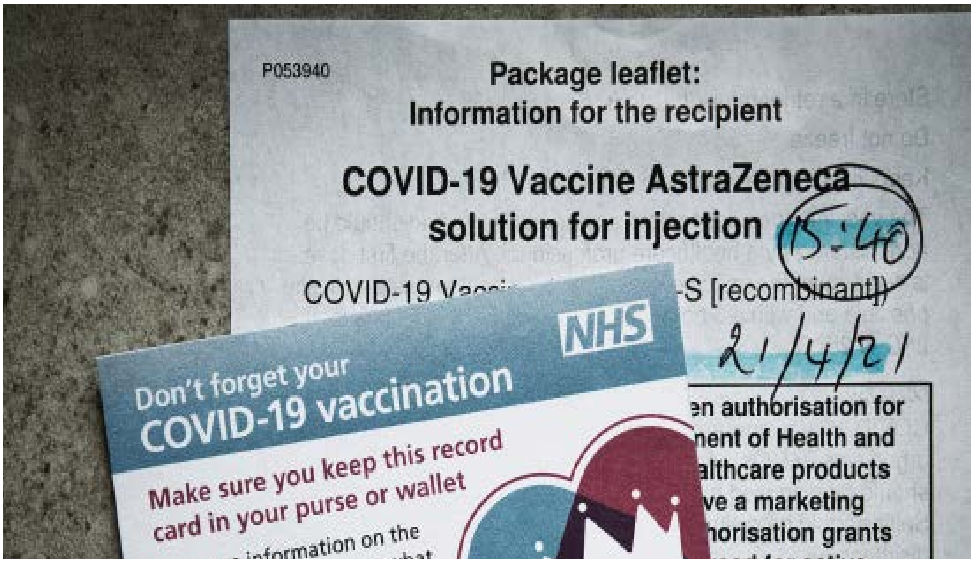
miaa

# Talking Fraud

Autumn 2024


P053940
Package leaflet:
Information for the recipient
COVID-19 Vaccine AstraZeneca
solution for injection
15:40
21/4/21
NHS
Don't forget your
COVID-19 vaccination
Make sure you keep this record
card in your purse or wallet

## Administrator sent to prison for creating fake Covid-19 certificates

A medical centre administrator, Marzena Pawlowska, was found guilty of creating over 100 fraudulent Covid-19 vaccination records. Pawlowska charged £300 for a single fake vaccination record and £500 for two, allowing unvaccinated individuals to falsely claim they were vaccinated.

Prosecutors emphasised that her actions posed a serious threat to public safety. They revealed that Pawlowska exploited her NHS role to issue these fake records, with suspicious activity being detected when records were created outside of her normal working hours, including weekends and during her annual leave. Notably, 42 of these fraudulent records were generated on dates when no vaccination clinics were held at the medical centre.

In April this year, Pawlowska pleaded guilty to charges of fraud by false representation and possession of criminal property at Peterborough Magistrates' Court. She was sentenced to two years in prison, and her employment at the medical centre ended in March 2022.

A spokesperson for the NHS in the East of England stated: *"Patients rightly expect anyone who works in a healthcare setting to adhere to the highest standards.*

*This illustrates that when serious criminal behaviour is identified, NHS England and law enforcement partners, in this case the National Crime Agency, will take the strongest action to protect the NHS."*

A National Crime Agency spokesperson added, *"The period following the outbreak of Covid 19 was a highly uncertain time for the public, which makes the offences committed by Marzena Pawlowska all the more appalling.*

*"Not only was she benefiting financially from her crimes, she was in a position of trust when creating these false documents and putting people at risk.*

*"By bringing her before the courts, with assistance from our partners in the NHS, the NCA ensured that the response was robust, preventing ongoing offending and protecting the wider public."*

In this edition:

# Be aware of QR Code Frauds

As technology progresses, more cashless ways for consumers to pay for goods or services are becoming available. And we are now seeing frauds involving these new methods, including QR code phishing, or "QRshing". QR codes can be used in a wide variety of ways, and can be included in emails instead of weblinks. One popular area for using this cashless method is car parking, and motorists are increasingly paying for their car parking using their phones, instead of cash or credit cards. Some car parks use apps whereas many others use a QR code scanning system.

