



# Fraud Counts Newsletter

## Spring 2024



### Introduction

Welcome to our latest edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on fraud cases currently in the media, how to stay vigilant when it comes to scams, advice and guidance on 'smart' security cameras and how to use them safely in your home, cyber security/setting good passwords, together with how to contact your Local Counter Fraud Specialist.

### Fraud cases in the media

#### **A hospital consultant and social media influencer sentenced after forging timesheets** (source - [Hospital consultant sentenced after forging timesheets](#) | News | NHSCFA)

This is a serious case of fraud committed by Dr. Kifayat Ullah, a hospital consultant and social media influencer. He was found guilty of defrauding the NHS of more than £50K by submitting false timesheets during his time as a locum at Kingston Hospital NHS Foundation Trust.

The fraud was uncovered by Local Counter Fraud Specialists and the NHS Counter Fraud Authority Fraud Hub, who conducted an audit at the Trust and identified discrepancies in the records presented. The Crown Prosecution Service agreed that the evidence warranted a charge of making a false instrument with intent it be accepted as genuine under the Forgery and Counterfeiting Act 1981.

At sentencing, Judge His Honour Trigilgas-Davey stated that Dr. Ullah's actions were driven by greed and brought disgrace upon himself and his profession.

Dr. Ullah was initially recruited as a locum consultant to help with the post-COVID backlog within the Trust. Despite requesting to reduce his hours to part-time working, he submitted 29 forged timesheets over six months, claiming he was working full time and was paid accordingly. Some timesheets were altered after receiving a genuine authorising signature, while others were completely fabricated by Dr. Ullah, who forged or copied signatures.

This case serves as a reminder of the importance of vigilance and robust systems to prevent and detect fraud within public services. It also exemplifies why a document must not be returned to someone once it has been authorised and underscores the severe consequences for those who choose to engage in such dishonest behaviour.





**NHS Doctor, who branded herself as ‘Dr Drips’, has been suspended** (source - [NHS’s ‘Dr Drips’ suspended after claiming treatments could help protect against Covid \(telegraph.co.uk\)](#))



Dr Nimra Arshad offered IV infusions on Instagram, claiming that they could help treat various diseases including anaemia, Parkinson’s disease, Alzheimer’s, and even protect patients from Covid.

Dr. Arshad, a locum junior doctor looking after dementia patients at The Poplars health facility in West Yorkshire, claimed her IV treatments would strengthen the immune system, lead to quick weight loss, boost athletic performance, and even help with pregnancy fatigue. She also claimed that her Vitamin C IV drip could help build immunity against Covid.

However, these claims were found to be misleading and exploitative, especially in the context of the pandemic. The General Medical Council (GMC) was alerted in March 2021 after concerns were raised about the efficacy of her medications and her social media posts. The Medical Practitioners Tribunal Service found Dr. Arshad guilty of serious professional misconduct and suspended her from medical practice for three months.

This case serves as a reminder of the importance of verifying the credibility of medical claims, especially those made on social media platforms.

**Fraudster who pretended to be the Queen’s Footman sentenced for eBay scam** (source - [Fraud and economic crime | The Crown Prosecution Service \(cps.gov.uk\)](#))

It’s important to remember that online platforms can be misused by individuals with malicious intent. In this case, Dru Marshall, who falsely claimed to be a Senior Footman at Windsor Castle, attempted to defraud eBay users by listing a walking stick he claimed belonged to the late Queen Elizabeth II.

Despite his claims that the venture was a joke or a social experiment, prosecutors were able to secure a conviction against him using extensive computer evidence, including his online search history. This case serves as a reminder of the importance of online vigilance and the need to verify the authenticity of items and the credibility of sellers when participating in online auctions.

Marshall was sentenced to a 12-month Community Order and ordered to complete 40 hours of unpaid work. This outcome demonstrates that fraudulent activities are taken seriously by the legal system and that perpetrators will be brought to justice.

Always exercise caution when dealing with online transactions to avoid falling victim to such scams.



