SEPTEMBER 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our September 2023 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

Boost Your Scam-Spotting Skills: Take the Quiz on Take 5 to Stop Fraud!"

In today's digital age, scams and frauds have become increasingly sophisticated, making it crucial for everyone to stay vigilant and well-informed. The Take 5 to Stop Fraud campaign is designed at raising awareness and protecting the public from fraud.

The internet is rife with deceptive schemes that can trick even the savviest of individuals. Are you confident in your ability to spot a scam? It's time to put your skills to the test!

You can find the quiz on the Take 5 to Stop Fraud website. There are 9 questions designed to boost your awareness and sharpen your scam-spotting skills.

The more informed individuals there are, the more difficult it becomes for scammers to find victims.

Remember, no one is immune to scams, but with the right knowledge you can reduce your risk significantly.

Fraud News

Stopping Scammers Targeting Job Seekers

This BBC article explores how fraudsters are targeting job seekers with fake offers of employment. The scammers are believed to be trying to steal personal data and encourage applicants to make unnecessary payments.

Carers thanked for spotting fraud against 101 year old

Another BBC article, this is the story of a care worker who raised the alarm that a 101 year old lady was possibly being scammed by international “clairvoyant” fraudsters.

Sheffield flat linked to £17m bribery case seized by SFO

The Serious Fraud Office have seized a flat in Sheffield after it was linked to a bribery case. The owner of the flat had facilitated bribes paid by a British company to secure £17 million worth of contracts in China. The SFO have already recovered £350,000 from the perpetrator.

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.

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.

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 are 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 Fraud

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, account hijacking, and the site being used to carry out fraud by offering fake job offers 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.
- 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.

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
- 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.

Fraud Prevention Masterclasses

The 2023/24 Fraud Prevention Masterclass programme has now launched. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. Further dates will be published later this year. We will be covering the following topics:

General Fraud Awareness	23rd October 11am, 12th December 10am
Fraud Awareness for Managers	1st November 10am, 16th January 11am
Cyber Fraud	25th October 10am, 14th December 10am
Payroll Fraud	9th November 2pm, 23rd January 10am
Procurement Fraud	24th October 10am, 11th December 1:30pm
Creditor Payment Fraud	13th November 11am, 16th January 10am
Fraud Awareness for HR	5th October 2pm, 6th December 11am
Recruitment Fraud	28th September 2pm, 16th November 2pm

If you'd like to book a place for any of these sessions, please contact yhs-tr.audityorkshire@nhs.net

Bespoke Training Sessions

The Local Counter Fraud Team are always happy to pop along to speak to individual teams. If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

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 on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

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 are on the next page.

CONTACT US

Acronym Decoder
LCFS - Local Counter Fraud Specialist
LSMS - Local Security Management Specialist
ICB - Integrated Care Board

Steve Moss
Steven.Moss@nhs.net / 07717 356 707

Head of Anti Crime Services / LCFS

Steve manages the Counter Fraud Team.

Marie Dennis (was Hall)
Marie.Dennis2@nhs.net / 07970 265 017

Assistant Anti Crime Manager covering all clients, and LCFS covering:

York and Scarborough Teaching Hospitals NHS Foundation Trust

NHS Professionals

Nikki Cooper
Nikki.Cooper1@nhs.net / 07872 988 939

LCFS Covering:
Humber Teaching NHS Foundation Trust

Humber and North Yorkshire ICB

Leeds Community Healthcare

Rosie Dickinson
rosie.dickinson1@nhs.net / 07825 228 175

LCFS Covering:
Harrogate and District NHS Foundation Trust

Spectrum Community Health CIC

West Yorkshire ICB

Shaun Fleming
ShaunFleming@nhs.net / 07484 243 063

LCFS and LSMS Covering:

Calderdale and Huddersfield NHS Foundation Trust

West Yorkshire ICB

Lincolnshire ICB

Rich Maw
R.Maw@nhs.net / 07771 390 544

LCFS Covering:

Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

Mid Yorkshire Teaching NHS Trust

Lee Swift
Lee.Swift1@nhs.net 07825 110 432

LCFS Covering:
Airedale NHS Foundation Trust
AGH Solutions
Bradford District Care NHS Foundation Trust
Leeds and York Partnership NHS Foundation Trust

You can also report fraud concerns to the NHS Counter Fraud Authority:
0800 028 40 60
https://cfa.nhs.uk/reportfraud

Follow us on Twitter - search for @AYCounter Fraud

Scan here to see previous editions of our newsletters