JUNE 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our June 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

FRAUD POLICY AT YOUR ORGANISATION

Your organisation will have its own policy on how to prevent and deal with fraud.

This policy may have a different name at each organisation, such as Anti-Fraud, Bribery and Corruption policy or Counter Fraud policy.

These policies contain really useful information about your organisation's commitment to reducing fraud, bribery and corruption and the work the Local Counter Fraud Specialists will do to help achieve this.

Every member of staff has a role to play in countering fraud and has an obligation to report anything that doesn't look right.

We'd recommend that all staff find their organisation's fraud policy and have a look through it.

NHS COUNTER FRAUD AUTHORITY STRATEGY 2023-2026

The NHS Counter Fraud Authority (NHSCFA) has just announced the launch of its strategy 2023-2026 detailing how the organisation proposes to work collaboratively with the health sector in identifying and preventing fraud in the NHS.

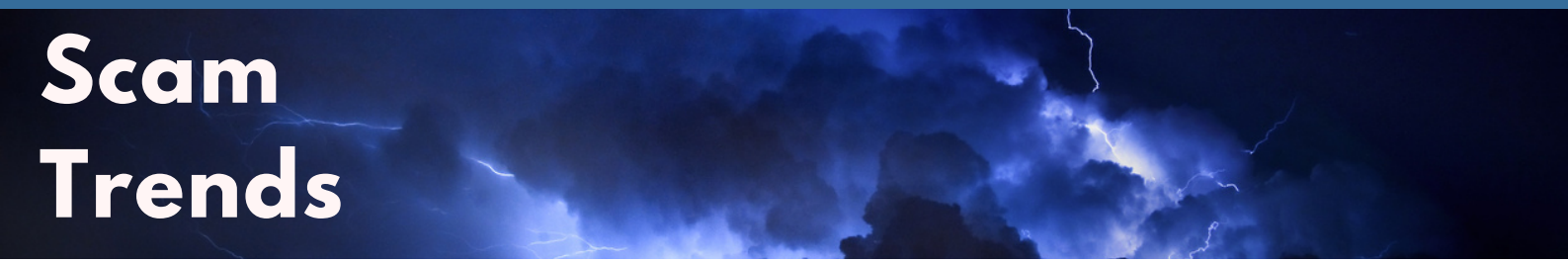
The strategy focusses on four key pillars:

- Understand,
- Prevent,
- Respond and
- Assure.

If you would like to learn more about the strategy it can be accessed using the following link:

NHSCFA Strategy 2023-26 | corporate publications | NHS Counter Fraud Authority

Scam Trends



Car Registration Fraud

Have you ever been sent driving fines or parking tickets that are for a vehicle you don't own?

If so, you may be on the receiving end of car registration fraud. Unfortunately, criminals are aware that they can register a vehicle at any address and under any name if they submit the right paperwork.

This can lead to any driving-related penalties such as speeding tickets and speeding fines being sent to an innocent person who has no link to the vehicle.

You can find out more information about this type of fraud on the Peter Barden website.

Advice

• Contact the DVLA and give them as much information as possible about the car which has been fraudulently registered under your details. You can send them copies of any fines or letters received about the vehicle, but hold on to the originals for your records.

• It may take up to 4 weeks, but the DVLA will be able to issue a letter which confirms that the car is not yours and is not associated to your address.

• Contact the organisation or police force who has issued the fine and let them know that your details have been used fraudulently. Explain that you have contacted the DVLA, and arrange to send them a copy of the proof that the vehicle is not yours once the DVLA has issued it.

• You can find more information on the DVLA website.

Mobile Phone Fraud Warning

A BBC news article has warned the public to be aware of fraudsters targeting mobile phone users. Thieves may watch you enter your phone's passcode before stealing your device from you when the opportunity arises.

If an unauthorised user gains access to your device, they will try using the same PIN / pattern to unlock your banking apps, will search through any saved notes on your phone looking for passwords and PIN numbers. They can also request password resets if you are logged into your emails on your phone.

