JUNE 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.

Don't Get Burnt by Fake Sun Cream!

As summer approaches, it's not just the sun we need to be wary of — fraudsters are ramping up their efforts too. One seasonal scam on the rise is the sale of counterfeit sun cream. These fake products can look convincing but leave you dangerously exposed. Here's what to watch for and how to protect yourself.

Be cautious of the following red flags:

- Too good to be true prices – unrealistic discounts online or at markets.
- Unknown sellers – stick to trusted shops and official brand websites.
- Packaging issues – check for spelling mistakes, poor quality logos, or worn packaging.
- Odd texture or smell – fake products often feel or smell different.
- Missing labels – a proper sun cream must display:
  - SPF rating
  - UVA logo (a circle with "UVA" inside)
  - Ingredients list
  - Expiry date

Using fake sun cream isn't just a waste of money — it is a serious health risk:
⚠️No Proper UV Protection – leaving you exposed to harmful UV rays.
⚠️Unknown Ingredients – potential for skin irritation or allergic reactions.
⚠️False Confidence – believing you're protected when you're not encourages unsafe sun exposure.

Your Quick Sun-Safety Checklist

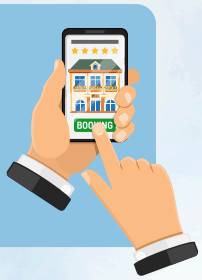
✓ Buy from trusted shops or official brand websites.
✓ Look for the correct SPF and UVA logo.
✓ Check packaging carefully for errors.
✓ Ensure the texture and scent seem normal.
✓ Report anything suspicious to Trading Standards via Citizens Advice (0808 223 1133).

Enjoy the sunshine — safely and sensibly. Don't let counterfeiters ruin your summer! Also please read the NHS advice on sunscreen and sun safety: Sunscreen and sun safety - NHS

Fraudsters Don't Take a Holiday – Stay Scam-Savvy This Summer!

Sunshine, holidays and festivals might be on the cards – but sadly, so are summer scams. Don't let fraudsters ruin your plans. Check out the list below to stay scam-savvy and keep your money safe this summer.

Be Careful with Holiday Accommodation Listings



Fraudsters often advertise fake holiday cottages or lodges, especially in UK hotspots.

Book through trusted booking sites or verify private listings independently before paying. Bank transfer requests are a major red flag.

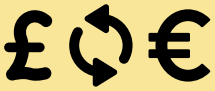
Avoid Fake Festival Tickets

Summer's festival season is a magnet for scammers selling non-existent tickets to sold-out events like Glastonbury, Latitude, or Boardmasters, to name a few.

Always buy tickets from official vendors – and never pay strangers via bank transfer, PayPal Friends & Family, or gift cards.

Watch Out for Holiday Money Scams

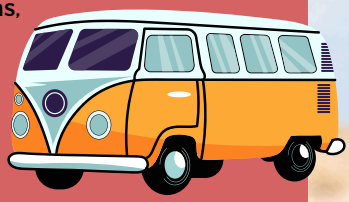
Fraudsters create fake currency exchange websites offering brilliant exchange rates for holiday money. Victims pay in advance – and the cash never arrives.



Use well-known, regulated providers for your travel money.

Beware of Fake Caravan, Campervan and Motorhome Sales

With the boom in staycations and road trips, scammers are advertising bargain caravans, campervans, and motorhomes online – especially on Facebook Marketplace and classified sites. Victims pay deposits or full amounts for vehicles that don't exist.



Avoid buying vehicles you haven't seen in person. Use secure payment methods and check seller reviews where possible.

Look Out for Fake Event or Attraction Vouchers

Scammers often promote bogus discount vouchers or free passes for popular UK attractions like Alton Towers, Thorpe Park, or Legoland during the summer holidays. Victims are tricked into clicking dodgy links or handing over personal details.

Verify offers directly with the official attraction website before clicking, sharing, or buying anything.

Scammers don't take a summer break – stay switched on while you switch off. Have a fantastic, safe and fraud-free summer!

Phishing Email Targeting NHS.net accounts

The Counter Fraud Team has been made aware of an email which has been sent to some NHS staff on their work email accounts. It claims that the nhs.net email data has been leaked and that the person's device is infected with spyware.

The email claims that the sender has managed to create compromising videos of the recipient, which they will circulate to the person's friends, family and colleagues within 48 hours.

The scammer states this can be avoided if the recipient transfers 1550$ (USD) of bitcoin to the sender's bitcoin wallet.

This type of phishing email is typically referred to as "sextortion". Often the sender will drop basic information into the email (such as that you have an @nhs.net account) as "proof" that they have compromised your account or device. In reality, this is basic information that they take from your email address.

These emails often contain numerous threats and information designed to make the recipient feel panicked into sending payment.

How to stay safe:

- If you receive an email of this nature, please forward it as an attachment to spamreports@nhs.net.
- Do not reply to the email as this may encourage the sender to continue contacting you.
- If you need any advice about suspicious emails received at work, please speak to your Local Counter Fraud Specialist who will be happy to assist.

Remote Access Scams

A remote access scam can lead to identity theft, financial loss and unauthorised access to your sensitive information.

These scams typically begin with a phone call, email, or pop-up message from someone claiming to be a representative of a trusted company, such as your bank or a tech support provider. They may tell you that your computer has a virus, your account has been compromised, or there's suspicious activity that needs urgent attention.

To "fix" the problem, they'll ask you to install software or grant remote access to your device. Once connected, the scammer can steal personal and financial information, install malware or ransomware, lock you out of your own system or trick you into paying for fake services

Common Tactics Used by Scammers

- Impersonating legitimate companies: they spoof caller IDs and use logos or email addresses that look real.
- Urgency and fear: scammers pressure you to act quickly, claiming your money or data is at immediate risk.
- Tech jargon: they use technical language to appear credible and confuse the victim.
- Fake screens or errors: some scams involve fake security alerts or error messages to convince you something is wrong.

How to Protect Yourself

- Never allow remote access to your device unless you are 100% certain of who you are dealing with.
- Don't trust unsolicited calls or messages. Reputable companies will not reach out unexpectedly to fix an issue.
- Verify independently. If you're unsure, hang up and contact the company directly through official channels.
- Install security software and keep your system up to date.

If You Think You've Been Scammed

1. Disconnect your device from the internet immediately.
2. Run a full security scan using reputable antivirus software.
3. Change your passwords, especially for banking, email, and sensitive accounts.
4. Notify your bank or credit card company if you've shared financial information.

Remote access scams rely on fear and trust. By staying calm, verifying claims, and refusing to give control of your device to strangers, you can protect yourself from falling victim.

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.