MAY 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our May 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

SECONDARY WORK REMINDER

Do you have more than one job? If so, you must follow your organisation's policies on secondary work.

You'll usually find the rules within the Conflicts of Interest / Standards of Business Conduct policies, and it may also be reflected in your contract of employment.

You will need to declare your other job to your line manager and seek approval if necessary. You may also need to submit a Conflicts of Interest declaration depending on the two roles.

If you are off sick, you should tell your GP about your second role.

This allows them to consider whether you need to be signed off sick from both jobs, or if you are well enough to do one of the roles but not the other. This can then be reflected on your FIT notes.

If you're in any doubt, please seek advice from your manager or HR.

GOVERNMENT CHANGES APPROACH TO FRAUD

With advances in technology, fraud is becoming easier to commit and more difficult to detect.

Fraud continues to hold the title of most committed crime in the UK and the government has announced a plan to try and stop scams at source.

This includes:

- Working with Ofcom to try and stop fraudsters being able to spoof phone numbers.
- Plans to stop mass spam texting.
- A ban on cold calling to sell financial products.
- An overhaul of the national fraud team.

It is hoped that these new measures will help prevent people becoming a victim of fraud and bring justice to those committing the crime.

You can read more about this here -

What the Prime Minister's Fraud Strategy means for you - GOV.UK (www.gov.uk)

Scam Trends

Bank Scam Calls

These scams involve the fraudster pretending to be from your bank's customer services or fraud team. They will claim your account is compromised and you need to move your money to a "safe account".

These fraudsters have various tools they can use to make themselves seem genuine and to carry out their scams:

- **Spoofing software** - disguises their real phone number and makes it look like they're calling from an official customer services number.
- **Line jammers** - these let the fraudster stay on the line even when you think you've hung up. They can then intercept your next calls.
- **Panic / urgency** - these fraudsters are experts in creating a sense of panic. They encourage you to take action quickly.
- **Open source research** - they might take on the identity of a known employee. They will then tell you to check "LinkedIn" to reassure yourself that they're a real employee.
- **Rehearsed lies** - the fraudster will be aware that your bank might challenge you if you move a lot of money at once. They'll tell you exactly what to say to bypass these checks.

Avoiding Bank Scam Calls

- Remember that the information showing on your caller ID may not be true.
- If you receive a call of this nature, hang up, then use a different phone (or wait 30 minutes) to call your bank. This helps you to avoid any line jammers the fraudster may have.
- Banks will never ask you to withdraw or transfer money for "security reasons".
- If you get an email or text asking you to click on a link to log into your bank, do not click the link. Instead, call your bank using the number on the back of your card, or open a web browser and type the bank's web address in manually.

TV Licence Scams

Action Fraud have warned that a new TV licence scam has been spotted doing the rounds.

Fraudsters have been sending out a phishing email template that claims that your TV licence will expire soon and that you must pay online immediately. Other victims have been sent emails which say there was a problem with their last payment, and that they need to update their details.

The emails include a link which takes you onto a dodgy website which looks very convincing. On this site, you are asked to enter your personal information and payment details.

Action Fraud have received 3,455 reports of this scam within a two week period.

Advice on Avoiding TV Licence Scams

- Genuine TV Licensing emails will include your name and part of your postcode.
- TV Licensing have published advice on how to spot fraudsters impersonating their services. You can find this on their website.
- Always be cautious about links sent in emails. It is safer to contact the organisation directly, using an official contact method (such as their customer services number or web chat function).
- You can send photos or screenshots of suspected TV licence fraud text messages to: textscam@tvlicensing.co.uk

Identity Theft

During 2022, identity theft rose by a third compared to 2021 (read more on the Forbes website). Identity theft is where a person's details are stolen, then used to take out loans or credit cards or access cash belonging to somebody else. You can read about identity theft on the Action Fraud website.

The majority of identity thefts start online. Fraudsters use tactics such as phishing emails, open source research (e.g. information from social media or public websites), and lists of compromised data from cyber attacks to steal a person's identity.

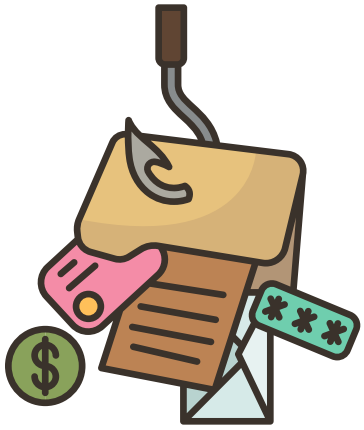
Identity Theft Advice

- It is vital to protect your online presence (including your emails, banking apps, shopping or social media accounts).
- Don't overshare your information online.
- Be suspicious of links in emails and text messages.
- Keep security software up to date.
- Use a strong, different password for every site.
- If possible, turn on Multi-Factor Authentication.
- Make sure your social media privacy settings are set appropriately.

