JANUARY 2025

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our first Counter Fraud Newsletter of 2025. 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.

New Year, New You: Is Your Fraud Protection Up to Date?

The start of a new year is the perfect time for a fresh start—so why not give your fraud defences a quick tune-up? Taking just a few simple steps now could save you a lot of hassle down the line.

First things first, when was the last time you updated your passwords? If you're still using "Password123" or your pet's name, it's definitely time for a change. Choose something strong and unique, and don't reuse passwords across accounts. You can find some useful advice on how to set a good password on the National Cyber Security Centre website here: Three random words - NCSC.GOV.UK

Next, have you turned on multi-factor authentication (MFA) yet? It's like adding a second lock to your front door—an extra step, but one that makes your accounts far more secure. More information about MFA can be found on the Microsoft support pages: Microsoft MFA Support Pages

Finally, why not brush up on your fraud prevention knowledge? Whether it's spotting phishing scams or staying alert to new tricks, a little training can go a long way. If you work at one of the NHS organisations that Audit Yorkshire provides counter fraud services to, you can access our Fraud Prevention Masterclass programme. Get in touch to find out more.

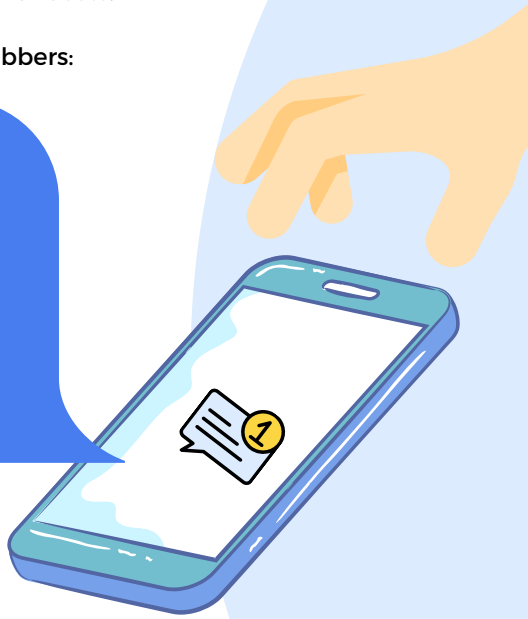
This year, let's all commit to keeping the NHS —and ourselves—a little safer. A few small actions now could make all the difference.

Phone thefts leading to fraud

The BBC have reported an increase of phone snatching on public transport. As if the stress of losing your actual phone isn't enough, thieves have also been draining bank accounts and taking out loans using information held on the phone. For some people, their whole life admin is contained in their handsets.

British Transport Police have listed the most common tactics used by phone grabbers:

- Stealing a phone from somebody who has fallen asleep.
- Lifting the phone from a seat or table when the owner is distracted.
- Targeting passengers on their phone near to the train doors – thieves snatch the phone and exit the train just as the doors are closing.



Here's how to protect yourself :

- Only have your phone out if you are using it. Otherwise, keep it out of sight.
- Use a zip pocket on your clothes or bag if you can, and avoid putting it in your back pockets as items are more likely to be stolen from there without you knowing about it.
- Be mindful of who is around you when on public transport, especially if you are near to the doors.
- Switch on your phone's tracker so that if it does go missing, you may be able to trace it.
- Add extra security to apps within your phone, such as your notes app if you use this to store log in details or sensitive information. Explore adding additional passwords, facial recognition etc. to help keep your information secure even if your phone is stolen.

You could also consider registering at "Immobilise". This is a register where you can log details of your valuables. Police may use this system to reunite found items with their owners. You can also download ownership certificates to help with insurance or police reports. You can find out more here - The National Property Register, for Phones, Gadgets, Bicycles & More...

Don't forget if you are a victim of a mobile phone theft, let your bank know too and keep an eye on your accounts for unusual activity. You can read the BBC article here - 'Train phone snatcher stole £21k from my bank apps' - BBC News

Scam Watch

Four Scams to Look Out for in 2025

As we start the new year, an article on This Is Money has highlighted four scams that they think we should all be wary of during 2025. You can read their full article by following this link: Fraud expert says these are the four scams to watch out for in 2025 | This is Money

Facebook Marketplace Scams

If you're considering some spring cleaning and want to declutter, you might be tempted to sell your items on Facebook Marketplace. Alternatively, you could be searching for a great deal on a specific item and come across an enticing listing.

However, beware of fraudulent sellers who may try to attract you with offers that seem too good to be true. They may request payment by bank transfer before breaking off contact, leaving you out of pocket and without what you hoped to buy.

To steer clear of such scams, make it a rule to pay only upon collection of the items, ensuring you receive exactly what you expected.

The same caution applies when dealing with buyers who ask you to ship items before payment; you might find that the promised payment never arrives.

Impersonation Scams

An “oldie but a baddie”, impersonation scams are certainly nothing new. Fraudsters pretend to be from a trusted organisation such as your bank, the police, a delivery company or utility provider. With the deadline for tax returns on the near horizon, you’re also likely to see fraudsters pretending to be from HMRC.

These scams are often done over email, text or phone call and involve the fraudster trying to persuade you to send them money. Please be very careful if you receive any emails or texts asking you to click on a link to make a payment. Always double check the sender’s details, and if in doubt, get in touch with the organisation directly on their official customer services number. If you suspect you’re on a phone call with a fraudster, hang up. Then, wait 15 minutes or use a different phone to call the organisation on their customer services number.