Fraudsters are targeting these QR code systems to obtain money and personal data from unsuspecting car park payees, setting up fake QR codes and placing them on payment meters disguised as a "quick pay" option. This is often involving putting a QR sticker over the genuine QR code. Victims of this fraud are having money taken from their bank accounts, and personal data "harvested" because they have unwittingly shared their banking/ personal details with the fraudsters via the dodgy QR code. You may also end up with a parking fine from the real car park owners, as you won't have really paid for your parking!

Our advice is to exercise particular caution if the QR code is in an open space, such as a station or car park, however that doesn't negate the risk that QR codes may have been altered in enclosed spaces, such as pubs and restaurants.

## How to prevent QR code fraud

● If you have any concerns about a website a QR code takes you to is genuine, access it from your web browser instead.
● Double-check the preview of the QR code link. When you scan a QR code, a preview of the URL should appear. Make sure the website address is legitimate. Look for a padlock symbol and an address that begins with "https://". Only those URLs are secure.
● Ensure your phone security is up to date as QR codes can be used to download malware on to your device.
**If you think you have fallen for a scam, contact your bank and/or Action Fraud**

# The latest HMRC related mandate fraud targeting Trusts & ICBs

**Paul Bell, MIAA Senior Anti-Fraud Manager reported that:** *"We have been made aware of a HMRC related scam whereby fraudsters have been sending either a letter or VAT 484 form purporting to be from organisations requesting a change of bank account details and HMRC have confirmed an unspecified change in writing to the business. This is prevalent in organisations where they are due a refund from HMRC.*
*If you get notified by HMRC that unspecified details have been amended, you must act quickly and someone needs to check that the Trust / ICB has, in fact, made such a change.*
*If a change of bank account change has been requested, it is imperative that you contact HMRC and let them know such a change has been bogus."*

## How to prevent HMRC fraud

● If you get notified by HMRC that unspecified details have been amended, you must act quickly –
check that the Trust / ICB has, in fact, made such a change.
● If an unauthorised change of bank account change has been requested, it is imperative that you contact HMRC and let them know such a change has been bogus.

## How to report fraud in the NHS

You can report any concerns you have about fraud or corruption in the NHS using this secure and confidential form. If you prefer you can speak annoymously on on **0800 028 4060** or online https://cfa.nhs.uk/reportfraud

You can also speak to a members of our team, contact details for all of our Anti-Fraud Specialists and Fraud managers are listed on page 7.

# Recent Cases

## Bodybuilder who sued NHS over ‘botched’ surgery is jailed

Sean Murphy, a 39-year-old bodybuilder from Ross-on-Wye, was sentenced to eight months in jail for attempting to defraud the NHS by falsely claiming he was disabled due to a failed biceps tendon surgery.

In his 2021 claim, Murphy sought over £580,000 in compensation, stating he could no longer play rugby, work, or lift weights.

However, evidence, including social media posts and videos, showed Murphy playing rugby, lifting heavy weights, and working shortly after the surgery.

The Wye Valley NHS Trust had admitted to substandard surgery and made interim payments, but Murphy’s dishonesty led to legal action.

The court found his claims fraudulent and ordered him to repay £50,000 in damages and costs. Mr. Justice Mould sentenced Murphy for contempt of court, emphasizing the seriousness of his deceit, especially during the Covid-19 pandemic, when NHS resources were critically needed. He stated that: *“I am satisfied that Murphy deliberately lied to each expert by volunteering the false impression that he had been unable to play rugby. The shortest period of imprisonment I am able to impose is eight months.”*

## Senior doctor who fraudulently claimed 300 hours of work is struck off

Dr. Uzair Irshad, a 38-year-old NHS consultant, was struck off the medical register after fraudulently claiming around £50,000 for hours he did not work.