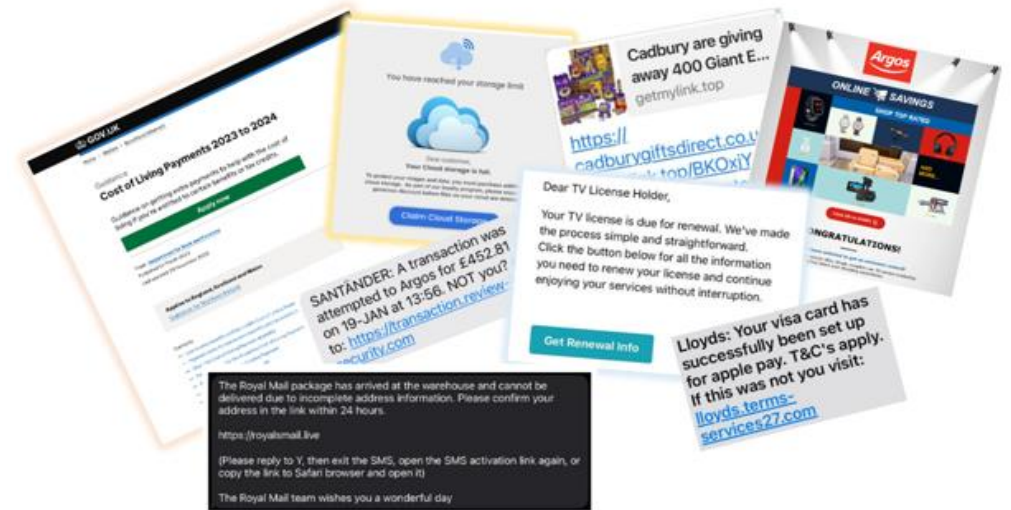
## Stay vigilant when it comes to scams (source - The latest scam alerts from Which? - Which? News)

### What do these scams have in common?

- They are all scams with the purpose to trick you into giving money or something of value to dishonest groups, individuals, or companies.
- Fraudsters are on the lookout for victims who let their guard down.
- They are all intended for you to make contact via an unsafe route.
- The scam asks you to share the link with others which spreads the scam further.

### Prevention:

- Do not follow suspicious links or reply to the message.
- If you are asked to pay for something online via a bank transfer, don't do it.
- Emails or messages littered with spelling and grammar mistakes are a scam giveaway.
- Cold calls or unexpected emails or messages should raise suspicion, especially if you're asked to give personal or payment details. It's very unusual for legitimate organisations to contact you and ask for sensitive information if you're not expecting them to. If you're not 100% convinced about the identity of the caller, hang up and contact the company directly.
- Never share your personal details with anyone if you can't confirm who they are. Scammers will often try and get valuable personal data from you, and they can use this to steal your money, or even to steal your identity.



### Methods of reporting:

To report scam texts, the message should be forwarded to 7726.

Suspicious websites can be reported to the National Cyber Security Centre - [report@phishing.gov.uk](mailto:report@phishing.gov.uk) or via - <https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website>

If the message is from an unknown number, you can report the sender on WhatsApp by opening the chat, tapping on the sender's contact details, and selecting 'Block and Report'.

Get Safe Online is an easy to use online tool which helps you to determine whether a website is likely to be legitimate or a scam before you visit it - <https://www.getsafeonline.org/checkwebsite/>







## Using 'smart' security cameras safely in your home



Smart cameras, such as security cameras and baby monitors, connect to the internet using your home Wi-Fi, allowing you to monitor your home remotely. However, this convenience can also pose a risk to your privacy if not properly secured.

In rare cases, live feeds or images from smart cameras can be accessed by unauthorised users. This is often due to cameras being shipped with default passwords set by the manufacturer, which are often well-known or easily guessable (like 'admin' or '00000'). Cybercriminals can exploit these default passwords to access the camera remotely and view live video or images in your home.

### To protect yourself, it's crucial to take a few steps:

	<b>Change the Default Password</b> - Always change the default password to a strong, unique password that is hard to guess.
	<b>Regularly Update Your Devices</b> - Ensure your smart devices, including your smart cameras, are regularly updated. Manufacturers often release updates that fix known security vulnerabilities.
	<b>Use Two-Factor Authentication</b> - If available, use two-factor authentication for an added layer of security.
	<b>Secure Your Wi-Fi Network</b> - Make sure your home Wi-Fi network is secure. Use a strong, unique password and consider using a network security protocol, such as WPA3.

**Remember, the security of your smart devices is as important as their functionality. Stay safe!**



## Setting good passwords

The start of a new calendar year can be a great time to start fresh and update your passwords. You'll often hear the Counter Fraud team advising that you need to make sure you use strong and unique passwords. For your work-related passwords, always follow the advice of your organisation's IT department.

## Why do passwords need to be unique?

A survey run by Google in 2019, found that 65% of people were reusing the same password for multiple accounts. When you consider how many different systems and services we log into, it's understandable that people often find it easier to rely on a single password that they are familiar with. However, this is a big risk.

