

Counter Fraud Newsletter

Welcome to this month's edition of the Counter Fraud Newsletter for NHS staff. You will find contact details for your Local Counter Fraud Specialist on the last page.

Hotel Booking Scam Warning

BBC Radio 4's Scam Secrets has recently highlighted holiday booking scams. We've covered this before, but with the holiday season approaching, this scam is doing the rounds again.

Fraudsters are using a convincing tactic that lets them send messages through the Booking.com platform itself. This can happen when a hotel's Booking.com account is hacked, giving criminals access to customer details and booking information.



Using that information, they contact customers and ask for urgent payment. They often say the booking will be cancelled unless the full amount is paid straight away.

Because the message comes through a genuine booking system, it can look completely legitimate. If you would like to read more, the full BBC Radio 4 article is available here: [BBC Radio 4 - Scam Secrets - Booking a holiday? Watch out for this hard-to-spot scam](#)

Avoiding the Scam

If you receive an unexpected request for full payment, check your original booking confirmation first. If the payment request does not match the agreed terms, contact the hotel directly using a trusted phone number.

Do not reply to the message or email the hotel back through the same channel, as their account may have been compromised.

Be cautious if the conversation suddenly moves to WhatsApp or another messaging app.

Take your time. Messages that create panic are designed to make you rush. If you are unsure, speak to the hotel directly before making any payment.

There has been an increasing number of cases where individuals have posed as legitimate healthcare workers, using false or shared identities to gain access to NHS wards.

In one case, a man worked for weeks as an agency nurse using another person's identity, wearing an NHS badge and carrying out clinical duties despite not being authorised to do so.



Agencies carry out identity checks when someone joins them, but they cannot guarantee that the same person attends the shift. Local NHS teams therefore have responsibility for confirming that the individual who turns up is the person booked to work.



Key warning signs for NHS staff

Be alert to agency / bank staff who:

- Avoid showing ID or wear their badge inconsistently.
- Give vague answers about their role, ward or employer.
- Resist supervision or scrutiny.
- Appear unfamiliar with basic procedures expected for their role.



What NHS staff must do

- Always check ID – badges should match the individual and role.
- Challenge politely but firmly if something doesn't feel right.
- Report concerns early to a line manager, Security or Local Counter Fraud Specialist.
- Do not assume someone else has already carried out checks.

Even small concerns can prevent serious risk if acted on early. Remember: agency staff and temporary workers must meet the same identity and safeguarding standards as substantive staff.



Protecting Yourself from Age Verification Fraud

Age verification plays an important role in keeping people safe, both online and offline. Whether buying alcohol, gambling, or accessing age-restricted services, businesses must ensure individuals are old enough.

As more services move online, digital age verification is increasingly common. Legitimate services may ask you to upload a photo of your ID, confirm your identity through your bank, or complete a one-off check with an approved third party.

However, criminals have recognised how familiar these checks have become—and are exploiting this trust. Fraudsters are creating convincing websites that appear to be legitimate age-verification portals but are designed to steal personal information.

If criminals obtain your documents, they may commit identity theft, apply for credit in your name, access financial accounts, or sell your details on the dark web. Many victims are unaware until the information has already been misused.



Red Flags

- Being redirected to a verification page unexpectedly—especially where it isn't normally required—is a warning sign.
- Genuine services usually request minimal information. Be cautious if you're asked for your National Insurance number, full bank details, or multiple documents.
- Legitimate services should clearly display:
 - Company name
 - Registered address
 - Privacy policy
 - Contact details
 - Missing or vague information is a red flag.
- Fake sites often use web addresses that closely resemble real brands but include spelling errors, extra characters, or unusual domain endings.
- Trusted UK services will reference GDPR compliance or recognised certification standards—fraudulent sites often do not.

How to Stay Safe

If you're unsure whether a request is genuine, go directly to the official website rather than clicking on links.

If you believe you've encountered—or shared information with—a fraudulent site, report it to:

- Report Fraud (to report scams)
- Your bank (if financial details were shared)
- The organisation being impersonated

Reporting quickly can help limit any potential damage.



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 **Report 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 Counter Fraud 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.