APRIL 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful. If you need any advice on fighting NHS fraud, you can find our contact details on the final page.

IN THIS EDITION

The National Fraud Initiative (NFI) Explained

The NFI was first introduced over 20 years ago. Every 2 years, it compares data held by public sector and private sector organisations. It is mandatory for the NHS to participate and the exercise is coordinated by the Home Office. You might remember seeing the NFI mentioned in emails from your Communications team, the Counter Fraud Newsletter, your organisation’s intranet or website, and on your payslip.

Staff payroll information is included in the exercise. If you have a second job, information from your other employer might also be included. If you claim benefits, receive a pension, have a current record with the Home Office or are the Director of a Company information from these records will also be included.

Payroll matches identify where employees have another job elsewhere. Checks are made to identify any potential issues, such as individuals working elsewhere during NHS sick leave or NHS working hours.

Declarations of Secondary Employment are also checked to ensure that these have been completed, where required.

If you have a second job, please remember to declare it to your manager and complete any forms which your organisation requires.

If you are off sick from one job but your GP says that you are fit to work in the second job, please ensure that your fit notes reflect this.

NFI Case Study

A full-time employee at Birmingham City Council was identified as having a job on the bank of a nearby NHS Trust, to pick up shifts “as and when” required.

The NFI highlighted that the salary for their “casual” NHS role was much higher than would normally be expected.

Enquiries revealed that the employee was actually receiving full time salaries from both organisations!

The investigation found that the individual was working from home, which facilitated their claim to be doing both roles at the same time.

The individual had also worked for one organisation whilst claiming to be unfit for work at the other.

The employee was dismissed from both roles. Recovery of the salary paid by the Council, which was in excess of £16,500, is being pursued.

Scam Trends

Disney+ Scam

Which? have received reports of emails pretending to be from Disney+.

One is offering a subscription of £3 for 12 months access. This offer for a 98% saving is blatantly too good to be true, but the emails are quite convincing as they use the right logos and branding, and advertise the latest TV shows.

Another email which has recently been received advises the 'customer' (without giving the customer's name – another red flag) that their membership has expired and to click on a link to extend their membership and get 90 days for free.

If anybody clicks on the link, they are taken to a fake website and asked to input their personal and bank details.

Most subscriptions will simply keep rolling until you decide to pause or cancel, so be wary of emails asking you to renew. For any streaming channels that you are signed up for, make a note of when your membership expires (if applicable) and renew any subscriptions on the service's website, not from an email link.

If you are worried about your account, please contact the organisation's customer services directly on an established contact route.

Your best bet is to either go to their website and find a web-chat or phone number.

You can also look for their verified social media accounts and reach out on there, but please be wary of copy cats who impersonate major brands on these platforms.

Beware of Dodgy "Buyers" on Social Media

You may have seen the recent BBC news article about a fraudster who bought a laptop advertised on Facebook Marketplace. He brazenly sat in the seller's house and showed himself transferring money on what later transpired to be a fake banking app. If you missed the article, you can read it here - 'Facebook scammer tricked his way into our home' - BBC News

Facebook, and other online selling platforms, are popular places to snap up a bargain. Unfortunately, they are also used by scammers to take advantage of shoppers.

Here's how to stay one step ahead.

- If you are selling an item, don't rely on being shown a transfer going through a banking app on the buyer's device. Check that the payment has been received into your own account before you release the goods.
- If the payment is in cash, check that you haven't been given counterfeit notes.
- If you are buying, make sure that the product or service actually exists.
- Be wary that goods being sold to you may be stolen. If you suspect this, ask for proof of purchase so that you know the item does belong to the seller.
- If the seller asks you to send your personal information to them, be wary and think what they could do with it.
- If the deal looks too good to be true, it may be an indicator that the product is stolen or doesn't exist.
- Don't be pressured to make a decision quickly. Sellers claiming they have lots of interested parties may be a genuine sales tactic, but also may be used to make you buy without thinking it through (and missing warning signs that it's a scam).
- Check the seller's profile. If it looks new with little information, it could be a sign that it has been set up as a throwaway account just to commit fraud. However, please bear in mind that some fraudsters will use hacked accounts to disguise their identity.

