JANUARY 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Happy New Year and welcome to our January 2024 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

Don't Take the Bait

Have you ever heard of a scam called "baiting"? This scam involves placing USB sticks (the bait) in public places like cafes or car parks, hoping people will pick them up and connect them to their own devices.

Here's how it works: scammers leave USB sticks in public spots with tempting labels like "Free Music" or "Important Files."

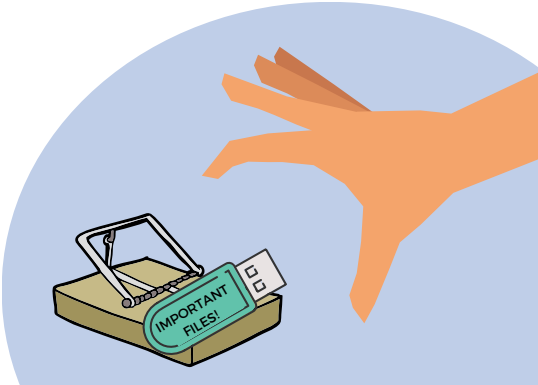
When curious individuals pick them up and connect them to their computers, they unknowingly let harmful software in. This can lead to serious problems, like stealing personal information or installing ransomware.

To stay safe from baiting scams, remember these tips:

- Don't plug in unknown devices: avoid connecting random USB sticks or other gadgets to your computer.
- Turn off auto-run: disable automatic program execution when you connect external devices to your computer.
- Educate your team: make sure your colleagues know about the risks of connecting unknown devices at work.
- Follow company rules: stick to your workplace's IT policy, and report any suspicious devices to your IT department.
- Update your security software: keep your antivirus and anti-malware tools up-to-date for added protection.
- Report strange devices: If you find a USB stick in public, don't connect it. Instead, tell the authorities or the place's management.

By being careful and following these tips, you can reduce the chances of falling for baiting scams and keep your devices and information safe.

You can read more about baiting here: https://www.makeuseof.com/what-is-a-usb-drop-attack/



Scam Trends and Fraud News

Salary Sacrifice Scam Alert

The Counter Fraud Team have been made aware of a scam where a fraudster used stolen NHS staff credentials to buy items through a salary sacrifice scheme.

Goods were purchased without the staff member's knowledge, and payment was taken from their monthly salary. The items ordered were delivered to the fraudster, so the victim only found out when they checked their pay slip and spotted unexpected deductions.

Thankfully this has only happened a few times, but it does highlight the importance of checking your pay slip even if you're not expecting to see a different amount.

Advice:

- Never share your ESR / email log in details with anybody else.
- Make sure to use strong and unique passwords for different accounts - including your email and ESR accounts. If you take advantage of a salary sacrifice scheme, have yet another password for that system. For more on this, please see the password advice article on the next page.
- Check your pay slips monthly and report anything unusual.
- If you print your pay slips out, shred or destroy them before discarding them to prevent anyone stealing your details.
- If you email your pay slip to yourself, we advise that you password protect it so that nobody else can open it.
- If in any doubt, please speak to your Local Counter Fraud Specialist (our details are on page 6).

Lottery Scams

Lottery scams are also known as prize draw or sweepstake scams. This type of scam usually starts with a letter, email or phone call claiming that you have won a substantial amount of money in a lottery.

Common lotteries named in this scam are Australian, Spanish or Canadian. The caller will usually say that they are an official at the lottery and will try to put you under a lot of pressure to act straight away or risk losing your winnings.

The scammers will either ask you to send them a copy of your passport or other personal information for 'proof of identity', and / or ask you to pay some kind of fee before they can release your prize.

If you do make a payment, the criminals will often ask for more, coming up with excuses for each charge. In some cases where banking details have been requested, instead of crediting the victim's account with the prize fund, the account has been emptied.

To prolong the crime, if a person has been coerced into handing over money or their details, the scammers will sometimes then pretend to be from their bank or law enforcement and offer to help them recover the lost money. Throughout this phase, the fraudsters may encourage the victim to transfer their remaining money into a "safe account" which is controlled by the criminals.

It is often easy to spot this as a ruse if you haven't actually purchased a lottery ticket. You can't win a competition you haven't entered. However, if you do enter lotteries or online competitions, it is harder to spot this type of scam.

If you are contacted by someone claiming you have won a prize, be very wary and do not share your financial information. Contact your bank immediately if you are concerned you've shared your bank details with a fraudster. You can find more information and advice on this type of fraud on the Action Fraud website.

Cyber Fraud - Setting Good Passwords

The start of a new calendar year can be a great time to start fresh and update your passwords. You'll often hear the Counter Fraud Team advising that you need to make sure you use **strong and unique** passwords.

Why do passwords need to be unique?

A survey run by Google in 2019 found that 65% of people were reusing the same password for multiple accounts.

When you consider how many different systems and services we log into, it's understandable that people often find it easier to rely on a single password that they are really familiar with. However, this is a big risk.

The danger comes when one of your accounts is breached. If a company that holds your data is targeted by cyber criminals, your log in credentials could end up being stolen and sold on. If you rely on a single password, accounts you hold elsewhere can also be hijacked.

For example, let's say that Company A is hacked and your user name and password are stolen. The cyber criminal is able to log into your account with Company A to look for more information - such as the email address linked to your account.

They try your password to see if they can get into your emails. If they get into your email account, they can go round lots of other services and reset your password, locking you out of your accounts. If you don't have the same password for your emails, you might think they'd just give up and move on.

However, they haven't quite finished. They will try logging into popular services - such as Amazon, PayPal, eBay, social media platforms etc. using your email address and the password that Company A lost. Any account which they manage to access gives them an opportunity to gather more information on you. Some accounts will also contain saved payment information, which can be used to place unauthorised orders.

For example, if they get into your Amazon account they can use your saved details to place high value orders which they could arrange to have delivered to Amazon lockers. They would also be able to steal your address which may help them to carry out identity theft.

Hopefully this example highlights why having unique passwords is so important.

How do you set a strong password?

Three is a Magic Number. The National Cyber Security Centre recommends that you use three random words to make strong and unique passwords. Doing this makes your password much longer (and therefore harder to guess or break), but keeps it easy to remember. If picking three random words is proving tricky, you could use a favourite song lyric or phrase that you find memorable.

Don't make it personal. You should not use any personal information in your passwords - things like your pet's name, your middle name, the place you were born etc. can be tracked down on social media and your online footprint. Even if you think your privacy settings are pretty good, friends and family who you are linked to online may be less diligent.

Characterful passwords. If you need to include special characters in your password, it is often tempting to replace letters that look similar (e.g. password becomes p@$sw0rd!) - however this tactic is well known to fraudsters. Instead, think about adding them in between your three random words : e.g. balloonhooklamp could be changed to @balloon?hook!lamp.

Take a strength test. To explore how small changes can increase your password strength, have a look at How Secure is My Password. This is a website where you can type in potential passwords and it tells you how long it would take a computer to crack them. For example, balloonhooklamp is estimated to take 1 thousand years to break, but adding symbols in increases that to 80 trillion years!

Don't recycle. Reusing passwords is risky - it's always safest to come up with a new password rather than slightly tweaking one you have used before.

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

The 2023/24 Fraud Prevention Masterclass programme is underway. 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	6th February 10:30am
Fraud Awareness for Managers	16th January 11am
Cyber Fraud	7th February 11am
Payroll Fraud	23rd January 10am
Procurement Fraud	15th February 2pm
Creditor Payment Fraud	16th January 10am, 12th March 2pm
Fraud Awareness for HR	20th February 10am
Recruitment Fraud	16th January 10am, 12th March 11am

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