APRIL 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our new-look 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

AUDIT YORKSHIRE COUNTER FRAUD ON TWITTER

The Counter Fraud Team at Audit Yorkshire are happy to announce that we now have our own Twitter account.

As well as focusing on NHS type frauds, it will share details of current scams that are circulating and how you can avoid them. Sharing such information is a major aid and tool in the prevention of fraud.

Please pay your part in preventing fraud and follow our page **@AYCounterFraud.**.

FRAUD FOCUS GROUP

Fraud is an ever present threat within the NHS and the Counter Fraud Team are looking for ways to raise awareness amongst all staff groups.

We are hosting an informal session delivered via Microsoft Teams on Thursday May 25th at 10am.

This focus group will be a safe environment where you can
- Learn about what the counter fraud team does.
- Find out about what our biggest threats are and how we are planning to combat these.
- Let us know how we are doing and what we can do to support you and your team to fight fraud.

We would welcome any member of staff. If you are available and would like to attend, please email **marie.hall15@nhs.net** and she will forward an invite.

Scam Trends

WhatsApp Code Scam

Fraudsters have been targeting WhatsApp users by posing as a friend and asking for a security code. The scam begins when a criminal gets access to another WhatsApp account which has you listed as a contact.

The fraudster, posing as your friend or someone that's a member of a WhatsApp group you're in, will then send you seemingly normal messages to try and start a conversation with you.

However, around the same time you will receive a text message from WhatsApp with a six-digit code. This is because the criminal has been trying to login to WhatsApp using your mobile number.

The criminal will claim that they sent you their code by accident and ask you to help them by sending it to them. Once the fraudster has this code, they can login to your WhatsApp account and lock you out.

The criminal will then use the same tactic with your WhatsApp contacts in an effort to steal more accounts and use them to perpetrate fraud.

What you need to do:

- If you are willing to do so, set up two-step verification to give an extra layer of protection to your account: Tap Settings > Account >Two-step verification > Enable.
- THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- Never share your account's activation code (that's the 6 digit code you receive via SMS)
- You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.

Tab Napping

This odd term is a type of phishing attack which can happen if you have several tabs open at once on your computer or laptop.

A 'same-origin policy' is a security feature which isolates websites from each other. The same-origin policy does have some 'holes' which websites use when interaction is necessary. It is through these holes which tabnapping can occur.

Hackers can use JavaScript to change the content of an open but inactive tab. Changes will usually be made to look like a default log in for your bank, emails or social media account.

When the user goes back to the tab, the hacker is hoping that they will assume they have been timed out and will put their log in details again. If the user logs in again, the hacker can harvest the details and use them to commit other offences, with the user being the victim.

Top tips to prevent tabnabbing:

- Close down a tab when you are finished with it and open a new one when you need it again instead of keeping lots of tabs open.
- If you do keep tabs open, have a system which means that you can spot if something changes. For example, always have tab 1 open for emails, tab 2 for an intranet and tab 3 for all other browsing.
- If the site you regularly visit looks different, such as an unusual layout or spelling errors, be suspicious.
- Check that the URL shows a secure protocol, such as HTTPS.
- Keep anti-virus and spyware up to date.

Eurovision Phishing

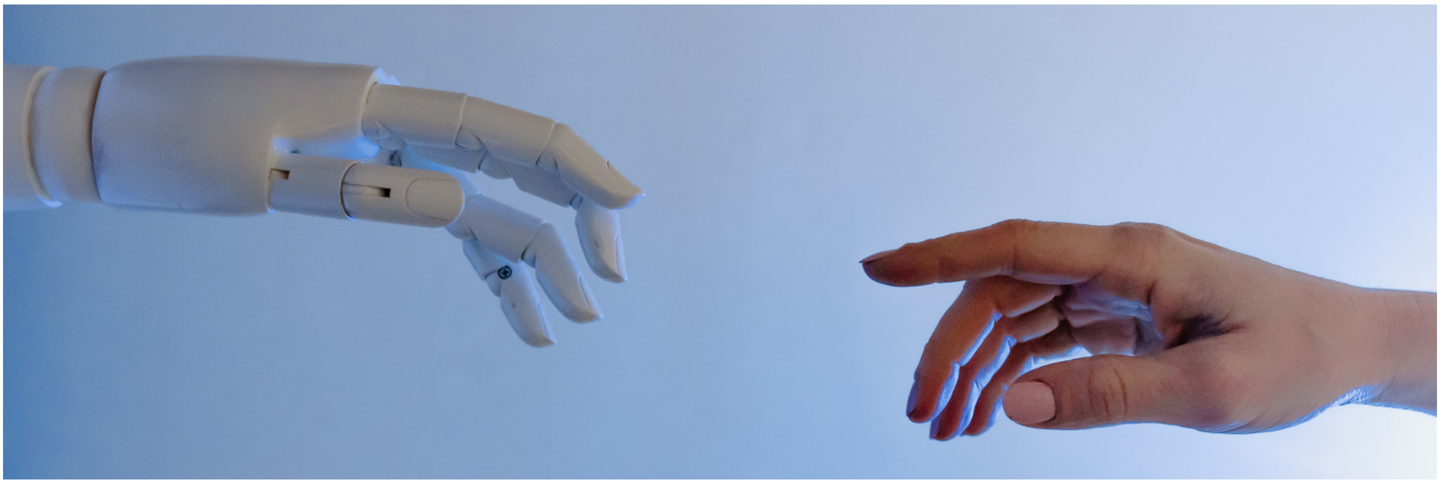
Cyber criminals are targeting hotels hosting people travelling to Liverpool for the Eurovision song contest event in May 2023. The online travel agent booking.com told the BBC they have seen evidence of "some accommodation partners being targeted by phishing emails."