The danger comes when one of your accounts is breached. If a company that holds your data is targeted by cyber criminals, your log in credentials could end up being stolen and sold on. If you rely on a single password, accounts you hold elsewhere can also be hijacked.

For example, let's say that Company A is hacked, and your username and password are stolen. The cyber-criminal is able to log into your account with Company A to look for more information - such as the email address linked to your account.

They try your password to see if they can get into your emails. If they get into your email account, they can go around lots of other services and reset your password, locking you out of your accounts. If you don't have the same password for your emails, you might think they'd just give up and move on.






However, they haven't quite finished. They will try logging into popular services - such as Amazon, PayPal, eBay, social media platforms etc. using your email address and the password that Company A lost. Any account which they manage to access gives them an opportunity to gather more information on you. Some accounts will also contain saved payment information, which can be used to place unauthorised orders. For example, if they get into your Amazon account, they can use your saved details to place high value orders which they could arrange to have delivered to Amazon lockers. They would also be able to steal your address which may help them to carry out identity theft.

Hopefully this example highlights why having unique passwords is so important.














## How do you set a good password?

	<p><b>Three is a magic number</b> - The National Cyber Security Centre recommends that you use three random words to make strong and unique passwords. Doing this makes your password much longer (and therefore harder to guess or break) but keeps it easy to remember. If picking three random words is proving tricky, you could use a favourite song lyric or phrase that you find memorable.</p>
	<p><b>Don't make it personal</b> - You should not use any personal information in your passwords - things like your pet's name, your middle name, the place you were born etc. can be tracked down on social media and your online footprint. Even if you think your privacy settings are pretty good, friends and family who you are linked to online may be less diligent.</p>
	<p><b>Characterful passwords</b> - If you need to include special characters in your password, it is often tempting to replace letters that look similar (e.g. password becomes p@\$w0rd!) - however this tactic is well known to fraudsters. Instead, think about adding them in between your three random words e.g. balloonhooklamp could be changed to @balloon?hook!lamp.</p>
	<p><b>Take a strength test</b> - To explore how small changes can increase your password strength, have a look at How Secure is My Password. This is a website where you can type in potential passwords, and it tells you how long it would take a computer to crack them. For example, balloonhooklamp is estimated to take 1 thousand years to break but adding symbols in increases that to 80 trillion years!</p>
	<p><b>Don't recycle</b> - Reusing passwords is risky - it's always safest to come up with a new password rather than slightly tweaking one you have used before.</p>



## Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance ([www.aswassurance.co.uk](http://www.aswassurance.co.uk)), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations. If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact your Local Counter Fraud Specialist (LCFS) below.

	<b>Gareth Cottrell – Counter Fraud Manager</b> ✉ <a href="mailto:gareth.cottrell@nhs.net">gareth.cottrell@nhs.net</a> ☎ 01872 258057 07814 002364		<b>Tracy Wheeler – LCFS</b> ✉ <a href="mailto:tracy.wheeler2@nhs.net">tracy.wheeler2@nhs.net</a> ☎ 01752 431378 07789 868568
	<b>Byron Kevern – LCFS</b> ✉ <a href="mailto:byron.kevern@nhs.net">byron.kevern@nhs.net</a> ☎ 07775 417508		<b>Sarah Smith – LCFS</b> ✉ <a href="mailto:sarah.smith10@uhbw.nhs.uk">sarah.smith10@uhbw.nhs.uk</a> ☎ 07467 685609
	<b>Sandra Bell – LCFS</b> ✉ <a href="mailto:sandra.bell19@nhs.net">sandra.bell19@nhs.net</a> ☎ 07467 685529		<b>Ian Halkerd – LCFS</b> ✉ <a href="mailto:ian.halkerd@uhbw.nhs.net">ian.halkerd@uhbw.nhs.net</a> ☎ 07788 300215
	<b>Sammy Donaldson – Trainee LCFS</b> ✉ <a href="mailto:s.donaldson1@nhs.net">s.donaldson1@nhs.net</a> ☎ 07467 685529		<b>Jazmine Noot - LCFS</b> ✉ <a href="mailto:jazmine.noot@uhbw.nhs.uk">jazmine.noot@uhbw.nhs.uk</a> ☎ 07502 877486
	<b>Tyla Balcombe – Trainee LCFS</b> ✉ <a href="mailto:tyla.balcombe@nhs.net">tyla.balcombe@nhs.net</a> ☎ 07584 619339		