Focus on Phishing

Like wasps at a picnic, phishing emails are one of those annoying facts of life. Whilst a lot of dodgy emails will be automatically diverted into your junk folder, some will land in your inbox. In this article, we'll look at how fraudsters try to avoid detection and how you can protect yourself.

Why do some dodgy emails end up in my inbox?



Email inboxes usually have a spam filter set up to divert suspicious messages away from your inbox. However, they aren't fool-proof and sometimes messages will slip past the filters. Just because an email has appeared in your inbox, doesn't mean that it's safe to interact with.

For NHSmail accounts, the spam filter is pretty good. However, fraudsters have worked out that they can bypass some security features by hijacking another NHSmail account. This is why you'll sometimes get weird emails that look like they've come from another NHS employee. Their account may have been hacked and they'll have no idea what has been sent from their email address!

What is the point of phishing emails?

Although phishing emails can seem like little more than a nuisance, they have the potential to cause a lot of damage. The email itself is often the first step in carrying out a more sinister attack. The sender may be intending to take over your account, steal confidential information, spread viruses, or trick you into making a payment that isn't necessary.

What about the phishing emails I get at work?

NHS phishing emails often appear to be aimed at hijacking your email address and password. To do this, the email will contain a link which takes you onto a phishing website. These sites are designed to look like something you would normally trust - common examples include Share Point and ESR.

What would they do with my account if they hijacked it?

If they get access to your NHSmail, they can use your hijacked account to target others. They will also look for sensitive data, passwords for other accounts, and any content that they can use in future frauds (such as copies of invoices, names / contact details of people you often email, and names of key systems).

If they get into your ESR account, they can change your bank details and steal your identity. They could also use the information they have collected to take out loans and other credit agreements in your name, without your knowledge.

Potential Signs of Phishing

- The email contains hidden links which you are directed to click.
- It tries to pressure you into taking action quickly.
- It has come from someone you don't know (e.g. an NHS employee at another Trust or a GP practice).
- It contains random logos for NHS services in an attempt to look genuine.
- Spelling and grammar issues, or unusual wording.

Keeping your accounts safe

- Never click on links if you're not sure whether the email is genuine.
- Be particularly cautious of emails claiming to be from ESR / Payroll and invites to view documents on secure sharing sites.
- Hover over links to see which website you're going to be taken to. Please look really closely - we have seen examples recently where the sender has set up fake "NHS" websites which can look legitimate at first glance.
- Check senders details closely - look for small changes like extra digits or slightly different suffixes (e.g. @nhst.net)
- Remember that NHS email addresses can be hijacked - just because the email has come from an @nhs.net account doesn't mean it's genuine.
- If in doubt, seek advice from your Local Counter Fraud Specialist.

Fraud Cases

Fraudulently Obtained Sick Pay Recovered

In 2020, one of our NHS Trusts took on a new starter. They attended work as expected for a few days, and then reported themselves as sick. They provided fit notes which indicated they were not well enough to work. After two months of sickness absence, they returned and completed a four week phased return. At the end of the phased return, they handed their notice in and left the Trust.

Information received gave cause for the Counter Fraud Team to review the person's work history. Enquiries revealed that whilst on their two month's sickness absence from the Yorkshire-based Trust, the person was working full time in the same job role at another NHS Trust. When they completed their phased return in Yorkshire, they were then signed off sick from their other full time post.

As a result of their conduct, they had managed to obtain two full-time wages for a period of 3 months. Neither employer was aware that this individual held a full-time contract of employment elsewhere.

The subject was interviewed under caution and admitted to the offence of Fraud by False Representation. A police caution was issued, and the individual was obliged to repay both employers the sick pay that they had dishonestly claimed.

The Yorkshire NHS Trust has now been reimbursed, and the caution will show on the subjects DBS checks for the next 6 years.

This case illustrates the importance of staff being aware of their responsibilities in relation to secondary employment, and speaking up if something doesn't seem right. For further information, please watch our 5 minute video about secondary employment and working whilst sick on Vimeo.

Training

The Local Counter Fraud Team are launching the 2023/24 Fraud Prevention Masterclass programme in June. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. This year, we will be covering the following topics:

- Procurement Fraud
- Fraud Advice for HR Staff
- General Fraud Awareness
- Fraud Awareness for Managers
- Cyber Enabled Fraud
- Recruitment Fraud
- Payroll Fraud
- Creditor Payment Fraud

A flyer with the dates and times for the sessions is going to be shared soon. If you'd like to receive the flyer directly, or to register your interest 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 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.

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**

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

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

LCFS Covering:
Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

The Mid Yorkshire Hospitals NHS Foundation 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