Between February 2019 and December 2020, while working as a locum dermatology consultant at NHS trusts in Doncaster and Barnsley, Irshad altered timesheets, claimed pay while on holiday, and forged colleagues’ signatures.

His dishonesty was uncovered when a suspicious colleague triggered an investigation by the NHS Counter Fraud Authority, leading to a misconduct hearing.

Despite admitting to 25 counts of dishonesty at the start of the tribunal in Manchester in July 2024, Irshad failed to provide a satisfactory explanation, claiming he *“lost control”* during the early days of the Covid-19 pandemic.

The tribunal found his actions to be at the *“higher end of the spectrum of dishonesty”*, both professionally and morally disgraceful, and deemed his conduct *“fundamentally incompatible”* with continued medical practice, resulting in his immediate removal from the medical register.

**If you are concerned about a potential fraud in your organisation contant your orgaisation’s counter fraud specalist or call the national fraud reporting number, 0800 028 4060 where you can talk in confidence or report concerns online via the NHSCFA website: cfa.nhs.uk/report-fraud/how-to-report-fraud**

# Recruitment Scams on the Rise

Fraudulent recruiters have been using social media platforms to dupe potential job seekers into divulging personal and financial information. Sophisticated frauds involving grooming of targeted individuals, shows the fake recruiter asking the unsuspecting job seeker to take part in a fake job interview, either over the phone or via social media platform, WhatsApp.

Fraudsters will conduct an interview and build rapport with the job seeker gaining their trust, with the sole aim of stealing their personal data and potentially inserting malware software on the job seeker's devices.

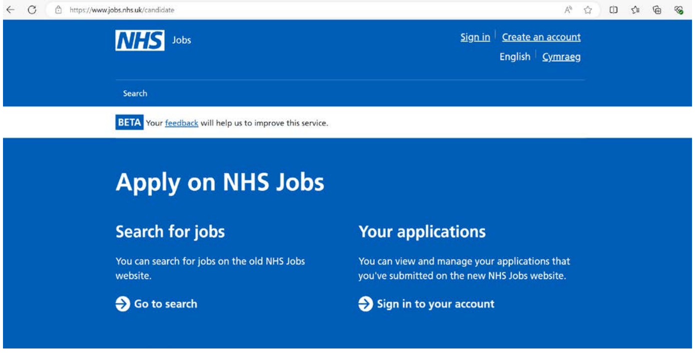
Malware is used to hack the targeted individuals' electronic devices, which then gives the fraudster access to a subject's personal information, passwords, and financial information.

This BBC report states that recruitment fraud is a sophisticated high volume, multistage crime that is hugely under reported. Latest figures from Action Fraud from 2022 show that 15 people reported being defrauded out of £20,040. New data shows that recruitment scams via text and WhatsApp, have jumped from £20,000 to £1 million, over the last 12 months.

## Recruitment in the NHS

NHS Business Services Authority provides the NHS Jobs service as part of their NHS workforce services directorate. NHS Jobs is the official online recruitment service for the NHS in England and Wales. It is the biggest marketplace for health jobs in the UK, with 45,000 jobs posted each month covering 350 roles from clinical roles, IT and support, to surgeons, and directors.

A member of our team described her recent recruitment experience into her new role within MIAA, "*The NHS recruitment process was professional, managed, and thorough. I applied for my current role via NHS jobs, where I was signposted to LUHFT's applicant tracking system "Trac jobs". I created a new Trac account and managed the whole recruitment process including application, interview and all the necessary pre-employment checks. The Recruitment team provided all their contact details and email addresses for advice and any questions during my onboarding.*



https://www.jobs.nhs.uk/candidate

BETA Your feedback will help us to improve this service.

Apply on NHS Jobs

Search for jobs

You can search for jobs on the old NHS Jobs website.

