OCTOBER 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

FRAUD AT HOME SPECIAL

Last month we looked at the top fraud risks within the NHS. This month, we're going to take a closer look at the different types of fraud that you might encounter outside of work.

There are far more fraud methodologies than we can cover in this newsletter - if you want to learn about a fraud type that's not covered in this edition, you can find lots of information in the Little Book of Big Scams and in previous editions of the newsletter.

Fraud Facts

Fraud is the most common offence in England and Wales, accounting for roughly 40% of crime. Fraud is an everyday risk that can have a serious financial and emotional impact on individuals and families.

So, what exactly is fraud? Simply put, it's when someone misleads you for personal gain, usually by tricking you into giving them money, personal information, or access to your accounts. These schemes can target you using a variety of tools and tactics, such as fraudulent emails, dodgy text messages, phone calls, or even door-to-door scams.

By understanding the common tactics used by fraudsters, you can better protect yourself and your loved ones. In this edition, we'll provide practical tips and advice to help you recognise and avoid a range of fraud methodologies.

Take Five to Stop Fraud

The Take Five to Stop Fraud Campaign provides three key steps you can take in response to any suspected scam:

- **STOP:** Take a moment to stop and think before parting with your money or information. It could keep you safe.
- **CHALLENGE:** Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **PROTECT:** Contact your bank immediately if you think you've been scammed and report it to Action Fraud at actionfraud.police.uk or on 0300 123 2040.

You can find lots more advice on the Take Five to Stop Fraud website, and can test your scam-spotting skills with their online quiz.

Phishing Emails

Phishing emails are fake messages that look like they're from a legitimate source, such as a bank, a trusted company, or even someone you know.

The aim is to trick you into revealing sensitive information, like passwords, credit card numbers, or personal details. These emails often contain links that lead to fake websites or attachments that can install harmful software on your device.

Phishing is closely linked to fraud because it's a method used by scammers to trick you into making unnecessary payments, to gain access to your accounts or to steal your identity.

Once they have your details, they can commit financial fraud, such as taking money from your bank account or using your identity for loans or credit cards.

Some common scams carried out via phishing emails include:

- Messages claiming you've won a prize,
- Pretending to be from a recognised company e.g. TV Licencing, utility companies, streaming services, the DVLA, insurance providers, Microsoft / Apple / Google etc.
- Emails that pretend to be from your bank asking you to "verify" your account details.

These emails often create a sense of urgency to make you act quickly, without thinking. The fraudster may lift logos and branding, and create convincing phishing websites that look genuine.

Developments in Artificial Intelligence are making it easier for cyber criminals to write convincing phishing emails. Where we used to see a lot of spelling and grammar mistakes in dodgy emails, this is becoming less common.

Although phishing is often the first step in a fraud attempt, it isn't always about fraud. For example, they might be trying to spread viruses and malware by sending you infected documents or leading you onto dodgy websites.

Avoiding this Fraud Type

- **Be cautious with emails**: Don't open emails or click on links from unknown or unexpected senders, especially if the message looks suspicious.
- **Verify the sender:** If an email seems unusual, check the sender's address carefully. Scammers often use addresses that look similar to trusted sources but with small differences.
- **Look for signs of emotional manipulation**: is the email trying to panic you, create a sense of urgency, or offer you an exciting reward?
- **Avoid sharing personal information:** Never share personal or financial information via email, even if the request seems urgent or legitimate.
- **Check the website:** Before clicking on a link, hover over it to see where it leads. If in doubt go "the long way around". For example, if the email is claiming to be from Netflix, rather than clicking on the link go to the official Netflix website and find their customer services contact details. Get in touch with them and ask them to tell you if the email is genuine.
- **Use security software:** Keep your email and antivirus software up to date to block malicious messages.

SMS Fraud (Smishing)

Smishing is a type of scam where fraudsters send fake text messages (SMS) to trick you into giving them personal information, like passwords, bank details, or even access to your accounts.

The term "smishing" comes from combining "SMS" (short message service) and "phishing" — which we just looked at on the previous page.

The text message usually looks like it's from a trusted source, such as your bank, a delivery company, or a government agency. It often contains a link or phone number asking you to verify your account, update your details, make a payment, or track a delivery.

Once you click the link or call the number, scammers may steal your personal data or ask for payments.

Common smishing scams include messages pretending to be from your bank saying there's a problem with your account, or claiming you've won a prize and need to pay a fee to claim it.

