## Counter Fraud Newsletter September 2023

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful.

# **Current Scam Trends**

**Fake Customer Services Accounts on X**

The Guardian has reported that customers using X (formerly known as Twitter) to contact companies to raise complaints or request refunds are being targeted by fake “verified” accounts.

On the platform, users can pay £11 a month to have a blue “verified” tick added to their profile. Some fraudsters are exploiting this option, setting up profiles designed to look like they belong to a verified member of the company’s customer services team. Having a blue tick makes the profiles look more convincing.

The fraudsters use these profiles to contact people who are seeking assistance - such as those who have lost out due to flight cancellations and delays. You can read more on the [Guardian website.](https://www.theguardian.com/technology/2023/aug/27/consumers-complaining-x-targeted-scammers-verification-changes-twitter?mc_cid=55e9518fe8&mc_eid=b70343a63c)

**Advice**
If you contact a company on social media, be aware that responses may be from fraudsters.

Look closely at the details. Giveaway signs of a fake customer services account can include:

* Small changes to the usual format of the account name (such as unexpected hyphens)
* The account has only been registered for a short time.
* The fraudster tries to move you onto a different platform (e.g. WhatsApp).

If you are in any doubt, use an alternative and official route to contact the company.

**Wilko Scams**

After Wilko announced that they have appointed administrators, at least ten fake websites sprang up which are designed to mimic the official Wilko site.

These sites are attempting to lure shoppers with “closing down sale” items which are not genuine. The sites offer goods at hugely discounted prices, such as electric bikes and sofas being advertised at £25. [Read more on the **i** website](https://inews.co.uk/news/consumer/wilko-sale-scam-explained-how-avoid-online-clearance-deals-2581710).

Fraudsters are hoping potential customers will part with their financial details in search of a bargain.

**Advice**

Wilko are no longer selling items online - they are only allowing people to shop in store.

Wilko have one legitimate website: www.wilko.com. Variations on this are fraudulent sites.

Offers that look too good to be true often are - and can hide nasty surprises.

If you think you have fallen victim to this scam, please report it to your bank and Action Fraud.

**Cost of Living Scam**

The Government are due to make further cost of living payments which will give the fraudsters an opportunity to try and deceive you. They will do this by pretending to be the Department for Work and Pensions (DWP) and could target you by phone, email or text.

The fraudsters are unlikely to know who is eligible and may contact you even if you are not entitled to a payment.

One of the text messages which has been seen is:

GOV: The £750.00 (GBP) Living Payment is ready, take action by accepting the payment via legalaid.income-division.com

This link leads to genuine looking website which asks for your name, address and bank details.

**Advice**

DWP have warned that you be need to be mindful if you receive any contact asking you to apply, accept or get in touch with somebody to receive the payment as this may be a scam.

If you are eligible, you do not need to apply to receive the payment. It is done automatically.

DWP will not ask you for personal details via text or email.

If you have entered your details on a site like this, contact your bank immediately. You can call 159 and the hotline will connect you to your bank.

Suspicious text messages can be forwarded to 7726 and dodgy emails can go to report@phishing.gov.uk

# **Cyber Security**

**Protect your profile, protect your pay.**

Since the start of the financial year we have seen a surge in fraudsters trying to divert salary payments by impersonating NHS staff. The fraudsters have set up fake email accounts and have contacted HR, Payroll and Finance departments asking for changes to employee bank details to be made.

The LCFS team were interested in how the fraudsters were identifying the names of NHS employees. A review of the attempts that had been made found that in 100% of cases, the person who was being impersonated had a publicly visible LinkedIn profile. In 70% of cases, the fraudster made direct contact with a named Payroll, HR or Finance employee at the same organisation who **also** had a visible LinkedIn profile.

All of these LinkedIn profiles had low privacy settings, meaning that the person's full name, job title, and place of employment could be viewed via search engine results. This meant that the fraudster didn't need their own LinkedIn account to get hold of this information.

LinkedIn has been the subject of several reports around security issues such as [fake profiles](https://www.cnbc.com/2022/06/17/fbi-says-fraud-on-linkedin-a-significant-threat-to-platform-and-consumers.html), [account hijacking](https://www.computing.co.uk/news/4122320/linkedin-surge-account-hijacking), and the site being used to carry out fraud by offering [fake job offers](https://www.linkedin.com/pulse/exposed-dark-side-linkedin-job-scammers-sagar-neupane) or phony investment opportunities. These same concerns also apply to other social media platforms, so even if you do not use LinkedIn it is important to review your privacy and security settings.