Go to search

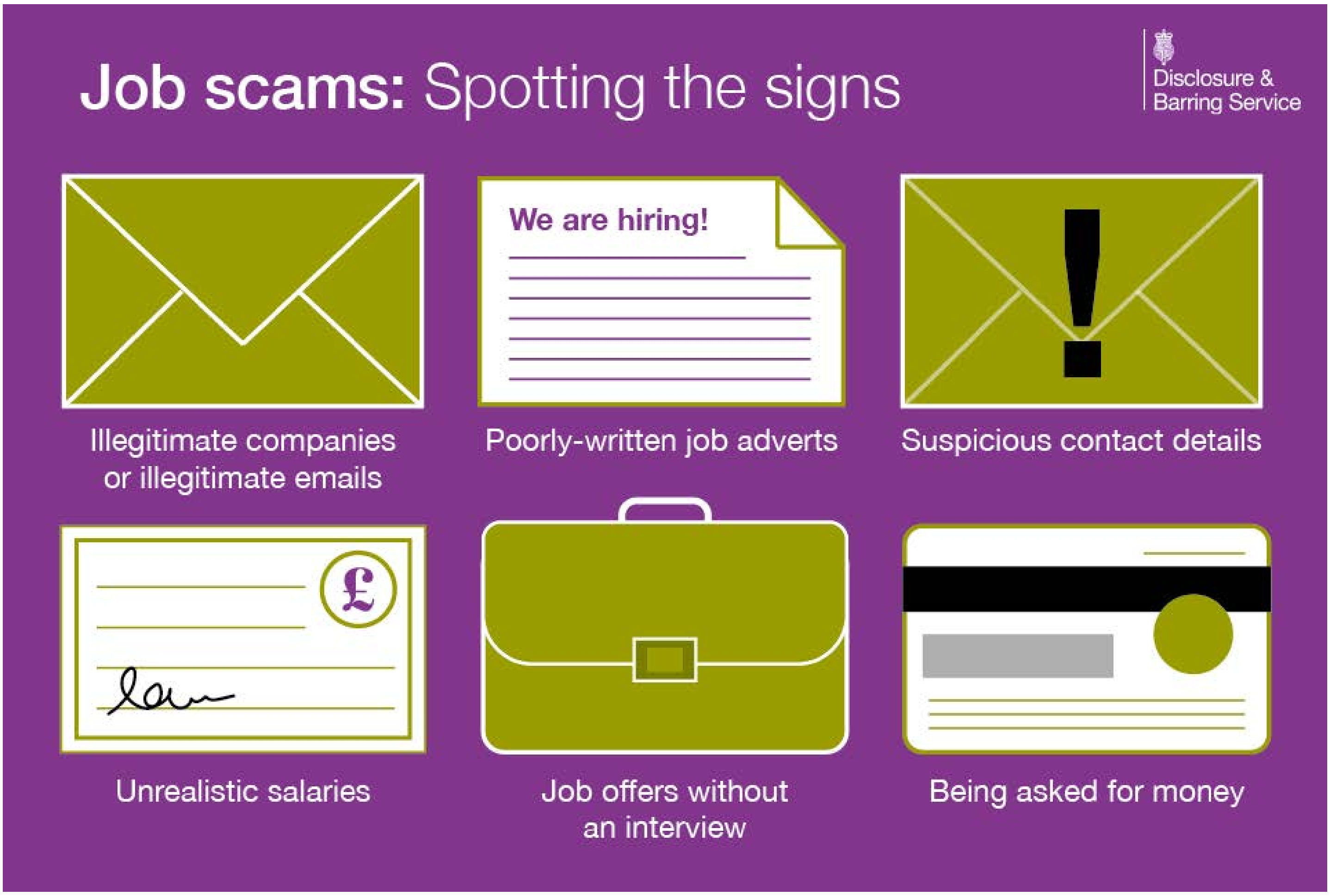
Your applications

You can view and manage your applications that you've submitted on the new NHS Jobs website.