Some fraudsters impersonate delivery services, notifying you of a missed delivery or insufficient postage having been paid. This scam methodology has been very popular over recent years, experiencing a particularly large surge in 2020 when more people were shopping online and therefore expecting numerous deliveries.

Although on the surface, a parcel delivery scam might look like it's only going to cost you £2-3 which is requested to cover redelivery, there's a more sinister plot behind the scenes.

When you fill in your name, address, and bank details, this gives the fraudster everything they need to target you in a follow up scam. For an example, see the Courier Fraud article on the next page.

Smishing fraudsters can make it harder to spot their attempts to defraud you by using "spoofing" software. This lets them disguise their phone number - they can replace it with a fake number, a number which belongs to the organisation they are impersonating, or with text - e.g. "HSBC Customer Services", "RoyalMail UK" etc.

It's also important to remember that you can't hover over links which appear in text messages, which you can do with suspected phishing emails. This makes it harder to identify where the link will take you.

Avoiding this Fraud Type

- **Be cautious of unexpected texts:** If you receive a text from an unfamiliar number or one claiming to be from a company but asking for personal information, be wary. Legitimate companies will rarely ask for sensitive details via text message.
- **Don't click on links in unsolicited messages:** Avoid clicking on links or attachments in unexpected messages, especially if they ask for personal or financial information.
- **Verify the sender:** If the message claims to be from your bank, delivery company, or another service, contact them directly using a known phone number or their official website. Don't reply to the suspicious message.
- **Use security features on your phone:** Enable spam filters and report suspicious texts to your mobile provider. Some providers allow you to forward scam texts to a designated number (e.g., 7726 in the UK).
- **Trust your instincts:** If something feels off, it probably is. Take a moment to think before acting on any message that asks for your personal details.

By staying vigilant and taking these precautions, you can reduce the risk of falling victim to smishing.

Courier Fraud

Courier fraud is a type of scam where criminals pose as bank officials, police officers, or government representatives to trick people into handing over money, bank cards, or personal information.

The fraudster typically contacts the victim by phone, claiming there's an urgent problem with their bank account or that they are helping with an investigation into fraud. They create a sense of panic to make the victim act quickly.

In one common version of the scam, the fraudster might tell the victim that their bank card has been compromised or that counterfeit money is being circulated through their account.

They will then instruct the victim to hand over their card, cash, or valuables to a courier, supposedly for "safe keeping" or "further investigation."

The fraudster may encourage the victim to head to their bank and to withdraw as much money as possible. They will coach the victim on what to say if the bank staff query why they are making such a large withdrawal. They may claim that staff in the bank are suspected of being involved in crime, and that this is why they must not tell them what the money is really being withdrawn for.

The key to courier fraud is the use of a fake courier, who comes to the victim's home to collect the items. In reality, the victim is handing over money or bank details directly to the criminals.

