

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud newsletter for NHS staff. We hope that you find the contents useful. If you need any advice on fighting NHS fraud, you can find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.




IN THIS EDITION


- Sun, Sea and Scams
- Beware of Rental Scams
- Amazon Prime Membership Scams
- Ticket Tout Fraud
- It happened to me! A true story of fraudsters in action.
- How to Report Fraud Concerns

Sun, Sea, and Scams

We all look forward to our holidays, and we want them to be as relaxing and fun as possible. While you're out exploring new places, it's good to keep a few simple tips in mind to protect yourself from scams. Don't worry—taking these precautions can help you focus on enjoying your trip!



**SCAM
SAFE**



Before You Head Off:

- Make sure your card company has your current contact details. This way, they can reach you if needed.
- Have your card company's 24-hour telephone number saved, just in case.
- Only take the cards you plan to use and leave the rest safely at home.

While You're Abroad:

- **Keep Your Card Close:** When paying, especially at restaurants or bars, make sure your card stays in sight.
- Never share your PIN, not even with someone who claims to be from the police or your card company.
- Always cover your PIN when entering it.
- Whenever possible, check your bank transactions to catch any unusual activity early.

When You Get Home:

- Check your bank statements carefully. If you see any charges you don't recognise, contact your bank.

Remember, these tips are just a way to stay aware and prepared. The world is full of wonderful experiences, and a little caution can help ensure your holiday memories are nothing but happy ones. Safe travels!



Scam Trends

Beware of Rental Scams

Imagine you've just settled in front of the TV for the evening in the house that you have recently bought when the doorbell rings. It's a young couple, who are excited to have their first look round the house they have just paid £700 to secure a rental agreement on. This scenario happened to a neighbour of one of the Counter Fraud team.

We covered different property scams in our October 23 newsletter. This type of fraud is on the rise, particularly in relation to student digs as learners are looking for a good deal on accommodation before the start of the next University year. The rental market remains competitive, and fraudsters have sensed an opportunity to mislead prospective renters into making up front payments using details of other people's homes as bait.

If you, or your friends / family are looking to rent a property, please see our tips to stay safe below.

- Be wary of an underpriced property. Check out the going rates in the area you are looking in.
- Use a reputable letting agent or be particularly vigilant if responding to an advert on Facebook marketplace or similar.
- View the property with an agent or landlord before handing over cash.
- You can check ownership of a property. It does cost £3 but may be worth doing for reassurance. You can check here - Search for land and property information - GOV.UK (www.gov.uk)
- If you do need to make a payment, make sure you do this with a credit card as this offers more protection. Make sure that any money transferred is going to a bank account rather than a money transfer service. You can do this via an online sort code checker.
- Ask to see copies of documents such as safety certificates or a HMO licence, and be wary if this cannot be provided immediately.
- If you buy a new property, ask the estate agent to remove all details from the internet as soon as you have completed the purchase. Fraudsters will often use photos from homes recently advertised for sale in their fake adverts.



Amazon Prime Membership Scams

Amazon is the second largest company in the world and as such has a huge number of users across the UK and the world. Amazon is often a target for fraudsters, due to its size and success. Many users of Amazon subscribe to its Prime membership service.

Prime membership has recently become the target for numerous scams, including unexpected emails, calls, and texts from fraudsters that often refer to an unauthorised charge for membership or notice of membership expiration. The fraudster then asks the targeted person to 'verify' their account by providing personal or payment information.

Dodgy emails may include fake email attachments and claim there is an issue with your payment or that a costly additional fee needs to be paid. Unexpected calls may claim that an expensive order has been placed on your account and that you need to provide a "one time pass code" to verify your identity - handing this over lets the fraudster hijack your account and lock you out.

How to avoid being scammed:

Visit the Message Centre on Amazon.co.uk or on the Amazon App to review genuine emails and communication from Amazon. If you need to verify your Prime membership status, authorise payments or make any changes to your account or billing information, simply log into your Amazon account, and go to 'Your Account.'

Customer Service are available 24hrs a day, seven days a week and can engage in online chat and answer questions.

Protect yourself and others

If you receive communication that you think may not be genuine, report it at www.amazon.co.uk/reportascam

Source: Amazon Prime Communications via email to all Prime members. [Click here to visit Amazon's scam advice page.](#)

Beware of Ticket Tout Fraud

The excitement of securing tickets to a favourite concert, sports event, or theatre show can quickly turn into a nightmare due to the growing scam of ticket tout fraud. Fraudsters exploit the high demand for tickets by re-selling them at inflated prices or, worse, selling counterfeit tickets which are invalid when scanned at the event venue.

Scammers employ various tactics to sell these tickets:

- **Fake Websites:** Fraudsters create professional-looking websites that mimic legitimate ticket sellers.
- **Social Media Scams:** They use social media platforms to reach a broader audience, often posting about "extra tickets" at appealing prices.
- **Phishing Emails:** Fraudulent emails with links to counterfeit websites can trick unsuspecting buyers into sharing personal and financial information.