The BBC news article includes the story of Jacopo de Simone who had £22k taken from his bank account after losing his phone on a night out.

You can read more on the BBC website.

Advice

• Protect your phone with biometric security measures (such as finger print or face unlock) if possible.

• Use strong and unique passwords for each account.

• Enable multi-factor authentication on your email account.

• Don't store passwords or pin numbers in the notes apps on your phone – consider a password manager instead.

• Be aware of your surroundings when accessing banking apps on your phone.

• Don't use public wi-fi to access anything sensitive such as financial apps.

Social Media Scams

Fraudsters have many ways of carrying out fraud over social media such as posting fake listings on selling pages. They may use hijacked accounts to post these fake items - so that potential buyers feel reassured when they check the sellers profile and see they've been on the platform for years.

They also use social media to find out about you, stealing information such as your name, job title and place of work for use in further fraud attempts, This is especially prevalent on LinkedIn.

Advice

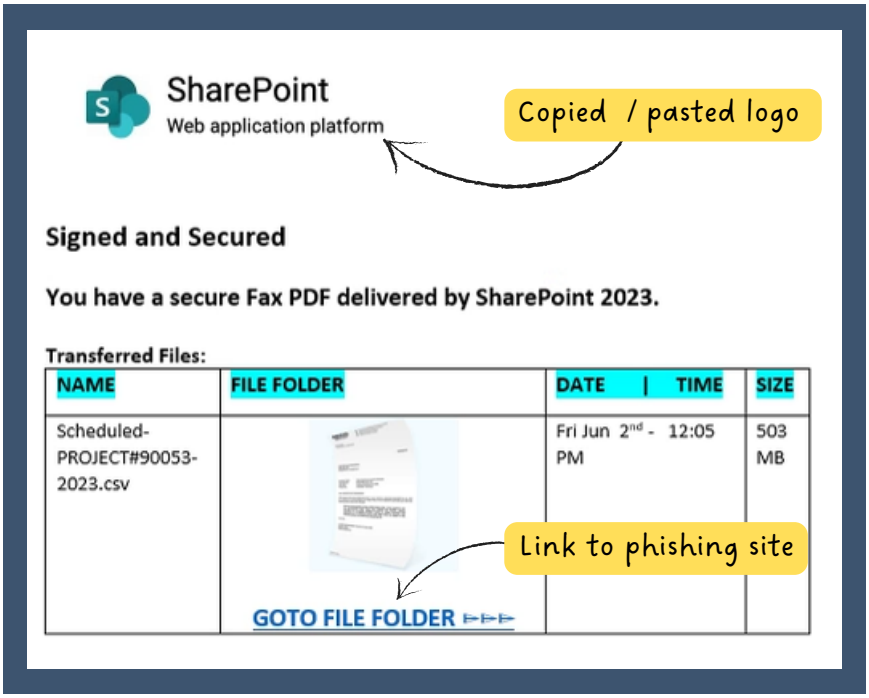
- Use the strongest security and privacy settings available on social media accounts.
- Be wary of offers that look too good to be true.
- Ignore unsolicited messages, and do not click on any links that are sent to you on social media.
- Activate Multi-Factor Authentication if it is available.
- Avoid quizzes that request personal information such as your childhood pet or the street you grew up on.

NHS Phishing Scams to Watch Out For

Phishing emails are often the first step in a fraud attempt. They are designed to trick you into taking action that isn't required - whether that is sharing your log in credentials, making a payment, or disclosing personal or sensitive data. Fraudsters can impersonate NHS colleagues and external partners to try and trick us into taking unnecessary action.

We have recently seen an increase in phishing emails encouraging receivers to click on a link to view a document within SharePoint.

SharePoint is a genuine application which is part of Microsoft Teams which allows documents to be shared and managed amongst users. Fraudsters are emailing NHS staff with a mock SharePoint invite, like the one shown below.