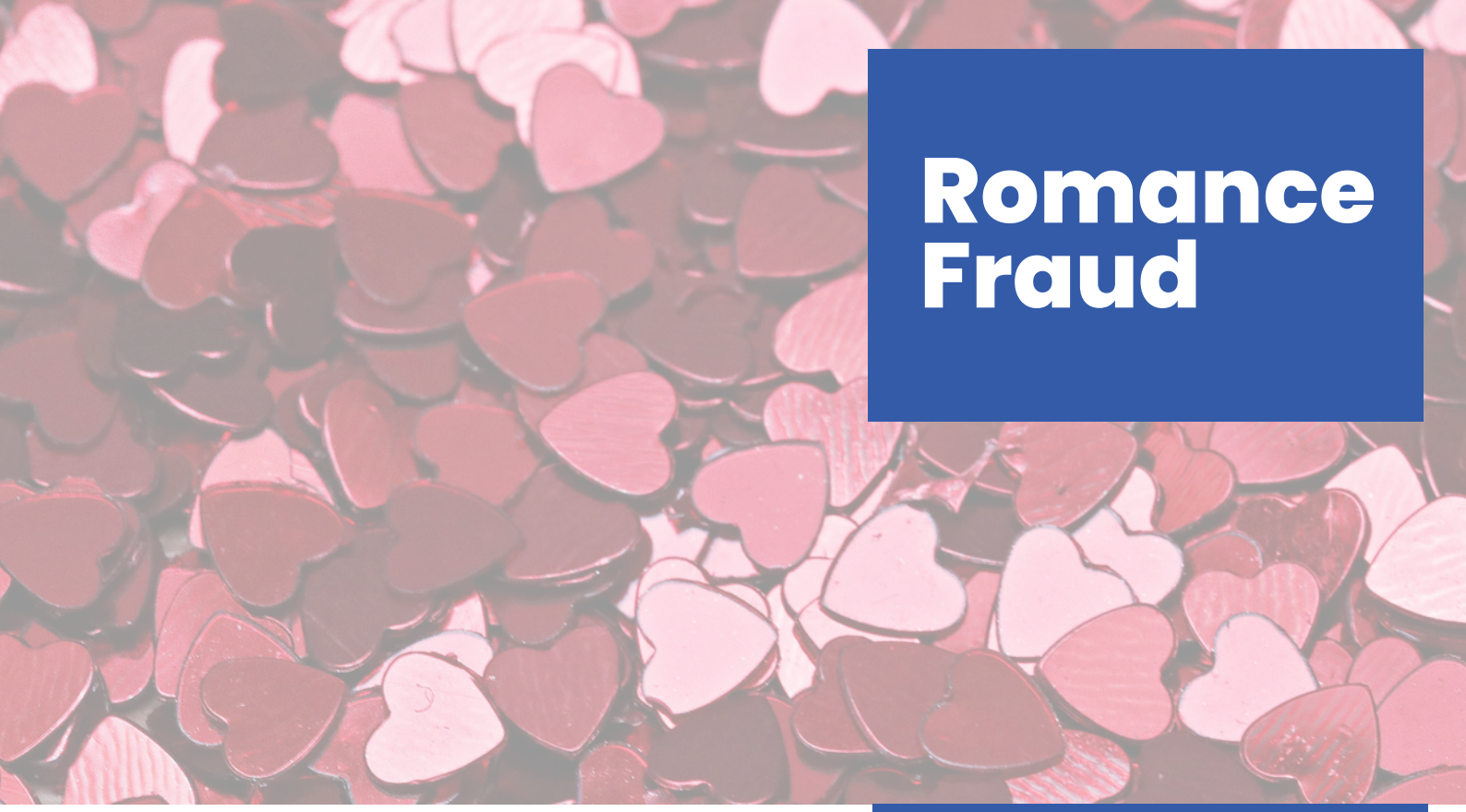
This type of fraud can target anyone. It may follow another type of fraud - for example, the victim may have accidentally handed their details to fraudsters as a result of a phishing email, online shopping scam, or dodgy text message. This gives the fraudster useful details such as who the person banks with, their name and address. They will quote these when making their call to the victim, lending themselves an air of authenticity.

It's important to remember that no legitimate bank, police officer, or government agency will ever ask for your card, PIN, to hand over cash via a courier, or to lie to your bank about the reasons for withdrawing money.

If you receive a suspicious call, hang up, wait 20 minutes, and contact your bank or the police on a known number to confirm the legitimacy of the request.

Avoiding this Fraud Type

- **Be cautious of unexpected calls**: If someone contacts you claiming to be from the police, your bank, or any government agency, be sceptical—especially if they ask for personal details or valuables.
- **Never give out your bank card or PIN:** No legitimate bank or official will ever ask for your PIN, card, or cash to be collected by a courier. If someone does, it's a scam.
- **Verify the caller:** If you're unsure, hang up and call back using a known number, like the one on your bank statement. Use a different phone line, or wait for 20 minutes, as fraudsters can sometimes stay connected to the line after you hang up. You might also be able to seek support from your bank via their website - many have a web chat function that you could use whilst you're waiting for the 20 minutes to pass by if you don't have a second phone available.
- **Never rush into decisions:** Fraudsters use urgency to pressure victims. Take your time and verify any claims before acting.
- **Report suspicious calls:** If you think you've been targeted, contact your bank immediately. If you have lost money, please report it to Action Fraud as well.



Romance Fraud

Romance fraud occurs when someone pretends to have a romantic interest in you to gain your trust and exploit you for financial gain. These scams often happen through online dating sites, social media platforms, or messaging apps.

The fraudster creates a fake profile, often using stolen pictures and false information, to appear attractive and trustworthy. They might take on the identity of a celebrity, or "catfish" by stealing photos posted by social media users.

The scam typically unfolds over weeks or even months, during which the fraudster builds an emotional connection with the victim.