Crypto Currency Scams

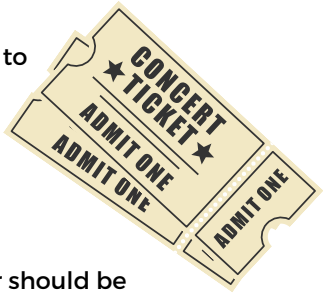
Following Donald Trump's election in the US in November, Bitcoin and other cryptocurrencies have surged in popularity, as more people choose to bet on the future of these tokens.

People need to be wary that even established cryptos like Bitcoin are still high risk investments, and so-called 'meme' coins rely solely on increasing their value by bringing in investors on the back of internet hype.

However, scammers also make use of this rush to buy, promoting fraudulent online broker platforms, often promising high returns. Some crypto scams see investors buy into an online currency, causing its value to rise before the scammers sell their own holdings and crash the market, leaving the victims with nothing.

It is essential that investors thoroughly research investments and seek advice from reputable sources before they buy - the Financial Conduct Agency has some useful information on their website.

Ticket Scams



Another classic scam, fraudsters are likely to continue trying to defraud fans by selling fake tickets to high-demand events. As many fans are willing to splash out to see their favourite acts or sports teams, criminals are keen to take advantage with fake listings.

To avoid falling victim to a scammer, those looking to buy tickets for these events need to make sure they only purchase tickets from verified sites – regardless of how good the offer is.

While there are legitimate ticket resale websites, individuals offering you tickets for a sold-out tour should be treated with caution.

Counter Fraud Specialist Rinsed of Loyalty Card Points!

It was December 22nd, my mind full of festive planning, when an email popped up in my inbox from my regular supermarket to tell me that I had spent £5 worth of points from their loyalty scheme that I'm signed up for. I knew I hadn't spent any points, so my first thought was that the email itself was a scam. It's a common tactic of fraudsters to send an email like that, encouraging you to click on the link hoping that you will then input your log in details into a dummy site. So, I ignored the email.

The following day and I received another email telling me that I had spent yet more points. In fact, I had apparently drained my balance to next-to-nothing. This second email made me realise that this was more than just phishing as the amount spent was pretty much what I knew I had saved up.

Time to phone the call centre. I checked the phone number on the loyalty scheme's website. This was the same as the one quoted on the emails, further lending to my suspicion that my points had been stolen rather than this being a phishing scam.

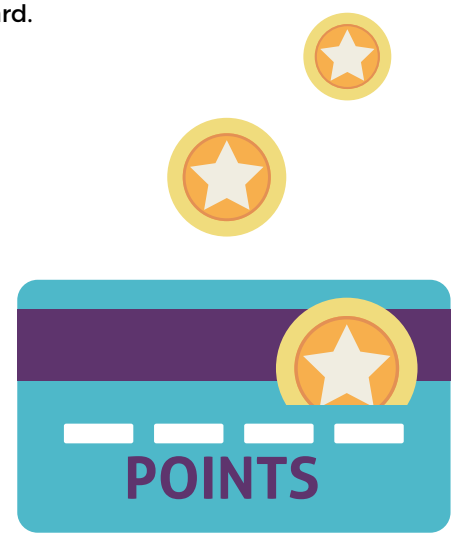
The helpline told me that my card had been used at local shops in London and Liverpool. I assured them that I hadn't left York in the last 24 hours and that my loyalty card was just mere inches away from me. Fortunately, the store sent me a replacement card and also refunded my stolen points.

How do loyalty card scams work?

This could have been a result of either my password being breached – from the store, or if I had used the same password elsewhere, from that site.

Although I didn't click on any links in an email, this could have been another way that a fraudster could have got my log in details. Once access has been gained into an online account, they can steal the points and take control of the account by locking the real account holder out.

Card cloning is also on the up. Only a few basic details are needed to duplicate a card.



How to protect yourself

- Treat card schemes like your bank account – they have a value after all.
- Use a strong password which you have not used for any other site.
- Use multi factor authentication if available.
- If you can sign up for email alerts for when points are spent, do so.
- Keep an eye on your card balance to spot unusual activity.
- If you receive letters or print out emails from the loyalty scheme, destroy them before disposing, making sure that your details and the card / membership number are not visible.
- Don't post pictures of your card on social media.

On the back of this, one of my New Year's resolutions is to set up a password manager to enable me to use strong, unique passwords for each site I access. I have also decided that I will not treat my loyalty cards like a pension pot. I'll use the points to treat myself rather than save them indefinitely.

Must go now, I have some shopping to do....

Action Fraud Booking.com Fraud Warning

If the cold snap has got you dreaming about summer holidays, you might have already started booking hotels and making travel plans.

Action Fraud have published a warning to holidaymakers to look out for a nasty scam. Fraudsters have managed to hack into the booking.com accounts of genuine hotels.

They then use the hotel's account to send in-app messages, emails and WhatsApp messages asking for a payment to be made, or for card details to be provided.

It can be very hard to spot these messages as they come from the hotel's real booking.com account - making them look authentic.

Avoiding this Scam

Full details on avoiding this scam can be found on the Action Fraud website: https://www.actionfraud.police.uk/alert/booking-com-alert

Our usual advice applies - if you get a message asking you to provide card details, or to make a payment, it's important to stop and do some checks.

The best approach would be to contact the hotel or Booking.com directly using their official customer services number.

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.