Cyber criminals take advantage of news and current events to scam customers. The usual advice applies if you believe you have become a victim: report to Action Fraud, relevant bank or credit card companies and/or your insurer.

Holiday Scams

Many of us will be looking forward to the summer, planning days out and holidays. Please be aware that fraudsters will post fake holiday adverts and event tickets online. This is particularly a risk on social media where accounts are easily hijacked, created and deleted.

Remember - if it looks too good to be true, then it probably is. You can find some really useful advice on Holiday Scams on the Which? website.



AI - Future Fraudster?

Artificial Intelligence (AI) has the potential to make life easier – indeed many of us already use AI in our daily lives. It pops up all the time - whether it's a smart speaker telling you the weather forecast, Maps letting you know that there's heavy traffic building up on your planned route, or Spotify compiling the ultimate playlist to transport you to your teenage years, AI is already embedded in our home and work environments.

Unfortunately, the development of more sophisticated AI tools, such as Chat GPT, brings with it many new fraud risks. Chat GPT generates text at the request of the user – and what makes it unique is that it produces text with a “human tone”. This makes it much harder to tell that the content has been produced by a machine.

At work you will almost certainly have received phishing emails that have been produced by a fraudster. Traditionally, these scam emails have had tell-tale warning signs, such as strange wording, or spelling and grammar errors that help us to spot them.

AI can create really convincing phishing emails as it is unlikely to contain spelling or grammar errors, and it has been designed to sound "human". There is also new AI powered voice generating software, which can allow a fraudster to "hijack" your voice using a 3 second clip of you speaking.

Alongside these developments, there has been a rapid growth in AI art generators. These have become very popular as the user can generate impressive, bespoke profile pictures / content for use on social media. Unfortunately, some of these apps have hidden viruses lurking behind the scenes which can compromise your device and data. You may also come across AI-enabled scams on social media sites, such as this one which was spotted on Linked In recently.

Keeping yourself safe

• Always be suspicious if you are asked to click on a link in an email or on a social media post.

• If you are on a desktop or laptop, you can use your mouse to hover over the link to see where it will take you.

• It is not easy to hover over links on touch screen devices. If in doubt, log into a desktop/laptop and hover over the link.

• Be wary about which apps you download – you can find some useful advice on safe app interaction on the Verified website.

In the Press

Guilty verdicts after fraud investigation uncovers bribery issues at NHS Trust

Two men have been found guilty of fraud and bribery offences against the NHS. A third man entered a guilty plea ahead of the seven week trial. The court heard that Hasan Abusheikha, a Theatre Manager at St Albans City Hospital Trust, had used his position to secure bribes from Elmo Emanuel, the CEO of Implants International and Xtremity Solutions Ltd. Another supplier, Jawid Khan of TSI Med Ltd. entered a guilty plea before the trial began.

It was found that Abusheikha had accepted bribes from Emanuel and Khan in exchange for making sure that the Trust procured medical equipment from their companies. Abusheikha was also convicted of accepting payments from two other suppliers. The total value of the offences was assessed as being more than £600,000.

All three men will be sentenced at St Albans Crown Court. The NHS Counter Fraud Authority and the Crown Prosecution Service will launch proceedings to try and recover money taken from the NHS. You can read more on the NHS Counter Fraud Authority website.

Three arrests in Personal Protective Equipment (PPE) fraud case

Three people have been arrested following a National Crime Agency investigation into international PPE fraud. A husband and wife are amongst those arrested. The male is suspected of setting up a UK company in order to run a PPE scam during 2020 which was global shortages in supplies of safety equipment. His wife is suspected of helping him to launder the proceeds.

The investigators believe the company agreed sales of PPE with a total of over $35 million to customers in the USA and Germany. Customers were told to pay an upfront fee to secure their order. They were informed that the fee would only be released once the contract conditions had been met. However, the company owners could access the account without delivering the goods agreed. The case is still open and the suspects are being interviewed. You can read more about this case on the National Crime Agency website.

Training

The Local Counter Fraud Team are currently refreshing the Fraud Prevention Masterclass programme ahead of their relaunch later this year. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. This year, we will be covering the following topics:

New!

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

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 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.Hall15@nhs.net / 07970 265 017

Assistant Head of Anti Crime 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 Hospital 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