Once trust is established, they fabricate stories of personal hardship or urgent financial needs—such as a medical emergency, legal troubles, or travel expenses, and ask for money.

Often, these requests escalate over time, with the scammer creating more elaborate excuses for needing funds.

In some recent cases, fraudsters have developed a new strategy. The fraudster claims they are unable to get onto their online bank, and asks if the victim can help them to move some money around. They send the victim log in details for what appears to be a genuine online banking platform.

The victim has actually logged into a fake online banking system which has been designed to make the fraudster look wealthy, and to build a sense of trust.

Later on, the scammer states that they are having further issues making payments. They ask for the victim to pay a bill on their behalf, stating they will repay them as soon as possible. The victim may feel this is low risk, because they have developed a relationship with the fraudster, and have seen firsthand that the person can easily afford to repay them.

Romance fraud can be particularly devastating because it exploits emotions, leaving victims not only financially harmed but also emotionally vulnerable.

Avoiding this Fraud Type

- **Be cautious with online relationships:** Take time to get to know someone and be wary of anyone who seems too eager to build a relationship quickly.
- **Look for red flags:** Be suspicious if they avoid meeting in person, refuse video calls, or always have excuses for why they can't visit.
- **Never send money:** No matter how convincing their story is, never transfer money or share personal financial information with someone you haven't met in person.
- **Check their profile:** Look for inconsistencies in their story, and reverse-search their profile pictures to see if they're stolen from elsewhere.
- **Talk to someone you trust:** If you're unsure, speak to a friend or family member about the situation before taking any action.

In the Press

BBC News - Romance Fraud up by 60%

BBC News - Cheshire Romance Fraud Victim Speaks Out After Losing £50k

Barclays Scam Bulletin - Men more likely to be victims of romance fraud, while women lose more money.

Online Shopping Fraud

In this scam, fraudsters list items like concert tickets, designer goods, or electronics at attractive prices, but the items don't actually exist. Once the victim makes a payment, they either receive nothing or a counterfeit product.

These scams often take place on social media - platforms such as Facebook Marketplace offer consumers a new way of shopping. It can be particularly attractive as items are less expensive than buying new, and there is a positive impact on the environment too.

Unfortunately, these platforms provide a rich hunting ground for fraudsters.

An article on Finder.com sets out some interesting statistics on online shopping scams:

- 80% of victims of online shopping scams are under the age of 50, with those in their 20s the most likely to be affected.
- Around two thirds (68%) of online shopping scams start on Facebook or Instagram.
- December is the worst month by far for online shopping scams. In December 2022, the reported losses to this fraud methodology were £50.7 million. In contrast, the month with the next highest loss was November 2022 which saw a total reported loss of £9 million.

You can read further details about this data on the Finder.com website.

December presents such a high risk because of the increase in online shopping that occurs from Black Friday until Christmas.

Fraudsters are also aware of key events and list fake tickets for sale in the run up to in-demand concerts by big artists like Oasis and Taylor Swift. These are particularly prevalent on social media, where the scammers may use hi-jacked / compromised accounts to lend some authenticity to their posts.

You may also come across fake shopping platforms - these are set up to mimic high value brands and are designed to steal your payment details. They tend to offer deals that are simply too good to be true. Fraudsters may promote these platforms on social media posts, turning commenting off so that other users can't alert each other to the risks.

Avoiding this Fraud Type

- **Shop from trusted websites:** Stick to well-known, reputable retailers and look for verified reviews (e.g. Trust Pilot) if you've never heard of the retailer before.
- **Look out for "too good to be true" offers:** Fraudsters will try to lure you in with deals that are designed to be so good that you are tempted to take a risk because you don't want to miss out. If a deal looks too good to be true, then it probably is!
- **Research the seller:** If using platforms such as eBay or Vinted, check the seller's reviews and ratings to ensure they are trustworthy. If you're using Facebook Marketplace be particularly wary as fraudsters use hijacked or throwaway accounts to operate.
- **Avoid paying by bank transfer:** Use secure payment methods like credit cards or services like PayPal, which offer protection in case of fraud. On Facebook Marketplace, don't pay in advance - instead opt for cash on collection and make sure you check the item works / is as described before parting with your money.
- **Be wary of high-pressure sales tactics:** Scammers often create a false sense of urgency to push you into making a quick decision.

By following these steps, you can better protect yourself from online shopping scams and avoid falling victim to fraud.

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.