If the recipient clicks on the link, it will ask them to "log in" to SharePoint with their NHS credentials. The person's email address and password will be harvested and used for criminal purposes. Clicking the link may also allow malware to be transferred to NHS systems.

To add credibility to these phishing emails, the fraudster may hack into genuine NHS email accounts to send them from.

Advice

- If you receive an email like this which you are not expecting and do not know the sender, **do not click on the link** and contact your IT department or report to spamreports@nhs.net.
- If you do know the sender, give them a call on their **official contact number or Microsoft Teams** to check if the link is genuine. Don't rely on any contact details within the email as these may belong to the fraudster.

Please note: this newsletter is intended to assist the majority of NHS staff, however, different systems and processes are used throughout the NHS. As a result, the guidance in this newsletter may not fully apply at your organisation. If you are in any doubt and would like some advice, **please contact your Local Counter Fraud Specialist** (you'll find our details on the final page).

Salary Diversion Fraud

As it has been reported in the press that many NHS staff are due to receive backdated pay in June, there is an increased risk that fraudsters may try and divert salary payments.

Salary Diversion Fraud often works in a similar way to the Share Point phishing email shown on this page.

Instead of sharing a link to a "secure file" the fraudster sends a link which they claim is for ESR. They often claim that there has been a problem with payroll or that the person's bank details are causing an issue.

This is intended to make the recipient feel anxious, and to click on the "link to ESR" without checking it is safe.

If you hover over the link with your mouse, you should be able to see the web address that it will really take you to.

If you click on the link, you will see a fake ESR page. If you enter your log in credentials, they will be stolen by the fraudster. They can then use your log in to amend your bank details.

Advice

- If you get any emails directing you to log into ESR, open a web browser and type in the address manually (https://my.esr.nhs.uk)
- ESR is set up so that if your bank details change, or if a new assignment is added to your profile, you will get an automated email from esr.wfmPROD@nhs.net. If you get an email from this address saying a change has been made and you didn't request it, or if you are not due to start a new assignment, please contact Payroll.
- Use a strong and unique password for ESR.
- Use the strongest privacy settings available on social media accounts.

In the Press

EHIC Fraudsters Jailed for £2 Million Scam

Two fraudsters who ran a European Health Insurance Card (EHIC) scam which made them over £2 million have been jailed. Brothers Damien and Dale Sartip Zadeh set up two deliberately misleading websites that implied people needed to pay a fee to get an EHIC card. They even paid for their websites to appear at the top of search engine results.

Their websites made a host of false claims – such as stating that the NHS does not provide multi-language support, travel support or telephone support, in an effort to convince people to use their websites. Their sites were also designed to look similar to genuine NHS and Government websites, deliberately confusing people who visited them.

When customers found out that they could have got their EHIC for free via the NHS, they sought refunds. In response, the Sartip Zadeh's refused to issue refunds and instead threatened legal action.

Damien was jailed for 9.5 years and Dale received an 8 year sentence. Their parents were also convicted of money laundering. You can read more about the story on the Yorkshire Live site.

Fraud Prevention Masterclasses

The 2023/24 Fraud Prevention Masterclass programme launched this month. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. The programme will run until February 2024, further dates will be published later this year. We will be covering the following topics:

General Fraud Awareness	20th June at 10am or 10th August at 2pm
Fraud Awareness for Managers	25th July at 10am or 14th September at 10am
Cyber Fraud	21st June at 9:30am or 15th August at 11am
Payroll Fraud	4th July at 10am or 8th September at 11am
Procurement Fraud	13th June at 2pm or 9th August at 2pm
Creditor Payment Fraud	19th July at 2pm or 12th September at 11am
Fraud Awareness for HR	13th June at 11am or 14th August at 10am
Recruitment Fraud	20th July at 13:30pm or 28th September at 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 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