Cyber Scams

Insta-scams

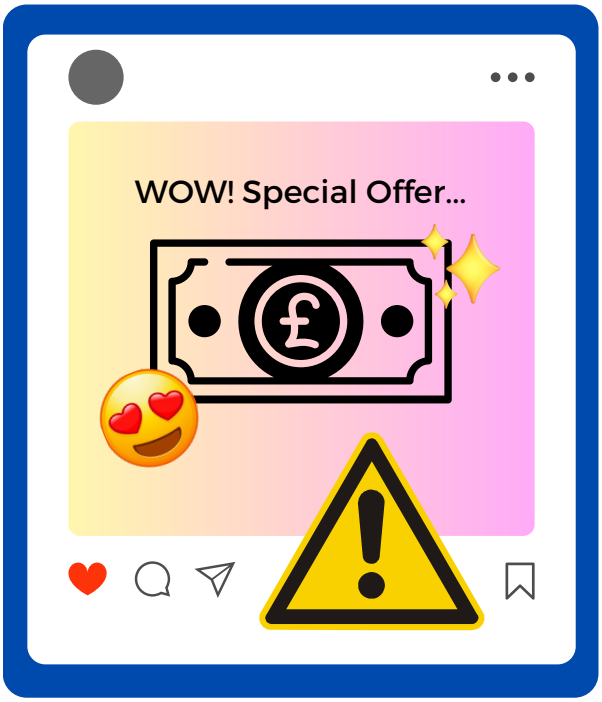
We've all been there - the work day is over, there's nothing good on TV, and you're scrolling through reel after reel on Instagram to unwind. However, there are fraudsters lurking in the shadows, using the platform for malicious purposes.

The fraudsters may use hijacked accounts, impersonate celebrities or use shiny, well-designed materials to front up their scams - making it hard to spot them from genuine users and services.

Common Instagram scams include:

- Fake prize draws, giveaways and raffles.
- False "celebrity endorsements" for dodgy investment schemes, particularly crypto-currency "opportunities".
- Romance scams.
- Impersonating friends / family to ask for money.

In March 2024 fraudsters even advertised bank notes for sale, which they claimed had "all expected security features" and "could be used anywhere".



The bank notes being offered would have been forgeries, but it's not clear that they actually existed in the first place. Any customer who did not receive their fake bank notes would be unlikely to go to the authorities to report the issue!

Please be aware of scams on social media sites, and look at what you see critically and objectively. If a £20 note is worth £20, why would anyone "sell" it for less? If you do see criminal or illegal posts on Instagram, please flag them via their reporting service. You can get more information on the Instagram support pages by clicking here.

Keeping your social media safe

Fraudsters like to hijack genuine social media accounts - it gives them an identity to hide behind and also allows them to target the victim's friends and family with various scams. So, how can you keep your account safe? Here are some top tips:

- Use strong passwords that cannot be easily guessed. In particular, don't use any personal information such as names of pets / loved ones, or favourite sports teams that might be picked out on social media. Even if your privacy settings are good, a friend or family member could be less cautious and give the information away without realising it! Use three unconnected words plus numbers and symbols for the best protection.

- Use multi-factor authentication / 2 factor authentication where it is available. That way, if someone does get hold of your password they won't be able to log in without a second layer of proof (usually a one-time password which is sent to your phone, or a biometric log in like a finger print scan).

- Be wary of phishing emails, texts, and messages. These are often used to hijack accounts by asking you to log in to a dummy website which is designed to look like a site or service that you trust. Don't click on links in emails, texts or DMs unless you are happy that they are genuine.

- Check your account logs to look for any suspicious or unfamiliar log in locations or devices. Many social media platforms and email providers give you the option to review recent activity. If you notice anything unusual, choose the option to log out of all devices, then change your password immediately. Read more on the Surrey Police Fraud Newsletter.

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.