MARCH 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our 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

Watch out for Easter Scams

Whilst full of chocolate and hot cross buns, or gorging on what we may have given up for lent, many of us will be in a sugar fuelled frenzy or slump.

Don't let this affect your judgement if you are making purchases or asked for information.

Here's a list of scams which usually rise around Easter time.

- **Fake giveaways**. A couple of years ago, a scam offering free chocolate Easter eggs was a way of obtaining personal details. If you see offers like this on social media, make sure that you go to the giveaway company's website to check if it is genuine. It is rare that you will get something for nothing. Don't get 'hatched' by a fake deal.

- **Charity scams**. As Easter is a Christian festival, fraudsters may target spiritually minded people by pretending to be legitimate charities hoping to make the world a better place. Don't click on links in emails to make donations, go to their secure site or call them instead. Keep your 'nest egg' secure.

- **E-cards**. Malware can be hidden in E-cards. 'Chicken' out if you receive any strange links or are asked to download a file.

- **Holiday scams**. As the weather brightens, travel related scams increase. For more information, see our article on page 2. 'Hop' away unless you are sure you're using legitimate companies.

Stay egg-stra vigilant and have a happy Easter.

Scam Trends

Beware of Holiday Scams

Action Fraud, the national fraud and cyber crime reporting service, has launched a holiday fraud campaign urging holiday goers to play it safe online and do their research before booking their trip.

Last year, 6,640 reports of holiday fraud were made to Action Fraud, and holiday makers lost a combined total of £ 12.3 million.

Holiday scams can include:

- "Free" holidays being offered as prizes for scam prize draws which are designed to steal your personal information.
- Fake listings for accommodation that either does not exist or which belongs to someone else, these listings can be propped up by fake or stolen reviews.
- Scam adverts offering hugely discounted travel fares (please see the train tickets article further down this page).
- Use of social media marketplaces to sell "unwanted" holiday packages or event tickets – this can be done using fake or hijacked profiles.

To keep yourself safe please remember:

- Offers that look "too good to be true" could be scams.
- If a listing states it is Atol Protected, make sure you are given an Atol certificate. You can also check if the travel company is covered using the Civil Aviation Authority website.
- Do not send payment for accommodation outside of official booking platforms. Scammers will often encourage you to pay by direct bank transfer.

There is some further, helpful advice on the Which? website.

Fake Train Ticket Adverts

Consumer advice service Which? have warned the public about scam adverts on social media offering "a year of rail travel for £3".

Most of the adverts seen so far impersonate Great Western Railway, but other rail providers may have their names and branding used.

Clicking on the advert will take you onto a phishing site which will steal your financial information and personal data. People may assume that the maximum loss would only be £3, but once fraudsters have your bank details they can use these to carry out further frauds.

Missed parcel scams work on this same methodology – the victim makes what they feel is a low risk transaction of a few pounds. A week or so later, they get a call from someone claiming to be from their bank's fraud team.

The fraudster tells the victim that their account has been compromised, and talks them into transferring all their money into a "safe account" which belongs to criminals.

Please remember the golden rule – if it looks too good to be true, it probably is!

Image from Which? Scam Alerts page

Staff Impersonation Scams

Phishing Emails Targeting Staff in Senior Roles

The Cyber Intelligence Team at the National Fraud Intelligence Bureau has been gathering information on a tactic that scammers are using to target staff in senior roles. Here's how it works...

The target gets an email which has come from a manager, director or other senior role at another organisation.

The email may come from a recognised work email address. However, that doesn't mean that the contents are safe! When they can, scammers will use real email accounts that they've hijacked because it makes their emails seem legitimate.

In this scam, the email asks the recipient to click on a link to open a document. When they click on the link, the target is asked to type in their email login details to view the file.

Here's the tricky part: once the target does that, the scammers have gained access to their email account. They can then use this newly compromised account to send the same phishing email to others, starting a chain reaction.

Once they're in a person's email account, they can find all sorts of information that could help them scam others in the future. Things like details about suppliers, copies of invoices, system names, and they can even request password resets for other services.

Here's what you can do to protect yourself:

- Be careful with emails that ask you to click on links and log in.
- Don't click on links in emails that you weren't expecting. You can hover your mouse over the link to see where it will take you.
- If you're not sure about an email, try to contact the sender using a method you know is safe, like calling them on their work phone or using Microsoft Teams.
- If you can't reach the sender, ask your Local Counter Fraud Specialist or IT team for help to check if the email is real.

Gift Card Scam

On the subject of impersonating staff, we have recently seen a spate of phishing emails sent to NHS staff asking for help purchasing gift cards.

These requests were designed to look as though they had come from an employee in a senior role at the organisation. There were some tell tale signs that the request was fraudulent:

- It had come from an @gmail.com account.
- It asked the recipient to keep the request secret.
- The email subject was generic / unusual: "TASK REQUEST"
- The message asked for the recipient to act quickly. Fraudsters often try and panic people into taking action quickly so that they don't have time to second guess the request.
- The email was signed off with the senior employee's name and job title but these are publicly visible. There was none of the usual information you'd expect to see in their signature – such as their direct contact number or organisation logo.

Fraudsters like to impersonate senior staff because they are often easy to identify online, and because they have the authority to sign off payments. Some staff may feel less confident challenging unusual requests from someone at the top of their organisation.

Please be wary of this fraud methodology. If you feel that an email is putting you under pressure to do something that is not in line with policy and procedure, or to keep a purchase secret, please bear in mind you could be being scammed.

If you receive a suspicious email, please contact your Local Counter Fraud Specialist or IT for support.

Can you spare 5 minutes?

The Counter Fraud Team are about to complete our annual Counter Fraud Functional Standard Returns.

It would be very helpful if you could spare 5 minutes to fill in a quick survey about your awareness of counter fraud measures.

The survey is just to capture awareness levels - so please don't worry if you don't know the answers. You can choose to respond anonymously, and can also use the survey to ask your Local Counter Fraud Specialist to set up some training for your team.

Your help with this is hugely appreciated, it will help inform the counter fraud work we do throughout 2024/25. If you are able to take the survey, please click the following link:

https://www.surveymonkey.com/r/CounterFraudSurvey

Fraud Prevention Masterclasses

If you would like to learn more about NHS fraud and how you can help to prevent it, please consider signing up to our Fraud Prevention Masterclasses. 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	18th April 2pm
Fraud Awareness for Managers	20th March 10am
Cyber Fraud	8th April 2pm
Payroll Fraud	22nd May 11am
Procurement Fraud	5th June 2pm
Creditor Payment Fraud	15th April 10am
Fraud Awareness for HR	15th May 1pm
Recruitment Fraud	4th June 10am

If you would 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