Sign in to your account

*In the past I have received emails from companies and recruiters I do not know who try to engage with me to offer me positions. First, I check out their credentials to see if they are known to me, next I look for anything untoward in their communications style, or an unprofessional email. My personal motto is 'If it looks odd or is too good to be true it usually is!' If I suspect a scam, I delete the email and make sure that I do not click on any links or attachments.*"

# How to recognise a potential fraud



## Job scams: Spotting the signs

Disclosure & Barring Service

Illegitimate companies or illegitimate emails

Poorly-written job adverts

Suspicious contact details

Unrealistic salaries

Job offers without an interview

Being asked for money

In the digital age, scammers have found new avenues to exploit unsuspecting job seekers. To protect yourself from falling victim to these frauds, it's crucial to identify how to recognise a fraud.

**1. Too good to be true:** If the job offer seems too good to be true, it is. Scammers often lure you in with promises of high salaries, minimal work, excellent benefits.

**2. Unsolicited job offers:** Legitimate employers do not reach out on WhatsApp, without any prior communication from you. If you receive a job offer from someone you have not previously had any contact with or from an unknown number, be cautious and report any concerns to Action Fraud. Tel **0300 123 2040**

**3. Fake Information:** Look out for any information that cannot be verified, legitimate employers should share information that you can validate.

**4. Be Vigilant:** Do not give out personal information such as your financial information, bank accounts, passwords, or personal ID information such as passports or driving licences.

**5. Grammar:** Typical red flag warnings in any communications are frequent grammatical errors, poor use of the English language, unprofessional communication styles, and generic emails like Yahoo, Hotmail or Gmail.

**6. Urgency:** Scammers use tactics like urgency to pressure you into making quick decisions. This is Social Engineering.

**7. Fake websites:** If in doubt check it out! Verify the website's authenticity by checking for an office address and contact details that can be verified. Companies house is a useful source to check out information you have been given.

**8. Request for money:** You should never have to send any monies to secure a job offer.

**9. No face-to-face Interaction:** If the entire hiring process is completed online through messaging without any face-to-face contact, you should remain suspicious.

**10. Do not get tricked:** Do not click on innocuous links or attachments in emails whether from known or unknown sources. If you are suspicious of a link, whether on website or email, report your concerns and delete the email.

**11. Trust your Instincts:** If something appears odd, too good to be true or you feel uncomfortable then stop, think, and report your concerns to Action Fraud, and let your Anti-Fraud Specialist know. WhatsApp also have advice on how to protect yourself from suspicious messages and scams.

# Insights into Fraud and Prevention

Talking
Fraud

Check out the Anti-Fraud team podcast, “Talking Fraud,” where they provide an engaging and insightful look into the world of fraud within the NHS and beyond. With years of experience investigating fraud across various organisations, the team offers a wealth of knowledge on how to identify, prevent, and tackle fraud.

Hosted by Darrell Davies, Regional Assurance Director, the podcast features Senior Anti-Fraud Managers Paul Bell, Claire Smallman, and Anti-Fraud Manager Kevin Howells, who share their expertise on all aspects of fraud and fraud prevention. As Darrell explains, *“Fraud can be committed by anyone—from patients avoiding payment for prescribed drugs, to staff and contractors submitting false timesheets or invoices, to external fraudsters committing bank mandate fraud by impersonating genuine suppliers.”*

## Episodes available

**NHS Fraud – What’s the Problem?**
Discover how the NHS Counter Fraud function was established and explore the current challenges, including the rise of Covid-related and cyber-enabled fraud.

**How Does an Anti-Fraud Service Work?**
Dive into the mechanics of fraud: What drives people to commit fraud against the NHS? The team shares insights into their roles, what Anti-Fraud Specialists do to combat fraud, and some of the real cases they’ve encountered.

**A deep dive into recent cases**
Take a deep dive into some of the cases that the team have worked on, looking at the methods and motivations of fraudsters. They share information on how to prevent ID and qualification fraud and how this can be prevented with frequent checks. They discuss breach of trust and why this is a key factor in assessing the suitability of a candidate for recruitment.