How to Buy Tickets Safely

To protect yourself from ticket tout fraud, here are our top tips:

- **Buy from official sources:** always purchase tickets directly from the event's official website, authorised ticket sellers, or reputable ticket marketplaces.
- **Be wary of secondary marketplaces:** if you need to use a secondary marketplace, ensure it offers a ticket guarantee, which most of the popular platforms offer.
- **Avoid suspicious offers:** be cautious of deals that seem too good to be true, especially those promoted on social media or through unsolicited emails.
- **Use secure payment methods:** consider using a credit card, which often offers further buyer protection, rather than bank transfers or debit cards.
- **Research the seller:** if buying from an individual or a less-known reseller, check their reviews and ratings. Be cautious of sellers with little to no transaction history.
- **Look for red flags:** misspellings, poor grammar and a lack of contact information on websites can be indicators of a scam.

For a recent example of a successful prosecution against ticket touts, check out this [National Trading Standards investigation](#) which also provides advice on how to stay safe from such scam.

It happened to me!

A member of staff shares their experience of being targeted by a fraudster.

"It was a Friday morning in my new job, and I was doing some final prep for a meeting that was due to start in 15 minutes, when I received a text saying that a transaction needed authorisation from a building society account, and if this wasn't me, to ring the number in the message. Now, I don't have a 'bank account' with this building society but I do have my mortgage with them, so I rang the number.

I spoke to a gentleman who was very convincing and willing to help, making me drop into conversation about other bank accounts and credit cards I had so that they could make sure that the 'scammers' hadn't accessed my other accounts.

Whilst all this is going on, I'm trying to cancel my meeting, explaining that I'm dealing with a personal fraud problem which shouldn't take too long to sort out! The stress of being caught out to fraud, being new to the job and having to cancel a meeting lowered my guard and stopped me from thinking straight.

Over the next 2 hours, he convinced me that he was able to see all my accounts as, because he worked for the fraud department of a major building society, some financial regulatory body gave him access to all my accounts. As a way of confirming my accounts, I gave them the size of my credit limits and over drafts.





He informed me that he could see some activities on my bank account that were pending to being blocked, and got me to check on my on-line app to see if they were visible or not - he said they weren't visible because he had stopped them from going through. He then said that he could see some similar activity on one of my credit cards.

He said he would cancel them, but in order for the cancellation to go through, he would need the last 3-digits on the back of my card, as well as the code that would come through to my phone from my credit card company (despite the messages saying not to give this code to anyone, even the police or bank staff!)

As said, I wasn't thinking straight during this, so very merrily submitted the information. Every now and then, he'd tell me to check my account to make sure nothing had gone through. Sometimes my app wouldn't open but it was OK, he was going to re-set it at his end - which he did.

Once he'd allegedly cancelled about £1,500 worth of transactions on that account, he moved onto my other credit card! I grew suspicious at this point and even called him out as a fraudster, at which point, he very calmly went through some pointers to reassure me and that he'd stop if I wanted, but that he could see these potential transactions that I couldn't. We carried on and 'cancelled' another £1,500 from that card at which point, now that 2 hours had passed, he said that all was done and hoped I enjoyed my bank holiday weekend.

Throughout this process, something just wasn't sitting correctly - I needed to speak to a human being. A quick call to my line manager to explain the situation and I was off into town to talk to a human to see if I'd actually spoken to the Fraud Department of the building society. On my walk, I ran through the morning's phone call: confirming the size of my accounts could flag how much they could take off me; they didn't need those codes for refunds but for buying; the resetting of my account is because they'd hacked into that and were changing details.

“Throughout this process, something just wasn't sitting correctly...”

In the building society, I explained what I'd done and showed them my phone. She very politely pointed out that she didn't think it was from them as sender of the message was a phone number, and messages from them would come up with their name. A conversation with another member of staff confirmed that it was a scam message, but that nothing had happened to my account.

Onto the bank next which confirmed that yes, there was £1,500 of activity that they had not authorised. I cancelled my card and proceeded to check my credit cards, both of which had to be done over the phone (one of which informed me that they required the 3-digit pin to confirm identity!).

I'd fortunately escaped losing money, but I'd cancelled all my cards on a bank holiday weekend and I needed to make up the best part of a day at work!

Months afterwards, I'm still checking my accounts (which I don't usually do) just to make sure. I also keep a close eye on my post to make sure I haven't 'signed up' for anything.”

Behind the scam - what really happened

The fraudster who targeted this staff member used the most effective tool in their arsenal by creating a sense of panic. As our friend describes above, they were busy at work and just wanted to get the problem sorted, which led to them making decisions they would not usually have made. The fraudster was very convincing, even offering to stop “helping” when he was challenged.



If you find yourself in a similar situation, remember these key points:

- Stop and think. Never feel pressured to respond immediately.
- Don't contact your bank / building society using the number provided in any text / email. Look up the number online or on the back of your bank card and use that.
- Wait 20 minutes or use a different phone just in case the fraudster is jamming the line.
- Whilst you may be asked for a pre agreed PIN, a bank will not send you a code to enter into your phone or read back to them.

If you have been a victim of fraud and would like to share your story, please drop us an email at yhs-tr.counterfraudyork@nhs.net. By sharing what has happened to you, you can help others to protect themselves.

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 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.

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**

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.