details of the debt they are collecting.

No Prior Notice: Before a bailiff visits, you should receive a written notice, court documents or other documentation regarding an owed debt.

Protecting Yourself from this Scam

⚠ As always, be suspicious of unsolicited contact.

🪪 Verify the bailiff's identity - ask for their name, company and certification number. You can cross check this information with the official register of enforcement agents: Certified Bailiff Register

📞 Report suspicious activity: if you suspect a scam please report it to Action Fraud. By reporting it, you can help to prevent other people from being targeted.

ℹ️ For further advice, you can find information on what you can do when visited by a bailiff on the GOV.UK website.

4 Text Scams to Watch Out For

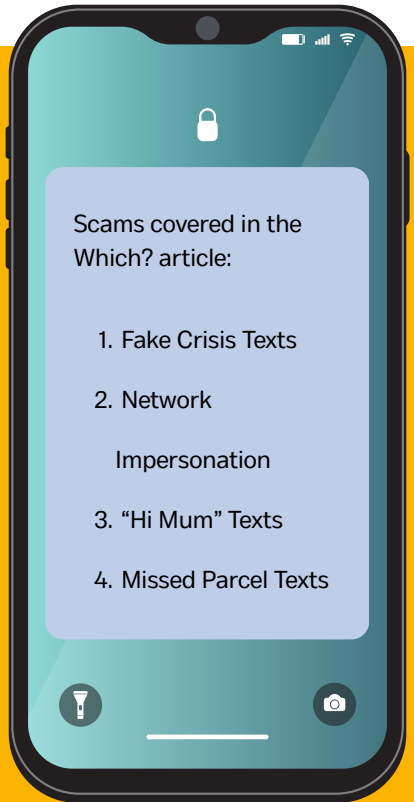
Consumer protection organisation, Which?, have put together a really helpful article on 4 common text scams that are doing the rounds.

We've covered many different types of scam texts in this newsletter over the years. Dodgy text messages remain popular with fraudsters as they can bombard thousands of phone numbers at once, and they can quickly change the content to match current events.

It's important to treat text messages with care, especially if they contain links or ask you to make phone calls, send a payment, or share your info.

You can report suspicious messages by forwarding them to 7726. Doing this allows phone companies to block dodgy phone numbers, to collect information of scammers, and to raise awareness to keep everyone safe.

Please take the time to read the article on the Which? website, where you'll find more information about the tactics being used.



Social Media Safety

You've just had the holiday of a lifetime, or have bought the most adorable puppy ever. Now you want to share pictures with everyone.

Social media has become a daily part of our lives, connecting us with friends, family, and communities across the globe. But as platforms grow, so do the number of scammers using them to trick users out of personal information and money.

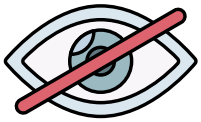
Here are a few tips for staying safe.

Watch Out for Imposters
Fraudsters create fake profiles that closely mimic real accounts. They could pretend to be one of your friends, a company or a charity. These profiles might message you, comment on a post with a link in it, or ask you for personal information.

If you are contacted by one of your friends on social media and something feels off, reach out to the person through another verified channel before responding.

Use Strong, Unique Passwords
Each social media account should have a different, strong password. Using a password manager can help you keep track of them.

Enabling two-factor authentication (2FA) adds an extra layer of security. Check what is available in the settings of your social media account.



Check Your Privacy Settings
Limit what you share publicly. Set your accounts to private if you're not comfortable with strangers viewing your content. Adjust who can send you messages, tag you, or view your friend list to reduce the chances of being targeted.

Social media should be a space for connection and creativity—not a trap for scammers. Staying alert, verifying information and staying secure can go a long way in protecting you from fraud.

Warning of Massive Increase in QR Scams

The BBC has reported that Organised Crime Groups (OCGs) are behind a sharp rise in scams linked to fraudulent QR codes. QR codes have been around for years, and became particularly popular during the Covid-19 pandemic. They're now a very common sight in public places, such as in car parks, restaurants and entertainment venues.

Unfortunately, fraudsters have identified that QR codes can lull people into a false sense of security. They look quite official, so can be misused by criminals trying to trick people into handing over their personal and financial information. Reports of QR fraud in 2024 have shot up to 14x the level reported in 2019.

Contactless payment hotspots (such as parking meters and restaurants) are common targets of criminals who stick their own QR codes over official signage and publicity materials.

Fraudulent and misleading codes have also been spotted on parcels, in emails and on television. Unfortunately, you can't tell if a code is dodgy until you've scanned it.

People who scan the malicious codes are directed to websites controlled by fraudsters and tricked into handing over data such as bank details, or into downloading malicious apps which steal their information and / or infect their device.

If you are being asked to use a QR code to make a payment, check carefully to see if there's any evidence of tampering. If possible, find a different way to pay.

Don't use QR codes to download apps - instead, go direct to your phone's app store and search for the correct app. Check reviews carefully before downloading apps. You can read more on the National Cyber Security Centre website.

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.