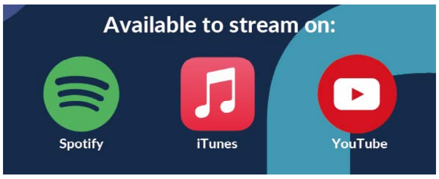
**Social Engineering and Cyber-Enabled Fraud**
This episode tackles the growing concern of cyber-enabled mandate fraud in the NHS, including “whale phishing,” where scammers impersonate CEOs or senior managers to manipulate employees into making costly mistakes. Learn the red flags to watch for and how to protect yourself and your organisation from these sophisticated scams.

**Understanding Conflicts of Interest in Healthcare**
In the season finale, the team delves into the complex issue of conflicts of interest in healthcare, from healthcare professionals to policymakers. They discuss what constitutes a conflict of interest, how it arises, and the regulations in place globally, with a focus on the NHS. Key topics include the Bribery Act, the importance of declaring interests, and maintaining transparency and integrity in decision-making.

Tune in for these thought-provoking discussions and stay ahead of evolving fraud threats. Protect yourself and your organisation with the valuable insights shared by the MIAA Anti-Fraud team.

## Listen Now!

**Download “Talking Fraud” on Spotify, Apple Music, or any of your preferred streaming platforms or via [https://www.buzzsprout.com/2080161/](https://www.buzzsprout.com/2080161/)**



# Useful Sources of Information

- MIAA Fraud alerts, blogs, and newsletters - Our fraud alerts and newsletters bring together rich sources of information relating to the latest scams and fraud cases so that our readers can be vigilant in work and at home.

- NHS Counter Fraud Authority - The NHS Counter Fraud Authority (NHSCFA) is a special health authority tasked to lead the fight against fraud, bribery and corruption in the NHS.

- CFA Report Fraud - You can use this online form to report fraud against the Department of Health and Social Care (DHSC) and the wider health group, including the NHS in England and Wales.

- Take Five to Stop Fraud – Take Five is a national campaign offering straightforward, impartial advice that helps prevent email, phone-based and online fraud - particularly where criminals impersonate trusted organisations.

- The National Cyber Security Centre – Organisation helping to make the UK the safest place to live and work online.

- Action Fraud - Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland.

- NHS Digital – Guidance on Phishing Emails - Find out how you can stay safe and vigilant against phishing emails, including advice on how to spot a suspicious email and how to report it.

# Contact your Anti-Fraud Specialist

Darrell Davies
Regional Assurance Director (Anti-Fraud)
☎ 07785 286381
✉ Darrell.Davies@miaa.nhs.uk

Paul Bell
Senior Anti-Fraud Manager
☎ 07552 253068
✉ Paul.Bell@miaa.nhs.uk

Claire Smallman
Senior Anti-Fraud Manager
☎ 07769 304145
✉ Claire.Smallman@miaa.nhs.uk

Sarah Bailey
Anti-Fraud Specialist
☎ 07721 488602
✉ Sarah.Bailey@miaa.nhs.uk

Linda Daisley
Anti-Fraud Specialist
☎ 07570 147318
✉ Linda.Daisley@miaa.nhs.uk

Kevin Howells
Anti-Fraud Manager
☎ 078257 32629
✉ Kevin.Howells@miaa.nhs.uk

Paul Kay
Anti-Fraud Specialist
☎ 07990 082328
✉ Paul.Kay@miaa.nhs.uk

Phillip Leong
Anti-Fraud Specialist
☎ 07721 237352
✉ Phillip.Leong@miaa.nhs.uk

Virginia Martin
Anti-Fraud Specialist
☎ 07551 131109
✉ Virginia.Martin@miaa.nhs.uk

Karen McArdle
Anti-Fraud Specialist
☎ 07774 332881
✉ Karen.McArdle@miaa.nhs.uk

Paul McGrath
Anti-Fraud Manager
☎ 07584 774761
✉ Paul.McGrath@miaa.nhs.uk

Neil McQueen
Anti-Fraud Specialist
☎ 07721 237353
✉ Neil.McQueen@miaa.nhs.uk

Andrew Wade
Anti-Fraud Specialist
☎ 07824 104209
✉ Andrew.Wade@miaa.nhs.uk