**Advice**

* On LinkedIn you can stop your profile details from showing up in search engine results. Instructions on how to do this can be found on the [LinkedIn help site](https://www.linkedin.com/help/linkedin/answer/a528138/control-your-public-linkedin-profile?lang=en-us&intendedLocale=en#:~:text=Tap%20your%20profile%20photo.,information%20from%20your%20public%20profile.).
* If you have an inactive or rarely used LinkedIn account, it is best to delete it.
* Never share personal or financial information with someone you have met on social media.
* Make sure you use a strong and unique password for each account.
* Always use Multi-Factor Authentication when it is available, this lowers the chance of your account being hijacked.
* Be wary of unsolicited contact and offers that are too good to be true.
* You can read more about job offer scams on the [Which? website](https://www.which.co.uk/consumer-rights/advice/job-scams-aFQaP4P9btJv).

**Dealing with Data Breaches**

Major data breaches frequently hit the headlines and it can be a horrible feeling finding out that your data has been compromised.

If data has been breached from a large organisation, it would be unusual for the criminals to start targeting individuals.

Instead, they will probably send demands for payment from the organisation they have attacked. They will threaten to release the data on the ‘dark web’ or sell it on to other criminals.

When data is breached, it is more likely to be information such as email addresses and phone numbers than your full bank details.

If your contact details are obtained by other criminals, they will use them in a secondary attack, that is, they will send you phishing emails or make phone calls to you pretending to be from organisations such as your bank or police.

**What to do**

* Don’t panic. Much information which is breached, such as name and email address, is not a high risk.
* Do keep an eye on your bank account and query any suspicious transactions or pending transactions immediately.
* Be vigilant to any unexpected emails and phone calls.
* Be particularly careful of any communications from the organisation the data was breached from. Criminals may pretend to be from the organisation and ask you to verify information, or click on a link to reset your password following their breach.
* You can check whether your personal email has been involved in a data breach on [Have I Been Pwned](https://haveibeenpwned.com)
* This will tell you what information has been breached and where this came from. For any breaches identified, we recommend you change your password and activate Multi Factor Authentication.

# **In the Press**

**Prison Sentence following £560k NHS fraud**

Thomas Elrick had been a senior manager at NHS Harrow Clinical Commissioning Group. His role gave him access to a budget and the ability to authorise payments worth up to £50,000.

Elrick abused this trusted position in order to pay invoices which added up to over £560k to a company which had not provided any services to the CCG. The company was a dormant business, and in fact, Elrick was sending the payments to his own bank account.

To try and cover up the fraud, Elrick used an email account of his deceased wife to send emails to the CCG. He even created false details regarding services he claimed had been provided by the dormant company.

Elrick had spent the money on expensive holidays and shopping. In interview he admitted the offences and has been sentenced to 3 years and 8 months in prison. You can read more on the [NHS Counter Fraud Authority website.](https://cfa.nhs.uk/about-nhscfa/latest-news/senior-manager-sentenced)

# **A Quick Guide to Reporting Fraud Concerns**

## **I have a concern that fraud may be being committed against the NHS.**You can contact the Counter Fraud team using our details below. You can also report your concerns to the NHS Counter Fraud Authority via their online reporting tool or hotline. If you making an anonymous report please give as much detail as possible as we won’t be able to contact you for more information.

## **I have a concern that fraud may be being committed against the general public.**

These concerns can be reported to Action Fraud (0300 123 2040). If someone has been actively defrauded it may also be appropriate to report to the police. If it is suspected that the victim’s bank account has been compromised, they will need to speak to their bank as a matter of urgency.

## **I have received a suspicious email to my NHS.net email address.**

Do not click on any links or attachments. Forward the suspect email as an attachment to spamreports@nhs.net. To do this, click on the “More” button which is next to the “Reply, Reply All, Forward” options. Choose “Forward as Attachment”.

## **I have received a suspicious email to another email account (not NHS.net).**

Do not click on any links or attachments. Forward the email to report@phishing.gov.uk. You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

## **I have received a suspicious text message.**

Do not click on any links in the text message! Forward the text message to 7726.

## **I have come across something and I’m not sure whether or not it is fraud related.**

You are very welcome to contact your Local Counter Fraud Specialist for advice and support, our details are below.

# **How to Contact Your Local Counter Fraud Specialist:**

Your Local Counter Fraud Specialist is: